ROBUST OPTIMIZATION OF PRIVATE COMMUNICATION IN MULTI-ANTENNA SYSTEMS

von

ANNE WOLF

Technische Universität Dresden

Robust Optimization of Private Communication in Multi-Antenna Systems

Anne Wolf

von der Fakultät Elektrotechnik und Informationstechnik
der Technischen Universität Dresden

zur Erlangung des akademischen Grades

Doktoringenieur

(Dr.-Ing.)

genehmigte Dissertation

Vorsitzende:	Prof. Dr.-Ing. habil. Renate Merker
Gutachter:	Prof. Dr.-Ing. Eduard A. Jorswieck Prof. Dr.-Ing. Ragnar Thobaben
Tag der Einreichung:	13.04.2015
Tag der Verteidigung:	02.06.2015

Danksagung

Mein Weg vom Beginn meiner Tätigkeit am Lehrstuhl Theoretische Nachrichtentechnik im Jahr 2005 bis zur Abgabe und Verteidigung dieser Dissertation im Jahr 2015 war (wie man schon an den Jahreszahlen sieht) lang und von außen gesehen sicher nicht immer geradlinig. Ich danke allen, die diesen Weg begleitet, unterstützt oder vielleicht auch nur beobachtet und dabei gleichzeitig darauf vertraut haben, dass er unter anderem auch einmal zu einer fertigen Dissertation führen wird.

Aus der Perspektive des Weges war da zunächst Prof. Adolf Finger, der mich als damaliger Lehrstuhlleiter im Jahr 2005 als wissenschaftliche Mitarbeiterin eingestellt und so den Startschuss für diesen Weg gegeben hat. Prof. Eduard A. Jorswieck hat mir dann mit seiner Übernahme des Lehrstuhls im Jahr 2008 die Tür zum Thema »Sicherheit auf der Übertragungsschicht« geöffnet und den Weg fortan fachlich begleitet. Ich danke ihm dafür, dass er mir die nötige Zeit gegeben und das entsprechende Vertrauen entgegengebracht hat, was mir ermöglichte, meinen Weg entsprechend meinen eigenen Prioritäten zu gehen, und dabei gleichzeitig immer da war, wenn ich seine Unterstützung benötigte.

Martin hat meinen langen Weg von Beginn an begleitet. Er war und ist der beste »Raumteiler« und Weggefährte, den ich mir wünschen konnte. Er versteht meine Definition von »Geradlinigkeit« des Weges und er hat diesen Weg all die Jahre nicht nur unterstützt, sondern mir manchmal auch erst dabei geholfen, ihn zu finden. Danke, dass Du immer da warst und bist, wenn Du gebraucht wirst, danke für unzählige Gespräche (viele fachliche, aber auch zahlreiche über »Gott und die Welt«) und einen sich nie erschöpfenden Süßigkeitenvorrat, aber auch für das Fernhalten jeglicher Ablenkung (inkl. der »Vertreibung« aller anderen Kollegen aus unserem Zimmer) in der »heißen Phase« kurz vor der Abgabe dieser Arbeit.

Beim Stichwort »Kollegen« fallen mir sofort noch Sabrina und Johannes ein. Sabrina ist ihren Weg zur Dissertation streckenweise mit mir gemeinsam (und oft auch durch die gleichen Projekte) gegangen und ist (neben vielem anderen) die wahrscheinlich beste Quelle von Literaturempfehlungen im Bereich »Sicherheit auf der Übertragungsschicht«. Und Johannes war der einzige, der sich von Martin in der »heißen Phase« nicht so leicht aus dem Zimmer vertreiben ließ – zumal er mit der Absicht kam, mir etwas von meiner Arbeit abzunehmen, damit ich in Ruhe schreiben konnte (und er hat beim Verlassen des Zimmers immer irgendetwas »mitgenommen«). Außerdem hat Johannes (neben Sabrina und Axel) inzwischen auch ungeahnte Qualitäten bei der zwischenzeitlichen Betreuung meiner Kinder im Arbeitsalltag entwickelt.

Mein großer Dank gilt natürlich auch allen anderen Kollegen (auch wenn sie hier nicht namentlich genannt werden) und meinen Freunden (besonders der Mittagsrunde und ganz speziell Thomas), die mir immer wieder mit Rat und Tat zur Seite standen oder manchmal auch einfach nur mit unbeschwerten Pausengesprächen für die nötige Abwechslung und kurzzeitige Befreiung vom Dissertationsstress und so für einen freien Kopf und neuen Schwung gesorgt haben.

Mein ganz besonderer Dank gilt meinem Kollegen und guten Freund Axel, der oft auch noch da ist, wenn ich gerade als Privatperson auf meinem Weg unterwegs bin. Danke für die Zeit, die Du mit mir verbracht hast und verbringst, danke, dass Du mich mit jeder Laune erträgst, danke für all die Gespräche in den letzten Jahren, das Aufrechterhalten meiner Lebensfunktionen in der »heißen Phase« vor der Abgabe und Verteidigung, danke für (auch nächtliches) Korrekturlesen der Arbeit und danke, dass Du mich so oft beim Holzeisenbahnspielen vertreten hast.

Eine ähnliche Aufzählung hätte auch Tassilo verdient, der sich oft allein mit zuerst einem und jetzt zwei Kindern beschäftigt hat oder mit ihnen unterwegs war, damit ich in Ruhe »mein Zeug« machen kann.

Auch die Omas (und ihre Männer) haben mir viele freie Wochenendtage zum Schreiben ermöglicht, indem sie Fridolin (und für die finale Überarbeitung jetzt auch Moritz) beaufsichtigt und »bespielt« haben. Meiner Mutter möchte ich an dieser Stelle auch dafür danken, dass sie mich stets meinen eigenen Weg hat gehen lassen, dass sie sich (mit ihren Kommentaren und sicher manchmal auch Bedenken) zurückgehalten hat, aber immer da war und ist, wenn sie gebraucht wird, und dass sie mir immer wieder zeigt, dass es viele alternative (und gleichberechtigte) Wege gibt.

Auf dem letzten Teilstück des Weges zum Dr.-Ing. gebührt der Dank vor allem Prof. Ragnar Thobaben, der sich (trotz Elternzeit und meiner sportlichen Zeitvorstellung) bereit erklärt hat, das zweite Gutachten meiner Dissertation zu übernehmen und für Rigorosum und Verteidigung nach Dresden zu kommen, sowie Prof. Renate Merker und Prof. Peter Birkholz, die sich als weitere Mitglieder der Promotionskommission Zeit für mich und meine Arbeit genommen haben und außerdem auch dazu beigetragen haben, dass ich an den Tag meiner Verteidigung nur angenehme Erinnerungen habe.

Eigentlich hätte ich auch einfach kurz sagen können: Danke für Eure Zeit und danke, dass Ihr mein Leben bereichert, indem Ihr seid, wie Ihr seid.

Anne Wolf
Dresden, Mai 2016

Kurzfassung

Der Fokus dieser Arbeit liegt auf der Abhörsicherheit der Datenübertragung, die auf der Übertragungsschicht, also durch geeignete Codierung und Ressourcenverteilung, erreicht werden kann. Die Grundlagen der Sicherheit auf der Übertragungsschicht wurden bereits in den 1970er Jahren von Wyner (1975), Csiszár und Körner (1978) formuliert. Jedoch ermöglicht erst der heutige technische Fortschritt, dass diese Ideen in zukünftigen Kommunikationssystemen Einzug finden können. Dies hat in den letzten Jahren zu einem gestiegenen Interesse an diesem Forschungsgebiet geführt.

In der Arbeit werden zwei Ansätze zur abhörsicheren Datenübertragung in Funksystemen analysiert. Dies ist zum einen die direkte Übertragung der Information zum gewünschten Empfänger, wobei der Sender gleichzeitig die Zuverlässigkeit und die Abhörsicherheit der Übertragung sicherstellen muss. Zum anderen wird ein zweistufiger Ansatz betrachtet: Die beiden Kommunikationspartner handeln zunächst einen gemeinsamen sicheren Schlüssel aus, der anschließend zur Verschlüsselung der Datenübertragung verwendet wird. Bei diesem Ansatz werden die Abhörsicherheit und die Zuverlässigkeit der Infomation getrennt voneinander realisiert.

Die Sicherheit der Nachrichten hängt maßgeblich davon ab, inwieweit zuverlässige Informationen oder verlässliche Annahmen über den Funkkanal zum Abhörer verfügbar sind. Die Annahme perfekter Kanalkenntnis ist für einen passiven Abhörer jedoch kaum zu rechtfertigen. Daher wird hier ein deterministisches Modell für die Unsicherheit über den Kanal zum Abhörer eingeführt, was zu einer Menge möglicher Abhörkanäle führt. Die Optimierung der sogenannten Worst-Case-Rate in einem Mehrantennensystem mit Gaußschem Rauschen wird für beide Ansätze betrachtet. Es wird analysiert, mit welcher Sendestrategie die maximale Rate erreicht werden kann, wenn gleichzeitig angenommen wird, dass der Abhörer den zugehörigen Worst-Case-Kanal besitzt, welcher die Rate der abhörsicheren Kommunikation jeweils auf ein Minimum reduziert.

Für beide Ansätze wird gezeigt, dass aus dem resultierenden Max-Min-Problem über die Matrizen des Mehrantennensystems ein äquivalentes Problem über die Eigenwerte der Matrizen abgeleitet werden kann. Die optimale Ressourcenverteilung für eine Summenleistungsbeschränkung über alle Sendeantennen wird charakterisiert. Für den jeweiligen Worst-Case-Kanal zum Abhörer, dessen Kanalgewinne einer Summenbeschränkung unterliegen, werden Waterfilling-Lösungen hergeleitet. Es wird gezeigt, dass für hohen Signal-Rausch-Abstand (engl. *signal-to-noise ratio*, SNR) alle Raten gegen endliche Grenzwerte konvergieren, wenn die Antennenzahl des Abhörers nicht beschränkt ist. Die Grenzwerte werden durch die Quotienten der Eigenwerte der Gram-Matrizen beider Kanäle bestimmt. Für den Ratenanstieg der direkten Übertragung ist bei niedrigem SNR nur die Differenz dieser Eigenwerte maßgeblich, wohingegen für den Verschlüsselungsansatz in dem Fall keine Abhängigkeit vom Kanal des Abhörers besteht. Ein Vergleich zeigt, dass das aktuelle SNR und die Qualität des Abhörkanals den einen oder anderen Ansatz begünstigen. Die direkte Übertragung ist bei niedrigem SNR und verhältnismäßig schlechten Abhörkanälen überlegen, wohingegen der Verschlüsselungsansatz von hohem SNR und vergleichsweise guten Abhörkanälen profitiert. Die Ergebnisse der Arbeit werden umfassend diskutiert und illustriert.

Abstract

The thesis focuses on the privacy of communication that can be ensured by means of the physical layer, i.e., by appropriately chosen coding and resource allocation schemes. The fundamentals of physical-layer security have been already formulated in the 1970s by Wyner (1975), Csiszár and Körner (1978). But only nowadays we have the technical progress such that these ideas can find their way in current and future communication systems, which has driven the growing interest in this area of research in the last years.

We analyze two physical-layer approaches that can ensure the secret transmission of private information in wireless systems in presence of an eavesdropper. One is the direct transmission of the information to the intended receiver, where the transmitter has to simultaneously ensure the reliability and the secrecy of the information. The other is a two-phase approach, where two legitimated users first agree on a common and secret key, which they use afterwards to encrypt the information before it is transmitted. In this case, the secrecy and the reliability of the transmission are managed separately in the two phases.

The secrecy of the transmitted messages mainly depends on reliable information or reasonable and justifiable assumptions about the channel to the potential eavesdropper. Perfect state information about the channel to a passive eavesdropper is not a rational assumption. Thus, we introduce a deterministic model for the uncertainty about this channel, which yields a set of possible eavesdropper channels. We consider the optimization of worst-case rates in systems with multi-antenna Gaussian channels for both approaches. We study which transmit strategy can yield a maximum rate if we assume that the eavesdropper can always observe the corresponding worst-case channel that reduces the achievable rate for the secret transmission to a minimum.

For both approaches, we show that the resulting max-min problem over the matrices that describe the multi-antenna system can be reduced to an equivalent problem over the eigenvalues of these matrices. We characterize the optimal resource allocation under a sum power constraint over all antennas and derive waterfilling solutions for the corresponding worst-case channel to the eavesdropper for a constraint on the sum of all channel gains. We show that all rates converge to finite limits for high signal-to-noise ratios (SNR), if we do not restrict the number of antennas for the eavesdropper. These limits are characterized by the quotients of the eigenvalues resulting from the Gramian matrices of both channels. For the low-SNR regime, we observe a rate increase that depends only on the differences of these eigenvalues for the direct-transmission approach. For the key generation approach, there exists no dependence from the eavesdropper channel in this regime. The comparison of both approaches shows that the superiority of an approach over the other mainly depends on the SNR and the quality of the eavesdropper channel. The direct-transmission approach is advantageous for low SNR and comparably bad eavesdropper channels, whereas the key generation approach benefits more from high SNR and comparably good eavesdropper channels. All results are discussed in combination with numerous illustrations.

Contents

Notation and Abbreviations xi

Introduction 1

Part I Fundamentals of Physical-Layer Security

1 Information-Theoretic Security 15
- 1.1 Notation and Preliminaries 15
- 1.2 Wiretap Scenario 16
- 1.3 Securing Communication by Resource Allocation and Coding 18
- 1.4 Key Generation with the Wiretap Channel 21

Part II Resource Allocation for Physical-Layer Security

2 Secrecy Rate Optimization 29
- 2.1 Basic Scenario 29
- 2.2 Multi-Carrier Scenario 35
- 2.3 Multi-Antenna Scenario 45

3 Worst-Case Studies for Secrecy Rate Optimization 49
- 3.1 Problem Statement and Equivalent Formulations 49
- 3.2 Worst-Case Optimization for Transmitters with Joint Encoding 55
- 3.3 Worst-Case Optimization for Transmitters with Parallel Encoding 77
- 3.4 Discussion 89

Part III Key Exchange for Physical-Layer Security

4 Secret-Key Rate Optimization 97
- 4.1 Basic Scenario 97
- 4.2 Multi-Carrier Scenario 104
- 4.3 Multi-Antenna Scenario 109

5 Worst-Case Studies for Secret-Key Rate Optimization 113

Part IV Conclusion

Summary and Future Work 135

Appendix

A Mathematical Background 141
A.1 The $[\cdot]^+$ Function 141
A.2 Equalities and Inequalities 142
B Additional Material 145
B.1 Proofs for Propositions in Chapter 3 145
B.2 Proofs for Propositions in Chapter 5 152

Bibliography 159

Notation and Abbreviations

Mathematical Notation

$\mathbb{N}$	set of natural numbers (without zero)
$\mathbb{Z}$	set of integer numbers
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
$\mathbb{U}_K$	set of unitary matrices of dimension $K \times K$
$\mathbb{P}_K$	set of permutation matrices of dimension $K \times K$
$a = (a_k)_{k=1}^K$	row vector a of length K with elements a_k, i.e., $a = (a_1, a_2, \ldots, a_K)$
$A = (a_{ij})_{i,j=1}^K$	square matrix A of dimension $K \times K$ with elements a_{ij}
$\lceil a \rceil$	smallest integer not less than a
$[a]^+$	$[a]^+ = \max\{a, 0\}$ for $a \in \mathbb{R}$, see Section A.1
$[a]_{\leq b}^+$	$[a]_{\leq b}^+ = \min\{[a]^+, b\}$ for $a, b \in \mathbb{R}$
$\lim_{x \to a} f(x)$	limit of a function f with variable x as x approaches a
$\liminf_{x \to \infty} f(x)$	limit inferior of a function f with variable x as x approaches ∞
$\ln(a)$	natural logarithm of the positive real number a
$\log_2(a)$	binary logarithm of the positive real number a
I_K	identity matrix of dimension $K \times K$
A^{T}	transpose of the complex matrix A
A^{H}	Hermitian transpose of the complex matrix A
$A^{\frac{1}{2}}$	prinicipal square root of the positive-semidefinite matrix A
$A \succeq 0$	positive semidefiniteness of the Hermitian matrix A
$\det(A)$	determinant of the complex square matrix A
$\mathrm{eig}(A)$	eigenvalues of the complex square matrix A (written as row vector)
$\mathrm{rank}(A)$	rank of the complex matrix A
$\mathrm{tr}(A)$	trace of the complex square matrix A
$\lvert a \rvert$	absolute value of the complex number a
$\lVert a \rVert$	Euclidean norm of the complex vector a
$\lVert a \rVert_1$	L_1 norm of the complex vector a
$\lVert A \rVert_{\mathrm{F}}$	Frobenius norm of the complex matrix A
$X \sim \mathcal{N}(\mu, Q)$	normal distribution with mean vector μ and covariance matrix Q for a random vector X in $\mathbb{R}^K$
$X \sim \mathcal{CN}(0, \sigma^2)$	circularly-symmetric complex normal distribution with zero mean vector and covariance matrix $\sigma^2 I_K$ for a random vector X in $\mathbb{C}^K$
$\Pr(\mathcal{X})$	probability of an event $\mathcal{X}$

p_X	probability mass / density function of a random vector X
$p_{X\|Y}$	conditional probability mass / density function of a random vector X given the random vector Y
$\mathbb{E}(X)$	expectation vector of the random vector X
$H(X)$	entropy of the random vector X
$H(X\|Y)$	conditional entropy of the random vector X given the random vector Y
$I(X;Y)$	mutual information between the random vectors X and Y
$T_f(x;a)$	Taylor series of a complex-valued function f with variable x at the point a

Selected Symbols

A	Gramian matrix of the channel matrix H
B	Gramian matrix of the channel matrix G
C_K	secret-key capacity
C_S	secrecy capacity
G	matrix of channel coefficients for the channel from Alice to Eve
H	matrix of channel coefficients for the channel from Alice to Bob
K	number of carriers
L	number of Alice's transmit antennas
M	number of Bob's receive antennas
N	number of Eve's receive antennas
P	constraint value for the maximum available transmit power at Alice
Q	Alice's transmit covariance matrix
R	transmission rate without secrecy constraints; additional superscripts and decorations see R_S
R_K	secret-key rate; additional superscripts and decorations see R_S
R_S	secrecy rate; additional superscripts and decorations: $\widetilde{R}_S$ eigenvalue notation $\bar{R}_S$ eigenvalue notation for adapted problem in $\langle 3.40 \rangle$ $R_S^\star$ Gramian notation R_S^+ maximized (worst-case) secrecy rate
R_T^+	rate expression that combines key generation rate and subsequent transmission rate for comparison of maximized secrecy and secret-key rates
R_W	worst-case secrecy or secret-key rate; additional superscripts and decorations see R_S
W	random variable for Alice's private message
X	random variable (or vector) for Alice's transmit signal (vector)
Y	random variable (or vector) for Bob's receive signal (vector)
Z	random variable (or vector) for Eve's receive signal (vector)

a	(vector of) channel gains for the channel from Alice to Bob
b	(vector of) channel gains for the channel from Alice to Eve
g	(vector of) channel coefficients for the channel from Alice to Eve
h	(vector of) channel coefficients for the channel from Alice to Bob
n	length of a codeword
q	Alice's power allocation (vector)
ζ	random variable (or vector) for Eve's noise
ξ	random variable (or vector) for Bob's noise
ρ	inverse noise variance
σ^2	noise variance
φ	function for the definition of secrecy rate (terms); additional superscripts and decorations see R_S
χ	constraint value for the channel from Alice to Eve
$\mathcal{B}$	constraint set for the worst-case channel to the eavesdropper; vector case with eigenvalue notation
$\mathcal{Q}$	constraint set for the power allocation strategy at the transmitter; scalar and vector case
$\mathcal{W}$	alphabet for Alice's private message
$\mathcal{X}$	alphabet for Alice's channel input
$\mathcal{Y}$	alphabet for Bob's channel output
$\mathcal{Z}$	alphabet for Eve's channel output
$\mathscr{B}$	constraint set for the worst-case channel to the eavesdropper; matrix case with Gramian notation
$\mathscr{G}$	constraint set for the worst-case channel to the eavesdropper; matrix case with channel matrix notation
$\mathscr{Q}$	constraint set for the power allocation strategy at the transmitter; matrix case

Abbreviations

KKT	Karush-Kuhn-Tucker
MIMO	multiple-input multiple-output
MISO	multiple-input single-output
SNR	signal-to-noise ratio

Introduction

In this chapter, we first want to clarify what the main focus of the thesis is. Afterwards, previous and related publications are introduced and discussed before a detailed outline of the thesis is given.

Motivation and Background

Based on the title of the thesis, which is *Robust Optimization of Private Communication in Multi-Antenna Systems*, we introduce the terms that are important for this thesis and discuss their meaning herein.

We consider *communication* in the sense of information or data transmission between two users over a noisy communication channel. For convenience, we focus on the transmission in one direction, i.e., from one user, which we usually identify as transmitter, to another, which is mainly referred to as intended receiver. In the following, the transmitter and the intended receiver are also called Alice and Bob, respectively. The premise of successful communication is its reliability, i.e., Alice has to ensure that Bob can recover the information from the symbols he receives. The performance measure of interest is the rate of this communication, i.e., the transmitted information per channel use.

The focus of this thesis is on the *privacy* of the communication, i.e., Alice has information that is intended for Bob and that she wants to transmit over the channel, while keeping anyone else completely ignorant of this information. The authentication of the users is not considered in the thesis. Instead, we assume that Alice has already ensured that she is communicating with Bob and vice versa. In addition to the transmitter and the receiver, we introduce a third user, the so-called eavesdropper, which is named Eve. Eve is a passive eavesdropper, i.e., she is a curious user of the system that overhears the communication between Alice and Bob and tries to extract the information if possible. This assumption implies that Eve knows everything that is essential for the operation of the system. Eve is not an active attacker, i.e., she does not try to influence the communication between Alice and Bob, e.g., by jamming, the interception of sent messages, the induction of own messages, or by trying to fake her identity.

We want to ensure the privacy of the communication by means of the physical layer, i.e., by appropriately chosen coding and resource allocation schemes. We consider information-theoretic security, which provides theoretically provable secrecy, in contrast to recent encryption / decryption algorithms, which ensure the secrecy of the information under

practically reasonable assumptions like a restriction of the computational power of the potential eavesdropper.

We study a wireless communication system, which in principle is susceptible to eavesdropping due to the inherent openness of the transmission medium. We consider a *multi-antenna scenario*, where all users, i.e., the transmitter and the receiver as well as the eavesdropper, are equipped with multiple antennas for transmitting or receiving the information that is sent over the channel.

We analyze two different approaches that can ensure the secrecy of the private information. One is the direct transmission of this information to the intended receiver, while its reliability and secrecy have to be ensured simultaneously by an appropriately chosen coding and resource allocation scheme. The other is a two-phase approach. In this case, the two legitimated users have to first agree on a common key, which should be completely unknown to the eavesdropper. This has to be realized by means of the physical layer and without any secret that was previously shared between Alice and Bob and that could be used as an advantage over the eavesdropper. Furthermore, we do this key agreement without a trustworthy third party, which is possibly involved in other key exchange protocols. Afterwards, the secrecy of the information can be ensured by encryption, while the subsequent transmission has only to guarantee the reliability of the encrypted message.

The term *optimization* refers to the interest of the transmitter, which is to obtain a possibly high rate with its limited resources, which could be for instance identified as transmit power, available frequency spectrum, or transmit antennas. In order to achieve this, Alice has to determine the best transmit strategy under some given constraints like a restriction on the sum power that is used over all antennas. A transmit strategy describes a resource allocation, which means a certain power allocation and a corresponding beamforming scheme for all transmit antennas in a multi-antenna scenario.

If the *robustness* of an approach is discussed, the main question that has to be answered is: What happens if important system parameters are not perfectly known to the transmitter? Since we consider the communication in a wireless system where the reliability and privacy of the information have to be guaranteed, the knowledge about the quality of the channels is a very important factor for the transmitter. For the channel to Bob, we could assume a certain channel estimation error, whose impact could be twofold. On the one hand, we can have the situation that the real channel is worse than the estimation, which would result in a transmission whose reliability is no longer ensured. On the other hand, the real channel could be better than its estimate, which would yield a situation where a certain rate is calculated and used for the transmission, although a higher rate would be achievable. However, we assume that Alice has perfect knowledge about the channel coefficients to the intended receiver throughout the thesis. We focus on the case that the transmitter does not have perfect knowledge about the channel coefficients to the eavesdropper. This information is important for the secrecy of the transmission. If it is not perfectly available, it is at least necessary to have reliable and justifiable assumptions about this channel. The assumption that perfect information about the channel to

Eve is available to Alice, which would be the best case for a transmission with secrecy constraints, can hardly be justified if a passive eavesdropper is considered. It is only reasonable under the assumption that Eve is another regular user of the communication system that also communicates with Alice, where we have to additionally assume that the reciprocity of the channel is given. The assumption of perfect channel knowledge can be relaxed by allowing an uncertainty about the eavesdropper channel. Such an uncertainty can be modeled stochastically with a random variable whose statistics is known to the transmitter, but this is not the focus of this thesis. Instead, we consider a deterministic model for the uncertainty, i.e., we formulate a reasonable restriction on the eavesdropper channel, which is for instance a constraint on the sum of all channel gains, which can correspond to a constraint on the overall receive power at the eavesdropper. This approach yields a set of possible eavesdropper channels that have to be considered by the transmitter. In this thesis, robust optimization consequently means that Alice aims to determine the best transmit strategy, which can yield a maximum rate, under the assumption that Eve can always observe the corresponding worst-case channel, which reduces the achievable rate to a minimum for the chosen transmit strategy.

Previous and Related Work

Shannon (1949) formulated the objective of secret communication: The intended receiver should be able to recover the private message without errors after the transmission over a communication channel, while nobody else should get any information about this message. For this purpose, Shannon analyzed the encryption of the message with a secret key that has to be known to both the transmitter and the intended receiver. The eavesdropper is completely ignorant of the key, but he can perfectly observe the transmitted codeword. The secrecy of the communication was measured by the average uncertainty that the eavesdropper has about this message. Ideally, this uncertainty, which is called equivocation, equals the a-priori uncertainty one has about the message. In order to achieve this, the uncertainty about the key must be at least as large as the uncertainty about the message, i.e., there must be at least one secret key bit for every bit of information (Bloch and Barros, 2011, Section 1.1).

About 25 years later, Wyner (1975) as well as Csiszár and Körner (1978) introduced the basic concept of physical-layer security. Wyner (1975) studied the degraded wiretap channel with finite input and output alphabets, where the transmitter encodes the private message into a codeword that is transmitted over a noisy channel to the intended receiver afterwards. The eavesdropper observes a degraded version of the receive signal over a further noisy channel. Thus, the transmitter and the intended receiver always have an advantage over the eavesdropper, which they can exploit to ensure the secrecy of the message. This approach was generalized and extended by Csiszár and Körner (1978). They analyzed a discrete wiretap scenario where the eavesdropper channel is not necessarily degraded with respect to the main channel to the intended receiver. Furthermore, they

introduced the concept of the broadcast channel with a confidential message. In this scenario, the transmitter has a common message, which is intended for both receivers, and a private message for one receiver, which should be kept perfectly secret from the other. In the same year, the physical-layer secrecy approach was also applied to the Gaussian wiretap channel by Leung-Yan-Cheong and Hellman (1978).

In the 1990s, first Maurer (1990, 1993) and then Ahlswede and Csiszár (1993) proposed and studied the fundamentals of secret-key agreement on the physical layer by additionally allowing public discussion between the two legitimated users. They showed that there exist communication strategies that allow the distillation of a common and secret key between two users on the physical layer in the presence of an eavesdropper. This key can be used afterwards to ensure the secrecy of a private message during the transmission by encryption.

For the last 10 years, the growing technical progress has motivated an increasing interest in the area of physical-layer security. Communication systems have been developed that offer for instance the computational power such that these ideas can find their way into future communication systems. More and more research groups have contributed results to the area of physical-layer security, which significantly broadened and diversified the topics that are considered. Thus, it is not possible to give a complete and detailed overview of all ongoing research in this area. Nevertheless, we will have a look at some selected research topics in the following. We focus on areas that are related to our work and the results of this thesis. Other research fields are only mentioned as supplements to this overview.

One main focus of the research in the last years was the analysis of physical-layer security first for fading channels and later also for multi-antenna (MIMO) systems. One challenge was to prove the secrecy capacity of such systems. Here, we exemplarily mention Khisti and Wornell (2007) as well as Oggier and Hassibi (2007), who derived the secrecy capacity of the MIMO wiretap channel.

Bloch et al. (2008) studied the impact of fading on the secrecy capacity of a wireless system with quasi-static fading channels by considering the average secrecy capacity and the probability of outage for the secrecy capacity. The authors considered the case that perfect channel state information about the eavesdropper channel is available, but also the case that the transmitter and the receiver have only partial knowledge about the eavesdropper channel. The interesting observation was that even if the average channel quality between transmitter and eavesdropper is better than the average channel between transmitter and intended receiver, the secrecy capacity can still be positive. A similar behavior was described by Gopala et al. (2008) and Liang et al. (2008c).

Another challenge has been to derive optimal resource allocation schemes for secrecy in multi-antenna systems under different constraints and assumptions. Li et al. (2007) solved the secrecy rate maximization problem for the Gaussian MISO wiretap channel, where multiple transmit antennas can be deployed by the transmitter, whereas only a

single receive antenna is used at both the intended receiver and the eavesdropper. The authors presented an analytical solution for this case by applying an appropriately defined coordinate transformation depending on the channel to the intended receiver and the eavesdropper. For the same model and under different channel fading assumptions, Shafiee and Ulukus (2007) showed that the optimal communication strategy in all cases is beamforming. Li and Ma (2011) considered a scenario where the communication over a MISO channel is overheard by multiple multi-antenna eavesdroppers. The authors studied the problem of transmit covariance optimization for the secrecy-rate maximization. They showed that this problem can be solved in a convex and tractable fashion with a semidefinite program and that beamforming is the optimal transmit strategy for the considered scenario.

The corresponding transmit optimization for the secrecy rate maximization of the MIMO wiretap channel is more difficult. The first method that solved the optimal power allocation problem for the Gaussian MIMO wiretap channel was proposed by Liu et al. (2009). It is a numerical method based on global optimization and called branch-and-bound algorithm with reformulation and linearization technique. Li et al. (2013) considered the MIMO secrecy rate maximization problem in the Gaussian wiretap channel under sum power and per-antenna power constraints. The authors reformulated this problem into an equivalent matrix problem that can be solved by alternating optimization. They presented an alternating optimization algorithm and developed a fast algorithm for each iteration. Recently, Cumanan et al. (2014) presented an approach based on Taylor series expansion for both the power minimization and the secrecy rate maximization of the MIMO wiretap channel. The authors proposed iterative algorithms to solve these problems under the assumption that the transmitter has perfect channel state information. Moreover, they incorporated channel uncertainties for both channels and showed that the resulting problems can be reformulated into semidefinite programs at low signal-to-noise ratios (SNR).

For multi-user systems, the broadcast scenario is of great interest. Liang et al. (2008c) investigated the fading broadcast channel with confidential messages, where the transmitter has a common message for two receivers and additionally a confidential information for one receiver that needs to be kept as secret as possible from the other. Under perfect channel state information, the authors studied first the parallel broadcast channel with independent subchannels. They established the secrecy capacity region for this model and derived the optimal power allocations for the parallel Gaussian broadcast channel that achieve the boundary of this secrecy capacity region. Moreover, they considered the ergodic and outage performance of this system. The secrecy capacity region of the MIMO broadcast channel is characterized by Liu et al. (2010). Bagherikaram et al. (2013) showed that secret dirty paper coding is optimal to achieve the secrecy capacity region.

In systems with multiple transmit and receive antennas, the spatial degrees of freedom further allow to support the privacy of the communication by transmitting artificial noise in order to generate additional interference at the eavesdropper. This approach was

first proposed by Negi and Goel (2005). The available transmit power is split into two parts. One is used to transmit the private message, whereas the other is used for the artificial noise, which is transmitted into the nullspace of the main channel in order to avoid additional interference at the intended receiver. This approach was further studied by the same authors in (Goel and Negi, 2008), where amplifying relays were used to support a single-antenna transmitter in securing the communication by transmitting artificial noise. Zhou and McKay (2009) considered again the wiretap scenario with a multi-antenna transmitter, where non-cooperating and cooperating eavesdroppers try to overhear the private communication. They analyzed the optimal power allocation between the information bearing signal and the artificial noise.

The idea of supporting the private communication by artificial noise was further developed by introducing additional helpers in the systems. The objective of these helpers, which are also denoted as friendly or cooperative jammers, is to create additional interference for the eavesdropper, which makes it more difficult for him to overhear the communication between the transmitter and the intended receiver. Jorswieck (2010) considered simple single-antenna helpers and showed that the channel parameters and the SNR determine whether such a helper can increase the achievable secrecy rates. Moreover, the MISO wiretap channel with perfectly informed multi-antenna helpers was studied. The optimal beamforming vectors were characterized and an algorithm was proposed that jointly optimized the beamforming vectors of the transmitter and the helper. Additionally, it was shown in (Wolf and Jorswieck, 2010b), that the optimal helper strategy generally is not zero-forcing beamforming with respect to the intended receiver, although this beamforming strategy is often chosen for the helper in the literature due to its simplicity. The ideas that a transmitter protects its transmission by additional artificial noise and that a helper can support the privacy of the communication was for instance combined in Dong et al. (2009). The authors introduced a multi-antenna relay that forwards the private message from a single-antenna transmitter to a single-antenna receiver, while it simultaneously protects this transmission with additional artificial noise. The idea of relay-assisted multi-hop communication is discussed in a various number of publications under many different assumptions. For instance, Ho et al. (2013) proposed a relay strategy that utilized both spectral and spatial resources to enhance the secrecy in a multi-antenna, multi-carrier interference channel. The growing number of users in the networks increases the complexity of the studied problems and approaches. From a practical point of view, there are not only cooperating users, but also scenarios with competing users, which makes it interesting to study such problems also from a game-theoretical perspective as in (Jorswieck and Mochaourab, 2009).

If the assumption of perfect channel state information about the eavesdropper channel is relaxed, the partial knowledge at the transmitter is often modeled stochastically. This yields a study of the ergodic secrecy rate or the secrecy outage probability. Moreover, it is possible to enhance the performance of the system with additional artificial noise as in (Gerbracht et al., 2010), where multiple antennas at the transmitter were exploited. Such investigations can be further extended to relay networks, where the relay operation modes

have to be considered in the discussion. For instance, Gabry et al. (2011) studied the outage performance for a scenario, where the relay can use the amplify-and-forward and the decode-and-forward strategy and the secret transmission is supported by cooperative jamming.

In contrast to this stochastical approach, it is also possible to formulate deterministic models for the channel uncertainties at the transmitter. Liang et al. (2007) studied the compound wiretap channel, which is a wiretap channel where the main and the eavesdropper channel can take a number of states. This model can equivalently be interpreted as a multicast scenario with multiple eavesdroppers, where the transmitter wants to transfer its information to all receivers and simultaneously keep it secret from all eavesdroppers. We refer to ⟨3.61⟩ for a more detailed discussion of this approach. Li and Ma (2011) considered a Gaussian MISO wiretap channel with multiple multi-antenna eavesdroppers, where the channel estimations at the transmitter are characterized by certain additive errors. A max-min optimization problem is obtained if the secrecy rate should be robustly maximized with respect to the possible channel errors. For this problem, the authors developed a semidefinite programming solution and showed that their approach outperforms non-robustly designed solutions, especially for high SNR. Li and Petropulu (2012) studied the Gaussian MISO wiretap channel with a single-antenna eavesdropper. The authors assumed that the channel estimation errors for both channels are bounded and can be described by a spherical uncertainty. They considered the maximization of the worst-case secrecy rate subject to a given power constraint. For this problem, they derived a related matrix whose eigenvalues yield the solution for the optimal transmit covariance matrix. Also Shi and Ritcey (2010) as well as Huang and Swindlehurst (2012) considered the robust beamforming problem for the Gaussian MISO wiretap channel. Shi and Ritcey (2010) assumed that all possible states of the eavesdropper channel are in a given set, which is known to the transmitter. Their objective was to find the optimized transmit covariance matrix for the maximized worst-case secrecy rate such that the eavesdropper is unable to decode under any channel realization in the set. They proposed to transfer this max-min optimization problem into a convex optimization problem that can be solved efficiently and obtained a generalized eigenvalue / eigenvector solution for their problem. Huang and Swindlehurst (2012) studied not only the direct transmission approach, but also a scenario where a multi-antenna helper supports the private communication for a system with bounded channel estimation errors for the channels. They obtained robust transmit covariance matrices based on worst-case secrecy rate maximization under both individual and global power constraints. For the individual power constraints, they showed that the max-min problem can be transformed into a quasi-convex problem that can be efficiently solved afterwards. For the global power constraint, they proposed a joint optimization approach of the transmit covariance matrices and power allocations for the transmitter and the helper.

All topics discussed above can also be considered in the context of secret-key generation and agreement. Jorswieck et al. (2013) and Engelmann et al. (2014) considered the secret-key generation problem in a source-type model, where the two legitimated partners

use the state of the multi-antenna communication channel between them as source of common randomness. In these publications, it was assumed that the eavesdropper has no possibility to observe a correlated version of the channel state realizations. The impact of the spatial channel correlation on the achievable secret-key rate was analyzed by Jorswieck et al. (2013) for a MIMO scenario. Based on this, Engelmann et al. (2014) discussed the optimal precoding scheme for the secret-key generation under spatial correlation for the MISO scenario. Tomasin and Jorswieck (2014) studied the problem of key agreement for a source-type model with wiretapper, which is obtained if a pilot-based channel estimation procedure is used for secret-key agreement in a multi-antenna scenario with correlated channels. The authors derived closed-form expressions of lower and upper bounds on the achievable secret-key rates and analyzed the training sequence optimization, where the known spatial channel correlation was taken into account.

Wong et al. (2009) studied the key generation approach for the channel-type model and extended the results of Ahlswede and Csiszár (1993) to continuous channel alphabets. They focused on a fast-fading Gaussian MIMO wiretap channel. We refer to ⟨5.31⟩ for a more detailed discussion of this approach.

Systems with competing and interfering multi-antenna links also play a role for the secret-key generation approach. For instance, Jorswieck (2013) considered a multi-antenna interference channel with a public discussion channel, where confidential messages should be transmitted. For this model, an achievable secret-key region was derived that can improve the achievable secrecy rate region. The non-cooperative transmit strategy problem was studied from a game-theoretical perspective, and it was shown that there exists a unique Nash equilibrium for a specifically designed utility function.

Vía (2014) considered the robustness of the secret-key generation for the channel-type model with a Gaussian MIMO wiretap channel. The transmitter's uncertainty about the eavesdropper channel was characterized by a bounded channel estimation error. The author studied the secret-key rate maximization problem with respect to the corresponding worst-case eavesdropper channel. We refer again to ⟨5.31⟩ for a more detailed discussion of this approach.

For the analysis of the efficiency of the secret-key sharing model, the possible attacker scenarios play an important role. With regard to active attacks like jamming, the source-type model with compound sources was studied in (Boche and Schaefer, 2013) and (Boche and Wyrembelski, 2013).

A further objective of physical-layer security is to enable the authentication of users. Here, we only exemplarily mention Xiao et al. (2007). The authors describe a physical-layer algorithm that combines channel probing with a hypothesis test in order to determine whether current and prior communication attempts are originated from the same user.

Another important topic for the realization of the physical-layer security ideas is the development of practical wiretap codes, which is also considered by a certain number of research groups.

Contribution and Outline

One important question, which directly arises if results from information-theoretic security shall be applied to wireless communication systems, is how to deal with the transmitter's uncertainty about the channel to a potential passive eavesdropper of the private communication, which inherently exists in such a scenario. Perfect knowledge about this channel, which was assumed in prior publications that provided a basis for today's research, is not a realistic assumption. This thesis contributes to the area of research that aims to reduce this problem in order to increase the practical relevance of the results. With the multi-antenna (MIMO) scenario, where all users of the system are allowed to have multiple transmit and receive antennas, we consider a very general setting, which yields results for special cases, i.e., the MISO and the multi-carrier scenario, as well.

We introduce an uncertainty model for the eavesdropper channel that is practically relevant. We propose a model with an upper bound on the sum of all channel gains. In combination with a sum power constraint at the transmitter, it corresponds to a constraint on the total receive power at the eavesdropper. The transmitter can parametrize this model based on his knowledge about the spatial situation, which yields reasonable and justifiable assumptions about the channel to the potential eavesdropper. In contrast to often used stochastic models, we use this deterministic model, since it allows a worst-case analysis with a related rate maximization for the given scenario. The results are maximum achievable rates and corresponding transmit strategies that simultaneously guarantee the secrecy of the private communication.

In this thesis, we analyze two physical-layer approaches that ensure the secrecy of the private information. If the direct-transmission approach is applied, the transmitter has to simultaneously ensure the reliability and the secrecy of the transmitted information. In contrast, the key generation approach consists of two phases, the key generation and the transmission phase. This allows the transmitter to handle both objectives separately. Although there are no explicit solutions for the maximization of the considered worst-case problems, we provide upper and lower bounds on these problems that are very close to each other. Hence, the remaining uncertainty about the maximum achievable rates vanishes nearly completely, and the derived bounds supersede the solution of the problems. Furthermore, the characterization of the lower bounds yields almost optimal transmit strategies.

An important outcome of this thesis is the comparison of both approaches, which are usually studied separately in the literature. Therefore, we suggest a performance measure for the key generation approach that does not only focus on the maximum achievable rate for the key generation, but also incorporates the effort that is necessary for the subsequent data transmission, which is a requirement for a fair comparison of both approaches. Thus, we obtain important propositions for the system design by showing which approach is to be preferred depending on the given system parameters as the total available power and the assumptions that can be made about the quality of the eavesdropper channel.

This thesis is organized as follows:

- In Chapter 1, an overview of models and corresponding performance measures for physical-layer security from the literature is provided. Thereby, we present two different approaches. One is the direct transmission of the private message to the intended receiver, while the reliability and the secrecy of the information have to be ensured by an appropriately chosen coding scheme. The other approach is composed of two phases. The legitimated communication partners first establish a common and secret key, which they use afterwards for a communication whose privacy is guaranteed by an encryption with this key. The first approach is considered in the Chapters 2 and 3, whereas the Chapters 4 and 5 focus on the second approach.

- In Chapter 2, results for the maximization of secrecy rates are presented and discussed for various scenarios. We first introduce a basic scenario, which is extended to a multi-carrier and a multi-antenna scenario afterwards. This chapter comprises not only the single-user case, where the transmitter intends to send a private message to the legitimated receiver in presence of an eavesdropper, but also the two-user case, where the transmitter has private messages for both receivers, which should be kept secret from the other. The results of this chapter provide a basis for the worst-case analysis of the secrecy rate in the next chapter.

- In Chapter 3, we consider the multi-antenna scenario from the previous chapter and relax the assumption that the transmitter has perfect knowledge about the eavesdropper channel. Instead, we allow an uncertainty about this channel and introduce an appropriate deterministic model, which results in a set of possible eavesdropper channels. The problem for the transmitter is now twofold. On the one hand, the worst-case channel has to be determined, which yields the minimum secrecy rate, for each feasible transmit strategy. On the other hand, the best transmit strategy has to be identified, which is the resource allocation that provides the maximum secrecy rate under the assumption that the eavesdropper observes the corresponding worst-case channel. In this chapter, we derive a vector problem, which is equivalent to the original matrix problem. Based on this vector problem, we consider the max-min optimization of the secrecy rate for two different transmitter structures. For both problems, we present the worst-case channel for each transmit strategy, characterize the optimal resource allocation under a sum power constraint over all antennas, and provide lower and upper bounds on the maximized worst-case secrecy rate, which are tight for low or high SNR. The results of this chapter are discussed together with numerous illustrations.

- In Chapter 4, results for the maximization of secret-key rates are presented and discussed. We focus on the scenarios that we have already introduced in Chapter 2 in the context of the secrecy rate maximization. This allows us to directly compare the results that were obtained for both approaches. Furthermore, the results of this chapter provide a basis for the worst-case analysis of the secret-key rate in the next chapter.

- In Chapter 5, the worst-case approach of Chapter 3 is applied to the secret-key generation problem in the multi-antenna scenario, which was introduced in Chapter 4. Again, we consider a deterministic model for the uncertainty about the eavesdropper channel, which yields a max-min problem for the transmitter. The aim is to identify an optimal transmit strategy, which maximizes the secret-key rate under the assumption that the eavesdropper is always able to observe the worst-case channel, which yields the minimum secret-key rate for the previously chosen transmit strategy. We show that this matrix problem can be reformulated as an equivalent vector problem over the eigenvalues of the involved matrices. We present the worst-case channel for each transmit strategy and characterize the optimal resource allocation under a sum power constraint over all antennas. Additionally, lower and upper bounds on the maximized worst-case secret-key rate are provided, which are tight for low or high SNR. We compare the results on the worst-case maximization of the secret-key rate with the results we obtained in Chapter 3 for the similar secrecy rate problem. Numerous illustrations support the discussion of the results.
- Finally, we summarize the results of the thesis and formulate open problems for further research.
- In Appendix A and B, additional material for the mathematical background and detailed proofs for important propositions of the thesis are provided.

Part I

Fundamentals of Physical-Layer Security

1 Information-Theoretic Security

In this chapter, we introduce the fundamentals of information-theoretic security, which can be used to ensure the privacy of a communication by means of the physical layer. We provide a short review of models and results from the literature. The description of models and performance measures mainly follows the presentations in (Liang et al., 2008a) and (Bloch and Barros, 2011). We refer to these publications for a more detailed overview. The fundamentals of information theory are for instance explained in (Cover and Thomas, 2006), (Yeung, 2008), and (Bloch and Barros, 2011).

1.1 Notation and Preliminaries

An overview and a short explanation of the mathematical notation in this thesis can be found at page xi. A summary of the most important symbols is provided at page xii.

⟨**1.1**⟩ **Notation (Upper-Case, Lower-Case and Various Calligraphic Symbols).** Throughout this thesis, we use lower-case letters for scalars and vectors, whereas matrices are denoted by upper-case letters. We deviate from the convention above in an information-theoretic context. We use the upper-case letters X, Y, and Z for random variables and random vectors describing channel inputs and channel outputs. Moreover, W is used to denote the random variable that is identified with the private message. The corresponding lower-case letters are used for the realizations of these random variables and vectors. This mainly occurs in this chapter and in the description of system models in the following chapters. Moreover, the upper case-letters K, L, M, and N are used for the number of carriers or antennas in various models that are introduced in the next chapters. Rates and capacities are denoted by R and C, respectively. Usually, sub- and superscripts are added to specify the rates and capacities more clearly.

Sets, which are used to define alphabets for random variables and constraint sets for optimization problems, are denoted by calligraphic letters. For the specification of constraint sets, two different calligraphic fonts are used. We write a calligraphic symbol like $\mathcal{Q}$ for constraint sets that are defined for scalars or vectors, whereas we use a calligraphic symbol like $\mathscr{Q}$ for sets formulating constraints on matrices.

⟨**1.2**⟩ **Binary Logarithm and Bit.** Throughout this thesis, we will use the binary logarithm for the computation of rates and capacities. Thus, all those values are measured in bit per channel use. For convenience, we omit the supplement *per channel use* and write only *bit* if we evaluate rate expressions below.

1.2 Wiretap Scenario

Figure 1.1: Communication system with a transmitter (Alice), a legitimated receiver (Bob), and an eavesdropper (Eve).

We are interested in the following scenario, which is illustrated in Figure 1.1. Alice wants to send a private message to Bob, which should be kept perfectly secret from Eve. In this communication system, Alice is the transmitter and Bob is the intended or legitimated receiver. We assume that Alice and Bob have already authenticated each other successfully. Eve is a passive eavesdropper, i.e., she listens to the communication between Alice and Bob and tries to extract as much information as possible, but she does not actively influence this communication process, e.g., by jamming.

In order to establish this private communication by means of the physical layer, Alice has the choice between two different approaches.

a) She can directly transmit the private message to Bob, while she ensures the reliability and secrecy of the information by appropriately chosen coding and resource allocation schemes. This approach, which is introduced in Section 1.3, is characterized by a performance measure that is called secrecy capacity.

b) Alternatively, Alice and Bob can first try to establish a common and secret key, which they can use afterwards for a communication whose privacy is guaranteed by an encryption with this key. For the key generation, Alice and Bob use the communication channel between them. Additionally, a public message exchange is necessary for the key agreement. This approach is introduced in Section 1.4. The process of key establishment is characterized by a performance measure that is called secret-key capacity.

The first approach has to simultaneously guarantee the reliability of the communication to the intended receiver and the secrecy of the information against eavesdropping. The advantage of the second approach is that the reliability and the secrecy of the information can be considered separately. A major drawback is that two subsequent communication processes are necessary, which both require resources like time and power, since Alice and Bob first need to generate a common key before the private information can be transmitted.

An important component of the models for both approaches is the so-called wiretap channel. Figure 1.2 shows an abstract illustration of this channel. From a structural perspective, the wiretap channel can be interpreted as a special case of a broadcast channel with two receivers, but Alice's intentions in these scenarios significantly differ from each other. In a broadcast scenario, Alice is interested in simultaneously transmitting her

message to all users, which clearly contrasts with her intention in the wiretap scenario. In the literature, there exist models that combine the broadcast and wiretap scenario to a broadcast channel with confidential messages, i.e., Alice has a common message and additional private messages for both users. This model, which was introduced by Csiszár and Körner (1978), is not within the focus of this thesis.

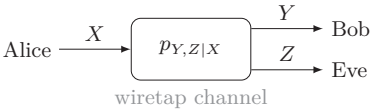


Figure 1.2: General model for a wiretap channel.

⟨**1.3**⟩ **Wiretap Channel.** The wiretap channel, which is illustrated in Figure 1.2, can be described by a channel input alphabet $\mathcal{X}$, which can be used by Alice, and two channel output alphabets $\mathcal{Y}$ and $\mathcal{Z}$ for the values that are observed by Bob and Eve, respectively. The relation between the channel input and the channel outputs is characterized by a conditional probability distribution. The transmission of symbols is modeled as memoryless and stationary. Thus, we can omit the time index and characterize the channel only for a single time slot, i.e., we make use of a single-letter representation. Therefore, the channel input and output can be described by random variables. We choose X for Alice's channel input. Bob's and Eve's channel outputs are identified by Y and Z, respectively. If the alphabets of the wiretap channel are finite, the input-output relation of the channel is described by a conditional probability mass function $p_{Y,Z|X}$, i.e., we have a probability mass function $p_{Y,Z|X}(\cdot,\cdot|x)$ for each input value $x \in \mathcal{X}$. If we consider real-valued alphabets, we restrict ourselves to channels that are characterized by a conditional probability density function $p_{Y,Z|X}$, i.e., we have a probability density function $p_{Y,Z|X}(\cdot,\cdot|x)$ for each input value $x \in \mathcal{X}$.

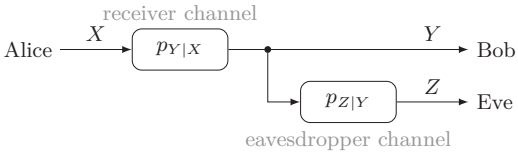


Figure 1.3: Model for the degraded wiretap channel.

⟨**1.4**⟩ **Degraded Wiretap Channel.** In order to analyze the secret communication in the wiretap scenario, Wyner (1975) introduced the degraded wiretap channel as depicted in Figure 1.3. Wyner's model, which is a special case of the wiretap channel in ⟨1.3⟩, is a discrete memoryless wiretap channel with finite channel alphabets. Alice communicates with Bob over a discrete memoryless channel, which is described by the input alphabet $\mathcal{X}$, the output alphabet $\mathcal{Y}$, and the conditional probability mass function $p_{Y|X}$. Eve observes a degraded version of Bob's signal, which is transmitted over a discrete memoryless

channel that is characterized by the input alphabet $\mathcal{Y}$, the output alphabet $\mathcal{Z}$, and the conditional probability mass function $p_{Z|Y}$. Thus, the conditional probability mass function of the wiretap channel can be written as $p_{Y,Z|X}(y,z|x) = p_{Y|X}(y|x)\,p_{Z|Y}(z|y)$ for all $(x,y,z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$. Equivalently, we can say that the random variables X, Y, and Z form a Markov chain in the order $X - Y - Z$. Another equivalent formulation is that the random variables X and Z are conditionally independent given the random variable Y.

Wyner's model was generalized by Csiszár and Körner (1978) to a discrete wiretap channel that is not necessarily degraded. This corresponds to the general wiretap model that is depicted in Figure 1.2 under the assumption of finite channel alphabets. With this model, Csiszár and Körner studied not only the wiretap scenario, but also the broadcast scenario with additional confidential messages.

⟨**1.5**⟩ **Gaussian Wiretap Channel.** The Gaussian wiretap channel, which is another special case of the wiretap channel in ⟨1.3⟩, was introduced by Leung-Yan-Cheong and Hellman (1978). In this model, Bob's and Eve's outputs are corrupted by additive white Gaussian noise. For each channel use, the Gaussian wiretap channel can be described by

$$Y = X + \xi \quad \text{and} \quad Z = X + \zeta,$$

where ξ and ζ are Gaussian random variables with $\xi \sim \mathcal{N}(0,\sigma^2)$ and $\zeta \sim \mathcal{N}(0,\vartheta^2)$ that are independent from each other and independent from the channel input X. Then, the corresponding conditional probability density function $p_{Y,Z|X}$ is a two-dimensional Gaussian density $p_{Y,Z|X}(\cdot,\cdot|x)$ for each input value $x \in \mathcal{X}$. Due to the independence of the noise variables, it can be written as $p_{Y,Z|X}(y,z|x) = p_{Y|X}(y|x)\,p_{Z|X}(z|x)$ for all $(x,y,z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$, where $p_{Y|X}(\cdot|x)$ and $p_{Z|X}(\cdot|x)$ are the Gaussian density functions of ξ and ζ that are shifted by x.

This model can be extended to the complex Gaussian wiretap channel with known additional attenuation coefficients h and g with $h, g \in \mathbb{C}$, which can be described by

$$Y = hX + \xi \quad \text{and} \quad Z = gX + \zeta,$$

where the noise is circularly-symmetric complex Gaussian distributed, i.e., $\xi \sim \mathcal{CN}(0,\sigma^2)$ and $\zeta \sim \mathcal{CN}(0,\vartheta^2)$.

1.3 Securing Communication by Resource Allocation and Coding

Now, we consider the following scenario. Alice uses the wiretap channel to transmit a private message to Bob. She wants that Bob can reliably decode this message, while it should be kept perfectly secret from Eve. Eve listens to the transmission from Alice to Bob and tries to decode the message.

⟨**1.6**⟩ **Encoding, Decoding, and Secrecy Capacity.** In order to ensure both reliability and confidentiality of the message, an appropriate coding and decoding scheme is necessary. We give an account of the corresponding results for the wiretap channel in ⟨1.3⟩ with finite alphabets, where we mainly follow the presentation in (Liang et al., 2008a, Chapter 2), but also add contributions from (Bloch and Barros, 2011, Section 3.4). Alice's private message for Bob is denoted by the random variable W, whereas Bob's estimation of this message, which is based on his observation of the channel output, is identified by $\hat{W}$. It is assumed that the message W is uniformly distributed over a message set $\mathcal{W}$. Alice has access to a source of local randomness, which can be described by the random variable V with realizations from a set $\mathcal{V}$. She uses an encoding function[1] $f_{\text{enc}}^{(n)} \colon \mathcal{W} \times \mathcal{V} \to \mathcal{X}^n$ that maps each message $w \in \mathcal{W}$ to a codeword $x^{(n)} \in \mathcal{X}^n$ of length n, depending on the recent realization $v \in \mathcal{V}$ of the local source of randomness. Afterwards, Alice transmits this codeword over the wiretap channel in n channel uses. Bob's and Eve's output sequences are $y^{(n)} \in \mathcal{Y}^n$ and $z^{(n)} \in \mathcal{Z}^n$, respectively. Bob uses a decoding function $f_{\text{dec}}^{(n)} \colon \mathcal{Y}^n \to \mathcal{W}$ that maps the received sequence $y^{(n)} \in \mathcal{Y}^n$ to an estimate $\hat{w} \in \mathcal{W}$ of the message. A $(2^{nR}, n)$ code of length n and rate R is defined as a message set $\mathcal{W}$ with $|\mathcal{W}| = \lceil 2^{nR} \rceil$ together with an encoding function $f_{\text{enc}}^{(n)}$ and a decoding function $f_{\text{dec}}^{(n)}$.

The performance measures for the private communication from Alice to Bob are the reliability and the secrecy of the transmission. The reliability is evaluated by the average block error probability, which is defined for a given code of length n as

$$P_e^{(n)} := \Pr(\hat{W} \neq W) = \frac{1}{|\mathcal{W}|} \sum_{w=1}^{|\mathcal{W}|} \sum_{\substack{\hat{w}=1 \\ \hat{w} \neq w}}^{|\mathcal{W}|} p_{\hat{W}|W}(\hat{w}|w).$$

The secrecy of the message W is measured by the equivocation rate, which is defined as

$$R_e^{(n)} := \frac{1}{n} H\left(W|Z^{(n)}\right),$$

where $H\left(W|Z^{(n)}\right)$ denotes the conditional entropy of the random variable W given Eve's receive sequence $Z^{(n)}$.

A rate-equivocation pair (R, R_e) is said to be achievable if there exists a sequence of $(2^{nR}, n)$ codes such that

$$\lim_{n \to \infty} P_e^{(n)} = 0 \quad \text{and} \quad R_e \leq \liminf_{n \to \infty} R_e^{(n)}.$$

The term perfect secrecy is used for the case $R = R_e$. The secrecy capacity C_S is the largest rate that is achievable with perfect secrecy. It is given by

$$C_S = \max_{p_{U,X}} \left(I\left(U;Y\right) - I\left(U;Z\right) \right),$$

[1] In Bloch and Barros (2011, Definition 3.1), the encoding function is defined as a function of the message and the realization of a local source of randomness. Alternatively, the encoder is introduced as a stochastic encoder that maps each message to a codeword according to a certain conditional probability function.

where $I(U;Y)$ denotes the mutual information between the random variables U and Y, and the auxiliary variable U satisfies the Markov chain relationship $U - X - (Y,Z)$. Note that the secrecy capacity of the wiretap channel depends on the probabilities $p_{Y,Z|X}$ only through the marginal probabilities $p_{Y|X}$ and $p_{Z|X}$, see (Bloch and Barros, 2011, Lemma 3.4). For a detailed explanation of the achievability proof and the proof of the converse, it is referred to (Liang et al., 2008a, Section 2.3 and 2.4).

⟨**1.7**⟩ **Secrecy Capacity (Degraded Wiretap Channel).** For the degraded wiretap channel with finite alphabets in ⟨1.4⟩, the secrecy capacity is given by[2]

$$C_S = \max_{p_X} \left(I(X;Y) - I(X;Z) \right).$$

⟨**1.8**⟩ **Secrecy Capacity (Gaussian Wiretap Channel).** The secrecy capacity of the Gaussian wiretap channel in ⟨1.5⟩ was derived by Leung-Yan-Cheong and Hellman (1978). It is given by

$$C_S = \max_{p_X} \left[I(X;Y) - I(X;Z) \right]^+,$$

where p_X is a probability density function that satisfies $\mathbb{E}\left(X^2\right) \leq P$, which yields

$$C_S = \left[\frac{1}{2} \log_2 \left(1 + \frac{P}{\sigma^2} \right) - \frac{1}{2} \log_2 \left(1 + \frac{P}{\vartheta^2} \right) \right]^+.$$

Thus, the secrecy capacity of the Gaussian wiretap channel corresponds to the difference between the capacity of the channel from Alice to Bob and the capacity of the channel from Alice to Eve if this difference is not negative. This result can be extended to the complex Gaussian wiretap channel with known additional attenuation coefficients h and g with $h, g \in \mathbb{C}$, where the noise is circularly-symmetric complex Gaussian distributed, i.e., $\xi \sim \mathcal{CN}(0, \sigma^2)$ and $\zeta \sim \mathcal{CN}(0, \vartheta^2)$. In this case, the secrecy capacity is given by

$$C_S = \left[\log_2 \left(1 + \frac{|h|^2 P}{\sigma^2} \right) - \log_2 \left(1 + \frac{|g|^2 P}{\vartheta^2} \right) \right]^+,$$

see (Bloch and Barros, 2011, Remark 5.1).

[2] For this channel, which is characterized by the Markov chain $X - Y - Z$, there also exists the formulation that the channel between the transmitter and the eavesdropper is physically degraded with respect to the main or receiver channel. In the literature, the condition above was relaxed by additionally introducing wiretap channels, where the channel between the transmitter and the eavesdropper is stochastically degraded with respect to the main channel or noisier or less capable than the main channel. For all these models, it was shown that the corresponding secrecy capacity is represented by the expression given above, see for instance (Bloch and Barros, 2011, Proposition 3.6 and Corollary 3.5).

⟨**1.9**⟩ **Secrecy Rate.** For the complex Gaussian wiretap channel in ⟨1.5⟩ and its extensions that we study in the next chapters, we introduce the secrecy rate R_S as

$$R_S := \left[\max_{p_X} I(X;Y) - \max_{p_X} I(X;Z) \right]^+ \leq C_S,$$

where p_X is the probability density function of the random variable (or the random vector) X whose second order moment is fixed to a certain transmit strategy, i.e., simply a transmit power in the basic scenario or a transmit covariance matrix in the multi-antenna scenario. Thus, we obtain an achievable secrecy rate expression that can be further optimized over the set of feasible transmit strategies.

1.4 Key Generation with the Wiretap Channel

In this section, we consider the problem of secret-key agreement, which was first introduced by Maurer (1990). We focus on the scenario that is shown in Figure 1.5. Alice and Bob use the wiretap channel together with an additional public channel in order to establish a common key that should be kept perfectly secret from Eve. Afterwards, Alice can ensure the secrecy of her private message for Bob by encryption with this previously generated key. The encrypted message can be transmitted over the channel from Alice to Bob, where Alice has only to guarantee the reliability of the transmission. Eve listens to the communication over both the wiretap and the public channel and tries to extract information about the key, which would allow her to get some information about the private message.

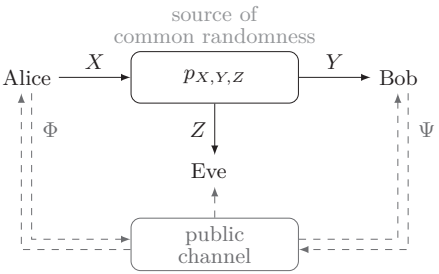


Figure 1.4: Source-type model for key generation.

Basically, there exist two different models for analyzing the secret-key problem. One is the so-called source-type model, the other is the so-called channel-type model. In this thesis, we focus on the channel-type model, but we also have a short look at the source-type model for the sake of completeness.

⟨**1.10**⟩ **Source-Type Model.** The source-type model, which is depicted in Figure 1.4, was investigated by Maurer (1993), Ahlswede and Csiszár (1993). In this model, Alice and Bob observe correlated sequences $X^{(n)}$ and $Y^{(n)}$, respectively, which are generated by a discrete memoryless source. Additionally, they can exchange messages over a noiseless public channel of unlimited capacity in order to agree on a common key that they want to keep perfectly secret from Eve. We refer to Ahlswede and Csiszár (1993) for a detailed description of the public communication strategy. Eve can perfectly overhear all messages that are transmitted over the public channel. It depends on the further details of this model in the literature, whether Eve is also able to observe a correlated sequence $Z^{(n)}$ of the discrete memoryless source[3]. Consequently, the corresponding performance measure, which is the secret-key capacity, is given by different expressions, see for instance (Liang et al., 2008a, Section 9.1). This model was extended to the Gaussian source-type model for secret-key agreement by Bloch and Barros (2011, Section 5.1.3), where Alice, Bob, and Eve observe correlated sequences that are generated by a memoryless source whose components are jointly Gaussian distributed.

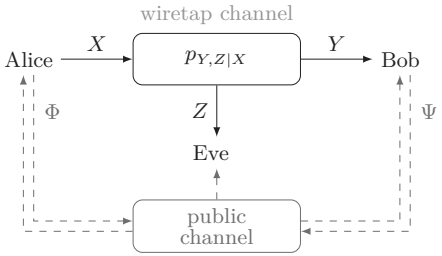


Figure 1.5: Channel-type model for key generation.

⟨**1.11**⟩ **Channel-Type Model.** The channel-type model for secret-key agreement, which is shown in Figure 1.5, was introduced by Ahlswede and Csiszár (1993). This model comprises a wiretap channel, which can be used for a transmission from Alice to Bob, and an additional public channel, which can be used for the exchange of public messages between Alice and Bob and vice versa. As originally introduced, we describe this model for a wiretap channel with finite alphabets. Altogether, the channels are used in k consecutive time slots, where the wiretap channel is used for transmission in exactly n (not necessarily consecutive) time instants and messages are exchanged over the public channel at the remaining $k - n$ time instants. Alice generates a sequence $X^{(n)}$, which she transmits in n selected channel uses over the wiretap channel in ⟨1.3⟩. This channel is characterized by its conditional probability mass function $p_{Y,Z|X}$. Bob and Eve observe the sequences

[3] Accordingly, Ahlswede and Csiszár (1993) as well as Liang et al. (2008a, Section 9.1) differentiate between Model S, where the eavesdropper has no access to information from the discrete memoryless source, and Model SW, where Eve can also observe a sequence from the source.

$Y^{(n)}$ and $Z^{(n)}$, respectively[4]. For the initial randomization of the public communication, there are two independent random variables V_{A} and V_{B}, which can be seen as individual sources of local randomness and only be accessed by Alice and Bob, respectively. The message that Alice transmits over the public channel at time i with $i \in \{1, 2, \ldots, k\}$ is denoted by Φ_i. This public communication is called forward transmission. Bob's messages over the public channel, which are denoted by Ψ_i with $i \in \{1, 2, \ldots, k\}$, are referred to as backward transmission. The messages for the wiretap as well as the public channel are generated causally based on all information that is available to Alice and Bob so far, i.e., Alice's channel input X_i at time i is a function of V_{A} and $\Psi^{(i-1)}$. Moreover, Alice message Φ_j for the public channel at time j is determined from V_{A} and $\Psi^{(j-1)}$, whereas Bob calculates his public message Ψ_j from V_{B}, $Y^{(j-1)}$, and $\Phi^{(j-1)}$. Finally, both users individually generate a key based on the received information, i.e., Alice generates a key κ_{A} from V_{A} and $\Psi^{(k)}$, whereas Bob calculates a key κ_{B} from V_{B}, $Y^{(n)}$, and $\Phi^{(k)}$. Both keys take values from the same finite set $\mathcal{M}$. We refer to Ahlswede and Csiszár (1993) for a detailed description of the public communication strategy for this model.

⟨**1.12**⟩ **Secret-Key Capacity.** For the channel-type model in ⟨1.11⟩, an achievable secret-key rate and the secret-key capacity are defined as in (Ahlswede and Csiszár, 1993) and (Liang et al., 2008a, Section 9.2). A secret-key rate R is achievable if for every $\epsilon > 0$ and sufficiently large n there exists a public communication strategy such that the keys κ_{A} and κ_{B} satisfy

$$\begin{aligned} \Pr(\kappa_{\mathrm{A}} \neq \kappa_{\mathrm{B}}) &< \epsilon, \\ \frac{1}{n} I\left(\kappa_{\mathrm{A}}; \Phi^{(k)}, \Psi^{(k)}, Z^{(n)}\right) &< \epsilon, \\ \frac{1}{n} H\left(\kappa_{\mathrm{A}}\right) &> R - \epsilon, \quad \text{and} \\ \frac{1}{n} \log_2 |\mathcal{M}| &< \frac{1}{n} H\left(\kappa_{\mathrm{A}}\right) + \epsilon. \end{aligned}$$

The conditions above can be interpreted as follows:

- Alice and Bob have generated a common key, i.e., both keys agree with high probability.
- The key is secret since the public communication has given away effectively no information about it.
- The rate of the key is measured by R.
- The generated key is approximately uniformly distributed over the set $\mathcal{M}$.

The largest achievable secret-key rate R is the secret-key capacity C_K. The so-called forward and backward secret-key capacities are the largest key rates possible if only a single forward or backward transmission is permitted. For the secret-key capacities, the

[4]Note that Ahlswede and Csiszár (1993) as well as Liang et al. (2008a, Section 9.2) differentiate between Model C, where the eavesdropper has no access to the communication channel between Alice and Bob, and Model CW, where Eve can also observe a sequence from the output of the wiretap channel.

following expressions exist in the literature, see for instance (Ahlswede and Csiszár, 1993, Theorem 2 and following Corollary):

- For the channel-type model with the general wiretap channel in ⟨1.3⟩, the forward secret-key capacity equals the secrecy capacity of the corresponding wiretap channel, which is given in ⟨1.6⟩.
- For the channel-type model with a degraded wiretap channel as in ⟨1.4⟩, which is characterized by the Markov chain $X - Y - Z$, both the forward secret-key capacity and the secret-key capacity equal the secrecy capacity of this wiretap channel, which is given in ⟨1.7⟩. It is achieved without using the public channel.
- If the wiretap channel satisfies $p_{Y,Z|X}(y,z|x) = p_{Y|X}(y|x)\, p_{Z|X}(z|x)$ for all $(x,y,z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$, which corresponds to the Markov chain $Y - X - Z$, the backward secret-key capacity and the secret-key capacity both equal

$$C_K = \max_{p_X} \left(I(X;Y) - I(Y;Z) \right),$$

  which generally is larger than the forward secret-key capacity.

The last result was extended by Wong et al. (2009) for the channel-type model with a Gaussian wiretap channel as in ⟨1.5⟩. The secret-key capacity, which equals the backward secret-key capacity, is given by

$$C_K = \max_{p_X} \left(I(X;Y) - I(Y;Z) \right),$$

where p_X is a probability density function that satisfies $\mathbb{E}\left(X^2\right) \leq P$.

⟨**1.13**⟩ **Secret-Key Rate.** Similar to the definition of the secrecy rate R_S in ⟨1.9⟩, we introduce the secret-key rate R_K for the channel-type model with the complex Gaussian wiretap channel in ⟨1.5⟩ and its extensions that we study in the next chapters as

$$R_K := \max_{p_X} \left(I(X;Y) - I(Y;Z) \right) \leq C_K,$$

where p_X is the probability density function of the random variable (or the random vector) X whose second order moment is fixed to a certain transmit strategy, i.e., simply a transmit power in the basic scenario or a transmit covariance matrix in the multi-antenna scenario. Thus, we obtain an achievable secret-key rate expression that can be further optimized over the set of feasible transmit strategies.

⟨**1.14**⟩ **Comparison of Secrecy and Secret-Key Rates.** If we intend to have a reasonably fair comparison between both approaches we introduced in Section 1.2, we have to take their different objectives into account. In the one case, Alice reliably transmits the data to Bob with rate R_S and simultaneously keeps it secret from Eve. In the other case, Alice and Bob generate a common key with rate R_K, which is kept secret from Eve, but they have not transmitted any data so far. Thus, it is necessary to incorporate the

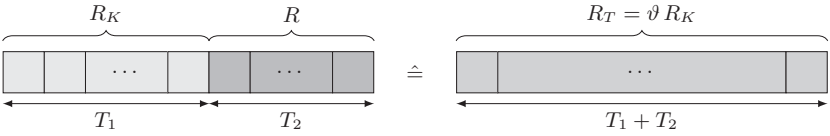


Figure 1.6: Time-division approach for key generation and data transmission.

subsequent data transmission for this case in order to enable a fair comparison between both approaches.

As soon as Alice and Bob agreed on a common and secret key of a certain length, they can use this key to encrypt information of the same length. Afterwards, this secured information can be transmitted over the channel with an achievable transmission rate without considering any further secrecy constraints. This time-division approach is illustrated in Figure 1.6. The first period is the key generation phase, which comprises T_1 channel uses. The second period is the data transmission phase, which lasts T_2 channel uses. In the first phase, we can generate key bits with rate R_K. In the second phase, the encrypted information can be transmitted with rate R, which can be larger than R_K since no secrecy constraints have to be regarded in this phase. The number of bits that are generated in the first phase and transmitted in the second phase are $T_1 R_K$ and $T_2 R$, respectively. Perfect secrecy can only be achieved if we have at least the same number of key bits as data bits. Thus, we set $T_1 R_K = T_2 R$. For the comparison with the secrecy rate R_S, we propose to calculate an average rate over both phases, which altogether comprise $T_1 + T_2$ time slots. Thus, we obtain

$$R_T = \frac{T_1 R_K}{T_1 + T_2} = \vartheta\, R_K,$$

where the factor ϑ is determined by

$$\vartheta = \frac{T_1}{T_1 + T_2} = \frac{R}{R + R_K}.$$

Note that this new rate expression indeed considers the power that is used by Alice for the transmission in the key generation phase and in the subsequent data transmission phase, but not the power that is additionally needed for the key agreement over the public channel and the encryption and decryption of the information at the transmitter and receiver, respectively.

Part II

Resource Allocation for Physical-Layer Security

2 Secrecy Rate Optimization

In the previous chapter, we have already introduced the main idea of physical-layer security that we want to consider in the following: Two users want to communicate in the presence of an eavesdropper who listens and tries to decode the message. The privacy of the communication should be ensured only by means of the physical layer, i.e., by appropriate coding and resource allocation. In this chapter, we will present the results on the achievable secrecy rates for various wireless systems. In the first section, we will introduce our basic model: the wiretap channel with attenuated Gaussian channels. We present an expression for the secrecy rate R_S and study its properties from a mathematical point of view. In the following sections of this chapter, we extend this model to multi-carrier and multi-antenna scenarios. We present results for the achievable secrecy rates or the secrecy capacities and provide power allocation strategies for the secrecy rate maximization. We focus on single-user scenarios, but we also give some results for the multi-user case.

⟨**2.1**⟩ **Publication Note.** A state-of-the-art overview of the results on single- and two-user secrecy rate maximization for multi-carrier and multi-antenna systems has already been published in (Jorswieck et al., 2010).

2.1 Basic Scenario

In our basic scenario, which is illustrated in Figure 2.1, Alice is the transmitter, who wants to ensure the privacy of a message that she sends to the legitimated receiver Bob, while the eavesdropper Eve listens and tries to decode this message.

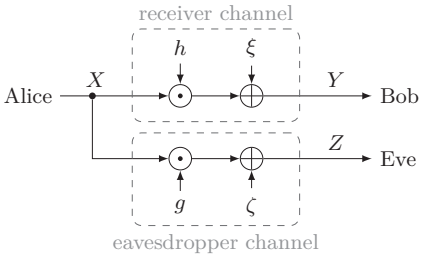


Figure 2.1: Wiretap channel with attenuated Gaussian channels, a transmitter (Alice), a receiver (Bob), and an eavesdropper (Eve).

⟨**2.2**⟩ **System Model.** We consider the complex Gaussian wiretap channel with additional attenuations of the transmit signal. This channel is used n time slots for the transmission of a codeword from Alice to Bob. For each channel use, the system model is described by

$$\begin{aligned} Y &= hX + \xi \quad \text{and} \\ Z &= gX + \zeta. \end{aligned}$$

We can skip the time index and use the generic variables X, Y, Z, ξ, and ζ since we have defined the wiretap channel in ⟨1.3⟩ as memoryless and stationary. In this model, X is a random variable representing Alice's transmit signal, Y and Z are random variables for Bob's and Eve's receive signal, respectively, h and g are complex-valued channel coefficients that model the signal attenuation for the channels from Alice to Bob and from Alice to Eve, respectively, and ξ and ζ are random variables representing the noise. We make the following assumptions:

- The complex-valued channel coefficients h and g satisfy $|h| \neq 0$ and $|g| \neq 0$, i.e., both channels allow a transmission from Alice to the corresponding receiver.
- The random variables X, ξ, and ζ are statistically independent.
- The noise variables ξ and ζ are circularly-symmetric complex Gaussian distributed with zero mean and variance σ^2, i.e., $\xi, \zeta \sim \mathcal{CN}(0, \sigma^2)$ with $\sigma^2 > 0$.
- There is a power constraint P with $P > 0$ at the transmitter, i.e., $\mathbb{E}\left(X^2\right) \leq P$.
- Bob and Eve perfectly know their individual channel coefficients. Furthermore, Eve is allowed to additionally know Bob's channel coefficient.
- Alice has full channel state information (CSI), i.e., she knows both channel coefficients perfectly. This assumption, which is essential for our further discussion, seems to be unrealistic in a wiretap setting where Eve only listens. But, it is justified if we think for instance at a cellular environment with a base station (Alice) and two users (Bob and Eve). Then Alice will know the channel coefficients if Bob and Eve use up- and downlink transmission and if we assume channel reciprocity in a time-division duplex system.

⟨**2.3**⟩ **Notation.** For both channels, we define the so-called channel gains $a := |h|^2$ and $b := |g|^2$, which satisfy $a > 0$ and $b > 0$. Moreover, we introduce the inverse noise variance $\rho := \frac{1}{\sigma^2}$ with $\rho > 0$ for high- and low-SNR discussions.

⟨**2.4**⟩ **Secrecy Rate.** For this model, the secrecy rate R_S, which we interpret as a function of the channel gains a and b and the transmit power q with $q \geq 0$, can be evaluated according to ⟨1.9⟩, which yields

$$\begin{aligned} R_S(a,b,q) &= \left[\varphi(a,b,q)\right]^+ \quad \text{with} \\ \varphi(a,b,q) &:= \log_2\left(1 + \frac{aq}{\sigma^2}\right) - \log_2\left(1 + \frac{bq}{\sigma^2}\right) = \log_2\left(\frac{\sigma^2 + aq}{\sigma^2 + bq}\right), \end{aligned}$$

where the random variable X needs to be circularly-symmetric complex Gaussian distributed with zero mean and variance q, i.e., $X \sim \mathcal{CN}(0, q)$, in order to achieve the channel capacities in ⟨1.9⟩ for a given transmit power q.

⟨**2.5**⟩ **Properties (Positivity).** Obviously, the function φ and thus the secrecy rate R_S are positive if and only if $a > b$ and $q > 0$, i.e., it depends on the relation between the channel states whether the transmitter can achieve a positive secrecy rate or not.

In the following, we consequently focus on the case where the channel from Alice to Bob has a higher gain than the channel from Alice to Eve. Then the evaluation of the first and second derivatives of φ and R_S provides the properties below.

⟨**2.6**⟩ **Calculations.** For the first derivatives, we have

$$\begin{aligned}
\frac{\partial}{\partial a}\varphi(a,b,q) &= \frac{1}{\ln 2}\left(\frac{q}{\sigma^2+aq}\right) && \text{with } \frac{\partial}{\partial a}\varphi(a,b,q) > 0 \text{ if } q > 0,\\
\frac{\partial}{\partial b}\varphi(a,b,q) &= -\frac{1}{\ln 2}\left(\frac{q}{\sigma^2+bq}\right) && \text{with } \frac{\partial}{\partial b}\varphi(a,b,q) < 0 \text{ if } q > 0,\\
\frac{\partial}{\partial q}\varphi(a,b,q) &= \frac{1}{\ln 2}\left(\frac{\sigma^2(a-b)}{(\sigma^2+aq)(\sigma^2+bq)}\right) && \text{with } \frac{\partial}{\partial q}\varphi(a,b,q) > 0 \text{ if } a > b.
\end{aligned}$$

For the second derivatives, we have

$$\begin{aligned}
\frac{\partial^2}{\partial a^2}\varphi(a,b,q) &= -\frac{1}{\ln 2}\left(\frac{q^2}{(\sigma^2+aq)^2}\right) && \text{with } \frac{\partial^2}{\partial a^2}\varphi(a,b,q) < 0 \text{ if } q > 0,\\
\frac{\partial^2}{\partial b^2}\varphi(a,b,q) &= \frac{1}{\ln 2}\left(\frac{q^2}{(\sigma^2+bq)^2}\right) && \text{with } \frac{\partial^2}{\partial b^2}\varphi(a,b,q) > 0 \text{ if } q > 0,\\
\frac{\partial^2}{\partial q^2}\varphi(a,b,q) &= -\frac{1}{\ln 2}\left(\frac{\sigma^2(a-b)\left(\sigma^2(a+b)+2abq\right)}{(\sigma^2+aq)^2(\sigma^2+bq)^2}\right) && \text{with } \frac{\partial^2}{\partial q^2}\varphi(a,b,q) < 0 \text{ if } a > b.
\end{aligned}$$

⟨**2.7**⟩ **Properties (Monotonicity).** For $a > b$ and $q > 0$, the function φ and the secrecy rate R_S in ⟨2.4⟩ are identical and

a) strictly monotonically increasing in a for fixed b and q,
b) strictly monotonically decreasing in b for fixed a and q, and
c) strictly monotonically increasing in q for fixed a and b.

⟨**2.8**⟩ **Properties (Convexity).** For $a > b$ and $q > 0$, the function φ and the secrecy rate R_S in ⟨2.4⟩ are identical and

a) a strictly concave function of a for fixed b and q,
b) a strictly convex function of b for fixed a and q, and
c) a strictly concave function of q for fixed a and b.

⟨**2.9**⟩ **Remark.** If we analyze the properties of R_S without the restriction $a > b$, we have to consider the influence of the outer $[\cdot]^+$ function, see ⟨A.2⟩. In this case, the monotonicity properties in ⟨2.7⟩ and the convexity in b in ⟨2.8⟩ can be preserved if the corresponding statements are relaxed to a formulation without "strictly", whereas the concavity in q and a is no longer given.

Now, we formulate the maximization problem for the secrecy rate in ⟨2.4⟩ and the system model specified in ⟨2.2⟩.

⟨**2.10**⟩ **Problem Formulation (Secrecy Rate Maximization).** For given channel gains a and b, the secrecy rate R_S in ⟨2.4⟩ should be maximized under a transmit power constraint $q \leq P$, i.e.,

$$\max_{q \in \mathcal{Q}} R_S(a, b, q) = \max_{q \in \mathcal{Q}} [\varphi(a, b, q)]^+ = \left[\max_{q \in \mathcal{Q}} \varphi(a, b, q) \right]^+ ,$$

where

$$\mathcal{Q} := \{q \in \mathbb{R} \,|\, q \geq 0 \text{ and } q \leq P\}$$

is the set of all feasible transmit powers. For the formulation of the problem above, we can exploit the interchangeability of the $[\cdot]^+$ function and the maximization over the set $\mathcal{Q}$, see ⟨A.3⟩.

⟨**2.11**⟩ **Remark.** With the optimization problem above, we want to simultaneously introduce a standard formulation for optimization problems, which we will use throughout this thesis. In order to specify the constraints on the problem, we always define a constraint set for each optimization variable, which can be a scalar, a vector or a matrix in the next chapters. Thereby, we differentiate between constraints on single components, e.g., non-negativity requirements, and constraints concerning all components of the optimization variable as sum or trace constraints. Due to the simplicity of the problem in the basic scenario, the resulting constraint set in ⟨2.10⟩ obviously specifies a simple interval that is feasible for the transmit power q.

⟨**2.12**⟩ **Properties (Convexity of the Problem).** The constraint set, which is a closed interval on $\mathbb{R}$, is convex. The only interesting case is $a > b$, where R_S is positive for any $q > 0$. In that case (with fixed a and b), the objective function is a concave function of q on the set $\mathcal{Q}$, see ⟨2.8⟩. Hence, we have a convex problem.

⟨**2.13**⟩ **Optimal Strategy (Power Allocation).** If the channel between Alice and Bob is better than the channel between Alice and Eve, i.e., $a > b$, the secrecy rate R_S is maximized by using full power at the transmitter, i.e., $q = P$. This directly follows from the corresponding monotonicity property in ⟨2.7⟩. Otherwise, the secrecy rate R_S is zero independently of the chosen power allocation at the transmitter, see ⟨2.5⟩. Then the transmitter consequently can choose the option not to transmit its message, i.e., $q = 0$.

⟨**2.14**⟩ **Secrecy Capacity.** From ⟨1.8⟩, we know that the secrecy capacity of the basic model in ⟨2.2⟩ is given by

$$C_S = \left[\log_2 \left(1 + \frac{aP}{\sigma^2} \right) - \log_2 \left(1 + \frac{bP}{\sigma^2} \right) \right]^+ .$$

In order to study the behavior of the secrecy rate for high and low SNR, we now interpret R_S in ⟨2.4⟩ as a function of the noise variance σ^2 (or its inverse ρ) for given channel gains a and b and a fixed value of P and look at the corresponding limits (if they exist) and some related performance measures.

⟨**2.15**⟩ **High-SNR Performance.** In the high-SNR regime, the secrecy rate R_S approaches the following limit:

$$\lim_{\sigma^2 \to 0} R_S(a, b, q) = \left[\log_2 \left(\frac{a}{b} \right) \right]^+ ,$$

which only depends on the quotient of the two channel gains, i.e., if the system is operating in the high-SNR regime, we can only have a vanishing gain in the secrecy rate when increasing the transmit power. This is in contrast to the scenario without secrecy constraints, where the achievable rate grows with the transmit power without converging to a limit.

⟨**2.16**⟩ **Low-SNR Performance.** In the low-SNR regime, the secrecy rate R_S clearly approaches the following limit:

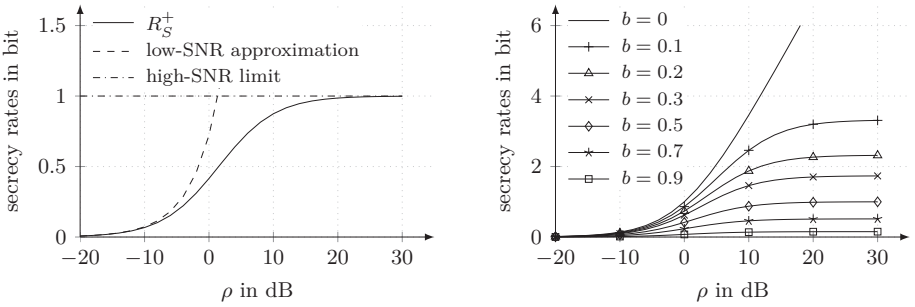
$$\lim_{\rho \to 0} R_S(a, b, q) = 0.$$

We can gain a little bit more insight if we consider the linear Taylor series representation of R_S at the point $\rho = 0$, which is

$$T_{R_S}(\rho; 0) = \frac{1}{\ln 2} (a - b)\, q\, \rho.$$

If the system is operating in the low-SNR regime, the increase of the secrecy rate is determined by the difference of the two channel gains. Without secrecy constraints, the factor for the rate increase would be determined by a.

⟨**2.17**⟩ **Illustration.** In order to illustrate the results of this section, we choose $a = 1$ and $P = 1$. For fixed P, a variation of the inverse noise variance ρ directly corresponds to a variation of the SNR. Figure 2.2 shows the maximized secrecy rate of the basic scenario, which is obtained using full power and denoted by R_S^+, as a function of the SNR. It increases with ρ since all other parameters are fixed. In (a), we see the maximized secrecy rate R_S^+ for $b = 0.5$ together with its low-SNR approximation according to ⟨2.16⟩ and its high-SNR limit according to ⟨2.15⟩. As expected, the maximized secrecy rate R_S^+ converges to 1 bit for high SNR, which corresponds to the calculated limit with



(a) low- and high-SNR behavior for $b = 0.5$

(b) influence of eavesdropper channel

Figure 2.2: The maximized secrecy rate R_S^+ for various eavesdropper channel gains and its low-SNR approximation and high-SNR limit.

$a = 1$ and $b = 0.5$. In (b), the influence of the eavesdropper channel gain is illustrated. The case $b = 0$ corresponds to a scenario without eavesdropper or equivalently to a transmission without secrecy constraints. The resulting curve represents an upper bound on all achievable secrecy rates. For the transmission without secrecy constraints, we have no limit for high SNR. In all other cases, the maximized secrecy rates converge to their high-SNR limits according to ⟨2.15⟩. We clearly observe that a better eavesdropper channel reduces the achievable secrecy rate. This influence of the eavesdropper channel gain can be noticed over the complete SNR range. However, it is more significant for high SNR, where the differences between the curves converge to constant gaps, which are characterized by the corresponding high-SNR limits.

⟨**2.18**⟩ **Remark (Fading).** In the model above, the channel coefficients h and g are constants. Depending on the relation of the channel gains, Alice is able to transmit the private message to Bob or not. Consequently, we have a constant secrecy rate that is either positive or zero all the time. We can extend this static model and define a system with quasi-static block flat fading. Then the channel coefficients h and g become random variables, which we call channel states. The value of such a channel state remains constant during the transmission of a complete codeword. Afterwards, the next channel state takes on a different value for the transmission time of the next codeword. All channel states of a channel are independent and identically distributed. Generally, the states of the channels from Alice to Bob and from Alice to Eve can be modeled as statistically dependent. Now we have a time-varying model, where the situation changes from block to block. For each pair of channel states known by Alice, the secrecy rate can be calculated according to ⟨2.4⟩. Then it is called instantaneous secrecy rate. Based on the statistics assumed for the channel coefficients and depending on Alice's knowledge about the eavesdropper channel, average or outage secrecy rates can be calculated (Bloch et al., 2008).

⟨**2.19**⟩ **Two-User Case.** In the single-user case, which we discussed so far, Alice has a private message for Bob, but no interest in a private communication with Eve. However, when Eve has a better channel than Bob, Alice cannot transmit her message to Bob, and the secrecy rate R_S is zero. If Alice additionally has a private message for Eve, she can decide depending on the channel conditions whether she communicates with Bob or with Eve. Then, Bob and Eve can play two different roles depending on Alice's decision: They are either the legitimated receiver of their own message or the potential eavesdropper of the other. Now Alice can always[5] choose the user with the better channel gain and transmit the corresponding private message with a positive secrecy rate, which yields a more efficient use of the available resources. This approach makes sense if we interpret the model as a quasi-static block flat fading system as described in ⟨2.18⟩, where the relation of the channel gains and thus the instantaneous secrecy rate change from block to block.

The system model in ⟨2.2⟩ can be extended to a multi-carrier or a multi-antenna system model, where Alice has more options than before. She can distribute the available power (under a sum power constraint) over a certain number of carriers or antennas to maximize the secrecy rate for the transmission to Bob. In the next sections, we will present maximization problems for the secrecy rate in multi-carrier or multi-antenna scenarios together with the optimal power allocation strategies.

2.2 Multi-Carrier Scenario

We extend our basic model from the previous section to a multi-carrier scenario, where Alice wants to send her private message to Bob in a system with K parallel carriers. Again, this message should be kept secret from the eavesdropper Eve. We study the optimal resource allocation for the secrecy rate maximization under a sum power constraint over all carriers.

⟨**2.20**⟩ **System Model (Extension to Multi-Carrier Scenario).** In order to extend the wiretap channel with attenuated Gaussian channels to a multi-carrier system with K carriers, the system model in ⟨2.2⟩ is used K times in parallel. Then, all variables that were scalars before become row vectors of length K. Consequently, we have a transmit signal vector $X = (X_k)_{k=1}^K$ at Alice and the receive signal vectors $Y = (Y_k)_{k=1}^K$ and $Z = (Z_k)_{k=1}^K$ at Bob and Eve, respectively. The attenuated Gaussian channels are characterized by the channel coefficient vectors $h = (h_k)_{k=1}^K$ and $g = (g_k)_{k=1}^K$ together with the noise vectors $\xi = (\xi_k)_{k=1}^K$ and $\zeta = (\zeta_k)_{k=1}^K$ as shown in Figure 2.3.

[5] The only exception is the case where both channel gains are equal, i.e., $a = b$. But if we model both channel gains as outcomes of independent continous random variables as discussed in ⟨2.18⟩, this occurs with probability zero.

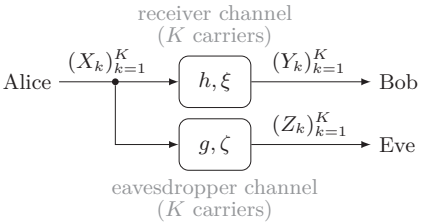


Figure 2.3: Wiretap channel for the multi-carrier scenario with K carriers.

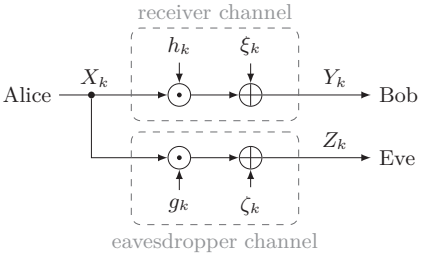


Figure 2.4: Wiretap channel with attenuated Gaussian channels.

For each carrier $k \in \{1, 2, \ldots, K\}$, the system model, which is shown in Figure 2.4, corresponds to the basic system model in ⟨2.2⟩. It can be described by

$$Y_k = h_k X_k + \xi_k \quad \text{and}$$
$$Z_k = g_k X_k + \zeta_k,$$

where the variables have the same meaning as before in ⟨2.2⟩. The additional index k refers to the corresponding variable on the k-th carrier. We directly transfer all relations and assumptions from the basic model in ⟨2.2⟩ to each carrier of the multi-carrier scenario. Additionally, it is required that the vectors X, ξ, and ζ are independent from each other. For each of these vectors, the components are independent and identically distributed. The power constraint becomes a constraint over all K carriers, i.e., $\mathbb{E}\left(\sum_{k=1}^K X_k^2\right) \leq P$.

⟨**2.21**⟩ **Notation.** We follow the conventions from our basic scenario and define the channel gains $a_k := |h_k|^2$ and $b_k := |g_k|^2$ for all $k \in \{1, 2, \ldots, K\}$. We introduce (row) vectors of length K for the collection of these channel gains, i.e., we have $a := (a_k)_{k=1}^K$ and $b := (b_k)_{k=1}^K$. In the same way, we define a power allocation vector $q := (q_k)_{k=1}^K$ for the transmit powers Alice uses on the K carriers.

⟨**2.22**⟩ **Secrecy Rate.** For this model, the secrecy rate R_S, which we understand as a function of the transmit power vector q and the channel gain vectors a and b, is the sum

over all secrecy rates per carrier and given by

$$R_S(a,b,q) = \sum_{k=1}^{K} [\varphi(a_k,b_k,q_k)]^+ \quad \text{with}$$
$$\varphi(a_k,b_k,q_k) := \log_2\left(1+\frac{a_k q_k}{\sigma^2}\right) - \log_2\left(1+\frac{b_k q_k}{\sigma^2}\right)$$

where $q_k \geq 0$ is the power that Alice allocates to carrier k in order to transmit her message to Bob. This directly follows from ⟨2.4⟩ if each carrier is studied independently.

⟨**2.23**⟩ **Properties (Positivity).** If we compare the channel gains on each carrier, we can generally assume that on some carriers the gain of the channel between Alice and Bob is greater than the gain of the channel between Alice and Eve, whereas on other carriers the situation is the other way around. From ⟨2.5⟩, it follows that we can only have a positive contribution to the secrecy rate R_S on those carriers where Bob has a better channel gain than Eve.

The properties below can be derived with the first and second derivatives we calculated for the secrecy rate of the basic scenario.

⟨**2.24**⟩ **Properties (Monotonicity).** With ⟨2.7⟩, we can provide some statements on the monotonicity of the function φ and the secrecy rate R_S in the components of the vectors a, b, and q under the assumption that all other variables are fixed. For all $k \in \{1,2,\ldots,K\}$ with $a_k > b_k$ and $q_k > 0$, the functions φ and R_S in ⟨2.22⟩ are

a) strictly monotonically increasing in a_k,
b) strictly monotonically decreasing in b_k, and
c) strictly monotonically increasing in q_k.

⟨**2.25**⟩ **Properties (Convexity).** The Hessian matrices of R_S with respect to a, b, and q are diagonal. For a and q, these matrices have only non-positive diagonal entries, see ⟨2.8⟩, i.e., they are negative semi-definite. Furthermore, we see that the Hessian matrix with respect to b has only non-negative diagonal entries, i.e., it is positive semi-definite. This allows us to formulate the convexity properties of R_S with respect to the vectors a, b, and q under the assumption that all other variables are fixed. The function R_S in ⟨2.22⟩ is

a) a concave function of a,
b) a convex function of b, and
c) a concave function of q.

⟨**2.26**⟩ **Problem Formulation (Secrecy Rate Maximization).** For given channel gain vectors a and b, the secrecy rate R_S in ⟨2.22⟩ should be maximized under a sum power constraint at the transmitter, i.e.,

$$\max_{q \in \mathcal{Q}} R_S(a, b, q) = \max_{q \in \mathcal{Q}} \sum_{k=1}^{K} \left[\varphi(a_k, b_k, q_k) \right]^+ ,$$

where

$$\mathcal{Q} := \left\{ q \in \mathbb{R}^{1 \times K} \,\middle|\, q_k \geq 0 \text{ and } \sum_{k=1}^{K} q_k \leq P \right\}$$

is the set of all feasible power allocation vectors.

⟨**2.27**⟩ **Properties (Convexity of the Problem).** The constraints describe a vector with individual lower bounds for the components and a sum constraint for all vector elements. This is a convex set. On this set, the objective function R_S is a concave function of q for fixed channel gain vectors a and b, see ⟨2.25⟩. Thus, the problem in ⟨2.26⟩ is convex.

The observation in ⟨2.23⟩ allows us to select the carriers that are relevant for the optimal transmit power allocation and thus to reduce the maximization problem.

⟨**2.28**⟩ **Optimal Strategy (Carrier Selection).** The optimal power allocation for the secrecy rate maximization uses zero power on all carriers where the gain of the channel from Alice to Bob is not greater than the gain of the channel from Alice to Eve, i.e.,

$$\forall\, k \in \{1, 2, \ldots, K \,|\, a_k \leq b_k\} : \; q_k = 0.$$

The remaining optimization problem is the maximization of the secrecy rate R_S by a power allocation strategy q that fulfills the sum power constraint in ⟨2.26⟩ and does not allocate power to carriers with $a_k \leq b_k$ for $k \in \{1, 2, \ldots, K\}$. The convexity of the optimization problem is clearly not influenced by this additional constraint. With the necessary Karush-Kuhn-Tucker (KKT) optimality conditions, which are also sufficient due to the convexity of the problem, we can derive the optimal power allocation for all carriers that are not switched off. We obtain an implicit solution, which is a type of waterfilling.

⟨**2.29**⟩ **Optimal Strategy (Power Allocation).** The optimal transmit strategy for the secrecy rate maximization problem in ⟨2.26⟩ fulfills ⟨2.28⟩ and uses the waterfilling solution

$$q_k(\mu) = \left[-\frac{c_k}{2} + \sqrt{\frac{d_k^2}{4} + \mu\, d_k} \right]^+$$

$$\text{with} \quad c_k := \sigma^2 \frac{a_k + b_k}{a_k b_k} \quad \text{and} \quad d_k := \sigma^2 \frac{a_k - b_k}{a_k b_k}$$

for the power allocation on all carriers with $a_k > b_k$ and $k \in \{1, 2, \ldots, K\}$. Due to the monotonicity in all components of q, see ⟨2.24⟩, the waterfilling parameter μ with $\mu \geq 0$ has to be chosen such that the power constraint is fulfilled with equality, i.e., $\sum_{k=1}^{K} q_k(\mu) = P$.

⟨**2.30**⟩ **Secrecy Capacity.** The secrecy capacity of the multi-carrier scenario in ⟨2.20⟩ with a sum power constraint over all carriers is obtained by the maximization of the sum of the secrecy rates of the individual channels, i.e.,

$$C_S = \max_{q \in \mathcal{Q}} \sum_{k=1}^{K} \left[\log_2 \left(1 + \frac{a_k q_k}{\sigma^2} \right) - \log_2 \left(1 + \frac{b_k q_k}{\sigma^2} \right) \right]^+ .$$

This was shown by Li et al. (2006), who also derived the corresponding optimal power allocation, which equals[6] the waterfilling solution in ⟨2.29⟩.

⟨**2.31**⟩ **Notation.** In order to simplify the notation of the next results, we introduce

$$\mathcal{K}_\mathrm{B} := \{k \in \{1, 2, \ldots, K\} \,|\, a_k > b_k\} \quad \text{and}$$
$$\mathcal{K} := \{k \in \{1, 2, \ldots, K\} \,|\, q_k > 0\} \subseteq \mathcal{K}_\mathrm{B},$$

which are both subsets of the set of carriers. $\mathcal{K}_\mathrm{B}$ is the set of all carriers that can be used for a transmission to Bob with a positive secrecy rate, whereas $\mathcal{K}$ is the set of carriers that are really used for the transmission to Bob.

In order to characterize the optimal power allocation for high and low SNR, we again interpret R_S in ⟨2.22⟩ as a function of the noise variance σ^2 (or its inverse ρ) for a fixed value of P.

⟨**2.32**⟩ **High-SNR Performance.** In the high-SNR regime, there exists a limit for the secrecy rate R_S, which is

$$\lim_{\sigma^2 \to 0} R_S(a, b, q) = \sum_{k \in \mathcal{K}} \log_2 \left(\frac{a_k}{b_k} \right).$$

This limit is determined by the quotients of the channel gains of the carriers that are used. Although it seems that the high-SNR limit is independent from the power allocation, it is influenced by the carrier selection, i.e., for the value of the limit it is relevant which subset of the carriers is used. Thus, the optimal power allocation that maximizes this secrecy rate limit in the high-SNR regime uses all possible carriers, i.e., it assigns $q_k > 0$ to all carriers $k \in \mathcal{K}_\mathrm{B}$.

[6] We were not aware of this publication when we studied the secrecy rate maximization in the multi-carrier scenario and independently obtained the solution in ⟨2.29⟩ for the optimal power allocation, see also comments in ⟨2.38⟩ and ⟨2.39⟩.

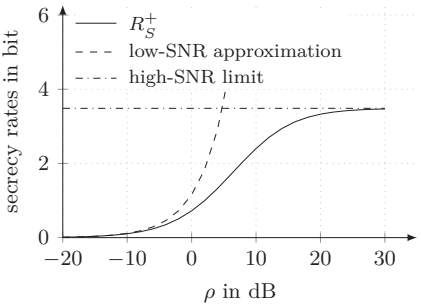
⟨**2.33**⟩ **Low-SNR Performance.** In the low-SNR regime, the limit of the secrecy rate R_S clearly is

$$\lim_{\rho \to 0} R_S(a, b, q) = 0.$$

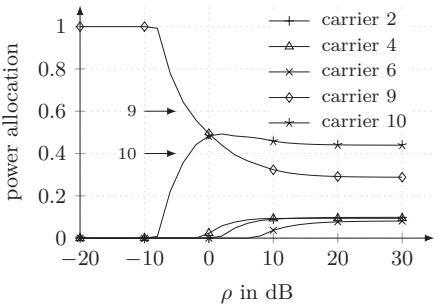
We calculate the linear Taylor series representation of R_S at the point $\rho = 0$ and obtain

$$T_{R_S}(\rho; 0) = \frac{1}{\ln 2} \sum_{k \in \mathcal{K}} (a_k - b_k)\, q_k\, \rho.$$

The increase of the secrecy rate in the low-SNR regime is determined by the differences of the channel gains of the carriers that are used. Thus, in the low-SNR regime, it is optimal to allocate full power to the carrier with the largest difference, i.e., $q_\ell = P$ with $\ell = \arg\max_{k \in \mathcal{K}_B} (a_k - b_k)$.



(a) maximized secrecy rate with high-SNR limit and low-SNR approximation



(b) optimal power allocation

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
0.4	1.8	0.6	2.2	1.1	1.2	1.6	0.1	1.4	0.9
b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}
0.5	1.5	1.1	1.8	1.5	1.1	2.0	1.7	0.6	0.3

Figure 2.5: The maximized secrecy rate R_S^+ and the corresponding power allocation.

⟨**2.34**⟩ **Illustration.** With Figure 2.5, we illustrate the results we obtained so far for the secrecy rate maximization in the multi-carrier scenario. We choose $K = 10$ carriers and $P = 1$ for the sum power constraint over these carriers. The gains for the channels from Alice to Bob and Eve are given in the table below the illustrations. We see that we have five carriers, which are the carriers 2, 4, 6, 9, and 10, where Bob has a better channel than Eve. According to ⟨2.23⟩, only these carriers will be used by Alice for the transmission to Bob. In (a), we see the maximized secrecy rate R_S^+ as increasing function of the SNR with its low-SNR approximation according to ⟨2.33⟩ and its high-SNR limit

according to ⟨2.32⟩. In (b), the corresponding optimal power allocation is shown over the SNR range. For low SNR, Alice allocates the complete power P to carrier 9, which is the carrier with the largest difference between the channel gains. This corresponds to the result of the low-SNR analysis in ⟨2.33⟩. With increasing SNR, Alice distributes the available power P to more and more carriers. Thereby, she prefers to activate carriers with a larger difference between the channel gains. For high SNR, she uses all possible carriers for the transmission to Bob. In this regime, the power allocation to the carriers depends on the quotient of the channel gains. Alice allocates more power to carriers with a larger quotient. We have already identified this high-SNR behavior in ⟨2.32⟩.

⟨**2.35**⟩ **Two-User Case.** Now we consider the two-user case in the multi-carrier scenario. Again, Alice wants to transmit private messages to Bob and to Eve, who are both interested in receiving their own message and eavesdropping the other. In addition to ⟨2.31⟩, we define

$$\mathcal{K}_{\mathrm{E}} := \{k \in \{1, 2, \ldots, K\} \,|\, b_k > a_k\}$$

as the set of carriers that Alice can use to transmit Eve's message with a positive secrecy rate. Thus, we have two disjoint sets of carriers for the transmission to Bob and Eve. In the two-user case, we can calculate the two secrecy rates

$$R_{S,\mathrm{B}}(a,b,q) := \sum_{k\in\mathcal{K}_{\mathrm{B}}} \log_2\left(1+\frac{a_k q_k}{\sigma^2}\right) - \log_2\left(1+\frac{b_k q_k}{\sigma^2}\right) \quad \text{and}$$
$$R_{S,\mathrm{E}}(a,b,q) := \sum_{k\in\mathcal{K}_{\mathrm{E}}} \log_2\left(1+\frac{b_k q_k}{\sigma^2}\right) - \log_2\left(1+\frac{a_k q_k}{\sigma^2}\right),$$

where $R_{S,\mathrm{B}}$ is the secrecy rate in ⟨2.22⟩, which is achievable for the transmission to Bob, and $R_{S,\mathrm{E}}$ is the secrecy rate that Alice can achieve for her message to Eve. In (Jorswieck and Wolf, 2008, Theorem 2), it was shown that the sum secrecy rate is maximized if a frequency-division approach is used, i.e., the transmitter exclusively supports the user with the maximum channel gain on each carrier. The sum secrecy rate that is achievable for both messages is then given by

$$\begin{aligned} R_S^{\Sigma}(a,b,q) &:= R_{S,\mathrm{B}}(a,b,q) + R_{S,\mathrm{E}}(a,b,q) \\ &= \sum_{k=1}^{K} \log_2\left(1+\frac{\max\{a_k,b_k\}\,q_k}{\sigma^2}\right) - \log_2\left(1+\frac{\min\{a_k,b_k\}\,q_k}{\sigma^2}\right). \end{aligned}$$

The sum secrecy rate maximization problem under a transmit power constraint can be formulated analogously to problem ⟨2.26⟩. Thus, the optimal power allocation strategy can be derived from the waterfilling solution in ⟨2.29⟩ by inserting $\max\{a_k, b_k\}$ instead of a_k and $\min\{a_k, b_k\}$ instead of b_k.

A generalization of this problem is the weighted sum secrecy rate maximization problem, which was presented by Jorswieck and Gerbracht (2009):

$$\max_{q \in \mathcal{Q}} R_S^{\kappa}(a, b, q, \kappa)$$

with $\mathcal{Q}$ as defined in ⟨2.26⟩, the weighted sum secrecy rate

$$R_S^{\kappa}(a, b, q, \kappa) := \kappa \, R_{S,\mathrm{B}}(a, b, q) + (1 - \kappa) \, R_{S,\mathrm{E}}(a, b, q),$$

and $\kappa \in [0, 1]$. The factor κ describes not only how the transmitter weights the rates of the two users, but it also allows us to calculate the secrecy rate region that is achievable for two users. The solution of this problem can be obtained with the KKT conditions as described above for the single-user case. This yields a waterfilling solution over all carriers $k \in \mathcal{K}_{\mathrm{B}} \cup \mathcal{K}_{\mathrm{E}}$ that generalizes ⟨2.29⟩ to

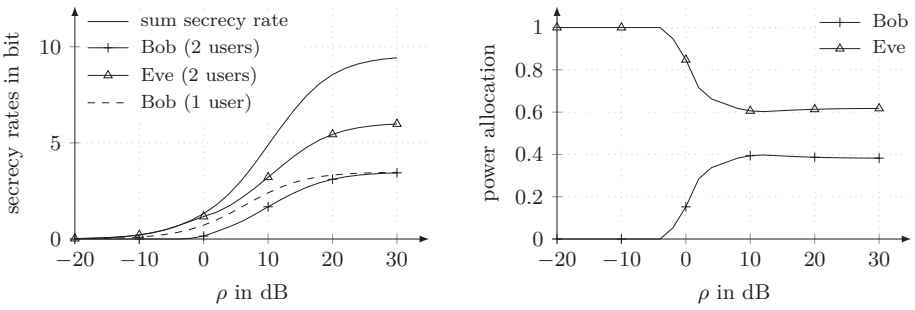
$$q_k(\mu) = \left[-\frac{c_k}{2} + \sqrt{\frac{d_k^2}{4} + \mu_k \, d_k} \right]^+$$

$$\text{with} \quad c_k := \sigma^2 \, \frac{a_k + b_k}{a_k b_k}, \quad d_k := \sigma^2 \, \frac{|a_k - b_k|}{a_k b_k}, \quad \text{and}$$

$$\mu_k := \begin{cases} \kappa \, \mu & \text{for } k \in \mathcal{K}_{\mathrm{B}} \\ (1 - \kappa) \, \mu & \text{for } k \in \mathcal{K}_{\mathrm{E}} \end{cases}.$$

Due to the monotonicity of the objective function, the waterfilling parameter μ has to be chosen such that the power constraint is fulfilled with equality, i.e., $\sum_{k=1}^{K} q_k(\mu) = P$. Note that the formulation of the waterfilling solution above is more general than the original solution presented by Jorswieck and Gerbracht (2009).

⟨2.36⟩ Illustration (Two-User Case). For the illustration of the two-user case in Figure 2.6, we continue the example we discussed in ⟨2.34⟩. In contrast to the single-user case, Alice can now use all $K = 10$ carriers for data transmission. As before, she can allocate power to the carriers 2, 4, 6, 9, and 10 for the transmission to Bob. Additionally, she can use the remaining five carriers for a parallel transmission to Eve. The maximized secrecy rates that are achievable for Bob and Eve in the two-user case are shown in (a). Furthermore, the resulting sum secrecy rate is plotted. For comparison, we also added the maximized secrecy rate for Bob from the single-user case. If we look at the achievable secrecy rates from Alice's perspective, we see that the sum secrecy rate for the transmission in the two-user case is considerably larger than the maximized secrecy rate from the single-user scenario, although Alice has to respect the same sum power constraint in both cases. Especially for high SNR, the gap between the rates becomes significant. We know from ⟨2.32⟩ that all carriers are used in this regime. Thus, the resulting high-SNR limit, which is calculated from the gain quotients of all ten carriers, is larger than before, where only five carriers could be used. From Bob's point of view, the additional transmission to



(a) maximized (sum) secrecy rates

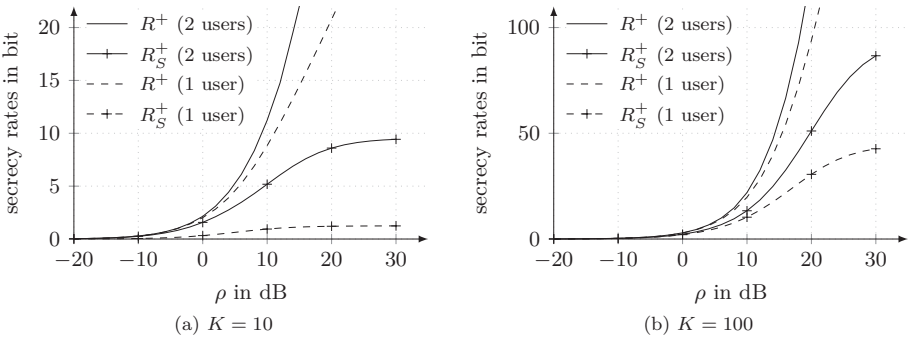
(b) user power allocation

Figure 2.6: The maximized secrecy rates and the corresponding user power allocation for the two-user case.

Eve is disadvantageous. Since the available power at the transmitter is shared between the two users, he can get only a fraction of the power he had before in the single-user case. The resulting power allocation per user is shown in (b). Consequently, Bob's secrecy rate is reduced compared to that from the single-user scenario. For low SNR, we know that Alice allocates only power to the carrier with the largest gain difference. This is carrier 8, which is reserved for the transmission to Eve. Thus, Bob's secrecy rate is zero in this regime. For high SNR, the influence of the power sharing diminishes and Bob's secrecy rate converges to the rate from the single-user case.

⟨**2.37**⟩ **Illustration (Cost of Secrecy).** In Figure 2.7, we compare the achievable rates with and without secrecy constraints for the single- and two-user case. The maximized secrecy rates are denoted by R_S^+, whereas the transmission rates without secrecy constraints are identified by R^+. The diagrams in (a) and (b) show the results that were obtained for a system with $K = 10$ and $K = 100$ independent carriers, respectively. For each carrier $k \in \{1, 2, \ldots, K\}$, the channel coefficients a_k and b_k were generated according to a circularly-symmetric complex Gaussian distribution with zero mean and variance two. We know that the transmission rate R^+ in a scenario without secrecy constraints is always an upper bound on the achievable secrecy rates. For high SNR, it grows to infinity, whereas all secrecy rates converge to a certain finite limit. The rate loss that results from the additional secrecy constraint can obviously be reduced in two ways. One possibility is to support also the second user, which then allows the transmitter to use all carriers. Another possibility is to increase the number of carriers. The asymptotic behavior of the rates cannot be changed in general, but the high-SNR behavior of the maximized secrecy rates is shifted to the right.

⟨**2.38**⟩ **Publication Note.** The main results discussed in this section have already been presented at the *1st International Workshop on Multiple Access Communications* in 2008



(a) $K = 10$ (b) $K = 100$

Figure 2.7: Comparison of achievable rates with and without secrecy constraints for the one- and two-user case.

and published in (Jorswieck and Wolf, 2008). In this paper, we studied the optimal resource allocation for the secrecy rate maximization in the multi-carrier scenario. We presented the secrecy rate expression in ⟨2.22⟩ and derived results on the carrier selection and the spectral power allocation for the single- and two-user case, which were a basis for ⟨2.28⟩, ⟨2.29⟩, and ⟨2.35⟩, but also for the high- and low-SNR discussion in ⟨2.32⟩ and ⟨2.33⟩.

⟨**2.39**⟩ **Related Work.** Li et al. (2006) considered the secrecy capacity of a system with multiple independent parallel channels. They showed that the secrecy capacity of the systems is the sum of the secrecy capacities of the individual channels, regardless of the models assumed for these channels. Then, the authors studied the special case with (real-valued) Gaussian channels that are subject to a sum power constraint. They derived the optimal power allocation for this problem, which corresponds to the waterfilling solution in ⟨2.29⟩, and discussed the carrier selection depending on the system parameters. They stated that the transmitter uses only channels where Bob has a higher gain than Eve and that these channels are ranked according to the difference of the channel gains. Consequently, Alice allocates the complete power to the channel with the largest difference for very low SNR. More channels are supported with increasing SNR, where the order is determined by the difference of the channel gains. These results correspond to the derivations and observations that we formulated in ⟨2.28⟩, ⟨2.33⟩, and ⟨2.34⟩. Unfortunately, we were not aware of this publication when we derived the results that we presented in this section of the thesis and in (Jorswieck and Wolf, 2008).

Liang et al. (2008c) considered the parallel broadcast channel with independent carriers, which they denoted as subchannels. They focused on the scenario with one transmitter and two receivers, where the transmitter wants to broadcast a common message to both receivers. Additionally, there is a confidential message for one receiver that should be kept

perfectly secret from the other. The authors analyzed this scenario from a information-theoretical perspective and characterized the secrecy capacity region of the broadcast channel. This result includes the secrecy capacity of the parallel wiretap channel as a special case, which is obtained if no common message should be transmitted. Moreover, it was shown that it is optimal to have independent inputs for each subchannel. For the Gaussian broadcast channel, which is a special case of the analyzed model, the secrecy capacity region is given. It was observed that the common message is sent over all subchannels, whereas the confidential message is only sent over those subchannels for which the output at the eavesdropper is a degraded version of the output at the intended receiver.

2.3 Multi-Antenna Scenario

In this section, we extend the basic model in ⟨2.2⟩ to a multi-antenna scenario, where Alice wants to send her private message to Bob in a system where all users have multiple transmit / receive antennas. As before, Eve is a passive eavesdropper who tries to decode Alice's message that was intended for Bob. We describe the general case where Alice, Bob, and Eve have multiple antennas, which is denoted as multiple-input multiple-output (MIMO) scenario. But we also have a glance on the special case where Bob and Eve have only a single antenna each, which is called multiple-input single-output (MISO) scenario. In contrast to the sections above, we restrict ourselves to the description of the system model, the introduction of the secrecy rate expression for this model, and the discussion of the properties of this function. This provides the basis for the worst-case analysis in the next chapter. The optimization of the secrecy rate for the multi-antenna scenario is not within the focus of this thesis. We refer the interested reader to the introduction of this thesis for some comments and approaches on the corresponding maximization problems under various constraints.

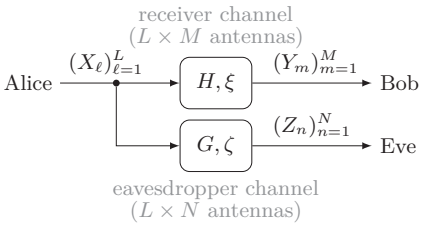


Figure 2.8: Wiretap channel for the multi-antenna scenario.

⟨**2.40**⟩ **System Model (Extension to Multi-Antenna Scenario).** We extend the basic model in ⟨2.2⟩ to a multi-antenna scenario, see Figure 2.8, where Alice has L transmit antennas, whereas Bob and Eve have M and N receive antennas, respectively.

Thus, we have a transmit signal vector X with $X^{\mathrm{T}} = (X_\ell)_{\ell=1}^{L}$ at Alice and the receive signal vectors Y and Z with $Y^{\mathrm{T}} = (Y_m)_{m=1}^{M}$ and $Z^{\mathrm{T}} = (Z_n)_{n=1}^{N}$ at Bob and Eve, respectively. The attenuated Gaussian channels are characterized by the channel coefficient matrices $H \in \mathbb{C}^{M\times L}$ and $G \in \mathbb{C}^{N\times L}$ together with the noise vectors ξ and ζ with $\xi^{\mathrm{T}} = (\xi_m)_{m=1}^{M}$ and $\zeta^{\mathrm{T}} = (\zeta_n)_{n=1}^{N}$. These noise vectors are modeled as Gaussian vectors $\xi, \zeta \sim \mathcal{CN}(0, \sigma^2)$, i.e., they have zero mean and diagonal covariance matrices $\mathbb{E}\left(\xi\xi^{\mathrm{H}}\right) = \sigma^2 I_M$ and $\mathbb{E}\left(\zeta\zeta^{\mathrm{H}}\right) = \sigma^2 I_N$.

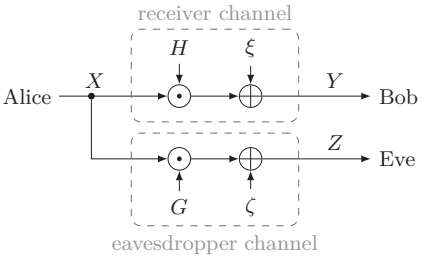


Figure 2.9: MIMO wiretap channel with attenuated Gaussian channels.

The system model, which is shown in Figure 2.9, can be described by

$$\begin{aligned} Y &= HX + \xi \quad \text{and} \\ Z &= GX + \zeta. \end{aligned}$$

We directly transfer all relations and assumptions from the basic model in ⟨2.2⟩ to this model for the multi-antenna scenario. The power constraint becomes a power constraint over all transmit antennas, which can be expressed as $\mathbb{E}\left(X^{\mathrm{H}}X\right) \leq P$, which is equivalent to $\mathrm{tr}(Q) \leq P$, where $Q \in \mathbb{C}^{L\times L} \succeq 0$ is Alice's transmit covariance matrix $Q := \mathbb{E}\left(XX^{\mathrm{H}}\right)$.

⟨**2.41**⟩ **Secrecy Rate.** For this model, the secrecy rate R_S, which we interpret as a function of the channel matrices H and G and the transmit covariance matrix Q with $Q \succeq 0$, can be evaluated according to ⟨1.9⟩, which yields

$$\begin{aligned} R_S(H,G,Q) &= \left[\varphi(H,G,Q)\right]^+ \quad \text{with} \\ \varphi(H,G,Q) &:= \log_2 \det\left(I_M + \rho\, HQH^{\mathrm{H}}\right) - \log_2 \det\left(I_N + \rho\, GQG^{\mathrm{H}}\right). \end{aligned}$$

⟨**2.42**⟩ **Notation.** We introduce the matrices A and B, which are the Gramian matrices of the channel matrices H and G, respectively. Thus, they are given by $A := H^{\mathrm{H}}H$ and $B := G^{\mathrm{H}}G$ with $A, B \in \mathbb{C}^{L\times L}$. Due to this construction, we have $A, B \succeq 0$, i.e., the matrices A and B are positive-semidefinite.

With this Gramian matrix notation, we introduce some equivalent expressions for the secrecy rate R_S, which are useful for the formulation of optimization problems and the derivation of their properties in the next chapters.

⟨**2.43**⟩ **Secrecy Rate (Equivalent Notation).** With Sylvester's determinant theorem, see ⟨A.7⟩, the secrecy rate R_S can be written as a function of the Gramian matrices A and B of the channel matrices H and G and the transmit covariance matrix Q. We write $R_S^\star$ instead of R_S if we refer to the secrecy rate in Gramian notation:

$$\begin{aligned} R_S^\star(A,B,Q) &= [\varphi^\star(A,B,Q)]^+ \quad \text{with} \\ \varphi^\star(A,B,Q) &:= \log_2 \det\left(I_L + \rho\, Q^{\frac{1}{2}} A Q^{\frac{1}{2}}\right) - \log_2 \det\left(I_L + \rho\, Q^{\frac{1}{2}} B Q^{\frac{1}{2}}\right) \\ &= \log_2 \det\left(I_L + \rho\, A^{\frac{1}{2}} Q A^{\frac{1}{2}}\right) - \log_2 \det\left(I_L + \rho\, B^{\frac{1}{2}} Q B^{\frac{1}{2}}\right), \end{aligned}$$

where $A^{\frac{1}{2}}$, $B^{\frac{1}{2}}$, and $Q^{\frac{1}{2}}$ are the (principal) square roots of the (positive-semidefinite) matrices A, B, and Q.

We formulate the convexity properties of the functions φ and $\varphi^\star$ in ⟨2.41⟩ and ⟨2.43⟩ with respect to their variables in order to derive the convexity properties of R_S and $R_S^\star$. For this purpose, we can use some statements from the literature.

⟨**2.44**⟩ **Properties (Convexity).** It is known that the $\log_2 \det$ function is concave on the set of positive-semidefinite matrices, see for instance (Cover and Thomas, 1988, Proof of Theorem 1). Thus, we can conclude that the function $\varphi^\star$ in ⟨2.43⟩ is

a) a concave function of A and

b) a convex function of B

since the argument of the $\log_2 \det$ function is a positive-semidefinite matrix, which is a linear function of the corresponding variable, in both cases. Additionally, the function φ in ⟨2.41⟩ is

c) a concave function of Q if the relation between the channel matrices H and G can be expressed[7] as $TH = G$ with $T \in \mathbb{C}^{N\times M}$ and $I_M - T^{\mathrm{H}}T \succeq 0$.

This is a result from Liang et al. (2009, Lemma C.1), who applied a previous result from Diggavi and Cover (2001, Lemma II.3). Note that: (i) The matrix T can only be unique if $M \leq L$. (ii) The proof in (Liang et al., 2009) requires that $(T^{\mathrm{H}}T)^{-1}$ exists. Hence, we have to require that $M \leq N$ and that T has full column rank. In addition, this result implies that the function $\varphi^\star$ in ⟨2.43⟩ is a concave function of Q if this holds for the correspondig φ, since the change in the notation according to ⟨2.42⟩ does not affect the properties of the function.

If we consider a convex set for the respective variable where φ or $\varphi^\star$ is positive, we can infer that each property formulated above also holds for the corresponding secrecy rate. Consequently, we can say that $R_S^\star$ in ⟨2.43⟩ is concave in A and convex in B in this case. Furthermore, we know that R_S in ⟨2.41⟩ is concave in Q if the channel matrices H and G fulfill the condition above and if we consider a convex set for Q where R_S is positive. The secrecy rate $R_S^\star$ is concave in Q if this holds for the correspondig secrecy rate R_S.

[7] Note that the same relation was formulated by Weingarten et al. (2007, Definition 1) for the degradedness of the MIMO wiretap channel.

⟨**2.45**⟩ **Secrecy Capacity.** The secrecy capacity of the multi-antenna wiretap channel was derived by Khisti and Wornell (2007) as well as Oggier and Hassibi (2007) for a model with real-valued random variables. The extension to complex-valued random variables yields

$$C_S = \max_{Q \in \mathcal{Q}} \left[\log_2 \det \left(I_M + \rho\, HQH^{\mathrm{H}} \right) - \log_2 \det \left(I_N + \rho\, GQG^{\mathrm{H}} \right) \right]^+ ,$$

see for instance (Bloch and Barros, 2011, Theorem 5.2).

⟨**2.46**⟩ **Special Case (Multiple-Input Single-Output Scenario).** The special case where Bob and Eve each have only a single antenna was studied by Li et al. (2007). Then, we have $M = N = 1$, and the channel matrices in ⟨2.40⟩ become row vectors of length L. Thus, we now write h and g instead of H and G. Li et al. (2007) studied the secrecy rate maximization problem under a sum power constraint over all antennas and applied a coordinate transformation with a unitary matrix in order to reduce this problem to a two-dimensional problem. The first column of the transformation matrix was defined as

$$w_{\mathrm{MRT}} := \frac{h^{\mathrm{H}}}{\|h\|},$$

which can be identified as the maximum-ratio beamforming vector for the channel from Alice to Bob. The second column is chosen such that it is normalized and orthogonal to the first column and lies in the space spanned by h and g. The remaining columns can be arbitrarily chosen such that they are a orthonormal basis for the remaining space and orthogonal to the first two columns. Li et al. (2007) showed that the optimal transmit covariance matrix $\tilde{Q}$ in the transformed (and reduced) space is given by $\tilde{Q} = Pww^{\mathrm{H}}$, where w is the generalized eigenvector that corresponds to the largest generalized eigenvalue of the matrices $I_2 + P\tilde{h}^{\mathrm{H}}\tilde{h}$ and $I_2 + P\tilde{g}^{\mathrm{H}}\tilde{g}$, where $\tilde{h}$ and $\tilde{g}$ are obtained by transforming the original channel vectors h and g and reducing them to the first two dimensions afterwards.

3 Worst-Case Studies for Secrecy Rate Optimization

In the previous chapter, we studied the secrecy rate maximization for various wiretap scenarios. For all these problems, we assumed that the transmitter Alice had perfect information about the channel to the eavesdropper Eve. This was motivated by the idea that Eve is not only a curious eavesdropper but also a regular user of the system, whose channel state is known to the transmitter due to some further communication processes. In this chapter, we want to relax the assumption on perfect information about the eavesdropper channel. We introduce a kind of partial information for the transmitter. The transmitter only knows that the eavesdropper's channel coefficients are subject to certain restrictions, i.e., all possible eavesdropper channels can be modeled by an infinite set, which reflects this constraint. We focus on the multi-antenna wiretap scenario, which is the most general case we presented in the last chapter. It can be used as a basis for the derivation of special cases representing the other scenarios we discussed before. In the first section of this chapter, we introduce the system model and the optimization problems. Then, we discuss these problems for a multi-antenna transmitter with only one wiretap encoder. We characterize the worst-case secrecy rate for each given transmit strategy and derive upper and lower bounds for the maximization of this worst-case secrecy rate under a sum power constraint over all antennas at the transmitter. Afterwards, we present a multi-antenna transmitter whose structure is better adapted to the properties of the given problem. We also study the worst-case secrecy rate and its maximization for this transmitter structure and compare the results for both transmitters.

3.1 Problem Statement and Equivalent Formulations

In this section, we introduce the system model for the worst-case study. We formulate the worst-case problem and the corresponding maximization problem for the worst-case secrecy rate. For this problem, we derive an equivalent formulation over the eigenvalues of the matrices that characterize the underlying system model.

⟨**3.1**⟩ **System Model.** We resume the system model of the MIMO scenario, which was specified in ⟨2.40⟩, with only one change. So far, we assumed that Alice has perfect knowledge about the channels to Bob and Eve. This is still true for the channel H to Bob, but about the channel G to Eve she now only knows that it underlies the following restriction:

$$\|G\|_{\mathrm{F}}^2 = \mathrm{tr}(G^{\mathrm{H}}G) \leq \chi \quad \text{with} \quad \chi \geq 0.$$

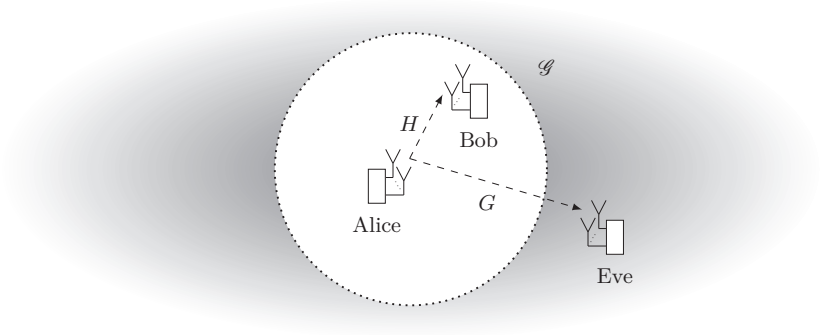


Figure 3.1: Illustration of the system model for the worst-case analysis of the secrecy rate in a MIMO scenario.

The constraint is formulated using the Frobenius norm $\|\cdot\|_{\mathrm{F}}$ of the eavesdropper channel G. It can be equivalently written as

$$\|G\|_{\mathrm{F}}^2 = \sum_{n=1}^{N} \sum_{\ell=1}^{L} |g_{n\ell}|^2 \leq \chi,$$

where the elements of the matrix G are denoted by $g_{n\ell}$. Thus, it corresponds to a constraint on the quality of the eavesdropper channel in the sense that it is an upper bound on the sum of all channel gains. Together with a sum power constraint at the transmitter, it can be interpreted as a constraint on the sum receive power at the eavesdropper. If Alice knows the minimum distance to Eve, she can correspondingly compute a suitable value for χ. Figure 3.1 illustrates the idea of this model. We have a multi-antenna transmitter, Alice, and two multi-antenna receivers, Bob and Eve. The matrix H for the MIMO channel to Bob is known to Alice, but there is some uncertainty about the matrix G of the MIMO channel to Eve.

For known channel matrices H and G, the secrecy rate R_S and the corresponding function φ were given in ⟨2.41⟩. With these functions, we formulate two (nested) optimization problems for the system model in ⟨3.1⟩. The first (or inner) problem is the identification of the worst-case secrecy rate for a given transmit covariance matrix. This is a minimization that is carried out over all possible eavesdropper channel matrices. The second (or outer) problem is the maximization of this worst-case secrecy rate over all transmit covariance matrices that fulfill the transmit power constraint. For both problems, we introduce two formulations. In each case, we start with a problem statement that directly uses the variables from the system model. Afterwards, we derive an equivalent formulation that is more suitable for the following analysis.

⟨**3.2**⟩ **Problem Formulation (Worst-Case Secrecy Rate).** For each given channel matrix H and each given transmit strategy, which is specified by the transmit covariance matrix Q, the corresponding worst-case secrecy rate R_{W} is the minimal secrecy rate that can be achieved if the minimization is carried out over all possible matrices for the channel from the transmitter to the eavesdropper, i.e.,

$$R_{\mathrm{W}}(H,Q) \coloneqq \min_{G\in\mathscr{G}} R_S(H,G,Q) = \min_{G\in\mathscr{G}} [\,\varphi(H,G,Q)]^+ = \left[\min_{G\in\mathscr{G}} \varphi(H,G,Q)\right]^+,$$

where

$$\mathscr{G} \coloneqq \left\{ G \in \mathbb{C}^{N\times L} \,\middle|\, \mathrm{tr}(G^{\mathrm{H}}G) \leq \chi \right\}$$

is the set of all possible matrices for the channel from the transmitter to the eavesdropper.

⟨**3.3**⟩ **Problem Formulation (Equivalent Notation).** With the Gramian matrix notation defined in ⟨2.42⟩ and the secrecy rate expression in ⟨2.43⟩, we can equivalently formulate the worst-case secrecy rate problem in ⟨3.2⟩ as

$$R^{\star}_{\mathrm{W}}(A,Q) \coloneqq \min_{B\in\mathscr{B}} R^{\star}_S(A,B,Q) = \min_{B\in\mathscr{B}} [\,\varphi^{\star}(A,B,Q)]^+ = \left[\min_{B\in\mathscr{B}} \varphi^{\star}(A,B,Q)\right]^+,$$

where $R^{\star}_{\mathrm{W}}$ is the worst-case secrecy rate adapted to the Gramian notation of the channel matrices and

$$\mathscr{B} \coloneqq \left\{ B \in \mathbb{C}^{L\times L} \,\middle|\, B \succeq 0 \text{ and } \mathrm{tr}(B) \leq \chi \right\}$$

is the set that corresponds to the set $\mathscr{G}$ in ⟨3.2⟩ such that

$$G \in \mathscr{G} \quad \Rightarrow \quad B \coloneqq G^{\mathrm{H}}G \in \mathscr{B} \quad \Rightarrow \quad G \in \left\{ \bar{G} \in \mathbb{C}^{N\times L} \,\middle|\, \bar{G}^{\mathrm{H}}\bar{G} = B \right\} \subseteq \mathscr{G}.$$

In order to analyze the properties of the optimization problem in ⟨3.3⟩, we can come back to the properties we listed for the MIMO secrecy rate and the corresponding maximization problem in the previous chapter.

⟨**3.4**⟩ **Properties (Convexity of the Problem).** It can be shown that the constraint set $\mathscr{B}$ is convex by applying the following properties: (i) The convex combination of two $(L\times L)$-dimensional positive-semidefinite matrices always produces a positive-semidefinite matrix of the same dimension. (ii) The trace function is linear. From ⟨2.44⟩, we can conclude that $\varphi^{\star}$ is a convex function of B on the set $\mathscr{B}$. Thus, we have a convex problem.

The transmitter aims to maximize this worst-case secrecy rate under a sum power constraint over all antennas. This results in a max-min optimization problem.

⟨**3.5**⟩ **Problem Formulation (Worst-Case Secrecy Rate Maximization).** For a given channel matrix H, the worst-case secrecy rate R_{W} in ⟨3.2⟩, which was determined over the known set $\mathscr{G}$, should be maximized under a sum power constraint over all antennas at the transmitter, i.e.,

$$\begin{aligned}\max_{Q\in\mathscr{Q}} R_{\mathrm{W}}(H,Q) &= \max_{Q\in\mathscr{Q}} \min_{G\in\mathscr{G}} R_S(H,G,Q)\\ &= \max_{Q\in\mathscr{Q}} \min_{G\in\mathscr{G}} \left[\varphi(H,G,Q)\right]^+ = \left[\max_{Q\in\mathscr{Q}} \min_{G\in\mathscr{G}} \varphi(H,G,Q)\right]^+,\end{aligned}$$

where

$$\mathscr{Q} := \left\{ Q \in \mathbb{C}^{L\times L} \,\middle|\, Q \succeq 0 \text{ and } \operatorname{tr}(Q) \leq P \right\}$$

is the set of all feasible transmit covariance matrices. We observe that this constraint set is convex. We have already obtained this result in ⟨3.4⟩ for the set $\mathscr{B}$, which was specified by comparable constraints.

In the formulation of the problem in ⟨3.5⟩, we assume that Alice knows the set $\mathscr{G}$ and consequently the dimension of the channel matrix G for the channel to Eve, i.e., the number N of antennas Eve is equipped with. In ⟨3.6⟩, we reformulate the problem and its constraints. In the resulting problem, the constraints do not require that Alice knows N. Later, we will assume that Eve can have an arbitrarily large number of antennas. Then, we will have a real worst-case scenario. But we will see that it is not necessary that Eve has more receive antennas than Alice uses to transmit the message if Eve has found the worst-case channel matrix.

⟨**3.6**⟩ **Problem Formulation (Equivalent Notation).** We use again the Gramian matrix notation defined in ⟨2.42⟩ and the secrecy rate expression in ⟨2.43⟩. Therewith, we equivalently reformulate the optimization problem in ⟨3.5⟩ and obtain

$$\begin{aligned}\max_{Q\in\mathscr{Q}} R^{\star}_{\mathrm{W}}(A,Q) &= \max_{Q\in\mathscr{Q}} \min_{B\in\mathscr{B}} R^{\star}_S(A,B,Q)\\ &= \max_{Q\in\mathscr{Q}} \min_{B\in\mathscr{B}} \left[\varphi^{\star}(A,B,Q)\right]^+ = \left[\max_{Q\in\mathscr{Q}} \min_{B\in\mathscr{B}} \varphi^{\star}(A,B,Q)\right]^+,\end{aligned}$$

with $\mathscr{Q}$ and $\mathscr{B}$ given in ⟨3.5⟩ and ⟨3.3⟩, respectively.

⟨**3.7**⟩ **Remark.** We can equivalently formulate the maximized worst-case problems in ⟨3.5⟩ and ⟨3.6⟩ without the outer $[\cdot]^+$ function. Since the constraint set $\mathscr{Q}$ contains the zero matrix, it is always guaranteed that the maximized worst-case secrecy rate is non-negative. But note that the outer $[\cdot]^+$ function is necessary in the formulation of the worst-case problems in ⟨3.2⟩ and ⟨3.3⟩ in order to ensure that the resulting rates are non-negative.

⟨**3.8**⟩ **Remark.** In the literature, a setting in ⟨3.5⟩ or ⟨3.6⟩ is occasionally called a game against nature: The first player, who is the transmitter in our case, aims to maximize the cost function, the secrecy rate R_S (or $R_S^\star$), and chooses a certain strategy, which we identify with the transmit covariance matrix Q. Then the second player, who corresponds to the nature and wants to minimize the cost function, is consequently aware of the first player's strategy and can react accordingly. In our case, the matrix G (or the corresponding Gramian matrix B) for the channel to the eavesdropper is chosen such that the resulting secrecy rate is minimized.

In the following, we will refer to the minimization in ⟨3.3⟩ and ⟨3.6⟩ as inner problem and to the maximization in ⟨3.6⟩ as outer problem.

⟨**3.9**⟩ **Notation.** We introduce the (row) vectors $a = (a_\ell)_{\ell=1}^L$, $b = (b_\ell)_{\ell=1}^L$, and $q = (q_\ell)_{\ell=1}^L$ of length L as

$$a := \operatorname{eig}(A), \quad b := \operatorname{eig}(B), \quad \text{and} \quad q := \operatorname{eig}(Q),$$

i.e., the vectors a, b, and q contain the eigenvalues of the matrices A, B, and Q, respectively.

⟨**3.10**⟩ **Properties.** For the matrices A, B, and Q and their eigenvalues, it holds:

a) The components of a, b, and q are non-negative since the matrices A, B, and Q are positive-semidefinite.
b) The rank of the matrices A and B is equal to the number of positive components in the eigenvalue vectors a and b, respectively. Due to the construction of the matrices, which was given in ⟨2.42⟩, we have $\operatorname{rank}(A) \leq \min\{L, M\}$ and $\operatorname{rank}(B) \leq \min\{L, N\}$.

⟨**3.11**⟩ **Further Assumptions.** For convenience, we assume $N \geq L$ in the further discussion. This ensures that the matrix $B \in \mathbb{C}^{L\times L}$ can have full rank.

We can reduce the optimization problem in ⟨3.6⟩ to an equivalent optimization problem over the eigenvalues of Q and B.

⟨**3.12**⟩ **Problem Formulation (Equivalent Problem).** For a given vector a, the worst-case secrecy rate should be maximized under a sum power constraint over all antennas at the transmitter, i.e.,

$$\begin{aligned}\max_{q\in\mathcal{Q}} \widetilde{R}_{\mathrm{W}}(a,q) &= \max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \widetilde{R}_S(a,b,q) \\ &= \max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \left[\widetilde{\varphi}(a,b,q)\right]^+ = \left[\max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \widetilde{\varphi}(a,b,q)\right]^+ .\end{aligned}$$

The vectors a and b contain the eigenvalues of the Gramian matrices A and B, which are derived from the channel matrices H and G, respectively. The vector q is the eigenvalue vector for the transmit covariance matrix Q. The function $\widetilde{R}_S$ with

$$\widetilde{R}_S(a,b,q) := [\,\widetilde{\varphi}(a,b,q)\,]^+ \quad \text{with}$$
$$\widetilde{\varphi}(a,b,q) := \sum_{\ell=1}^{L} \left(\log_2\left(1+\rho\, a_\ell q_\ell\right) - \log_2\left(1+\rho\, b_\ell q_\ell\right)\right)$$

is a secrecy rate expression that only depends on the eigenvalues of the matrices A, B, and Q. The function $\widetilde{R}_{\mathrm{W}}$ is the worst-case secrecy rate for this case, which is defined as

$$\widetilde{R}_{\mathrm{W}}(a,q) := \min_{b\in\mathcal{B}} \widetilde{R}_S(a,b,q) = \min_{b\in\mathcal{B}} [\,\widetilde{\varphi}(a,b,q)\,]^+ = \left[\min_{b\in\mathcal{B}} \widetilde{\varphi}(a,b,q)\right]^+ .$$

The constraint sets for this problem are defined as

$$\mathcal{Q} := \left\{ q = (q_\ell)_{\ell=1}^{L} \in \mathbb{R}^{1\times L} \;\middle|\; q_\ell \geq 0 \text{ and } \sum_{\ell=1}^{L} q_\ell \leq P \right\} \quad \text{and}$$
$$\mathcal{B} := \left\{ b = (b_\ell)_{\ell=1}^{L} \in \mathbb{R}^{1\times L} \;\middle|\; b_\ell \geq 0 \text{ and } \sum_{\ell=1}^{L} b_\ell \leq \chi \right\}.$$

The equivalence of this optimization problem with the problem formulated in ⟨3.6⟩ is proven by a detailed and commented reformulation process, which is provided in ⟨B.1⟩ in the appendix.

⟨**3.13**⟩ **Remark.** The remark in ⟨3.7⟩ can analogously be applied to the reformulated problem in ⟨3.12⟩, i.e., the outer $[\cdot]^+$ function is not relevant for the maximized secrecy rate problem.

⟨**3.14**⟩ **Notation (Overview).** The following diagram provides an overview of the different secrecy rate notations we introduced so far for the worst-case maximization and shows the connections between them. For the introduction of the eigenvalue notation, we have already exploited the properties of the function together with the max-min optimization problem, while the transition from the original to the Gramian notation was only a substitution of variables.

	original notation		Gramian notation		eigenvalue notation
secrecy rate	$R_S(H,G,Q)$	$\longrightarrow$ $A := H^{\mathrm{H}}H$, $B := G^{\mathrm{H}}G$	$R_S^\star(A,B,Q)$	$\longrightarrow$ $a := \mathrm{eig}(A)$, $b := \mathrm{eig}(B)$, $q := \mathrm{eig}(Q)$	$\widetilde{R}_S(a,b,q)$
	$\downarrow \min_{G\in\mathcal{G}}$		$\downarrow \min_{B\in\mathcal{B}}$		$\downarrow \min_{b\in\mathcal{B}}$
worst-case secrecy rate	$R_{\mathrm{W}}(H,Q)$		$R_{\mathrm{W}}^\star(A,Q)$		$\widetilde{R}_{\mathrm{W}}(a,q)$

3.2 Worst-Case Optimization for Transmitters with Joint Encoding

In this section, we analyze the properties of the eigenvalue problem in ⟨3.12⟩. We derive an optimal strategy for the inner problem and characterize the optimal strategy for the outer problem. We present lower and upper bounds on the maximized worst-case secrecy rate and discuss its low- and high-SNR behavior.

⟨3.15⟩ Secrecy Rate. The secrecy rate expression $\widetilde{R}_S$ of the eigenvalue problem in ⟨3.12⟩ looks very similar to the secrecy rate R_S that was derived for the multi-carrier scenario in ⟨2.22⟩. But there is one significant difference: the application of the $[\cdot]^+$ function. In the secrecy rate expression of the multi-carrier case, every summand was ensured to be non-negative, whereas single summands in the secrecy rate expression in ⟨3.12⟩ are allowed to be negative as long as the complete secrecy rate is non-negative. From a technical point of view, negative rate terms are not possible. Hence, it seems necessary to point out that the secrecy rate expression $\widetilde{R}_S$ in ⟨3.12⟩ does not reflect a sum rate expression, where individual (non-negative) rates are added up. It is rather one rate expression for an achievable secrecy rate in a multi-antenna scenario, where the transmitter uses one wiretap encoder of a corresponding rate to assign codewords to each message. From this point of view, it seems to be more plausible to write the secrecy rate expression $\widetilde{R}_S$ in ⟨3.12⟩ as

$$\widetilde{R}_S(a,b,q) = \left[\sum_{\ell=1}^{L} \log_2\left(1+\rho\, a_\ell q_\ell\right) - \sum_{\ell=1}^{L} \log_2\left(1+\rho\, b_\ell q_\ell\right)\right]^+ .$$

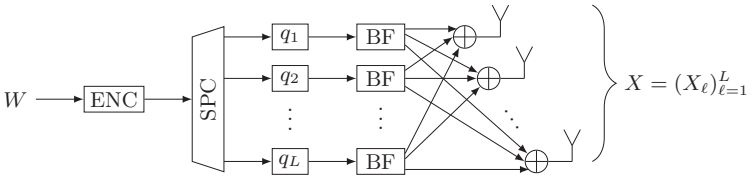


Figure 3.2: Structure of multi-antenna transmitter with one wiretap encoder.

Figure 3.2 illustrates the transmitter structure for this case. The transmitter has only one wiretap encoder for joint encoding, which maps messages to codewords with a certain rate. The output of this encoder is converted into up to L parallel data streams, which are individually processed afterwards. Note that the exact number of supported data streams depends on the chosen transmit strategy q. The symbols of each data stream are transformed into a vector output for the L transmit antennas with appropriate weighting factors and corresponding beamforming strategies. These weighting factors and beamforming strategies result from the solution of problem ⟨3.12⟩ and its derivation

from problem ⟨3.6⟩. They can be obtained by calculating the eigenvalues q and the eigenvectors of the optimal transmit covariance matrix Q. The latter are derived from the eigenvectors of the Gramian matrix A for the channel to the legitimated receiver, see derivation of ⟨3.12⟩.

We apply the properties we specified for the secrecy rate of the basic scenario in Section 2.1 to derive the properties of the function $\widetilde{\varphi}$ and the secrecy rate $\widetilde{R}_S$ in ⟨3.12⟩.

⟨3.16⟩ Properties (Monotonicity). The derivatives in ⟨2.6⟩ provide the basis for some statements on the monotonicity of the function $\widetilde{\varphi}$ and the secrecy rate $\widetilde{R}_S$ in the components of the vectors a, b, and q under the assumption that all other variables are fixed. For all $\ell \in \{1, 2, \ldots, L\}$ with $q_\ell > 0$, the function $\widetilde{\varphi}$ in ⟨3.12⟩ is

a) strictly monotonically increasing in a_ℓ,
b) strictly monotonically decreasing in b_ℓ,
c) strictly monotonically increasing in q_ℓ if $a_\ell > b_\ell$, and
d) strictly monotonically decreasing in q_ℓ if $a_\ell < b_\ell$.

These properties directly hold for the secrecy rate $\widetilde{R}_S$ if the function $\widetilde{\varphi}$ is positive. Otherwise, the formulations above have to be relaxed by omitting the word "strictly".

⟨3.17⟩ Properties (Convexity). The Hessian matrices of $\widetilde{\varphi}$ with respect to a, b, and q are diagonal. The analysis of the derivatives in ⟨2.6⟩ delivers the following insights: For a and b, these matrices have only non-positive and non-negative diagonal entries, i.e., they are negative and positive semi-definite, respectively. Unfortunately, the sign of the ℓ-th diagonal element of the Hessian matrix with respect to q depends on the relation of a_ℓ and b_ℓ, i.e., this matrix generally is neither positive nor negative (semi-)definite. We can formulate the convexity properties of $\widetilde{\varphi}$ with respect to the vectors a, b, and q under the assumption that all other variables are fixed. The function $\widetilde{\varphi}$ in ⟨3.12⟩ is

a) a concave function of a and
b) a convex function of b, but
c) generally neither a concave nor a convex function of q.

The first two properties directly hold for the secrecy rate $\widetilde{R}_S$ if the function $\widetilde{\varphi}$ is positive on the set that is considered for the respective variable.

⟨3.18⟩ Properties (Convexity of the Problem). The constraint sets $\mathcal{Q}$ and $\mathcal{B}$, which are given in ⟨3.12⟩, are convex. We noticed this before for the identically structured set of all feasible transmit power allocation vectors in the multi-carrier scenario in ⟨2.27⟩. The function $\widetilde{\varphi}$ in ⟨3.12⟩ is a convex function of the vector b. Thus, the minimization of $\widetilde{\varphi}$ over $b \in \mathcal{B}$ is a convex problem. But we cannot say that the outer maximization over $q \in \mathcal{Q}$ in ⟨3.12⟩ is a convex problem. Since the concavity of the function $\widetilde{\varphi}$ with respect to q is not given for all $b \in \mathcal{B}$, we also cannot state that the max-min problem in ⟨3.12⟩ is a saddle-point problem in general[8].

[8] Note that it would be sufficient to have quasiconcavity of the function $\widetilde{\varphi}$ with respect to q in order to have a saddle-point problem.

In the following, we will refer to the minimization and the maximization in ⟨3.12⟩ as inner problem and outer problem, respectively.

⟨**3.19**⟩ **Further Assumptions.** We assume that the channel to Bob is better than the worst-case channel Eve is looking for, i.e., $\sum_{\ell=1}^{L} a_\ell > \chi$. Otherwise the worst-case secrecy rate $\widetilde{R}_{\mathrm{W}}$ would be zero for each vector $q \in \mathcal{Q}$, which could simply be achieved by choosing $b_\ell = a_\ell$ for all $\ell \in \{1, 2, \ldots, L\}$.

⟨**3.20**⟩ **Optimal Strategy (Outer Problem).** For the maximization of the worst-case secrecy rate, the transmitter takes the number of receive antennas at the intended receiver into account. The vector a, which specifies the channel from Alice to Bob, clearly determines which components of the optimal power allocation vector q can be non-zero. For the transmitter, it only makes sense to allocate a positive value to those components of q where the corresponding component of a is non-zero, since only terms with $a_\ell > 0$ for $\ell \in \{1, 2, \ldots, L\}$ contribute to a positive secrecy rate. This is especially relevant for the case, where Bob has less antennas than Alice, i.e., $M < L$. In this case, we have $\operatorname{rank}(A) \leq M$ for the channel from Alice to Bob. Consequently, the vector a of length L, which contains the eigenvalues of A, has at most M positive components. Hence, this also holds for the optimal power allocation vector q.

Furthermore, we can also characterize the minimum number of non-zero components in the optimal power allocation vector q. The transmitter has to ensure that the worst-case secrecy rate is positive. Consequently, the components q_ℓ that are used by Alice for the transmission to Bob have to be chosen such that the sum of the corresponding a_ℓ is larger than χ. Otherwise, the worst-case channel would simply be $b_\ell = a_\ell$ for all positive elements q_ℓ of the power allocation vector q, which would in turn result in a zero worst-case secrecy rate.

Note that we cannot state that the optimal power allocation vector q always uses full power P, since the (worst-case) secrecy rate is not monotonic with respect to q_ℓ. Its behavior depends on the relation between a_ℓ and b_ℓ as specified in ⟨3.16⟩.

⟨**3.21**⟩ **Optimal Strategy (Solution of Inner Problem).** The power allocation vector q, which is chosen by the transmitter, clearly determines which components of the worst-case vector b can be non-zero. It only makes sense to allocate a positive value to those components of b where the corresponding component of q is non-zero, since $q_\ell = 0$ with $\ell \in \{1, 2, \ldots, L\}$ nulls the ℓ-th summand of the secrecy rate $\widetilde{R}_S$ independently of the chosen b_ℓ. For the components of b that correspond to a non-zero component of q, the optimal strategy for the inner problem is known as standard waterfilling, which was used by Telatar (1995) in the derivation of the capacity of multi-antenna Gaussian channels, and is given by

$$b_\ell(\nu) = \left[\nu - \frac{1}{\rho q_\ell}\right]^+$$

for all $\ell \in \{1, 2, \ldots, L\}$ with $q_\ell > 0$. Due to the monotonicity in all components of b, the waterfilling parameter ν with $\nu \geq 0$ has to be chosen such that the sum constraint of the set $\mathcal{B}$ is fulfilled with equality, i.e., $\sum_{\ell=1}^{L} b_\ell(\nu) = \chi$.

The number of positive components in the worst-case vector b equals the rank of the corresponding worst-case matrix B. This in turn yields the number of rows in the worst-case channel matrix G, which is the minimum number of antennas that Eve needs. Obviously, Eve needs exactly the same number of antennas for eavesdropping as Alice uses to transmit the message if Eve has found such a worst-case channel matrix. Generally, we can state that it is not necessary that Eve has more than L antennas in this worst-case secrecy rate scenario, where the worst-case channel matrix G is chosen for a known transmit covariance matrix Q. More precisely, we can say that it is sufficient if N equals $\min\{L, M\}$, since we know from ⟨3.20⟩ that Alice adapts her transmit strategy to the number of antennas that Bob is equipped with.

Now, we want to investigate how the component ordering of the vector a determines the component ordering of the optimal vectors q and b that solve ⟨3.12⟩.

⟨**3.22**⟩ **Further Assumptions.** Without loss of generality, we assume that the eigenvalues of the positive-semidefinite matrix A, which are collected in the vector a, are sorted in descending order, i.e., $a_1 \geq a_2 \geq \ldots \geq a_L \geq 0$.

⟨**3.23**⟩ **Optimal Strategy (Vector Ordering).** The worst-case vector b has the same (component) ordering as the power allocation vector q. This can be shown by using a result from Fiedler (1971), which is part of ⟨A.8⟩ in the appendix. Note that the solution for the inner problem in ⟨3.21⟩ reflects this ordering. With the same result, it can be proven afterwards that the optimal power allocation vector q, which maximizes the worst-case secrecy rate in ⟨3.12⟩, adopts the ordering of the vector a. Hence, we obtain that the vectors q and b that are optimal for ⟨3.12⟩ are both ordered like the vector a. The detailed and commented derivation for this can be found in ⟨B.2⟩ in the appendix. With ⟨3.22⟩, we can write

$$a_1 \geq a_2 \geq \ldots \geq a_L \geq 0 \quad \Rightarrow \quad \begin{aligned} &q_1 \geq q_2 \geq \ldots \geq q_L \geq 0 \quad \text{and} \\ &b_1 \geq b_2 \geq \ldots \geq b_L \geq 0. \end{aligned}$$

⟨**3.24**⟩ **Notation.** We define $J := \min\{L, M\}$, which is the maximum number of non-zero components in the vector a.

⟨**3.25**⟩ **Properties.** From the characterization of the optimal strategies in ⟨3.20⟩ and ⟨3.21⟩, we know that J is the maximum number of non-zero components in the optimal vectors q and b. Together with the vector ordering result above, it follows that only the first J components can be positive and we get

$$\forall \ell \in \{1, 2, \ldots, J\} : \quad q_\ell \in \left[0, \frac{P}{\ell}\right] \qquad \text{and}$$

$$b_1 \in \left[\frac{\chi}{J}, \chi\right], \qquad \forall \ell \in \{2, 3, \ldots, J\}: \quad b_\ell \in \left[0, \frac{\chi}{\ell}\right]$$

for the optimal vectors q and b. For the characterization of the first component of the worst-case vector b, we assumed that the system parameters are given such that the maximized worst-case secrecy rate is positive. In this case, the sum constraint for the vector b is fulfilled with equality, i.e., $\sum_{\ell=1}^{L} b_\ell = \chi$, which follows from the monotonicity properties in ⟨3.16⟩. Otherwise, a definitely secure transmission is not possible with this approach, and the transmitter could consequently choose the zero vector for q, which would in turn lead to a zero vector for b.

⟨3.26⟩ Properties (Saddle-Point Condition). In ⟨3.18⟩, we stated that the problem in ⟨3.12⟩ is not a saddle-point problem in general, since the concavity of the function $\widetilde{\varphi}$ with respect to the power allocation vector q is not guaranteed for all vectors $b \in \mathcal{B}$. But with the characterization of the worst-case vector b in ⟨3.25⟩, we can formulate a sufficient condition for the existence of a saddle-point problem. We know that the worst-case vector b fulfills $b_\ell \leq \frac{\chi}{\ell}$ for all $\ell \in \{1, 2, \ldots, J\}$. Consequently, we can add this further constraint to the set $\mathcal{B}$ without affecting the solution of the problem in ⟨3.12⟩. Then, we can state the following: If χ is sufficiently small, i.e.,

$$\forall \ell \in \{1, 2, \ldots, J\}: \quad \chi \leq \ell \, a_\ell,$$

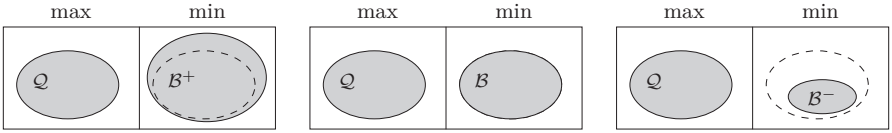
the function $\widetilde{\varphi}$ is concave with respect to the power allocation vector q for all vectors b in this additionally constrained set, which in turn yields that the problem in ⟨3.12⟩ becomes a saddle-point problem. Then, the max-min problem can equivalently be expressed as min-max problem. In this case, we can additionally observe a secondary effect. This sufficiently small χ simultaneously ensures that the function $\widetilde{\varphi}$ is monotonically increasing in each component q_ℓ of the power allocation vector q, which yields that the optimal vector q uses full power P.

Now, we want to derive lower and upper bounds on the maximized worst-case secrecy rate in ⟨3.12⟩.

⟨3.27⟩ Bounds on Outer Problem. If we have sets $\mathcal{B}^-$ and $\mathcal{B}^+$ with $\mathcal{B}^- \subseteq \mathcal{B} \subseteq \mathcal{B}^+$, we can manipulate the inner minimization problem in ⟨3.12⟩ in order to obtain

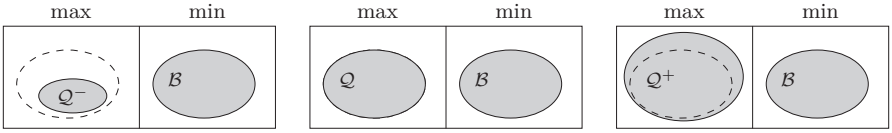
$$\max_{q \in \mathcal{Q}} \min_{b \in \mathcal{B}^+} \widetilde{R}_S(a, b, q) \leq \max_{q \in \mathcal{Q}} \min_{b \in \mathcal{B}} \widetilde{R}_S(a, b, q) \leq \max_{q \in \mathcal{Q}} \min_{b \in \mathcal{B}^-} \widetilde{R}_S(a, b, q)$$

as bounds on the maximized worst-case secrecy rate. Using a set $\mathcal{B}^- \subset \mathcal{B}$ instead of the set $\mathcal{B}$ is equivalent to adding further constraints to the inner minimization problem. As a consequence, we obtain an upper bound on the solution of the max-min problem in ⟨3.12⟩. In contrast, incorporating a set $\mathcal{B}^+ \supset \mathcal{B}$ into the inner minimization problem corresponds to relaxing some constraints of the set $\mathcal{B}$, which yields a lower bound on the original problem.



$$\max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}^+} \widetilde{R}_S(a,b,q) \leq \max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \widetilde{R}_S(a,b,q) \leq \max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}^-} \widetilde{R}_S(a,b,q)$$

(a) bounds obtained by changing the constraint set of the inner minimization problem



$$\max_{q\in\mathcal{Q}^-} \min_{b\in\mathcal{B}} \widetilde{R}_S(a,b,q) \leq \max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \widetilde{R}_S(a,b,q) \leq \max_{q\in\mathcal{Q}^+} \min_{b\in\mathcal{B}} \widetilde{R}_S(a,b,q)$$

(b) bounds obtained by changing the constraint set of the outer maximization problem

Figure 3.3: Derivation of bounds on the maximized worst-case secrecy rate.

Similarly, we can use some sets $\mathcal{Q}^-$ and $\mathcal{Q}^+$ with $\mathcal{Q}^- \subseteq \mathcal{Q} \subseteq \mathcal{Q}^+$ to modify the outer maximization problem. Thereby, we can derive the following bounds:

$$\max_{q\in\mathcal{Q}^-} \min_{b\in\mathcal{B}} \widetilde{R}_S(a,b,q) \leq \max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \widetilde{R}_S(a,b,q) \leq \max_{q\in\mathcal{Q}^+} \min_{b\in\mathcal{B}} \widetilde{R}_S(a,b,q).$$

This idea is illustrated in Figure 3.3.

⟨**3.28**⟩ **Notation.** We introduce the vectors $\beta := (\beta_\ell)_{\ell=1}^L$ and $\iota := (\iota_\ell)_{\ell=1}^L$ with $\beta_\ell, \iota_\ell \geq 0$ for all $\ell \in \{1, 2, \ldots, L\}$ and the corresponding sets

$$\mathcal{B}_\beta := \left\{ b = (b_\ell)_{\ell=1}^L \in \mathbb{R}^{1\times L} \,\middle|\, 0 \leq b_\ell \leq \beta_\ell \right\} \quad \text{and} \quad \dot{\mathcal{Q}}_\iota := \{\iota\}\,.$$

With these sets, we will provide simple upper and lower bounds for the maximized worst-case secrecy rate.

⟨**3.29**⟩ **Upper Bounds.** We want to derive upper bounds on the maximized worst-case secrecy rate by modifying the inner minimization problem as shown in ⟨3.27⟩. We can use every fixed vector $\beta \in \mathcal{B}$ for the derivation of such an upper bound. We simply set $\mathcal{B}^- := \mathcal{B}_\beta$, which adds further per-component constraints to the vector b in compliance with the original sum constraint since we choose $\beta \in \mathcal{B}$. The advantage of using a set $\mathcal{B}_\beta$ instead of the set $\mathcal{B}$ in the max-min problem is that the worst-case vector b is then independent from the chosen transmit strategy q. The set $\mathcal{B}_\beta$ contains only individual constraints for the vector components of b. In ⟨3.16⟩, we stated that the secrecy rate $\widetilde{R}_S$ is

monotonically decreasing in each component of the vector b. Thus, the worst-case secrecy rate $\min_{b\in\mathcal{B}_\beta} \widetilde{R}_S(a,b,q)$ is given by $\widetilde{R}_S(a,\beta,q)$ for all $q \in \mathcal{Q}$. Due to this monotonicity, the lowest bounds are obtained if β is chosen such that it fulfills the sum constraint of the set $\mathcal{B}$ with equality. This characterization of the worst-case secrecy rate for the bounds simplifies the outer maximization. We can apply the waterfilling solution in ⟨2.29⟩, which was derived for the multi-carrier scenario, to calculate the optimal transmit strategy q for the bounds. In this case, it is optimal to use full power P, since this waterfilling solution allocates only non-zero values to those components of the vector q where the relation between the channels ensures that the resulting rate monotonically increases in these q_ℓ.

An interesting special case is given by a uniform allocation over the first J' components of β, which simultaneously are the only non-zero components of this vector, where J' is chosen such that $J' \in \{1,2,\ldots,J\}$. Thus, we get vectors $\beta = (\beta_\ell)_{\ell=1}^L$ with

$$\forall \ell \in \{1,2,\ldots,J'\}: \quad \beta_\ell = \frac{\chi}{J'} \quad \text{and} \quad \forall \ell \in \{J'+1, J'+2, \ldots, L\}: \quad \beta_\ell = 0.$$

In the discussion of the low- and high-SNR performance, we will later see that such an allocation can yield tight bounds on the maximized worst-case secrecy rate in these regimes.

⟨**3.30**⟩ **Lower Bounds.** In order to apply the same approach for the derivation of lower bounds, we have to use a set $\mathcal{B}^+ \supseteq \mathcal{B}$ that relaxes the constraints given by the set $\mathcal{B}$. If we want to use $\mathcal{B}^+ := \mathcal{B}_\beta$, we have to specify an appropriate vector β such that $b \in \mathcal{B}_\beta$ is guaranteed for all $b \in \mathcal{B}$. Thus, one possible lower bound can be derived with $\beta = (\chi)_{\ell=1}^L$. But we cannot expect that this choice provides a good lower bound since this vector allows much more "powerful" eavesdropper channels than the original set $\mathcal{B}$. We can exploit the structure of the optimal vector b according to ⟨3.23⟩ to improve this approach. Initially, we need a set $\mathcal{B}' \subset \mathcal{B}$ that fulfills

$$\min_{b\in\mathcal{B}'} \widetilde{R}_S(a,b,q) = \min_{b\in\mathcal{B}} \widetilde{R}_S(a,b,q)$$

for all $q \in \mathcal{Q}$. Then, it is sufficient to use a set $\mathcal{B}^+$ with $\mathcal{B}^+ \supseteq \mathcal{B}'$ for the derivation of a lower bound, even if we have $\mathcal{B}^+ \not\supseteq \mathcal{B}$. Such a set is given by $\mathcal{B}_\beta$, where the vector $\beta = (\beta_\ell)_{\ell=1}^L$ is specified by

$$\forall \ell \in \{1,2,\ldots,J\}: \quad \beta_\ell = \frac{\chi}{\ell} \quad \text{and} \quad \forall \ell \in \{J+1, J+2, \ldots, L\}: \quad \beta_\ell = 0.$$

Nevertheless, this will not significantly improve the lower bounds that can be obtained by modifying the inner minimization problem.

Thus, we now focus on the derivation of lower bounds by changing the constraint set of the outer maximization problem as shown in ⟨3.27⟩. Using a set $\mathcal{Q}^- \subseteq \mathcal{Q}$ instead of $\mathcal{Q}$ adds further constraints to the outer problem, which yields a lower bound on the maximized worst-case secrecy rate. Simple lower bounds can be obtained with $\mathcal{Q}^- := \dot{\mathcal{Q}}_\iota$,

where ι is an arbitrary vector with $\iota \in \mathcal{Q}$. Obviously, the optimal transmit strategy q is now independent from b and $\max_{q \in \dot{\mathcal{Q}}_\iota} \min_{b \in \mathcal{B}} \widetilde{R}_S(a,b,q)$ equals $\min_{b \in \mathcal{B}} \widetilde{R}_S(a,b,\iota)$, which corresponds to the calculation of the worst-case secrecy rate for a fixed power allocation vector $\iota \in \mathcal{Q}$. Thus, the lower bound can simply be obtained by applying the waterfilling solution that was derived for the inner problem in ⟨3.21⟩. Note that a good lower bound provides a power allocation strategy that results in a nearly optimum worst-case secrecy rate. The transmitter can simply choose the power allocation ι that was used for the derivation of this lower bound.

Again, an interesting special case are vectors ι whose only non-zero components are determined by a uniform allocation over these components. Exploiting the ordering of the optimal vector q according to ⟨3.23⟩, we would allocate these non-zero values to the first L' components of ι, where L' is chosen such that $L' \in \{1, 2, \ldots, L\}$. In the discussion of the low- and high-SNR performance, we will later see that such an allocation can yield tight bounds on the maximized worst-case secrecy rate in these regimes.

In order to characterize the optimal strategies for high and low SNR, we take the same approach as before and interpret $\widetilde{R}_S$ in ⟨3.12⟩ as a function of the inverse noise variance ρ for a fixed value of P.

⟨**3.31**⟩ **High-SNR Performance.** For the high-SNR regime, we calculate the limit for the secrecy rate $\widetilde{R}_S$, which is

$$\lim_{\rho \to \infty} \widetilde{R}_S(a,b,q) = \left[\lim_{\rho \to \infty} \sum_{\ell=1}^{L} \log_2 \left(\frac{1 + \rho\, a_\ell q_\ell}{1 + \rho\, b_\ell q_\ell} \right) \right]^+ = \left[\sum_{\ell \in \mathcal{L}} \log_2 \left(\frac{a_\ell}{b_\ell} \right) \right]^+,$$

where

$$\mathcal{L} := \{ \ell \in \{1, 2, \ldots, L\} \,|\, q_\ell > 0 \}$$

is the set of vector components that is used for the transmission to Bob. Obviously, this limit exists if and only if $b_\ell > 0$ holds for all $\ell \in \mathcal{L}$. If we consider the worst-case maximization of this high-SNR limit, we see that the optimal vector b, which corresponds to the worst-case channel to the eavesdropper, has positive components at exactly the same positions as the transmit power allocation vector q, i.e., $b_\ell > 0$ holds for all $\ell \in \mathcal{L}$, whereas $b_\ell = 0$ holds for all $\ell \notin \mathcal{L}$. Furthermore, we see that the optimal strategy for b converges to a uniform allocation over these vector components, i.e.,

$$\forall \ell \in \mathcal{L} : \; b_\ell = \frac{\chi}{|\mathcal{L}|}.$$

The maximum of this worst-case high-SNR limit is not directly influenced by the values chosen for the components of the power allocation vector q, but it is relevant which vector components are used for the transmission. Since we assumed that the components of the

vector a are decreasingly ordered, we can state with ⟨3.23⟩ that $q_1 \geq q_2 \geq \ldots \geq q_{L'} > 0$ and $q_{L'+1} = q_{L'+2} = \ldots = q_L = 0$ hold for the optimal vector q. Thus, the remaining problem in the high-SNR regime is

$$\max_{L'} \left[\sum_{\ell=1}^{L'} \log_2 \left(a_\ell \, \frac{L'}{\chi} \right) \right]^+$$

with $L' \in \{1, 2, \ldots, J\}$, which is to determine the optimal number L' of positive components in the vector q. If we treat this worst-case high-SNR limit as a function of L', we can state that its behavior significantly depends on the values of the vector a, which characterizes the channel between Alice and Bob. Let us consider the above sum for a certain L' and $L'+1$: The worst-case high-SNR limit increases by adding the $(L'+1)$-th term to the sum if and only if

$$\log_2 \left(\frac{a_{L'+1}}{\chi} \right) > L' \log_2 L' - (L'+1) \log_2 (L'+1)$$

is fulfilled. Hence, the worst-case high-SNR limit is not necessarily increasing or unimodal in L', and we have to search over the complete set specified for L' to find the global maximum.

⟨**3.32**⟩ **Low-SNR Performance.** As expected, the limit of the secrecy rate $\widetilde{R}_S$ is

$$\lim_{\rho \to 0} \widetilde{R}_S(a, b, q) = 0$$

in the low-SNR regime. Thus, we consider the linear Taylor series representation of $\widetilde{R}_S$ at the point $\rho = 0$, which is

$$T_{\widetilde{R}_S}(\rho; 0) = \left[\frac{1}{\ln 2} \sum_{\ell \in \mathcal{L}} (a_\ell - b_\ell) \, q_\ell \, \rho \right]^+$$

with $\mathcal{L}$ as defined in ⟨3.31⟩. The worst-case maximization of this linear Taylor series representation is a (nested) linear programming problem. The optimal vector b, which corresponds to the worst-case channel to the eavesdropper, has only one positive component. The value χ is assigned to the vector component that corresponds to the largest component of the transmit power allocation vector q. With the vector ordering from ⟨3.22⟩ and ⟨3.23⟩, we can write $b_1 = \chi$ and $b_2 = b_3 = \ldots = b_L = 0$ for the optimal b. The optimal transmit power allocation vector q, which maximizes the worst-case linear Taylor coefficient, uses a uniform allocation of the complete sum power P over the first L' components of the vector q, i.e., $q_1 = q_2 = \ldots = q_{L'} = \frac{P}{L'}$ and $q_{L'+1} = q_{L'+2} = \ldots = q_L = 0$. The corresponding derivation is provided in ⟨B.3⟩ in the appendix. The remaining problem in the low-SNR regime consequently is

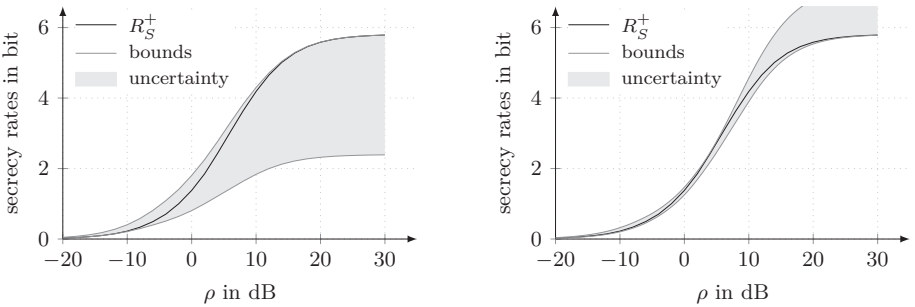
$$\max_{L'} \left[\frac{1}{\ln 2} \left(\left(\sum_{\ell=1}^{L'} a_\ell \right) - \chi \right) \frac{P}{L'} \, \rho \right]^+$$

with $L' \in \{1, 2, \ldots, J\}$, which is to determine the optimal number L' of positive components in the vector q. Now we want to interpret the above worst-case linear Taylor coefficient as a function of L'. This coefficient is either increasing or decreasing or unimodal in L'. Hence, we can start the search for the global maximum with $L' = 1$, increment it if and only if

$$a_{L'+1} > \frac{1}{L'} \left(\left(\sum_{\ell=1}^{L'} a_\ell \right) - \chi \right),$$

which will lead to a higher rate than obtained before, and stop this process as soon as the condition above is not satisfied any more being sure that we found the global maximum.

⟨**3.33**⟩ **Illustration (Bounds).** For the illustration of the results we obtained so far, we consider a scenario, where Alice and Bob have four antennas each, i.e., we have $L = M = 4$. We assume that Eve has at least the same number of antennas. We can set $N = 4$ for our worst-case discussion since we know that this number will be sufficient if Eve has found the worst-case MIMO channel G. The MIMO channel H between Alice and Bob is characterized by the eigenvalues a of its Gramian matrix $A = H^{\mathrm{H}}H$. These eigenvalues shall be given by $a = (3.9, 1.5, 1.0, 0.6)$. Alice aims to maximize the worst-case secrecy rate under a transmit power constraint, which is specified by $P = 1$. She looks for the optimal eigenvalues q of her transmit covariance matrix Q under this constraint. The norm constraint on the channel matrix G for the channel from Alice to Eve is specified by $\chi = 2$. According to ⟨3.12⟩, this corresponds to a sum constraint on the eigenvalues b of the Gramian matrix $B = G^{\mathrm{H}}G$.



(a) $\beta = \left(\frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}\right)$ and $\beta = \left(\chi, \frac{\chi}{2}, \frac{\chi}{3}, \frac{\chi}{4}\right)$

(b) $\beta = \chi \frac{a}{\|a\|_1}$ and $\iota = P \frac{a}{\|a\|_1}$

Figure 3.4: Upper and lower bounds on the maximized worst-case secrecy rate R_S^+ and the remaining uncertainty regions between the bounds.

Figure 3.4 shows upper and lower bounds on the maximized worst-case secrecy rate of this scenario as a function of the SNR, which was changed by a variation of the inverse

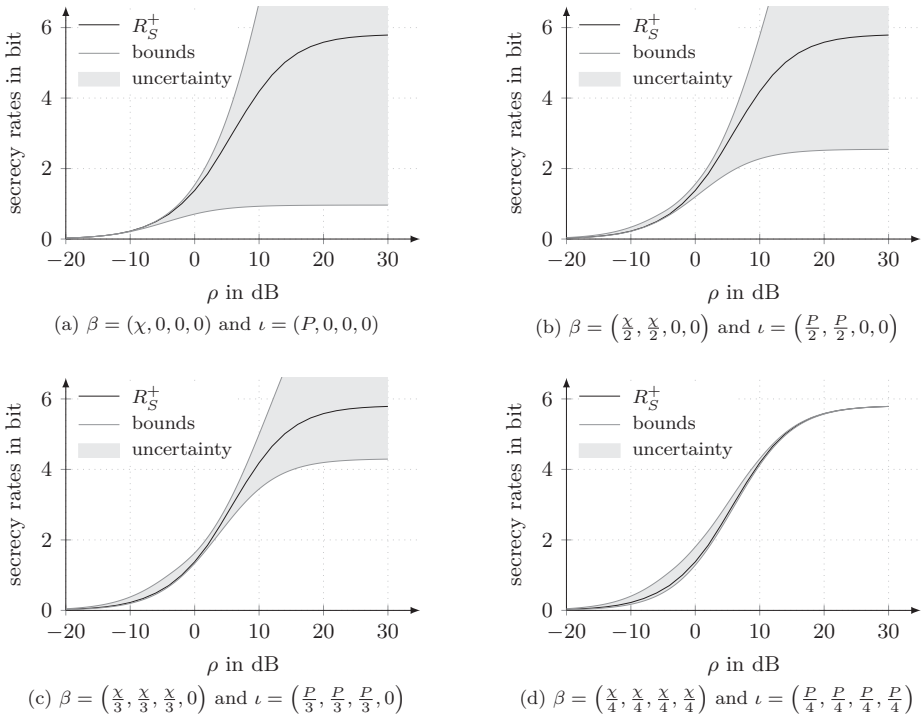
noise variance ρ for fixed P. The area between the upper and lower bound is called uncertainty region. The maximized worst-case secrecy rate, which is denoted by R_S^+, is also included in the diagrams. Strictly speaking, it is an approximation, which was found by exhaustive search over all possible power allocation vectors q whose components are ordered according to $\langle 3.23 \rangle$, where we used a step size of 0.050 for each component.

For (a), the upper and lower bound were derived by manipulating the inner minimization according to $\langle 3.27 \rangle$, i.e., using a set $\mathcal{B}_\beta$ instead of the set $\mathcal{B}$. Due to the characterization of the optimal vector b in $\langle 3.25 \rangle$, we used $\beta = \left(\frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}\right)$ and $\beta = \left(\chi, \frac{\chi}{2}, \frac{\chi}{3}, \frac{\chi}{4}\right)$ for the upper and lower bound, respectively. We see that we choose a quite good parametrization for the upper bound. Especially for high SNR, this bound comes very close to the maximized worst-case secrecy rate R_S^+. In contrast, the lower bound is indeed good for low SNR, but the gap between this bound and the rate R_S^+ grows dramatically with increasing SNR, which then results in a large uncertainty about the real value of R_S^+. This behavior was predictable since the components of the vector β add up to $\frac{25}{12}\chi$, which is more than twice of the constraint of the original problem. Thus, we assume for this bound that the channel to the eavesdropper can be much better than it can be in reality. This difference affects especially the high-SNR performance of the bound. We see that this approach is not good enough for the derivation of bounds that leave only a small uncertainty about the real value of the maximized worst-case secrecy rate R_S^+.

For (b), we slightly changed our method. The upper bound was again computed by using a set $\mathcal{B}_\beta$ instead of the set $\mathcal{B}$ for the inner minimization. But the lower bound was obtained by manipulating the outer maximization, i.e., using a set $\dot{\mathcal{Q}}_\iota$ instead of the set $\mathcal{Q}$, which can provide bounds that are closer to the desired value R_S^+. The remaining question is then: What are appropriate choices for the vectors β and ι in order to obtain tight bounds on the maximized worst-case secrecy rate? For the diagram in (b), a scaled version of the eigenvalue vector a was used for both parameters β and ι, i.e., we had $\beta = \chi \frac{a}{\|a\|_1}$ and $\iota = P \frac{a}{\|a\|_1}$. We see that this choice leads to a much better lower bound for our example, but there is a clear gap between the upper bound and the desired value for high SNR.

In the following, we will derive further bounds and always use the following approach: Upper bounds are obtained by additionally constraining the set $\mathcal{B}$ that is used for the inner minimization by using a set $\mathcal{B}_\beta$ with an appropriately chosen vector β. Lower bounds are computed with further constraints on the set $\mathcal{Q}$ that is used for the outer maximization, which corresponds to using a set $\dot{\mathcal{Q}}_\iota$ with an appropriately chosen vector ι. The uncertainty about the real value of the maximized worst-case secrecy rate R_S^+ can be reduced by combining the contributions of multiple upper or lower bounds. For the SNR range of interest, we always look for the minimum upper and the maximum lower bound values.

Simple upper and lower bounds can be derived by assigning equal values to all non-zero components of the vectors β and ι. Following the ordering result for the optimal vectors b



(a) $\beta = (\chi, 0, 0, 0)$ and $\iota = (P, 0, 0, 0)$

(b) $\beta = \left(\frac{\chi}{2}, \frac{\chi}{2}, 0, 0\right)$ and $\iota = \left(\frac{P}{2}, \frac{P}{2}, 0, 0\right)$

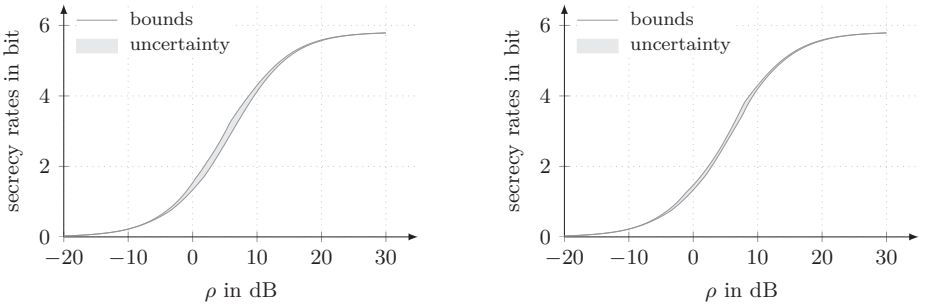
(c) $\beta = \left(\frac{\chi}{3}, \frac{\chi}{3}, \frac{\chi}{3}, 0\right)$ and $\iota = \left(\frac{P}{3}, \frac{P}{3}, \frac{P}{3}, 0\right)$

(d) $\beta = \left(\frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}\right)$ and $\iota = \left(\frac{P}{4}, \frac{P}{4}, \frac{P}{4}, \frac{P}{4}\right)$

Figure 3.5: Upper and lower bounds on the maximized worst-case secrecy rate R_S^+ and the remaining uncertainty regions between the bounds.

and q in $\langle 3.23 \rangle$, the non-zero values should optimally be allocated to the first components of the vectors. In Figure 3.5, such bounds are shown for the example given above, where the number of non-zero components in the vectors β and ι was increased from 1 to 4. The vectors β and ι were chosen such that they fulfill the sum constraints of the sets $\mathcal{B}$ and $\mathcal{Q}$ with equality. From the low-SNR discussion in $\langle 3.32 \rangle$, we know that the optimal b for low SNR has only one non-zero component, which is $b_1 = \chi$. This vector was chosen for the derivation of the upper bound in the diagram in (a). Consequently, we can see that this bound is tight in the low-SNR regime. For high SNR, we have stated in $\langle 3.31 \rangle$ that the optimal b uses a uniform allocation over all components that correspond to non-zero components of the power allocation vector q. In the derivation of the upper bound, b is first fixed and the corresponding optimal q is calculated afterwards. Thus, we cannot guarantee that q uses exactly the same non-zero components as the previously chosen b,

i.e., we not necessarily have a tight upper bound for high SNR with this approach. But if it turns out that the non-zero components of both vectors are the same, we then know that we have a tight upper bound for this SNR regime. If we rather consider the lower bound, the calculation order of the two vectors is altered. We know that only the number of non-zero components of the power allocation vector q is important for the high-SNR behavior and that a uniform allocation over certain components of q results in a uniform allocation over the same components of b, which is optimal here. Hence, we can conclude that one of the upper bounds in Figure 3.5 must be tight for high SNR. Consequently, we can say that the maximum lower bound that is obtained over all possible uniform allocations for q is always tight in this regime.



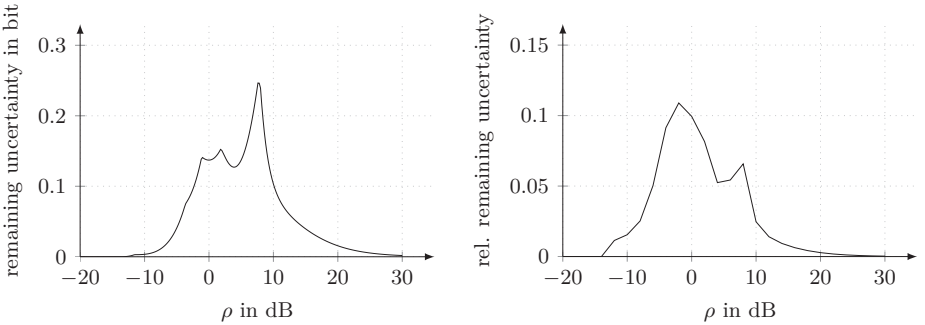
(a) bounds from Figure 3.5

(b) bounds from Figure 3.4 and Figure 3.5

Figure 3.6: Minimum upper and maximum lower bounds on the maximized worst-case secrecy rate R_S^+ and the remaining uncertainty regions between the bounds.

Figure 3.6 shows minimum upper and maximum lower bounds for the example above. In (a), we combined only bounds that were derived with uniform allocations in the context of Figure 3.5. The remaining uncertainty region is only a small corridor over the complete SNR range, i.e., we can specify the value of the maximized worst-case secrecy rate R_S^+ everywhere with only small possible deviations from the real value by calculating and analyzing four simple upper and lower bounds each. Furthermore, the maximum lower bound provides a power allocation strategy that results in a nearly optimum secrecy rate. We can simply choose the power allocation ι that was used for the derivation of the lower bound that is best for the SNR of interest. In (b), we additionally considered the contributions from the bounds in Figure 3.4. These bounds further improve the uncertainty region for medium SNR.

In Figure 3.7, the absolute and relative values of the remaining uncertainty are shown for the minimum upper and maximum lower bounds in Figure 3.6 (b). In (a), we see that the remaining uncertainty, which results from the difference of the upper and lower bounds, tends to zero for low and high SNR. For these regimes, we have a characterization of the

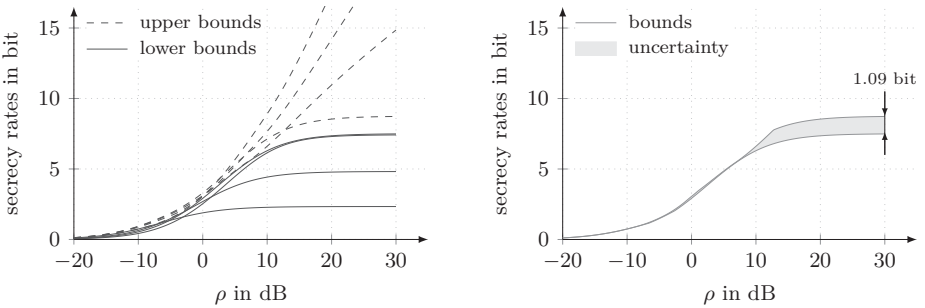


(a) absolute values of remaining uncertainty

(b) relative values of remaining uncertainty

Figure 3.7: Absolute and relative values of the remaining uncertainty between the bounds in Figure 3.6 (b).

optimal strategies, which enables us to choose appropriate parameters for tight bounds. For medium SNR, the uncertainty takes its largest values due to the fact that we do not have an accurate characterization of the optimal strategies for this range. However, the remaining uncertainty is always below about 0.25 bit. Note that this uncertainty can be further reduced if more bounds are evaluated. In addition, the diagram in (b) illustrates the relative values of the remaining uncertainty with respect to the maximized worst-case secrecy rate R_S^+ that we determined for this example. In principle, we observe the same behavior over the SNR. Moreover, we see that the largest deviation from the real value is about 10%.

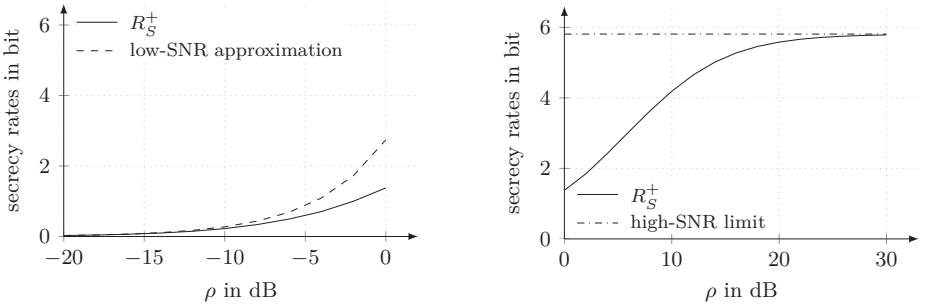


(a) bounds from uniform allocations

(b) remaining uncertainty region

Figure 3.8: Upper and lower bounds on the maximized worst-case secrecy rate R_S^+ and the remaining uncertainty region between the minimum upper and maximum lower bound.

Finally, we consider another example. We slightly modify the scenario studied so far by introducing another eigenvalue vector a for the Gramian matrix A of the MIMO matrix H for the channel from Alice to Bob. This eigenvalue vector is now given by $a = (10.1, 2.8, 1.9, 0.2)$. All other parameters introduced above remain unchanged. The upper and lower bounds that can be calculated with uniform allocations that meet the sum constraints of the corresponding sets with equality and the remaining uncertainty region after evaluating the minimum of the upper and the maximum of the lower bound are shown in Figure 3.8. From (b), we observe that there is a non-vanishing gap between the upper and lower bound for high SNR, which is about 1 bit. This is in contrast to the example above, where we could not observe such a gap. Thus, we have here a larger remaining uncertainty than before. Nevertheless, we can get a good estimate of the maximized worst-case secrecy rate R_S^+ even for high SNR. From the discussion above, we know that the maximum lower bound is not only tight for high SNR, but it also provides the appropriate power allocation strategy to come very close to the maximized worst-case secrecy rate R_S^+ in this regime. Thus, we can conclude that the gap for high SNR is a result of the fact that we do not always get a good upper bound with uniform allocations.



(a) low-SNR approximation (b) high-SNR limit

Figure 3.9: The maximized worst-case secrecy rate R_S^+ with its low-SNR approximation and its high-SNR limit.

⟨**3.34**⟩ **Illustration (High- and Low-SNR Behavior).** We continue the example that was specified by the vector $a = (3.9, 1.5, 1.0, 0.6)$ for the channel from Alice to Bob and that we discussed in detail in ⟨3.33⟩. In Figure 3.9, the optimized low-SNR approximation from ⟨3.32⟩ and the maximized worst-case limit according to ⟨3.31⟩ are shown for this scenario. We observe that the optimized low-SNR approximation is very close to the maximized worst-case secrecy rate R_S^+ if the SNR is less than -10 dB. If the SNR goes beyond this point, the approximation grows faster than the original function resulting in an increasing gap between both functions. For the high-SNR regime, we see that the maximized worst-case secrecy rate R_S^+ converges to the maximized worst-case limit we calculated before. Beyond 20 dB, it is already close to this limit.

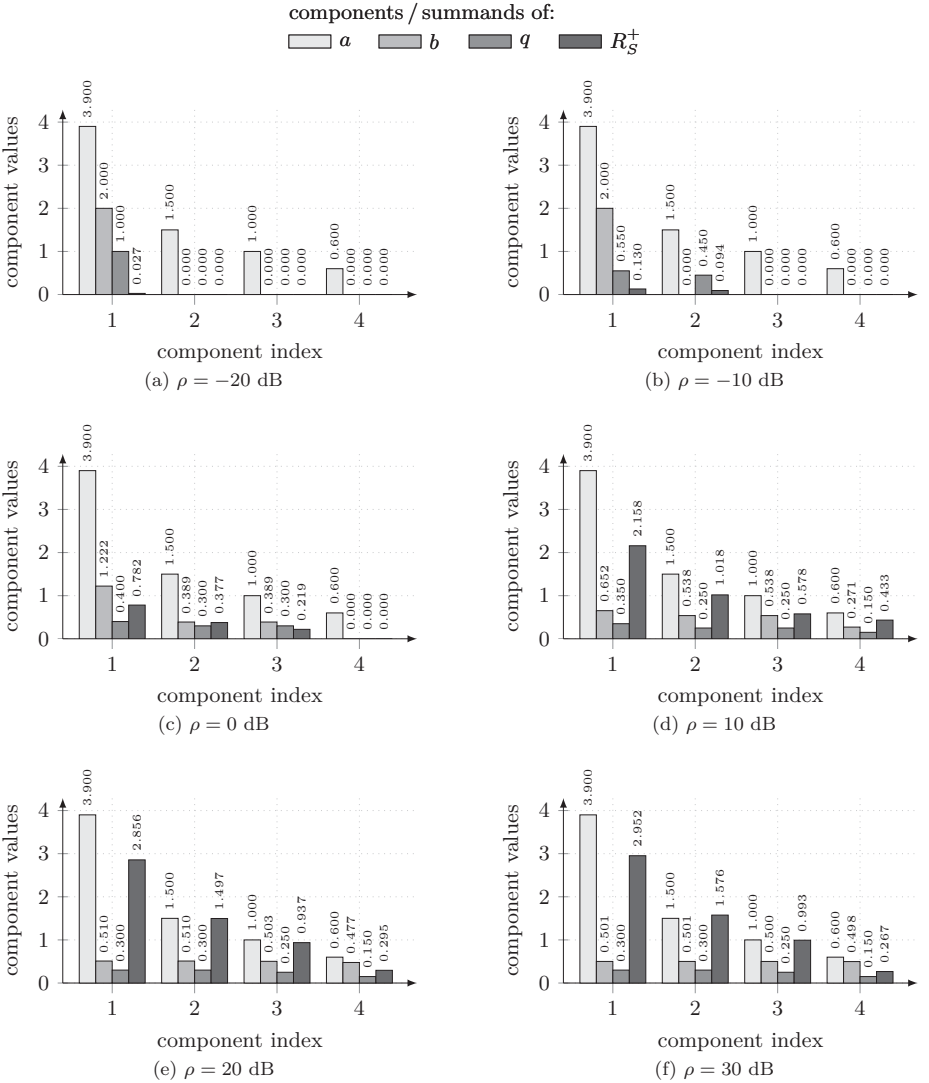
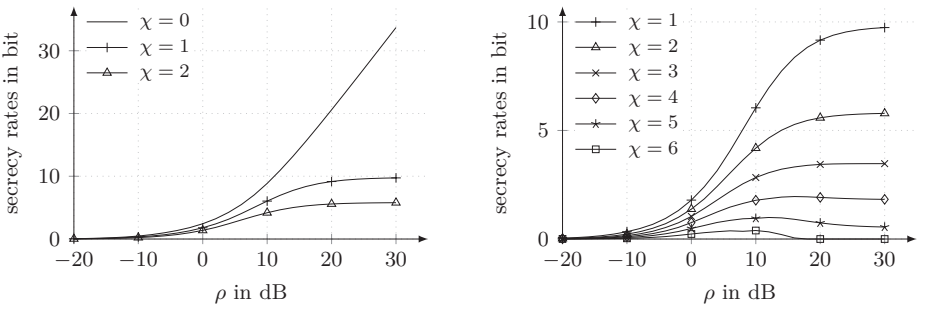


Figure 3.10: Optimal vectors corresponding to the maximized worst-case secrecy rate R_S^+ for selected SNR values.

⟨**3.35**⟩ **Illustration (Optimal Strategies).** We continue the main example from ⟨3.33⟩. As already stated above, the maximized worst-case secrecy rate R_S^+, which we wanted to use for some comparisons, was found by an exhaustive search. Now, we want to have a closer look on these results in detail. The channel from Alice to Bob was characterized by a four-value vector, which was given by $a = (3.9, 1.5, 1.0, 0.6)$. Alice aims to find the optimal power allocation vector q that maximizes the worst-case secrecy rate under the assumption that Eve can always find the corresponding worst-case channel, which is characterized by the vector b. With these vectors, the resulting maximized worst-case secrecy rate can be calculated. The values of each component index contribute to exactly one term in the sum of the overall secrecy rate, which can be seen in ⟨3.12⟩. In Figure 3.10, the values of the optimal vectors and the resulting secrecy rate summands are shown for selected SNR values. Now, we can see the predicted low- and high-SNR behavior in detail. From the analysis in ⟨3.32⟩, it follows that the optimal vector b, which corresponds to the worst-case channel from Alice to Eve, always has only one non-zero component for low SNR, i.e., $b_1 = \chi$. For our example, we can observe this behavior for $\rho = -20$ dB and -10 dB in the diagrams in (a) and (b). The corresponding power allocation vector q shows a different behavior for these cases. For $\rho = -20$ dB, the worst-case secrecy rate is maximized by allocating full power P to the first component of q, whereas the optimal q for $\rho = -10$ dB uses the first two components with nearly the same power. With increasing SNR, the number of non-zero components in both vectors grows first to 3 and later to 4, which can be seen in the diagrams in (c) and (d). For $\rho = 20$ dB and 30 dB, we can observe in (e) and (f) the high-SNR behavior we predicted in ⟨3.31⟩. The worst-case vector b has non-zero components at exactly the same positions as the power allocation vector q. Furthermore, we see that the optimal strategy for b tends to a uniform allocation over these components. Here, all components of both vectors are used. Note that it is not necessarily optimal for an arbitrary set of parameters to set all components of the vector q to non-zero values.

⟨**3.36**⟩ **Illustration (Variation of Channel Constraint).** We continue the example above by analyzing the influence of the parameter χ, which constrains the quality of the channel from Alice to Eve. In Figure 3.11, the maximized worst-case secrecy rate R_S^+ is shown for various values of χ. As expected, an increase in χ, which allows the eavesdropper channel to be more "powerful", reduces the finally obtained secrecy rates. For high SNR, the influence of the channel constraint parameter χ is more noticeable than for low SNR. The case $\chi = 0$ in (a) represents a scenario without eavesdropper or without secrecy constraints. Then, the optimal power allocation strategy is given by standard waterfilling, which was presented by Telatar (1995). Below $\rho = 0$ dB, the curves for $\chi = 0, 1$ and 2 do not differ much from each other. With growing SNR, the gaps between the curves increase. In the high-SNR regime, the gap between the curves for $\chi = 1$ and 2 remains nearly constant. It represents the difference between the high-SNR limits for these cases. In contrast, the curve for the case $\chi = 0$ grows with increasing SNR, which results in an increasing gap between the cases with and without secrecy constraints.



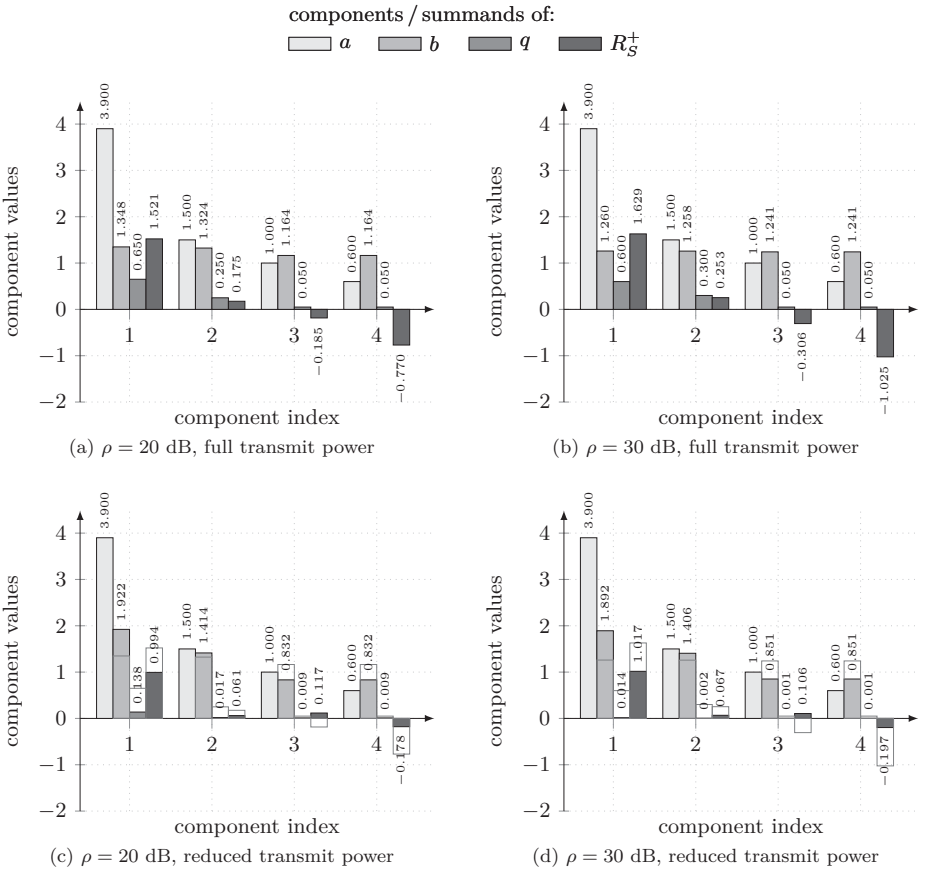
(a) comparison with / without secrecy constraints

(b) influence of channel constraint parameter χ

Figure 3.11: The maximized worst-case secrecy rate R_S^+ that was found for various values of the constraint parameter χ for the channel from Alice to Eve.

For all curves in Figure 3.11, it is assumed that the transmitter uses full power P. In the exhaustive search for the maximized worst-case secrecy rate, only the allocation of this power to the components of q was changed. In (b), it can be observed for $\chi \geq 4$ that the maximum worst-case secrecy rate that was found by this search does not continously grow with increasing SNR. It is only an increasing function until a certain point, whose position varies with the chosen parameters. If the SNR grows beyond this point, the rate even decreases. This is not a very common behavior. Usually, it is expected that a (secrecy) rate grows with the SNR. The reason for this behavior is the joint encoding approach, where full power is not necessarily optimal to maximize the worst-case secrecy rate. Depending on the parameters for the channel to Bob and the value that was chosen for the constraint parameter χ for the channel to Eve, it can indeed be advantageous to reduce the transmit power.

⟨**3.37**⟩ **Illustration (Power Scaling).** We continue our example and focus now on the case where the constraint parameter for the quality of the channel from Alice to Eve is given by $\chi = 5$. Thus, the eavesdropper channel is significantly more "powerful" than before, but still less "powerful" than the main channel from Alice to Bob, which makes a secure communication from Alice to Bob possible. In Figure 3.11, we saw the maximized worst-case secrecy rate that can be found if full power is assumed to be used at the transmitter. For this example, we observe the following behavior with growing SNR: The rate increases until a certain point, which is approximately located at $\rho = 12$ dB, and decreases if the SNR grows beyond this point. Now, we want to have a more detailed look at the strategies chosen for high SNR. Figure 3.12 shows the best power allocation vector q, the corresponding worst-case vector b, and the resulting secrecy rate summands for $\rho = 20$ dB and 30 dB, which were found by an exhaustive search for the example with the eavesdropper channel constraint set to $\chi = 5$. For the diagrams in (a) and (b), we used



(a) $\rho = 20$ dB, full transmit power

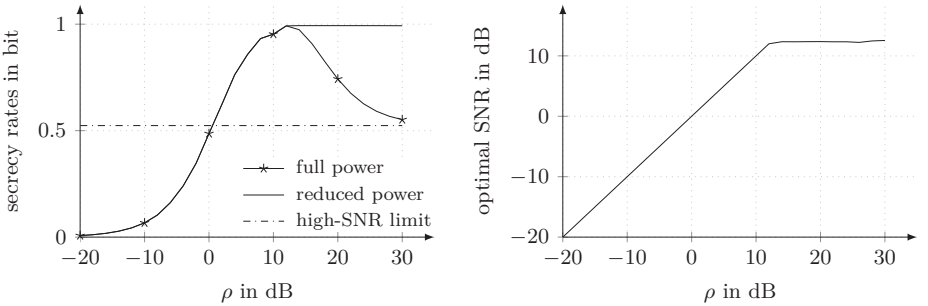
(b) $\rho = 30$ dB, full transmit power

(c) $\rho = 20$ dB, reduced transmit power

(d) $\rho = 30$ dB, reduced transmit power

Figure 3.12: Optimal vectors corresponding to the maximized worst-case secrecy rate R_S^+ that was found for selected SNR values.

full power at the transmitter. We know and observe for high SNR that the worst-case strategy, which is given by the vector b, converges to a uniform allocation over all vector components that correspond to non-zero components of the power allocation vector q. If the value that is consequently assigned to b_ℓ is greater than the corresponding value a_ℓ of the main channel, i.e., we have $b_\ell > a_\ell$ for an arbitrary $\ell \in \{1, 2, \ldots, J\}$, the resulting secrecy rate summand will be negative. This can occur if the parameters are given such that $a_J < \frac{\chi}{J}$. Then, the transmitter has the choice (i) to use the first J components of the vector q for the transmission knowing that the positive contribution from the components with $a_\ell > b_\ell$ will exceed the negative contribution resulting from the components with $a_\ell < b_\ell$ or (ii) to reduce the number of components of the vector q that are used for the transmission, which simultaneously allows the eavesdropper to concentrate the values allocated for its worst-case channel only on these components, which in turn results in higher values there and consequently decreases the possible positive contributions from these components. The drawbacks of these cases are the following: Firstly, it is not guaranteed that we can find a situation with $a_\ell > b_\ell = \frac{\chi}{L'}$ for all components $\ell \in \{1, 2, \ldots, L'\}$ by reducing the number $L' \in \{1, 2, \ldots, L\}$ of non-zero components of the vector q. Such a situation is given in our example in Figure 3.12. Secondly, the characteristic of the logarithm function works against the approach of compensating negative summands in the secrecy rate expression by positive ones for high SNR. The logarithm function is not only monotonically increasing but also concave in the SNR. Thus, a growing SNR amplifies negative terms much more than positive terms. Hence, it is possible to have a situation where it is not desirable to further increase the SNR.



(a) worst-case secrecy rates for full and reduced transmit power

(b) optimal SNR in dB

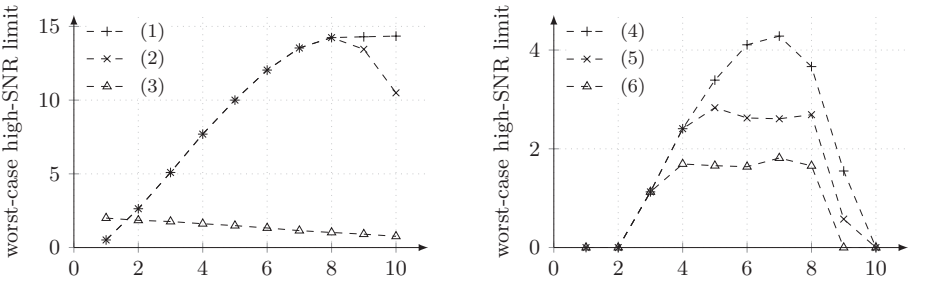
Figure 3.13: The maximized worst-case secrecy rate R_S^+ that was found with full and reduced transmit power and the corresponding optimal SNR for the power reduction.

From the discussion above, we see that it is not necessarily optimal to use full transmit power, especially for high SNR. If we allow Alice to reduce the transmit power if necessary, she can avoid to operate in the high-SNR regime in such a case and obtain higher secrecy

rates with this reduced transmit power than she would obtain with full power. For the illustrations in Figure 3.12 (c) and (d), we have taken the same setting as for (a) and (b), but we additionally allowed the transmitter to reduce its transmit power, which can yield a higher worst-case secrecy rate than before. We observe that Alice avoids to operate in the high-SNR regime in this example. For $\rho = 20$ dB, she reduces her transmit power to approximately one-sixth of the available power. For $\rho = 30$ dB, the transmit power is further reduced to about one-fiftieth of the maximum value P. We see that the transmitter tries to fix the SNR to roughly 12 dB, which yields the maximum worst-case secrecy rate for this example. Comparing the two cases with full and reduced transmit power, we further see that the optimal transmit strategy is chosen such that a uniform worst-case assignment for the vector b is avoided. For components that correspond to a higher value in the vector a for the main channel, more power is allocated than for components with a corresponding smaller value in a. Due to the reduction of the overall transmit power, we obtain less from the components with a positive contribution to the secrecy rate, but we simultaneously avoid or significantly reduce the negative contribution from the other components. Finally, the resulting worst-case secrecy rate, which is obtained by adding all these summands, is greater than the secrecy rate that was obtained before with full power. In Figure 3.13 (a), the worst-case secrecy rates for $\chi = 5$ can be compared for the cases with full and reduced transmit power. The corresponding optimal SNR, which is adjusted by reducing the transmit power for growing ρ, is shown in (b). We see that both secrecy rates are identical up to about $\rho = 12$ dB. Beyond this point, the rate for full transmit power decreases as already observed before, while the worst-case secrecy rate for reduced transmit power stays approximately constant. Note that the rate with full transmit power converges to the calculated high-SNR limit, while the curve for the secrecy rate with reduced transmit power remains above this limit by avoiding to be in the high-SNR regime.

⟨**3.38**⟩ **Illustration (High-SNR Limit).** In ⟨3.31⟩, we discussed the high-SNR behavior of the worst-case secrecy rate. We derived an expression for the worst-case high-SNR limit of the secrecy rate, which depends on the number L' of positive values in the chosen power allocation vector q. Figure 3.14 shows this limit as a function of L' with $L' \in \{1, 2, \ldots, 10\}$ for various parameter sets, which are given below the diagrams. These sets were chosen to illustrate that the different behavior of this function significantly depends on the given parameters.

In (a), we have positive values for the worst-case high-SNR limit over the complete range specified for L', but we see that we can obtain for instance an increasing as well as a unimodal or decreasing function of L', which corresponds to the parameter sets given by (1), (2), and (3), respectively. In (b), we see that the worst-case high-SNR limit is not necessarily positive over the complete range given for L'. Moreover, we observe unimodal and bimodal behavior of the function, which results from the parameter sets (4) and (5) / (6), respectively. For the latter cases, the global maximum of the function is achieved for different values of L'. For the parameters in (5), the first local maximum



(a) $\chi = 20$ (b) $\chi = 50$

	χ	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
(1)	20	28.6	21.7	16.3	12.8	8.1	5.5	3.2	1.6	0.9	0.8
(2)	20	28.6	21.7	16.3	12.8	8.1	5.5	3.2	1.6	0.5	0.1
(3)	20	80.0	4.5	2.8	1.9	1.5	1.2	1.0	0.9	0.8	0.7
(4)	50	28.6	21.7	16.3	12.8	8.1	5.5	3.2	1.6	0.5	0.1
(5)	50	28.6	21.7	16.3	12.8	5.5	2.9	2.8	2.6	0.5	0.1
(6)	50	28.6	21.7	16.3	7.8	4.0	3.3	3.2	2.2	0.5	0.1

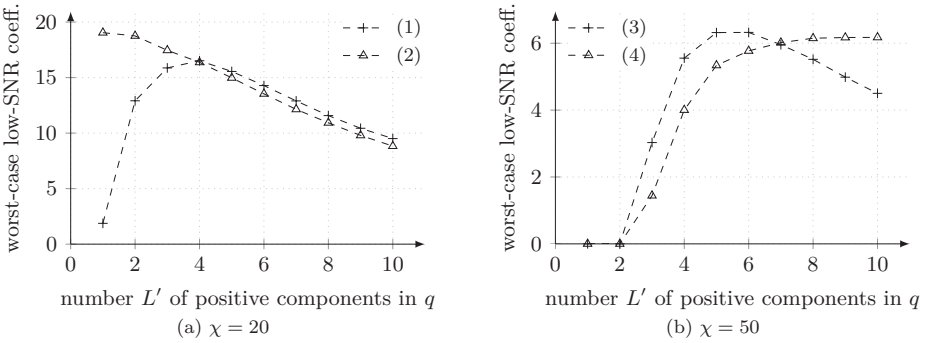
Figure 3.14: The worst-case high-SNR limit as a function of the number L' of positive components in the power allocation vector q.

simultaneously is the global maximum, whereas the second local maximum provides the largest worst-case high-SNR limit for the parameters in (6).

⟨**3.39**⟩ **Illustration (Low-SNR Approximation).** In ⟨3.32⟩, we discussed the low-SNR behavior of the worst-case secrecy rate. We derived an expression for the linear Taylor series coefficient of the worst-case secrecy rate in the low-SNR regime, which depends on the number L' of positive values in the chosen power allocation vector q. Figure 3.15 shows this coefficient as a function of L' with $L' \in \{1, 2, \ldots, 10\}$ for various parameter sets, which are given below the diagrams. These sets were chosen to illustrate the different behavior of this function depending on the given parameters.

We noticed that this coefficient is unimodal in L' in general, which simplifies the search for its global maximum as explained in ⟨3.32⟩. We observe this behavior for the parameter sets (1) and (3). The parameter sets (2) and (4) illustrate the possible special cases, which are a monotonically decreasing or increasing behavior over the complete range. Additionally, we see in (b) that the calculated coefficients are not necessarily positive[9] over the complete range given for L'.

[9] Originally negative coefficients, which would lead to a zero worst-case secrecy rate approximation, are set to zero in this illustration.



	χ	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
(1)	20	21.3	16.6	15.1	12.8	8.1	5.5	3.2	1.6	0.9	0.8
(2)	20	33.2	12.8	10.3	9.1	6.5	4.4	2.6	1.7	0.5	0.1
(3)	50	33.2	12.8	10.3	9.1	6.5	4.4	2.6	1.7	0.5	0.1
(4)	50	21.3	16.6	15.1	8.1	7.4	5.5	5.2	4.9	4.4	4.3

Figure 3.15: The linear Taylor series coefficient of the worst-case secrecy rate approximation in the low-SNR regime as a function of the number L' of positive components in the power allocation vector q.

3.3 Worst-Case Optimization for Transmitters with Parallel Encoding

In this section, we analyze the properties of the eigenvalue problem in ⟨3.12⟩ with an alternative secrecy rate expression, which results from a transmitter structure that is better adapted to the characteristics of the optimization problem. For this adapted problem, we derive the optimal strategy for the inner problem and characterize the optimal strategy for the outer problem. We present lower and upper bounds on the resulting maximized worst-case secrecy rate and discuss its low- and high-SNR behavior. All results are compared to the corresponding results from the previous section.

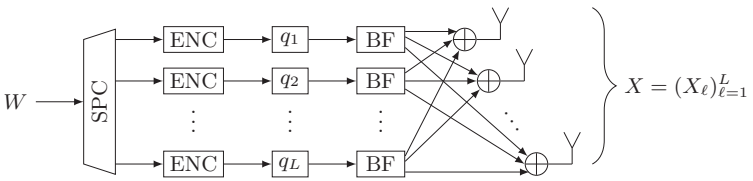


Figure 3.16: Structure of multi-antenna transmitter with parallel wiretap encoders.

We consider a multi-antenna transmitter with L parallel wiretap encoders, which is illustrated in Figure 3.16. The binary representation of the message can be split up in at most L parallel streams. Each of these information streams is encoded with an individual rate that results from the optimization problem that is analyzed in this section. Afterwards, certain weighting factors and beamforming vectors are applied to the encoded data streams as described before in the context of Figure 3.2. The main difference between the transmitters in Figure 3.2 and Figure 3.16 is the order of the serial-to-parallel conversion and the wiretap encoding. The transmitter in Figure 3.16 exploits the fact that the optimal eigenvectors for the original matrix problem in ⟨3.6⟩ diagonalize this problem, i.e., it can be equivalently expressed as a vector problem over the eigenvalues of the involved matrices. This diagonalization process yields up to L independent parallel channels between transmitter and receiver (or eavesdropper), which can be encoded individually with an appropriately adapted rate.

⟨**3.40**⟩ **Problem Formulation (Worst-Case Secrecy Rate Maximization).** For the system model in ⟨3.1⟩ and the adapted transmitter structure in Figure 3.16, the adapted secrecy rate expression for the eigenvalue problem is given by

$$\bar{R}_S(a,b,q) := \sum_{\ell=1}^{L} \left[\,\bar{\varphi}(a_\ell, b_\ell, q_\ell)\right]^+ \quad \text{with}$$
$$\bar{\varphi}(a_\ell, b_\ell, q_\ell) := \log_2\left(1+\rho\, a_\ell q_\ell\right) - \log_2\left(1+\rho\, b_\ell q_\ell\right).$$

The worst-case secrecy rate for this case is defined as

$$\bar{R}_{\mathrm{W}}(a,q) := \min_{b\in\mathcal{B}} \bar{R}_S(a,b,q) = \min_{b\in\mathcal{B}} \sum_{\ell=1}^{L} \left[\,\bar{\varphi}(a_\ell, b_\ell, q_\ell)\right]^+ .$$

The complete problem can be formulated as follows: For a given vector a, the worst-case secrecy rate $\bar{R}_{\mathrm{W}}$ should be maximized under a sum power constraint over all antennas at the transmitter, i.e.,

$$\max_{q\in\mathcal{Q}} \bar{R}_{\mathrm{W}}(a,q) = \max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \bar{R}_S(a,b,q) = \max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \sum_{\ell=1}^{L} \left[\,\bar{\varphi}(a_\ell, b_\ell, q_\ell)\right]^+ .$$

The constraint sets for these problems remain unchanged, i.e., they are given in ⟨3.12⟩.

In contrast to the secrecy rate expression $\widetilde{R}_S$, which was analyzed in the previous section, the secrecy rate $\bar{R}_S$ of the adapted problem corresponds to the secrecy rate of the multi-carrier scenario that was presented in 2.2. Thus, we can directly apply its properties to the problem above.

⟨**3.41**⟩ **Properties (Positivity of Secrecy Rate Summands).** From ⟨2.23⟩, we know that a secrecy rate summand $\bar{\varphi}(a_\ell, b_\ell, q_\ell)$ with $\ell \in \{1, 2, \ldots, L\}$ is only positive if $a_\ell > b_\ell$

holds. The application of the $[\cdot]^+$ function in the adapted secrecy rate expression $\bar{R}_S$ ensures that these secrecy rate summands cannot become negative. Consequently, we can conclude that the optimal worst-case strategy always fulfills

$$\forall \ell \in \{1, 2, \ldots, L\} : \quad b_\ell \in [0, a_\ell] \, .$$

Exploiting the properties above, we can formulate an equivalent optimization problem.

⟨**3.42**⟩ **Problem Formulation (Equivalent Problem).** The problem in ⟨3.40⟩ can be equivalently formulated as

$$\max_{q \in \mathcal{Q}} \bar{R}_{\mathrm{W}}(a, q) = \max_{q \in \mathcal{Q}} \min_{b \in \bar{\mathcal{B}}} \bar{R}_S(a, b, q) = \max_{q \in \mathcal{Q}} \min_{b \in \bar{\mathcal{B}}} \sum_{\ell=1}^{L} \bar{\varphi}(a_\ell, b_\ell, q_\ell),$$

where the constraint set $\bar{\mathcal{B}}$ with $\bar{\mathcal{B}} \subset \mathcal{B}$ is defined as

$$\bar{\mathcal{B}} := \left\{ b = (b_\ell)_{\ell=1}^{L} \in \mathbb{R}^{1 \times L} \;\middle|\; 0 \leq b_\ell \leq a_\ell \text{ and } \sum_{\ell=1}^{L} b_\ell \leq \chi \right\}.$$

With this characterization, we can relate this problem to the original eigenvalue problem in ⟨3.12⟩:

$$\max_{q \in \mathcal{Q}} \min_{b \in \bar{\mathcal{B}}} \bar{R}_S(a, b, q) = \max_{q \in \mathcal{Q}} \min_{b \in \bar{\mathcal{B}}} \widetilde{R}_S(a, b, q) \geq \max_{q \in \mathcal{Q}} \min_{b \in \mathcal{B}} \widetilde{R}_S(a, b, q).$$

For this relation we exploited two facts: (i) The two objective functions $\bar{R}_S$ and $\widetilde{R}_S$ are identical for all $b \in \bar{\mathcal{B}}$, and (ii) relaxing the constraints for the minimization by using the set $\mathcal{B}$ instead of $\bar{\mathcal{B}}$ can only decrease the resulting value of the optimization problem.

⟨**3.43**⟩ **Properties (Monotonicity and Convexity).** We can directly adopt the properties of the secrecy rate from the multi-carrier scenario in 2.2. If we consider the properties with respect to the vector $b \in \bar{\mathcal{B}}$, we will not observe any difference to the properties we derived for the secrecy rate expression in ⟨3.16⟩ and ⟨3.17⟩ in the previous section. The secrecy rate $\bar{R}_S$ is strictly monotonically decreasing in b_ℓ with $\ell \in \{1, 2, \ldots, L\}$ if we have $a_\ell > 0$ and $q_\ell > 0$. Furthermore, it is a convex function of $b \in \bar{\mathcal{B}}$. But we can observe that the additional constraints in $\bar{\mathcal{B}}$ ensure monotonicity and convexity properties of $\bar{R}_S$ with respect to $q \in \mathcal{Q}$, which were not given for $\widetilde{R}_S$ in the previous section. The secrecy rate $\bar{R}_S$ is strictly monotonically increasing in q_ℓ with $\ell \in \{1, 2, \ldots, L\}$ if we have $a_\ell > b_\ell$. Moreover, it is a concave function of $q \in \mathcal{Q}$ since $a_\ell \geq b_\ell$ is guaranteed for all $\ell \in \{1, 2, \ldots, L\}$ if we have $b \in \bar{\mathcal{B}}$.

⟨**3.44**⟩ **Properties (Saddle-Point Problem).** In ⟨3.18⟩, we have already stated that the sets $\mathcal{Q}$ and $\mathcal{B}$ are convex. Since the convexity of such a set is not influenced by additional upper bounds for the vector components, we can conclude that the set $\bar{\mathcal{B}}$ is

convex, too. Thus, we obtain that the inner minimization problem in ⟨3.42⟩ is a convex problem. This corresponds to the characterization of the inner problem in ⟨3.18⟩ in the previous section. The difference is that it is now guaranteed that we have a saddle-point problem, since $\bar{R}_S$ is a concave function of $q \in \mathcal{Q}$ for all $b \in \bar{\mathcal{B}}$ and a convex function of $b \in \bar{\mathcal{B}}$ for all $q \in \mathcal{Q}$. Consequently, we can equivalently write

$$\max_{q \in \mathcal{Q}} \min_{b \in \bar{\mathcal{B}}} \bar{R}_S(a, b, q) = \min_{b \in \bar{\mathcal{B}}} \max_{q \in \mathcal{Q}} \bar{R}_S(a, b, q).$$

The interchangeability of the minimization and maximization for convex-concave functions is for instance known as Sion's minimax theorem, although Sion's formulation comprises a significantly larger class of functions. With this theorem, Sion extended and unified some already existing minimax theorems, see (Sion, 1958) and references therein.

⟨**3.45**⟩ **Optimal Strategy (Outer Problem).** The transmitter makes the power allocation decision based on the vector a, which specifies the channel from Alice to Bob. It is only interested in allocating positive values to those components of q where the corresponding component of a is non-zero. Moreover, the components q_ℓ that are used for the transmission have to be chosen such that the sum of the corresponding a_ℓ is larger than χ. Hence, the characterization of the optimal power allocation vector q is very similar to that of the previous section, which was given in ⟨3.20⟩. The only difference is that we now know that the optimal power allocation vector q always uses full power P, since the monotonicity in the components of q is guaranteed.

⟨**3.46**⟩ **Optimal Strategy (Solution of Inner Problem).** As before in ⟨3.21⟩, it only makes sense that the worst-case vector b has positive components where the corresponding component of the power allocation vector q is non-zero. The optimal strategy is adapted to the new problem by incorporating the additional upper bounds for the components of the vector b, and we now obtain the waterfilling solution

$$b_\ell(\nu) = \left[\nu - \frac{1}{\rho q_\ell} \right]^+_{\leq a_\ell}$$

for all $\ell \in \{1, 2, \ldots, L\}$ with $q_\ell > 0$. As before, the monotonicity with respect to all components of b yields that the waterfilling parameter ν with $\nu \geq 0$ has to be chosen such that the sum constraint of the set $\bar{\mathcal{B}}$ is fulfilled with equality, i.e., $\sum_{\ell=1}^{L} b_\ell(\nu) = \chi$, which is feasible if we assume that $\sum_{\ell=1}^{L} a_\ell > \chi$ is given. Note that this waterfilling solution is similar to cap-limited waterfilling, which was presented by Papandreou and Antonakopoulos (2008) in the context of bit and power loading optimization for constrained multi-carrier systems with total and peak-power constraints.

⟨**3.47**⟩ **Optimal Strategy (Vector Ordering).** For the problem in ⟨3.12⟩, we derived some results on the component ordering of the optimal vectors q and b based on the component ordering of the vector a. For the optimization problem in ⟨3.42⟩, we cannot

apply the same approach as above. Thus, no comparable ordering results can be provided for the current problem, which mainly influences the characterization of bounds on the outer problem.

⟨**3.48**⟩ **Bounds on Outer Problem.** The general approach for deriving bounds on the solution of the outer problem in ⟨3.42⟩ can be taken from ⟨3.27⟩. Upper bounds can be calculated with the approach presented in ⟨3.29⟩. Instead of the constraint set $\bar{\mathcal{B}}$, a set $\mathcal{B}_\beta$ with $\beta \in \bar{\mathcal{B}}$ can be used for the inner minimization problem. Then, the waterfilling solution in ⟨2.29⟩, which was derived for the multi-carrier scenario, can be applied to calculate the optimal transmit strategy for the bound. A simple lower bound can be obtained with the same approach by using a set $\mathcal{B}_\beta$ with $\beta = (\chi)_{\ell=1}^{L}$. As already presented in ⟨3.30⟩, better lower bounds can be found by changing the constraint set of the outer problem. We can analogously use a set $\dot{\mathcal{Q}}_\iota$, where ι is an arbitrary vector with $\iota \in \mathcal{Q}$, instead of the set $\mathcal{Q}$ as constraint for the outer maximization problem. Then, we can simply apply the adapted waterfilling solution for the inner problem, which was presented in ⟨3.46⟩. Note that upper bounds on the solution of problem ⟨3.42⟩ are also upper bounds on problem ⟨3.12⟩, whereas lower bounds that were derived for problem ⟨3.12⟩ can simultaneously be used for problem ⟨3.42⟩. This directly follows from the relation between both problems, which was discussed in ⟨3.42⟩.

In order to characterize the optimal strategies for high and low SNR, the secrecy rate expression $\bar{R}_S$ in ⟨3.40⟩ is now interpreted as a function of the inverse noise variance ρ for a fixed value of P.

⟨**3.49**⟩ **High-SNR Performance.** For the high-SNR regime, we calculate the limit for the adapted secrecy rate expression $\bar{R}_S$, which is

$$\lim_{\rho\to\infty} \bar{R}_S(a,b,q) = \lim_{\rho\to\infty} \sum_{\ell=1}^{L} \left[\log_2 \left(\frac{1+\rho\, a_\ell q_\ell}{1+\rho\, b_\ell q_\ell} \right) \right]^+ = \sum_{\ell\in\mathcal{L}} \left[\log_2 \left(\frac{a_\ell}{b_\ell} \right) \right]^+ ,$$

where

$$\mathcal{L} := \{\ell \in \{1,2,\ldots,L\} \,|\, q_\ell > 0\}$$

is the set of vector components that is used for the transmission to Bob. Similar to ⟨3.31⟩, we can state that this limit exists if and only if $b_\ell > 0$ holds for all $\ell \in \mathcal{L}$. The optimal strategy for the worst-case vector b, which is given in ⟨3.46⟩, would again converge to a uniform allocation over these vector components if there were no individual upper bounds for the components of b. But for the problem in ⟨3.42⟩, we obtain $b_\ell(\nu) = [\nu]^+_{\leq a_\ell}$ with $\sum_{\ell=1}^{L} b_\ell(\nu) = \chi$ if $\sum_{\ell=1}^{L} a_\ell > \chi$ holds. This corresponds to a kind of uniform allocation over the active components of b, where the individual upper bounds possibly clip the value of some components, which in turn increases the values of the other components.

Compared to the high-SNR behavior of problem ⟨3.12⟩, the optimal strategy for the outer problem significantly changes due to the altered properties of the secrecy rate

expression. We see that the positive components of the power allocation vector q activate the summands of the high-SNR limit above, but the concrete values of the components do not matter, i.e., the sum power constraint is not relevant in this case. Each of these high-SNR summands yields a positive (or zero) contribution to the limit. Furthermore, we know that the worst-case vector b, which results from a certain power allocation q, is characterized by a (possibly clipped) uniform allocation over all components that are used by the transmitter. We can conclude that using an additional component in q can only decrease the values of the corresponding worst-case vector b, which in turn increases the high-SNR limit, since none of the already existing summands is reduced and an additional non-negative summand is added to the high-SNR limit. Consequently, it is always optimal to use all components of q in order to obtain the maximum worst-case high-SNR limit.

⟨**3.50**⟩ **Low-SNR Performance.** As expected, the limit of the secrecy rate $\bar{R}_S$ is

$$\lim_{\rho \to 0} \bar{R}_S(a, b, q) = 0$$

in the low-SNR regime. Again, the linear Taylor series representation of the secrecy rate at the point $\rho = 0$ is calculated, which yields

$$T_{\bar{R}_S}(\rho; 0) = \frac{1}{\ln 2} \sum_{\ell \in \mathcal{L}} [a_\ell - b_\ell]^+ \, q_\ell \, \rho$$

with $\mathcal{L}$ as defined above for the high-SNR discussion. If we consider the optimization of the linear Taylor series coefficient, we can benefit from the saddle-point property of the low-SNR approximation, which allows us to equivalently interchange the maximization over the set $\mathcal{Q}$ and the minimization over the set $\bar{\mathcal{B}}$. Let us first analyze the min-max problem. For each given vector $b \in \bar{\mathcal{B}}$, the transmitter would obviously allocate full power P to the component of q that corresponds to the largest factor $[a_\ell - b_\ell]^+$ in order to maximize the linear Taylor series coefficient in the low-SNR regime. The worst-case strategy consequently tries to reduce the largest value $[a_\ell - b_\ell]^+$ as much as possible. Let us assume that the vector a is ordered decreasingly, i.e., $a_1 \geq a_2 \geq \ldots \geq a_L$. Thus, the optimal strategy for the worst-case vector b can be described as follows: We start with $b_1 = b_2 = \ldots = b_L = 0$ and reduce the largest coefficient by allocating $b_1 = a_1 - a_2$. Then, the largest factors in the Taylor series representation are $a_1 - b_1$ and a_2, which are reduced afterwards by adding the difference $a_2 - a_3$ to the first two components of the vector b. This procedure is continued until the components of b add up to χ. This approach corresponds to a waterfilling solution for the worst-case vector b, which is given by

$$b_\ell(\nu) = [a_\ell - \nu]^+$$

with $\ell \in \{1, 2, \ldots, L\}$, where the waterfilling parameter ν with $\nu \geq 0$ is chosen such that the sum constraint of the set $\bar{\mathcal{B}}$ is fulfilled with equality, i.e., $\sum_{\ell=1}^{L} b_\ell(\nu) = \chi$. A consequence of this worst-case strategy is that the transmitter, who wants to maximize

the linear Taylor series coefficient, generally observes multiple components in the vector $([a_\ell - b_\ell]^+)_{\ell=1}^L$ that take the maximum value of this vector. Thus, the optimal power allocation vector for the min-max problem is not unique. The transmitter can arbitrarily distribute the power P over the components that correspond to the maximum value of $([a_\ell - b_\ell]^+)_{\ell=1}^L$, whereas all other components of q are set to zero.

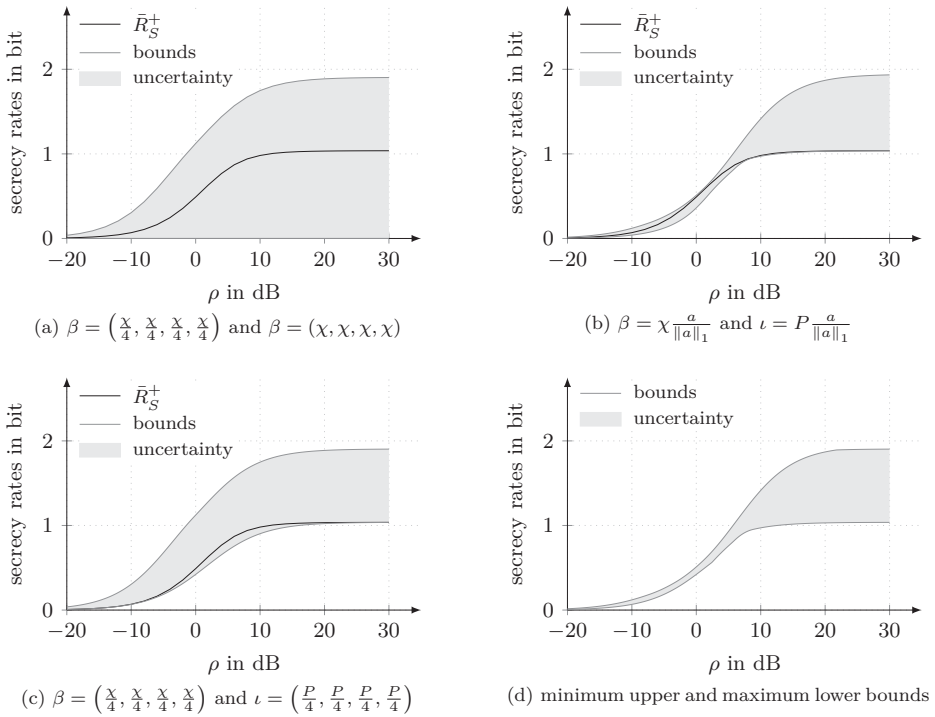
Let us now switch to the equivalent max-min problem. For each given vector $q \in \mathcal{Q}$, the worst-case vector b is mainly interested in reducing the component of the vector $([a_\ell - b_\ell]^+)_{\ell=1}^L$ that corresponds to the largest component of the power allocation vector q as much as possible. Since each component of the vector b is bounded by $b_\ell \leq a_\ell$, the worst-case vector can also reduce the factor for the second largest component if χ is large enough. The procedure is continued until χ is completely distributed. The transmitter, who can predict this worst-case reaction, consequently choses a uniform allocation of the complete power P over the first components of q. The optimal number of positive components in q can be predetermined by the transmitter depending on the values of the vector a for the channel to the intended receiver and the constraint χ on the channel to the eavesdropper. Based on a uniform power allocation over a certain number of components in q, the resulting worst-case strategy for the low-SNR approximation is not unique. The value χ can be arbitrarily distributed over the components of b that correspond to the non-zero components of q, only the individual upper bounds on the components of b have to be considered. Comparing the max-min and the min-max problem, we can conclude that we clearly have an optimal strategy for the outer problems, but the induced reactions for the inner problems are not unique. Thus, the optimization order affects which strategy combinations are optimal, but the resulting value of the optimization problems is not influenced. In comparison with ⟨3.32⟩, we have again the situation that the altered properties of the secrecy rate expression change the optimal strategies for the optimization problem.

⟨**3.51**⟩ **Properties (Equivalence of Eigenvalue Problems).** According to ⟨3.42⟩, the original eigenvalue problem in ⟨3.12⟩ and the adapted problem in ⟨3.42⟩ only differ in the constraint set for the inner minimization. Hence, they are equivalent if the worst-case vector $b \in \mathcal{B}$ that is optimal for the original problem ⟨3.12⟩ also fulfills $b \in \bar{\mathcal{B}}$. In ⟨3.26⟩, a sufficient condition was formulated that ensures that the original eigenvalue problem in ⟨3.12⟩ is a saddle-point problem. If this condition is fulfilled by the given parameters it is guaranteed that $b \in \bar{\mathcal{B}}$ holds for the worst-case vector of both problems, i.e., they are equivalent in this case.

⟨**3.52**⟩ **Parameters for Comparison of Maximized Worst-Case Secrecy Rates.** In order to compare the results of the previous section with the outcome of the current section, we take the parameters from the example that we introduced in ⟨3.33⟩. If we consider the eigenvalue vector $a = (3.9, 1.5, 1.0, 0.6)$, which characterizes the channel between Alice and Bob, together with the originally introduced constraint $\chi = 2$ for the channel to Eve, we observe that these parameters fulfill the saddle-point condition in ⟨3.26⟩, i.e., the original optimization problem in ⟨3.12⟩ and the adapted problem in ⟨3.42⟩

are equivalent. In this case, the transmitter cannot gain any advantage from the more complex transmitter structure in Figure 3.16 compared to the transmitter structure in Figure 3.2.

This situation significantly changes if we consider $a = (3.9, 1.5, 1.0, 0.6)$ together with $\chi = 5$ as in ⟨3.37⟩. Now, we have a parameter combination where the saddle-point condition in ⟨3.26⟩ is not fulfilled. Moreover, we observed in Figure 3.12 that the worst-case vector b that corresponds to a full-power vector q causes negative summands in the maximized worst-case secrecy rate, i.e., we have $b \notin \bar{\mathcal{B}}$ for the worst-case vector b in this case. Thus, we will use this parameter combination in the following to compare the secrecy rates that are achievable for the problems in ⟨3.12⟩ and ⟨3.42⟩.



(a) $\beta = \left(\frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}\right)$ and $\beta = (\chi, \chi, \chi, \chi)$

(b) $\beta = \chi \frac{a}{\|a\|_1}$ and $\iota = P \frac{a}{\|a\|_1}$

(c) $\beta = \left(\frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}\right)$ and $\iota = \left(\frac{P}{4}, \frac{P}{4}, \frac{P}{4}, \frac{P}{4}\right)$

(d) minimum upper and maximum lower bounds

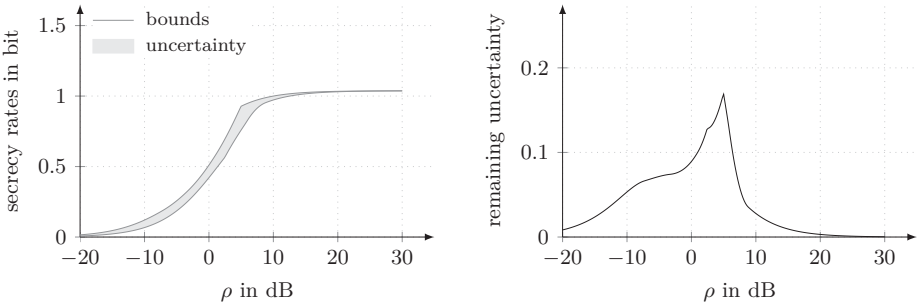
Figure 3.17: Upper and lower bounds on the maximized worst-case secrecy rate $\bar{R}_S^+$ and the remaining uncertainty regions between the bounds.

⟨**3.53**⟩ **Illustration (Bounds).** Figure 3.17 shows upper and lower bounds on the maximized worst-case secrecy rate for the adapted problem in ⟨3.42⟩ as a function of the SNR.

The area between the upper and lower bounds is the remaining uncertainty about the exact value of the maximized worst-case secrecy rate, which is denoted by $\bar{R}_S^+$. Strictly speaking, it is an approximation of the maximized worst-case secrecy rate, which was determined by an exhaustive search over all possible power allocation vectors q. The corresponding set was run through with a step size of 0.010 for each component.

For (a), the upper and lower bound were derived by manipulating the inner minimization according to ⟨3.27⟩. For the derivation of the upper bound, we used $\beta = \left(\frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}\right)$. This parameter choice yielded a relatively good upper bound on the original problem in ⟨3.12⟩, see Figure 3.4. But it is not a comparably good choice for an upper bound on the adapted problem in ⟨3.42⟩. We have $\beta_3 > a_3$ and $\beta_4 > a_4$, which is not a reasonable choice since we know that $b_\ell \leq a_\ell$ optimally holds for all $\ell \in \{1, 2, \ldots, L\}$. Allocating higher values than optimal to the last two components of β unnecessarily reduces the values that can be assigned to the first two components of this vector, which prevents us from obtaining a tight upper bound. The lower bound was derived with $\beta = (\chi, \chi, \chi, \chi)$. We know from ⟨3.33⟩ that we cannot expect to get a good lower bound by manipulating the constraint for the inner minimization, since we have to relax the sum constraint on the vector b too much. The absence of an appropriate ordering result for the components of the optimal vectors yields a parameter choice that is even more far away from optimal than the comparable lower bound for the original problem in Figure 3.4. In our example, we obtain zero for the lower bound since we have $\beta_\ell > a_\ell$ for all $\ell \in \{1, 2, \ldots, L\}$.

In the following, we will again derive upper bounds by manipulating the inner minimization, but we will change the constraint set for the outer maximization in order to derive upper bounds. We can use the vectors that we have already introduced in ⟨3.33⟩ for the bound derivation. In (b) and (c), we exemplarily see the bounds that we obtain by scaled versions of the parameter vector a and by a uniform allocation over all four vector components. We observe that the lower bounds are relatively good over the complete SNR range and even tight for high SNR. We could expect the latter from the high-SNR discussion in ⟨3.49⟩, where we concluded that it is optimal to use all components of the power allocation vector q for the transmission to Bob independently of the chosen values. If we analyze the upper bound for (b), we see that it is relatively good for low and medium SNR, but we can observe a large gap between this bound and the exact value of $\bar{R}_S^+$ for high SNR. Obviously, the chosen parameter vector β significantly differs from the worst-case vector for high SNR. The diagram in (d) shows the minimum upper and maximum lower bounds we found by evaluating a certain number of upper and lower bounds over the complete SNR range. Therefore, we considered not only the bounds above, but also bounds we derived from uniform allocations over a certain number of non-zero vector components, where we decided to always use the first vector components and varied their number, cf. Figure 3.5. Thus, we used exactly the same vectors as in ⟨3.33⟩ for the bound derivation. Unfortunately, the remaining uncertainty is comparably large for high SNR due to the absence of a tight upper bound. Nevertheless, we know that the maximum lower bound is tight for high SNR, which provides us nearly the exact value of the maximized worst-case secrecy rate in this regime.



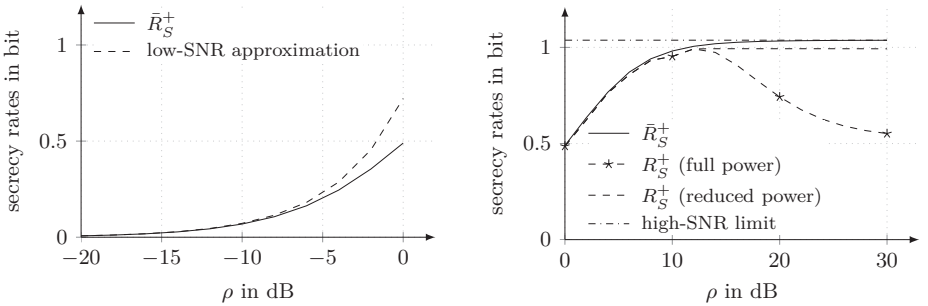
(a) uncertainty with improved upper bound

(b) absolute values of remaining uncertainty

Figure 3.18: Remaining uncertainty about the value of $\bar{R}_S^+$ with improved upper bound for high SNR.

If we want to further reduce the remaining uncertainty for high SNR, we have to look for the worst-case vector in this regime. From the high-SNR discussion in ⟨3.49⟩, we know that this is a kind of uniform allocation over all components of b, where the corresponding values from a represent individual upper bounds on the components, which in turn increases the values of the other components. Having this in mind, we can calculate a new upper bound with $\beta = (1.9, 1.5, 1.0, 0.6)$, which is the high-SNR worst-case vector for our example. Figure 3.18 (a) is an improved version of the diagram in Figure 3.17 (d), where the upper bound was updated by additionally considering this new upper bound. Now, we have a relatively small uncertainty over the complete SNR range we considered. In (b), the absolute values of the remaining uncertainty are shown, which are calculated as the difference of the best upper and lower bound. We observe that this uncertainty grows with ρ until about $\rho = 5$ dB. Afterwards, we see the effect of the improved upper bound. Since both bounds are tight for high SNR, the remaining uncertainty tends to zero with further increasing ρ.

⟨3.54⟩ Illustration (High- and Low-SNR Behavior). In Figure 3.19, the high- and low-SNR behavior of the maximized worst-case secrecy rate $\bar{R}_S^+$ of the adapted problem in ⟨3.42⟩ is illustrated. The low-SNR approximation in (a) is calculated according to ⟨3.50⟩. The resulting low-SNR worst case vector for the min-max problem is $b = (3.4, 1.0, 0.5, 0.1)$, which for instance corresponds to a power allocation vector q with a uniform allocation over all four components. Note that for low SNR, there is no difference between the achievable rates for the problems ⟨3.12⟩ and ⟨3.42⟩. In (b), we see that the maximized worst-case secrecy rate $\bar{R}_S^+$ converges to the limit that was calculated with all vector components from a and b according to ⟨3.49⟩. For comparison, we added the rates that were achievable for the original problem in ⟨3.12⟩. With increasing SNR, we can observe the growing gap between the rates of both problems that were obtained using full transmit



(a) low-SNR approximation (b) high-SNR limit

Figure 3.19: The maximized worst-case secrecy rate $\bar{R}_S^+$ with its low-SNR approximation and its high-SNR limit.

power. The rate that was obtained in ⟨3.37⟩ for the original problem with significantly reduced transmit power comes close to the maximized worst-case secrecy rate $\bar{R}_S^+$ we calculated for the adapted problem. This is very interesting since we can get nearly the same rate with a simpler transmitter structure, see Figure 3.2, and a significantly lower transmit power, see Figure 3.13.

⟨3.55⟩ Illustration (Optimal Strategies). Figure 3.20 shows the values of the optimal vectors and the resulting secrecy rate summands for selected SNR values. Now, we can see the predicted low- and high-SNR behavior in detail. In (a), we see that the transmitter has chosen a uniform allocation of the available power P for $\rho = -20$ dB. From the discussion in ⟨3.50⟩, it follows that this is the optimal power allocation vector for low SNR if the optimization problem is formulated as max-min problem as in the simulation. The resulting worst-case vector for the low-SNR approximation is not unique, but the waterfilling solution in ⟨3.46⟩ yields a unique solution for the secrecy rate minimization, which is the worst-case vector b given in this diagram. In (b), (c), and (d), we can see how the optimal power allocation vector q and the corresponding worst-case vector b change with the variation of the SNR from $\rho = -10$ dB to 10 dB. We see that Alice always uses all components of the vector q for the transmission to Bob. This behavior can be explained by the relatively high value that was chosen for the channel constraint χ on the eavesdropper channel. Thus, the transmitter has to use at least a certain number of components in order to ensure that the worst-case secrecy rate is positive, see ⟨3.45⟩. In (e) and (f), which show the results for $\rho = 20$ dB and 30 dB, we see that the worst-case vector b takes exactly the values that result from the high-SNR analysis in ⟨3.49⟩ and that we have already used for calculating the minimum upper bound for high SNR in ⟨3.53⟩. Furthermore, we notice that this worst-case behavior is induced by a power allocation vector that uses all components, although the main part of the available power is

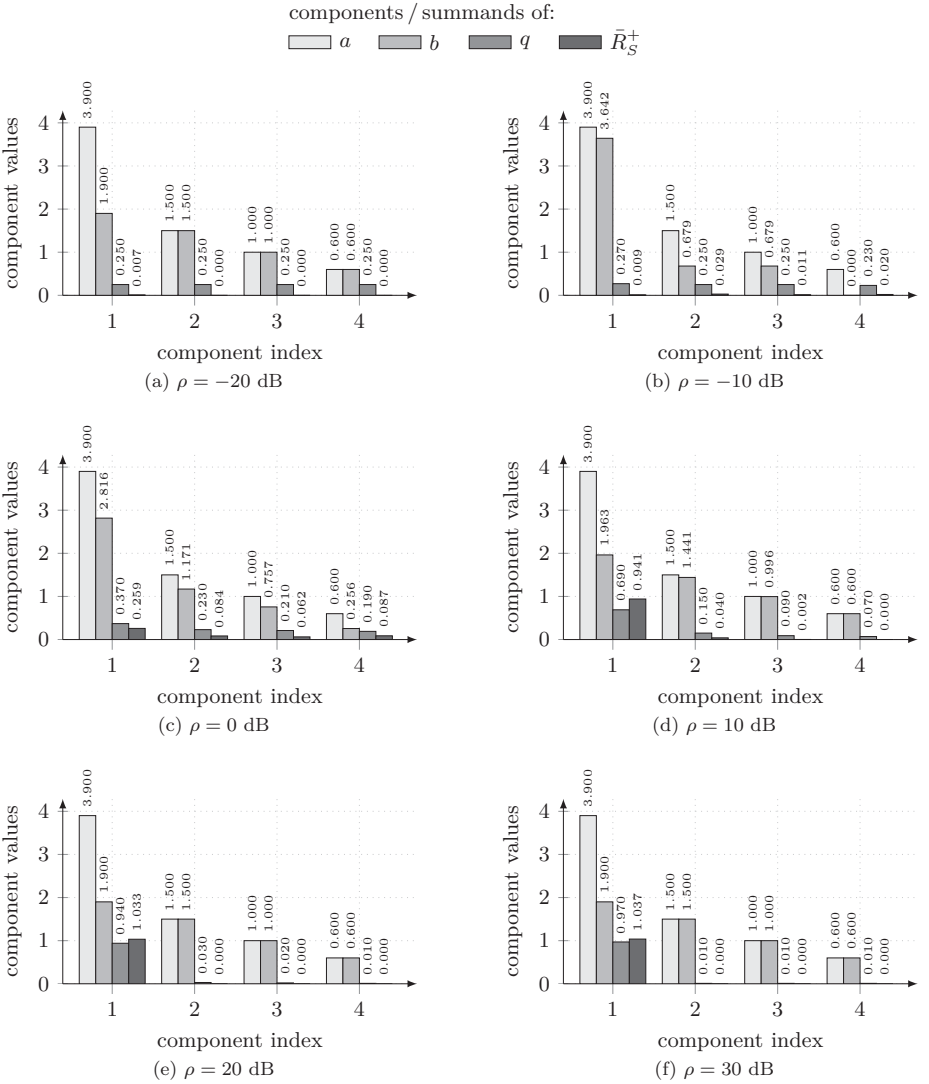


Figure 3.20: Optimal vectors corresponding to the maximized worst-case secrecy rate $\bar{R}_S^+$ for selected SNR values.

assigned to the first component, which corresponds to the largest value in a and therefore promises the largest quotient between the components of a and b, which in turn yields the largest contribution to the overall rate. In comparison with Figure 3.12, where we analyzed the same example for the original problem in ⟨3.12⟩, we see that the values of the worst-case vector b do not exceed the corresponding values of a anymore, which in turn avoids negative summands in the secrecy rate expression and consequently increases the maximized worst-case secrecy rate. This is clearly the effect of the adapted transmitter structure in Figure 3.16.

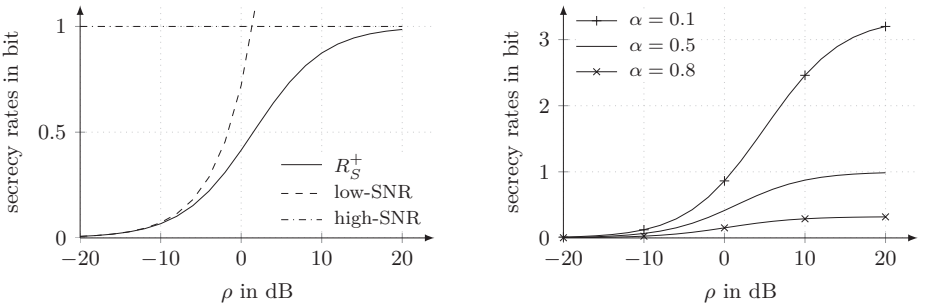
3.4 Discussion

⟨**3.56**⟩ **Special Case (Multiple-Input Single-Output Scenario).** Now, we want to discuss the MISO scenario, where the intended receiver Bob has only one antenna, i.e., we set $M = 1$. All other assumptions we made in this chapter remain unchanged. As before, we assume that the transmitter Alice is equipped with L antennas and that the eavesdropper Eve is allowed to have $N > L$ antennas. Due to the restriction that the receiver Bob has only one antenna in this scenario, the transmitter uses only one data stream and one wiretap encoder, i.e., the two eigenvalue problems we discussed in the previous sections are always equivalent. The channel matrix H, which characterizes the channel from Alice to Bob, reduces to a (row) vector of length L. Thus, we now write h instead of H. The corresponding Gramian matrix $A = h^{\mathrm{H}}h$ has rank one, i.e., the only non-zero component in the eigenvalue vector a is $a_1 > 0$ and the eigenvalue decomposition of A can be written as $A = \frac{h^{\mathrm{H}}}{\|h\|}(a_1)\frac{h}{\|h\|}$. Thus, only the first components of the optimal power allocation vector q and the worst-case vector b are non-zero, and we obtain $q_1 = P$ and $b_1 = \chi$ for these vectors if we assume that $a_1 > \chi$. The corresponding transmit covariance matrix, which maximizes the worst-case secrecy rate in the MISO scenario, is $Q = \frac{h^{\mathrm{H}}}{\|h\|}(P)\frac{h}{\|h\|}$, i.e., it can be identified as maximum-ratio transmission to the intended receiver Bob using full power. For the worst-case channel matrix, we obtain the rank-one matrix $B = \frac{h^{\mathrm{H}}}{\|h\|}(\chi)\frac{h}{\|h\|}$ in Gramian notation, which yields the vector $g = \sqrt{\chi}\frac{h}{\|h\|}$ for the worst-case channel from Alice to Eve, i.e., the worst-case channel to Eve equals a scaled version of the channel h from Alice to Bob in the MISO scenario. With $\chi = \alpha\, a_1$ and $\alpha \in [0, 1]$, we obtain the following expression for the maximized worst-case secrecy rate

$$R(\alpha) := \log_2\left(1 + \rho\, a_1 P\right) - \log_2\left(1 + \rho\, \alpha\, a_1 P\right) = \log_2\left(\frac{1 + \rho\, a_1 P}{1 + \rho\, \alpha\, a_1 P}\right),$$

which corresponds to the secrecy rate of the basic scenario we discussed in Section 2.1. The case $\alpha = 0$ corresponds to a MISO scenario without eavesdropper or to a transmission without secrecy constraints, whereas the case $\alpha = 1$ leads to zero for the (maximized) worst-case secrecy rate, i.e., a definitely secure transmission is not possible since the eavesdropper channel is as "powerful" as the main channel. The high-SNR limit can

be expressed as $-\log_2(\alpha)$. The low-SNR approximation that we obtain with the linear Taylor series representation equals $T_R(\rho;0) = \frac{1}{\ln 2}(1-\alpha)\,a_1 P\rho$.



(a) secrecy rate and high- / low-SNR approximations for $\alpha = 0.5$

(b) influence of the channel quality ratio α

Figure 3.21: The maximized worst-case secrecy rate R_S^+ of the MISO scenario for several values of the channel quality ratio α.

Figure 3.21 shows the maximized worst-case secrecy rate R_S^+ of the MISO scenario, where the channel from Alice to Bob is characterized by $a_1 = 1$. As before, we assumed that the transmit power constraint was set to $P = 1$. In (a), this rate and its high- and low-SNR approximations are given for $\alpha = 0.5$, i.e., the eavesdropper channel has only one-half of the gain of the main channel. For the illustration in (b), we varied the channel quality ratio α. We see that the behavior of the curves is very similar to those of the MIMO scenario we discussed before.

⟨3.57⟩ Application to Multi-Carrier Scenario. The results from Section 3.3 can be transferred to a related multi-carrier scenario. We resume the system model of the multi-carrier scenario in ⟨2.20⟩, where Alice can use up to K carriers for the transmission to Bob, and analogously apply the modifications we made for our worst-case discussion in ⟨3.1⟩ and ⟨3.12⟩. Thus, we obtain a setting, where Alice knows her channel gains to Bob perfectly, but has only very limited knowledge about her channel to Eve. It is only known that the sum of her channel gains to Eve over all carriers is not larger than χ, which corresponds to the definition of the set $\mathcal{B}$ in ⟨3.12⟩. She aims to maximize the worst-case secrecy rate for her private communication to Bob under a sum power constraint over all carriers and the assumption that Eve is able to find the worst-case channel gains for eavesdropping this confidential message. The resulting problem formulation corresponds to the max-min problem in ⟨3.40⟩ with $L = M = N = K$. Thus, all results that we derived for this problem in the previous section can directly be applied to this multi-carrier scenario. For a multi-carrier scenario, we can assume that $a_k > 0$ holds for all

$k \in \{1, 2, \ldots, K\}$. Thus, there is no constraint on the maximum number of positive components of the power allocation vector q.

Note that the worst-case secrecy rate maximization for the multi-carrier scenario cannot directly be derived as a special case of the worst-case secrecy rate maximization for the multi-antenna scenario. We have to use the adapted problem in ⟨3.40⟩ in order to obtain the right secrecy rate expression. That is in contrast to the case without secrecy constraints, where the multi-carrier scenario can be seen as a special case of the MIMO scenario, and the corresponding system model and rate can be simply obtained by inserting diagonal matrices for the MIMO channel matrices.

⟨**3.58**⟩ **Extension to Multiple Eavesdroppers.** The system model in ⟨3.1⟩ and the results derived for it in this chapter considered only one eavesdropper, who is introduced as Eve. Nevertheless, all results can be applied to a system with multiple non-cooperating eavesdroppers as well. The study above focused on the worst-case eavesdropper, who is characterized by the worst-case channel matrix, for a secure transmission from the transmitter Alice to the legitimated receiver Bob. The resulting secrecy rate was maximized under the assumption that this communication is always wiretapped by an eavesdropper Eve with the corresponding worst-case channel matrix, which depends on the currently chosen transmit strategy. Thus, all other eavesdroppers at positions where they observe a channel matrix that does not correspond to the worst-case channel matrix have a disadvantage compared to Eve. Hence, each transmission between Alice and Bob that is secure with respect to Eve simultaneously is a definitely secure transmission regarding all these other eavesdroppers.

The results for the case of multiple cooperating eavesdroppers can also be derived from the results above. Let us assume that we have T cooperating eavesdroppers whose channel matrices are denoted by $G_1, G_2, \ldots, G_T$ with $T \in \mathbb{N}$. Each eavesdropper can have an individual number of receive antennas, i.e., we have $G_t \in \mathbb{C}^{N_t \times L}$ with $N_t \in \mathbb{N}$ for $t \in \{1, 2, \ldots, T\}$. For each of these eavesdropper channel matrices G_t, the channel condition in ⟨3.1⟩ is fulfilled, i.e., we have $\|G_t\|_{\mathrm{F}}^2 \leq \chi$. We can interpret these T cooperating eavesdroppers as one eavesdropper with a channel matrix $G \in \mathbb{C}^{N \times L}$ with $N = \sum_{t=1}^{T} N_t$, which is constructed by a vertical concatenation of the matrices $G_1, G_2, \ldots, G_T$. For this new channel matrix G, we obtain a new channel condition, which can be calculated using the definition of the Frobenius norm together with the channel conditions of the individual eavesdropper channels:

$$\|G\|_{\mathrm{F}}^2 = \sum_{t=1}^{T} \|G_t\|_{\mathrm{F}}^2 \leq T\chi.$$

Thus, we can reduce the problem of T cooperating eavesdroppers to the original problem with a more "powerful" eavesdropper by adapting the channel condition as shown above.

⟨**3.59**⟩ **Extension to other Constraint Sets.** In the system model in ⟨3.1⟩, we considered a MIMO wiretap channel and introduced a constraint on the eavesdropper channel

using the Frobenius norm of this channel. Then, we formulated an optimization problem for the secrecy rate maximization under the assumption that the eavesdropper Eve always finds the worst-case channel for wiretapping the communication between the transmitter Alice and the legitimated receiver Bob, see ⟨3.5⟩. This problem was reduced to a problem over the eigenvalues of the transmit covariance matrix and the Gramian matrix of the channel to the eavesdropper, see ⟨3.12⟩. In this reformulation process, the constraint on the eavesdropper channel turned into a restriction on the sum of the eigenvalues of the Gramian matrix of this channel matrix. In order to support this reformulation, it was necessary and sufficient that the constraint on the eavesdropper channel was unitarily invariant. Consequently, we can alternatively use any other constraint set for the eavesdropper channel that is unitarily invariant and we are able to do the same transformation steps for reducing the original problem as shown above. In addition to the considered Frobenius norm, we could also use other Schatten p-norms including the spectral and the Ky Fan k-norm. However, there are other matrix norms that can be of interest for system design, which are not unitarily invariant. We can for instance think of the maximum norm or the row / column sum norm. Nevertheless, we can exploit the equivalence of all matrix norms, which allows us to upper- and lower-bound an arbitrary matrix norm by another matrix norm, which could be chosen such that it is unitarily invariant. Thus, we can for instance use the (unitarily invariant) spectral norm for the derivation of bounds on the maximized worst-case secrecy rate if a system with peak-power constraints is considered.

⟨**3.60**⟩ **Publication Note.** Some ideas and results discussed in this chapter have already been presented at the *44th Asilomar Conference on Signals, Systems, and Computers* in 2010 and published in (Wolf and Jorswieck, 2010a). In this paper, we introduced the worst-case scenario with a deterministic model for the uncertainty about the eavesdropper channel in the multi-antenna scenario. From the perspective of the transmitter, we studied the secrecy rate maximization problem under the assumption that the eavesdropper can observe the worst-case channel for each chosen transmit strategy. This publication mainly contained the idea of reformulating the original matrix problem of the MIMO scenario into a vector problem over the eigenvalues of the involved matrices. Thus, it provided the basis for the formulation of the eigenvalue problem in ⟨3.12⟩ and the adapted problem in ⟨3.42⟩. Additionally, it comprised the derivation of the solution of the inner (worst-case) problem for the transmitter structure with parallel encoders as in ⟨3.46⟩. Moreover, simple upper and lower bounds were introduced, and some aspects of the high- and low-SNR behavior were discussed in this publication. Thus, it was also a basis for the results in ⟨3.27⟩–⟨3.30⟩ as well as in ⟨3.49⟩ and ⟨3.50⟩. A short overview of the results of (Wolf and Jorswieck, 2010a) was also included in (Jorswieck et al., 2015).

In ⟨3.59⟩, we discussed how the results of this chapter could be extended to the maximization of worst-case secrecy rates in a multi-antenna scenario with other constraint sets. Based on this, we formulated corresponding propositions, which were presented at the *7th IEEE International Workshop on Information Forensics and Security (WIFS)* in 2015 and published in (Wolf et al., 2015), after the submission of this thesis. In this paper, we studied the problem above under more generalized constraints, i.e., the max-min problem

with input constraints on the transmit covariance matrix and state constraints on the eavesdropper channel. We presented not only results for unitarily invariant constraints, which allowed us to reduce the initial problem to a problem over the eigenvalues, but we also showed how this approach could be applied to a more general class of optimization problems with other constraints that are of interest for the system design. This was illustrated by an example with peak power constraints for all transmit antennas.

⟨**3.61**⟩ **Related Work.** Liang et al. (2007) introduced the compound wiretap channel as a generalization of Wyner's wiretap model. It allows the main and the eavesdropper channel to take a number of possible states. The transmitter has to ensure that the receiver can always decode the transmitted message while it is kept perfectly secret from the eavesdropper independently of the current states of both channels. This model can equivalently be interpreted as a multicast channel with multiple eavesdroppers, where each possible state of the main channel corresponds to a legitimated receiver while each eavesdropper channel state is associated with an individual eavesdropper. From this point of view, the transmitter wants to transmit its message to all receivers while keeping it secret from all eavesdroppers. It is assumed that the channel states are known to the corresponding receivers or eavesdroppers and that they remain constant during one transmission. This study on the compound wiretap channel was continued and detailed by the same authors in (Liang et al., 2008b) and (Liang et al., 2009). First, the authors analyzed the discrete memoryless compound wiretap channel. An expression for the achievable secrecy rate was established as a worst-case result considering the worst receiver together with the best eavesdropper. The input scheme needs to balance the rates for all receiver-eavesdropper pairs, which generally yields non-optimal results for each pair. Afterwards, the authors of these publications derived the secrecy capacity for the degraded and the semideterministic compound wiretap channel. Later, the parallel Gaussian compound wiretap channel was analyzed. The secrecy capacity and the secrecy degrees of freedom were given for the degraded parallel Gaussian compound wiretap channel with one receiver and multiple eavesdroppers. Finally, the authors presented the secrecy capacity of the degraded MIMO compound wiretap channel and expressions for an achievable secrecy rate and an achievable secrecy degree of freedom for the general MIMO compound wiretap channel. From this perspective, the model we used in this chapter is a combination of the semideterministic compound wiretap channel and the general MIMO compound wiretap channel. We used a general MIMO scenario, but we relaxed only the assumption of perfect channel knowledge for the eavesdropper channel. For the main channel to the legitimated receiver we further assumed that the transmitter knows the channel perfectly. In contrast to the model in (Liang et al., 2009), we considered an infinite number of possible eavesdropper states. These states were modeled as a set that was characterized by a certain constraint. The focus of this chapter was the derivation of an equivalent vector problem and the solution for the max-min problem for this special constraint set.

At the same time as Liang et al. (2007), Liu et al. (2008) studied parallel Gaussian compound wiretap channels. The authors of this publication focused on the class of non-

degraded channels with only one possible channel realization for the legitimated receiver and derived the secrecy capacity for this model.

An example for another approach for a worst-case analysis of a secrecy rate problem can be found in (Anand and Chandramouli, 2010). The authors considered a model that clearly differs from those we discussed so far. They studied a system with multiple transmitter-receiver pairs who want to communicate in presence of an eavesdropper under the assumption that each user of the system has only one antenna. Thus, there are multiple transmitters who choose their strategies and optimize their rates individually. The eavesdropper is interested to wiretap the communication of each link. The authors introduced the notion "logical location" for the vector representing the eavesdropper channel gains for all links. They formulated the worst-case secrecy rate problem from a game-theoretical perspective and aimed to determine the optimal logical location of the eavesdropper, which results in minimum secrecy capacity for all transmitter-receiver pairs.

⟨**3.62**⟩ **Summary.** In this chapter, we considered a MIMO wiretap channel where the assumption of perfect channel knowledge was relaxed for the eavesdropper channel. Instead, we formulated a constraint on this channel using its Frobenius norm in order to model an infinite set of eavesdropper channels. For this model, we introduced the worst-case secrecy rate problem, which is to find the worst-case channel for wiretapping the communication between the transmitter and the legitimated receiver for each given transmit strategy. Afterwards, we added the problem of maximizing this worst-case secrecy rate under a transmit power constraint over all antennas. We discussed the properties of this max-min problem and derived an equivalent vector problem over the eigenvalues of the involved matrices.

For this problem, we characterized the optimal strategies considering the number of positive vector components, their ordering, and possible value ranges. Based on this, a waterfilling solution for the worst-case problem was presented as well as relatively tight lower and upper bounds on the solution of the outer maximization problem. For the high- and low-SNR regime, we discussed the behavior of the worst-case secrecy rate together with the corresponding optimal strategies. Especially for high SNR, the importance of scaling the overall transmit power was shown.

Afterwards, we presented a slightly modified transmitter whose structure was adapted to the characteristics of the max-min problem. This yielded another expression for the secrecy rate, which ensured higher achievable rates than the approach before. We also discussed optimal strategies as well as the high- and low-SNR behavior for this problem and showed similarities and differences between both problems.

All results of this chapter were illustrated in detail. Moreover, it was shown how these results can be applied to a related multi-carrier scenario. Finally, we discussed the application to scenarios with multiple cooperating eavesdroppers and to scenarios with other constraints on the eavesdropper channel.

Part III

Key Exchange for Physical-Layer Security

4 Secret-Key Rate Optimization

The focus of this chapter is the secret-key agreement between two legitimated users on the physical layer. They want to agree on a common key and keep it secret from an eavesdropper who can observe some information of this key agreement process and tries to extract the key from the available information. In this chapter, we present some results on the achievable secret-key rates for various wireless systems and compare them to the results we previously obtained for the achievable secrecy rates of the same systems. In the first section, we introduce our basic model together with the corresponding expression for the secret-key rate R_K and its properties. In the next sections, we extend this model to multi-carrier and multi-antenna scenarios and present results for the achievable secret-key rates and provide power allocation strategies for the secret-key rate maximization.

4.1 Basic Scenario

In the basic scenario, which is illustrated in Figure 4.1, two users, Alice and Bob, want to agree on a common and secret key in the presence of an eavesdropper Eve who tries to listen to their communication and to extract the key from the information that is available to her. For the integrated wiretap channel, we have the same setting as above for the secrecy rate discussion, i.e., Alice is the transmitter, Bob the legitimated receiver, and Eve the eavesdropper.

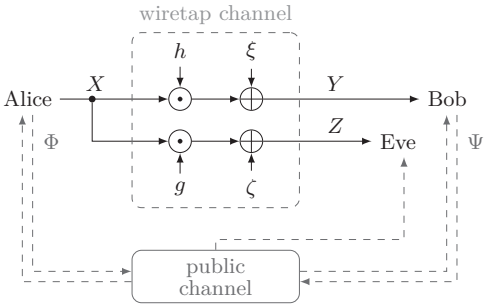


Figure 4.1: System model of the basic scenario for secret-key agreement with a transmitter (Alice), a receiver (Bob), and an eavesdropper (Eve).

⟨**4.1**⟩ **System Model.** The system model is derived from the general channel-type model for secret-key generation, which was presented in ⟨1.11⟩. This model consists of the combination of a wiretap and a public channel. Our prior assumptions on the public channel remain unchanged. For the wiretap channel, we now use the basic model from ⟨2.2⟩, which we originally introduced for the secrecy rate discussion. In order to overview this model again, we refer to the most important variables of this model in the following. The random variables X, Y, and Z describe Alice's channel input and Bob's and Eve's channel output, respectively. The main and the eavesdropper channel are attenuated Gaussian channels, which are characterized by their channel coefficients h and g or the corresponding channel gains $a := |h|^2$ and $b := |g|^2$ with $a, b > 0$. The random variables for the noise of these channels are ξ and ζ. For both channels, the noise variance is assumed to be σ^2 with $\sigma^2 > 0$. Its inverse is denoted by ρ. Alice's transmit power is denoted by q with $q \geq 0$. It underlies a transmit power constraint, which is given by P. A more detailed explanation of this wiretap model can be found in ⟨2.2⟩.

⟨**4.2**⟩ **Secret-Key Rate.** For this model, the secret-key rate R_K, which we interpret as a function of the channel gains a and b and the transmit power q with $q \geq 0$, can be evaluated according to ⟨1.13⟩, which yields

$$R_K(a,b,q) = \log_2\left(1 + \frac{(a+b)q}{\sigma^2}\right) - \log_2\left(1 + \frac{bq}{\sigma^2}\right) = \log_2\left(\frac{\sigma^2 + (a+b)q}{\sigma^2 + bq}\right),$$

where the random variable X needs to be circularly-symmetric complex Gaussian distributed with zero mean and variance q, i.e., $X \sim \mathcal{CN}(0,q)$, in order to achieve the maximum mutual information in ⟨1.13⟩ for a given transmit power q.

⟨**4.3**⟩ **Properties (Positivity).** Obviously, the secret-key rate R_K is always positive for $q > 0$ since the first term is greater than the second one independently of the relation of channel gains a and b. This is a main difference to the secrecy rate R_S of the corresponding scenario, whose positivity was only given for $a > b$.

We evaluate the first and second derivatives of the secret-key rate R_K for $a, b > 0$ and $q \geq 0$ to derive its monotonicity and convexity properties.

⟨**4.4**⟩ **Calculations.** For the first derivatives, we obtain

$$\begin{aligned}
\frac{\partial}{\partial a} R_K(a,b,q) &= \frac{1}{\ln 2}\left(\frac{q}{\sigma^2 + (a+b)q}\right) \geq 0, \\
\frac{\partial}{\partial b} R_K(a,b,q) &= -\frac{1}{\ln 2}\left(\frac{aq^2}{(\sigma^2 + (a+b)q)(\sigma^2 + bq)}\right) \leq 0, \\
\frac{\partial}{\partial q} R_K(a,b,q) &= \frac{1}{\ln 2}\left(\frac{a\sigma^2}{(\sigma^2 + (a+b)q)(\sigma^2 + bq)}\right) > 0.
\end{aligned}$$

For the second derivatives, we have

$$\begin{aligned}
\frac{\partial^2}{\partial a^2} R_K(a,b,q) &= -\frac{1}{\ln 2}\left(\frac{q^2}{(\sigma^2+(a+b)q)^2}\right) \leq 0,\\
\frac{\partial^2}{\partial b^2} R_K(a,b,q) &= \frac{1}{\ln 2}\left(\frac{aq^3(2\sigma^2+aq+2bq)}{(\sigma^2+(a+b)q)^2(\sigma^2+bq)^2}\right) \geq 0,\\
\frac{\partial^2}{\partial q^2} R_K(a,b,q) &= -\frac{1}{\ln 2}\left(\frac{a\sigma^2\left(a\sigma^2+2b(\sigma^2+(a+b)q)\right)}{(\sigma^2+(a+b)q)^2(\sigma^2+bq)^2}\right) < 0.
\end{aligned}$$

⟨**4.5**⟩ **Properties (Monotonicity).** For $a, b > 0$ and $q \geq 0$, the secret-key rate R_K is

a) monotonically increasing in a for fixed b and q,
b) monotonically decreasing in b for fixed a and q, and
c) strictly monotonically increasing in q for fixed a and b.

⟨**4.6**⟩ **Properties (Convexity).** For $a, b > 0$ and $q \geq 0$, the secret-key rate R_K is

a) a concave function of a for fixed b and q,
b) a convex function of b for fixed a and q, and
c) a strictly concave function of q for fixed a and b.

⟨**4.7**⟩ **Remark.** For $q > 0$, the properties in ⟨4.5⟩ and ⟨4.6⟩ can be formulated more precisely by adding "strictly" to each statement that had to be formulated without it before.

⟨**4.8**⟩ **Problem Formulation (Secret-Key Rate Maximization).** For given channel gains a and b, the secret-key rate R_K in ⟨4.2⟩ should be maximized under a transmit power constraint $q \leq P$, i.e.,

$$\max_{q \in \mathcal{Q}} R_K(a,b,q)$$

where

$$\mathcal{Q} := \{q \in \mathbb{R} \,|\, q \geq 0 \text{ and } q \leq P\}$$

is the set of all feasible transmit powers, which we have already defined in ⟨2.10⟩ in the context of the maximization of the secrecy rate R_S.

⟨**4.9**⟩ **Properties (Convexity of the Problem).** The constraint set $\mathcal{Q}$ is convex, and the objective function is a concave function of q on this set. Consequently, we have a convex problem.

⟨**4.10**⟩ **Optimal Strategy (Power Allocation).** From ⟨4.3⟩ and ⟨4.5⟩, we know that we can always achieve a positive secret-key rate for $q > 0$ and that this rate is growing with q. Thus, we see that it is optimal to use full power at the transmitter, i.e., $q = P$ for the problem in ⟨4.8⟩.

⟨**4.11**⟩ **Relation to Secrecy Rate.** The comparison between the secrecy rate R_S in ⟨2.4⟩ and the secret-key rate R_K in ⟨4.2⟩ shows that both functions only differ in the first term. For all channel gains a and b and each transmit power $q > 0$, the first term of R_K is always greater than the corresponding term of R_S. Thus, we obtain $R_K(a, b, q) \geq R_S(a, b, q)$ for all possible parameter combinations, which directly yields

$$\max_{q \in \mathcal{Q}} R_K(a, b, q) \geq \max_{q \in \mathcal{Q}} R_S(a, b, q).$$

⟨**4.12**⟩ **Secret-Key Capacity.** In this basic scenario, we have a channel-type model with a wiretap channel that is characterized by infinite input and output alphabets and the Markov chain property $Y - X - Z$. The corresponding secret-key capacity under a second order moment constraint for X was derived by Wong et al. (2009). From ⟨1.12⟩, we know that the secret-key capacity for our basic scenario is given by

$$C_K = \log_2\left(1 + \frac{(a+b)P}{\sigma^2}\right) - \log_2\left(1 + \frac{bP}{\sigma^2}\right).$$

In order to study the behavior of the secret-key rate for high and low SNR, we now interpret R_K in ⟨4.2⟩ as a function of the noise variance σ^2 (or its inverse ρ) for given channel gains a and b and a fixed value of P and look at the corresponding limits (if they exist) and some related performance measures.

⟨**4.13**⟩ **High-SNR Performance.** In the high-SNR regime, the secret-key rate R_K approaches the following limit:

$$\lim_{\sigma^2 \to 0} R_K(a, b, q) = \log_2\left(1 + \frac{a}{b}\right).$$

We observe the same behavior as above for the secrecy rate R_S of the corresponding scenario. The high-SNR limit exists and is determined by the quotient of the two channel gains, i.e., increasing the transmit power results only in a vanishing rate gain in the high-SNR regime. Comparing the two limits, we see that the high-SNR limit of the secret-key rate R_K is always greater than the limit of the corresponding secrecy rate R_S.

⟨**4.14**⟩ **Low-SNR Performance.** In the low-SNR regime, the secret-key rate R_K clearly approaches the following limit:

$$\lim_{\rho \to 0} R_K(a, b, q) = 0.$$

Thus, we consider the linear Taylor series representation of R_K at the point $\rho = 0$, which is

$$T_{R_K}(\rho; 0) = \frac{1}{\ln 2} a\, q\, \rho.$$

We observe that the increase of the secret-key rate R_K in the low-SNR regime depends on the gain of the main channel, but not on the gain of the eavesdropper channel. Consequently, it is greater than the increase of the corresponding secrecy rate R_S, which was determined by the difference of the gains of both channels. Moreover, the increase of the secret-key rate R_K is identical to the increase of the rate in a scenario without secrecy constraints.

⟨**4.15**⟩ **Comparison of Secrecy and Secret-Key Rates.** In order to ensure a relatively fair comparison between the maximized secrecy rate and the maximized secret-key rate, we pick up the idea from ⟨1.14⟩. We incorporate the subsequent data transmission into the achievable rate for the key generation scenario. In the following, we use the rate

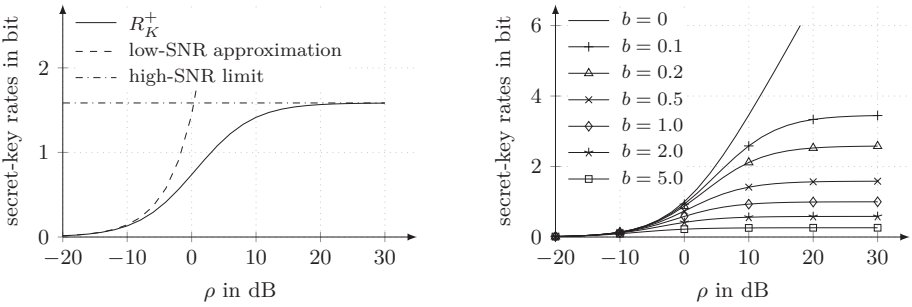
$$R_T^+ := \vartheta\, R_K^+ \quad \text{with}$$
$$\vartheta := \frac{R^+}{R^+ + R_K^+}$$

for the comparison with the maximized secrecy rate R_S^+, where ϑ is the rate comparison factor, which is calculated with the maximized secret-key rate R_K^+ and the maximized transmission rate R^+, which is determined by

$$\max_{q \in \mathcal{Q}} R(a, q) \quad \text{with}$$
$$R(a, q) := \log_2 \left(1 + \frac{aq}{\sigma^2}\right).$$

Note that the optimal transmit strategies for R^+, R_S^+, and R_K^+ generally differ from each other, although it is using full power P for all three rates in this basic scenario.

⟨**4.16**⟩ **Illustration (High- and Low-SNR Behavior).** We continue the example in ⟨2.17⟩ in order to be able to directly compare the achievable secrecy and secret-key rates, i.e., we choose again $a = 1$ and $P = 1$. Figure 4.2 shows the maximized secret-key rate of the basic scenario, which is obtained using full power and denoted by R_K^+, as a function of the SNR. For fixed parameters a, b, and q, it increases with ρ. In (a), we see the maximized secrecy rate R_K^+ for $b = 0.5$ together with its low- and high-SNR approximation according to ⟨4.14⟩ and ⟨4.13⟩, respectively. The maximized secret-key rate R_K^+ converges to approximately 1.585 bit for high SNR, which corresponds to its calculated limit with $a = 1$ and $b = 0.5$. As expected, this limit exceeds the limit of the maximized secrecy rate of the same scenario.



(a) low- and high-SNR behavior for $b = 0.5$

(b) influence of eavesdropper channel

Figure 4.2: The maximized secret-key rate R_K^+ for various eavesdropper channel gains and its low-SNR approximation and high-SNR limit.

The influence of the eavesdropper channel gain is illustrated in (b). The rate for the transmission without secrecy constraints, which is identical to a scenario without eavesdropper, is represented by $b = 0$. The resulting curve serves as an upper bound on all achievable secret-key rates. In contrast to this rate, all maximized secret-key rates converge to an individual finite limit for high SNR, which can be calculated according to ⟨4.13⟩. Furthermore, we see that the low-SNR increase of the maximized secret-key rates is independent from the eavesdropper channel gain. Thus, the low-SNR behavior of the secrecy and secret-key rate differs, whereas the high-SNR behavior is in principle the same for both cases. We clearly observe that a better eavesdropper channel reduces the achievable secret-key rate. This influence of the eavesdropper channel gain, which can be noticed over the complete SNR range, is more significant for high SNR, where the differences between the curves converge to the constant high-SNR limit gaps. Additionally, we see that positive secret-key rates can be obtained independently of the relation of the channel gains. For $b > a$, we still get positive values for the secret-key rate, whereas we would always obtain zero for the secrecy rate with the same parameters.

⟨**4.17**⟩ **Illustration (Comparison of Secrecy and Secret-Key Rates).** We proceed with the example above, which uses the parameters $a = 1$ and $P = 1$. Figure 4.3 shows a comparison of the maximized secrecy rate R_S^+, the maximized secret-key rate R_K^+, and the combined rate expression R_T^+, which is calculated according to ⟨4.15⟩ in order to allow a relatively fair comparison of R_S^+ and R_K^+ by additionally considering the subsequent data transmission with rate R^+ in the key generation approach. The aforementioned rates are illustrated for selected values of the eavesdropper channel gain.

For the illustration in (a), we choose $b = 0.2$, which corresponds to a comparably bad eavesdropper channel. In this case, there is no large difference between the maximized secrecy rate R_S^+ and the maximized secret-key rate R_K^+ over the complete SNR range.

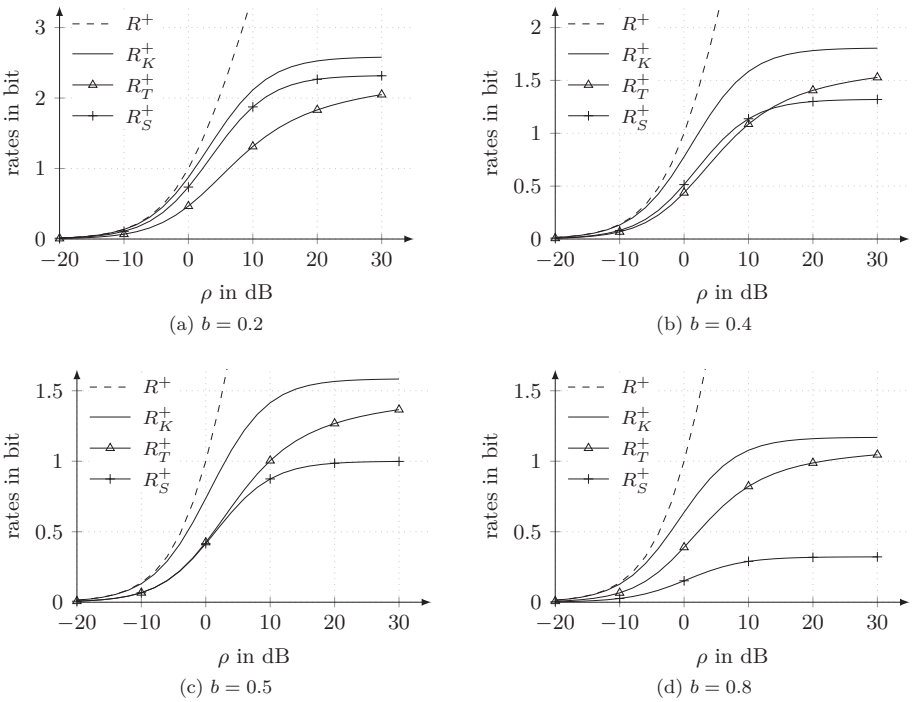


Figure 4.3: Comparison of the maximized secrecy rate R_S^+, the maximized secret-key rate R_K^+, and the combined rate expression R_T^+.

Thus, the additional data transmission in the key generation approach is comparably cost-intensive, which yields a combined rate expression R_T^+ that is less than the maximized secrecy rate R_S^+ in the simulated SNR range from $\rho = -20$ dB to 30 dB. Consequently, the transmitter cannot benefit from the key generation approach here, i.e., Alice should prefer the direct transmission with the maximized secrecy rate R_S^+ instead. Note that the comparison factor ϑ, which is defined in $\langle 4.15 \rangle$, always converges to 1 for high SNR, which follows from the completely different high-SNR behavior of R_K^+ and R^+. Hence, the combined rate R_T^+ will always be superior to the maximized secrecy rate R_S^+ if the SNR is high enough.

In (b), (c), and (d), we observe that the relation between the maximized secrecy rate R_S^+ and the combined rate R_T^+ for the key generation approach changes with a better eavesdropper channel. Although a higher gain for the eavesdropper channel yields a

general decrease of the rates R_S^+ and R_K^+, it also implies a growing gap between the maximized secret-key rate R_K^+ and the maximized secrecy rate R_S^+. Thus, the effort for the additional data transmission in the key generation approach pays off more and more. For $b = 0.4$, we see that Alice should prefer the direct transmission with the maximized secrecy rate R_S^+ below approximately -13 dB, whereas the key generation approach is superior for higher SNR. If the eavesdropper channel is characterized by $b = 0.5$, there is no clear difference between both approaches below approximately 0 dB. For higher SNR, the key generation approach should be preferred again. For an eavesdropper channel gain of $b = 0.8$, the key generation approach clearly yields higher rates over the complete SNR range. If the gain of the eavesdropper channel is further increased, we finally obtain a situation where all secrecy rates are zero. Then, only the key generation approach is suitable for a secret transmission to Bob.

4.2 Multi-Carrier Scenario

In this section, we extend the basic scenario we studied above to the multi-carrier scenario. Alice and Bob want to agree on a common key using a system that contains a wiretap channel with K parallel carriers. Again, this key should be kept secret from the eavesdropper Eve. We study the optimal resource allocation for the secret-key rate maximization under a sum power constraint over all carriers.

⟨**4.18**⟩ **System Model (Extension to Multi-Carrier Scenario).** For the key agreement in a multi-carrier system, we use the channel-type model from ⟨1.11⟩ together with the multi-carrier wiretap channel that was presented in ⟨2.20⟩. Consequently, we have K parallel carriers, which Alice can use to transmit her information.

⟨**4.19**⟩ **Secret-Key Rate.** For this model, the secret-key rate R_K, which we understand as a function of the transmit power vector q and the channel gain vectors a and b, is the sum over all secret-key rates per carrier and given by

$$R_K(a,b,q) = \sum_{k=1}^{K} \left(\log_2 \left(1 + \frac{(a_k + b_k) q_k}{\sigma^2} \right) - \log_2 \left(1 + \frac{b_k q_k}{\sigma^2} \right) \right),$$

where $q_k \geq 0$ is the power that Alice allocates to carrier k for the transmission of the information to Bob. This is a direct consequence of ⟨4.2⟩ if each carrier is studied independently.

⟨**4.20**⟩ **Properties (Positivity).** We see that we have a positive contribution to the secret-key rate from each carrier $k \in \{1, 2, \ldots, K\}$ with $q_k > 0$ independently of the relation of the corresponding channel gains a_k and b_k.

The monotonicity and convexity properties of the secret-key rate R_K can be derived applying the first and second derivatives that were calculated in ⟨4.4⟩ in the context of the basic scenario.

⟨**4.21**⟩ **Properties (Monotonicity).** With ⟨4.5⟩, we can provide some statements on the monotonicity of the secret-key rate R_K in the components of the vectors a, b, and q under the assumption that all other variables are fixed. We assume that $a_k, b_k > 0$ and $q_k \geq 0$ holds for all $k \in \{1, 2, \ldots, K\}$. Then, the secret-key rate R_K in ⟨4.19⟩ is

a) monotonically increasing in a_k,
b) monotonically decreasing in b_k, and
c) strictly monotonically increasing in q_k.

⟨**4.22**⟩ **Remark.** The first two statements on the monotonicity of R_K can be formulated more precisely by adding "strictly" to each statement if we assume that $q_k > 0$ holds for the corresponding carrier $k \in \{1, 2, \ldots, K\}$.

⟨**4.23**⟩ **Properties (Convexity).** The Hessian matrices of R_K with respect to a, b, and q are diagonal. For a and q, these matrices have only non-positive diagonal entries (see ⟨4.6⟩), i.e., they are negative semi-definite. Furthermore, we see that the Hessian matrix with respect to b has only non-negative diagonal entries, i.e., it is positive semi-definite. This allows us to formulate the convexity properties of R_K with respect to the vectors a, b, and q under the assumption that all other variables are fixed. The secret-key rate R_K in ⟨4.19⟩ is

a) a concave function of a,
b) a convex function of b, and
c) a concave function of q.

⟨**4.24**⟩ **Problem Formulation (Secret-Key Rate Maximization).** For given channel gain vectors a and b, the secret-key rate R_K in ⟨4.19⟩ should be maximized under a sum power constraint at the transmitter, i.e.,

$$\max_{q \in \mathcal{Q}} R_K(a, b, q)$$

where

$$\mathcal{Q} := \left\{ q \in \mathbb{R}^{1 \times K} \;\middle|\; q_k \geq 0 \text{ and } \sum_{k=1}^{K} q_k \leq P \right\}$$

is the set of all feasible power allocation vectors, which we have already defined in ⟨2.26⟩ in the context of the maximization of the secrecy rate R_S.

⟨**4.25**⟩ **Properties (Convexity of the Problem).** The convexity of the constraint set $\mathcal{Q}$ was shown in ⟨2.27⟩. For fixed channel gain vectors a and b, the secret-key rate R_K is a concave function of q on this set. Thus, we have a convex problem.

According to ⟨4.20⟩, we can basically use each carrier $k \in \{1, 2, \ldots, K\}$ in order to obtain a positive secret-key rate. This is an essential difference to the secrecy rate maximization of the multi-carrier scenario, where we only got a positive rate on carriers with $a_k > b_k$. Nevertheless, the optimal power allocation strategy for the secret-key rate maximization problem in ⟨4.24⟩ can directly be derived from the waterfilling solution in ⟨2.29⟩, which was derived for the secrecy rate maximization problem of the multi-carrier scenario.

⟨**4.26**⟩ **Optimal Strategy (Power Allocation).** The optimal transmit strategy for the secret-key rate maximization problem in ⟨4.24⟩ is the waterfilling solution

$$q_k(\mu) = \left[-\frac{c_k}{2} + \sqrt{\frac{d_k^2}{4} + \mu\, d_k} \right]^+$$

$$\text{with} \quad c_k := \sigma^2 \, \frac{a_k + 2b_k}{(a_k + b_k) b_k} \quad \text{and} \quad d_k := \sigma^2 \, \frac{a_k}{(a_k + b_k) b_k}$$

for the power allocation on all carriers $k \in \{1, 2, \ldots, K\}$. Due to the monotonicity in all components of q, the waterfilling parameter μ with $\mu \geq 0$ has to be chosen such that the power constraint is fulfilled with equality, i.e., $\sum_{k=1}^{K} q_k(\mu) = P$.

⟨**4.27**⟩ **Relation to Secrecy Rate.** We compare the secrecy rate R_S in ⟨2.22⟩ and the secret-key rate R_K in ⟨4.19⟩. For all channel gain vectors a and b and each given power allocation vector $q \in \mathcal{Q}$, we clearly have the relation $R_K(a, b, q) \geq R_S(a, b, q)$. If we consider the maximization of these rates over all $q \in \mathcal{Q}$, we have to take into account that the optimal strategies for both problems differ from each other. We know that the relation between the rates also holds for the power allocation vector that maximizes the secrecy rate R_S. But this vector is not necessarily optimal for the secret-key rate R_K. Consequently, we can write

$$\max_{q \in \mathcal{Q}} R_K(a, b, q) \geq \max_{q \in \mathcal{Q}} R_S(a, b, q).$$

In order to characterize the optimal power allocation for high and low SNR, we again interpret R_K in ⟨4.19⟩ as a function of the noise variance σ^2 (or its inverse ρ) for a fixed value of P.

⟨**4.28**⟩ **High-SNR Performance.** In the high-SNR regime, there exists a limit for the secret-key rate R_K, which is

$$\lim_{\sigma^2 \to 0} R_K(a, b, q) = \sum_{k \in \mathcal{K}} \log_2 \left(1 + \frac{a_k}{b_k} \right),$$

where

$$\mathcal{K} := \{ k \in \{1, 2, \ldots, K\} \,|\, q_k > 0 \}$$

is the set of carriers that Alice uses for the transmission to Bob. Note that we have already defined this set in ⟨2.31⟩. We see that this limit is determined by the quotients of the channel gains of the carriers that are used. From this, we can conclude that the optimal strategy that maximizes the secret-key rate limit in the high-SNR regime is to allocate non-zero power to all carriers $k \in \{1, 2, \ldots, K\}$. The comparison with the high-SNR limit of the secrecy rate R_S shows that for both limits the quotients of the channel gains are relevant. The main difference is the set of carriers that is optimally used in this regime. For the secrecy rate problem, only a subset of carriers is used, which is selected according to the relation of the channel gains of the carriers, while all carriers are used otherwise. The difference in the carrier selection together with the slightly differing rate expression always yields a greater high-SNR limit for the secret-key rate R_K compared to the secrecy rate R_S of the same scenario.

⟨**4.29**⟩ **Low-SNR Performance.** In the low-SNR regime, the limit of the secret-key rate R_K clearly is

$$\lim_{\rho \to 0} R_K(a, b, q) = 0.$$

We calculate the linear Taylor series representation of R_K at the point $\rho = 0$ and obtain

$$T_{R_K}(\rho; 0) = \frac{1}{\ln 2} \sum_{k \in \mathcal{K}} a_k \, q_k \, \rho.$$

The increase of the secret-key rate in the low-SNR regime is independent from the gains of the eavesdropper channel. It is only determined by the gains of the main channel and the carriers that are used for the transmission. Consequently, it is optimal to allocate full power to the carrier with the largest gain for the channel to the legitimated receiver. The resulting rate increase in the low-SNR regime is equal to that of a system without secrecy constraints and superior to the increase of the secrecy rate R_S in the same scenario.

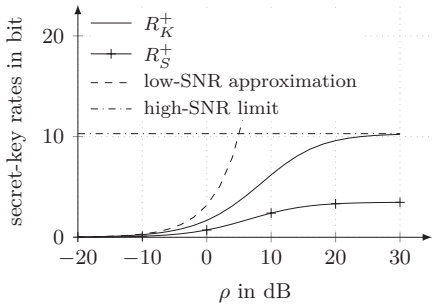
⟨**4.30**⟩ **Comparison of Secrecy and Secret-Key Rates.** For the comparison of both rates, we consider a combination of the secret-key rate and the subsequent data transmission for the key generation approach. As in ⟨4.15⟩, we use the combined rate

$$R_T^+ := \vartheta \, R_K^+ \quad \text{with}$$
$$\vartheta := \frac{R^+}{R^+ + R_K^+}.$$

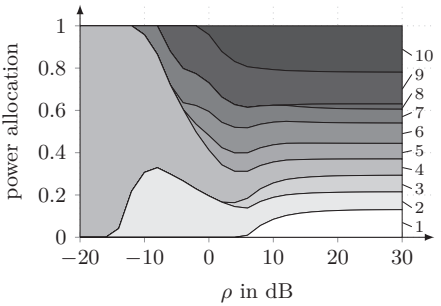
For the calculation of the rate comparison factor ϑ, we need the maximized secret-key rate R_K^+ and the maximized transmission rate R^+, which is determined by

$$\max_{q \in \mathcal{Q}} R(a, q) \quad \text{with}$$
$$R(a, q) := \sum_{k=1}^{K} \log_2 \left(1 + \frac{a_k q_k}{\sigma^2}\right).$$

The optimal transmit strategy for R^+ is standard waterfilling, see (Telatar, 1995), which clearly yields another power allocation vector than ⟨4.26⟩.



(a) maximized secret-key rate with high-SNR limit and low-SNR approximation



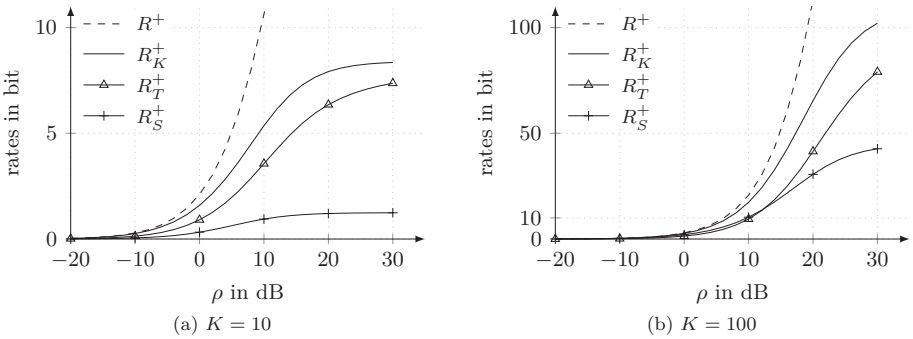
(b) optimal power allocation

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
0.4	1.8	0.6	2.2	1.1	1.2	1.6	0.1	1.4	0.9
b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}
0.5	1.5	1.1	1.8	1.5	1.1	2.0	1.7	0.6	0.3

Figure 4.4: The maximized secret-key rate and the corresponding power allocation.

⟨**4.31**⟩ **Illustration (High- and Low-SNR behavior).** Figure 4.4 illustrates the results we obtained for the secret-key rate maximization in the multi-carrier scenario. Continuing the example in ⟨2.34⟩, we choose again $K = 10$ carriers, $P = 1$ for the sum power constraint over these carriers, and the channel gains given in the table below the illustration. In contrast to the secrecy rate maximization in ⟨2.34⟩, Alice can use all channels for the transmission to Bob independently of the relation of the gains. In (a), the maximized secret-key rate R_K^+ is shown as function of the SNR with its low-SNR approximation according to ⟨4.29⟩ and its high-SNR limit according to ⟨4.28⟩. For comparison, the maximized secrecy rate R_S^+, which has already been shown in Figure 2.5, is also added. In (b), we choose a stacked plot to show the corresponding optimal power allocation over the SNR range. For low SNR, Alice allocates the complete power P to carrier 4, which is the carrier with the largest gain for the channel to Bob. The gain of the channel to Eve is not relevant in this case. This corresponds to the result of the low-SNR analysis in ⟨4.29⟩. With increasing SNR, Alice activates more and more carriers, where the order only depends on the gains of the channel to Bob. For high SNR, she finally uses all carriers. This high-SNR behavior has already been discussed in ⟨4.28⟩.

⟨**4.32**⟩ **Illustration (Comparison of Secrecy and Secret-Key Rates).** The example in ⟨2.37⟩ is continued in the following. Figure 4.5 compares the maximized secrecy and secret-key rates for different numbers of carriers with independently generated gains.



(a) $K = 10$ (b) $K = 100$

Figure 4.5: Comparison of the maximized secrecy rate R_S^+, the maximized secret-key rate R_K^+, and the combined rate R_T^+.

For the case with $K = 10$ carriers, which is illustrated in (a), we observe a relatively large gap between the maximized secret-key rate R_K^+ and the maximized secrecy rate R_S^+ over nearly the complete SNR range. Thus, Alice can mostly benefit from choosing the key generation approach, which yields the rate R_T^+ in average, instead of directly transmitting the information with the maximized secrecy rate R_S^+. With an increasing number of carriers, the relative differences between the individual rates shrink, which supports the approach of directly transmitting and ensuring the information at the same time. For the illustration in (b), $K = 100$ carriers were used. For low SNR, the maximized secrecy rate R_S^+ is greater than the combined rate R_T^+ for the key generation approach, although the differences are relatively small. Only if the SNR exceeds approximately $\rho = 12$ dB, we can observe that the key generation approach becomes more and more superior to the direct transmission with rate R_S^+. For high SNR, we know from the discussion in ⟨4.17⟩ that the combined rate R_T^+ converges to the maximized secret-key rate R_K^+, which is always greater than the maximized secrecy rate R_S^+, see ⟨4.27⟩.

4.3 Multi-Antenna Scenario

In this section, we extend the basic model from Section 4.1 to a multi-antenna scenario, where the two legitimated users, Alice and Bob, can use multiple transmit / receive antennas for their key agreement communication. Their common key should be kept secret from the eavesdropper Eve, who is also equipped with multiple antennas. Similar to Section 2.3, we restrict ourselves to the introduction of the system model and the corresponding secret-key rate expression, and the discussion of the properties of this function, which provides the basis for the worst-case analysis in the next chapter.

⟨**4.33**⟩ **System Model (Extension to Multi-Antenna Scenario).** For the key agreement in a multi-antenna scenario, we use the channel-type model from ⟨1.11⟩ together with the multi-antenna wiretap channel that was presented in ⟨2.40⟩. Consequently, we have a system, where Alice has L antennas to transmit her information. Bob and Eve have M and N receive antennas, respectively.

⟨**4.34**⟩ **Secret-Key Rate.** For this model, the secret-key rate R_K, which is interpreted as a function of the channel matrices H and G and the transmit covariance matrix Q with $Q \succeq 0$, can be evaluated according to ⟨1.13⟩, which yields

$$R_K(H, G, Q) = \log_2 \det\left(I_L + \rho\,(H^{\mathrm{H}}H + G^{\mathrm{H}}G)\,Q\right) - \log_2 \det\left(I_L + \rho\,G^{\mathrm{H}}G\,Q\right).$$

A detailed derivation of a comparable secret-key rate expression was done by Wong et al. (2009). The authors evaluated the mutual information and the resulting differential entropy expressions in the context of fast-fading MIMO wiretap channels.

With the Gramian matrix notation in ⟨2.42⟩, we introduce an equivalent expression for the secret-key rate R_K, which is useful for the formulation of optimization problems and the derivation of their properties.

⟨**4.35**⟩ **Secret-Key Rate (Equivalent Notation).** The secret-key rate R_K can be written as a function of the Gramian matrices A and B of the channel matrices H and G and the transmit covariance matrix Q. We write $R_K^\star$ instead of R_K if we refer to the secret-key rate in Gramian notation:

$$\begin{aligned} R_K^\star(A, B, Q) &= \log_2 \det\left(I_L + \rho\,(A+B)\,Q\right) - \log_2 \det\left(I_L + \rho\,B\,Q\right) \\ &= \log_2 \det\left(I_L + \rho\,Q^{\frac{1}{2}}(A+B)\,Q^{\frac{1}{2}}\right) - \log_2 \det\left(I_L + \rho\,Q^{\frac{1}{2}}B\,Q^{\frac{1}{2}}\right) \\ &= \log_2 \det\left(I_L + \rho\,(A+B)^{\frac{1}{2}}Q\,(A+B)^{\frac{1}{2}}\right) - \log_2 \det\left(I_L + \rho\,B^{\frac{1}{2}}Q\,B^{\frac{1}{2}}\right). \end{aligned}$$

In order to formulate the convexity properties of the secret-key rate in ⟨4.35⟩ with respect to its variables, we can use the properties that were presented for the secrecy rate in ⟨2.44⟩ together with some additional statements from the literature.

⟨**4.36**⟩ **Properties (Convexity).** The secret-key rate $R_K^\star$ in ⟨4.35⟩ is

a) a concave function of A and

b) a convex function of B.

Similar to the derivation in ⟨2.44⟩, we can argue that the first property holds since the $\log_2 \det$ function is concave for positive-semidefinite matrices. Thus, $R_K^\star$ is concave in $(I_L + \rho\,Q^{\frac{1}{2}}(A+B)\,Q^{\frac{1}{2}}) \succeq 0$, which in turn is a linear function of the matrix A. The second property follows from (Diggavi and Cover, 2001, Lemma II.3). With $(\rho\,Q^{\frac{1}{2}}A\,Q^{\frac{1}{2}}) \succeq 0$, we can conclude from this lemma that $R_K^\star$ is convex in $(I_L + \rho\,Q^{\frac{1}{2}}B\,Q^{\frac{1}{2}}) \succeq 0$, which in turn is a linear function of the matrix B.

Moreover, the secret-key rate $R_K^\star$ is

c) a concave function of Q if the relation between the matrices $(A+B)^{\frac{1}{2}}$ and $B^{\frac{1}{2}}$ can be expressed as $T\,(A+B)^{\frac{1}{2}} = B^{\frac{1}{2}}$ with $T \in \mathbb{C}^{L\times L}$ and $I_L - T^{\mathrm{H}}T \succeq 0$, where it is required that $(T^{\mathrm{H}}T)^{-1}$ exists in order to apply the proof from (Liang et al., 2009, Lemma C.1). The conditions above are clearly fulfilled if the matrices A and B have full rank[10], which implies that Bob and Eve have at least as many antennas as Alice, i.e., $M, N \geq L$.

[10] If we consider the concavity of the function $R_K^\star$ with respect to Q in the context of a maximization problem over all Q in a given set, we possibly can find other constraints, which are not as strict as the conditions above, that ensure the concavity of the secret-key rate $R_K^\star$ with respect to all Q in this certain set.

5 Worst-Case Studies for Secret-Key Rate Optimization

For the secret-key rate discussion in the previous chapter, we assumed that the transmitter Alice has perfect information about the channel to the eavesdropper Eve. In this chapter, we drop this assumption and introduce again a kind of partial information about the eavesdropper channel, which is available to the transmitter. It is only known that the coefficients of the eavesdropper channel are subject to a restriction, which allows us to model all possible eavesdropper channels by an infinite set reflecting this constraint. We focus again on the multi-antenna scenario, which can be used as a basis for the derivation of special cases representing the other scenarios we discussed before. First, we introduce the system model and the corresponding optimization problems. We then characterize the worst-case secret-key rate for each given transmit strategy. Afterwards, we derive and discuss upper and lower bounds for the maximization of this worst-case secret-key rate under a sum power constraint over all antennas at the transmitter.

⟨**5.1**⟩ **System Model.** We adopt the system model of the MIMO scenario, which was specified in ⟨4.33⟩, which is a combination of the fundamental channel-type model for key generation according to ⟨1.11⟩ and the multi-antenna wiretap channel from ⟨2.40⟩. Similar to the changes we made in ⟨3.1⟩, we specify a constraint for the channel G to Eve in order to model Alice's uncertainty about the real channel state of the eavesdropper channel. We formulate this constraint using the Frobenius norm of the channel G:

$$\|G\|_{\mathrm{F}}^2 = \mathrm{tr}(G^{\mathrm{H}}G) \leq \chi \quad \text{with} \quad \chi \geq 0.$$

As before, we still assume that Alice has perfect knowledge about the channel H to Bob. For the following worst-case discussion, we allow Eve to have more antennas than Alice, i.e., we assume $N \geq L$.

For known channel matrices H and G, the secret-key rate R_K was given in ⟨4.34⟩. With this function, we formulate two optimization problems for the system model in ⟨5.1⟩. The first problem is the identification of the worst-case secret-key rate for a given transmit covariance matrix, which corresponds to a minimization over all possible eavesdropper channel matrices. The second problem is the maximization of this worst-case secret-key rate over all transmit covariance matrices that fulfill the transmit power constraint. We formulate both problems with the variables from the system model and the corresponding Gramian notation, which is more suitable for the following analysis.

⟨**5.2**⟩ **Problem Formulation (Worst-Case Secret-Key Rate).** For each given channel matrix H and each given transmit strategy, which is specified by the transmit covariance matrix Q, the corresponding worst-case secret-key rate R_{W} is the minimal secret-key

rate that can be achieved if the minimization is carried out over all possible matrices for the channel from the transmitter to the eavesdropper, i.e.,

$$R_{\mathrm{W}}(H,Q) := \min_{G\in\mathscr{G}} R_K(H,G,Q),$$

where

$$\mathscr{G} := \left\{G \in \mathbb{C}^{N\times L} \,\middle|\, \mathrm{tr}(G^{\mathrm{H}}G) \leq \chi\right\}$$

is the set of all possible matrices for the channel from the transmitter to the eavesdropper, which we have already defined in ⟨3.2⟩. With the Gramian matrix notation defined in ⟨2.42⟩ and the corresponding secret-key rate expression in ⟨4.35⟩, we can equivalently formulate the worst-case secret-key rate problem as

$$R^{\star}_{\mathrm{W}}(A,Q) := \min_{B\in\mathscr{B}} R^{\star}_K(A,B,Q),$$

where $R^{\star}_{\mathrm{W}}$ is the worst-case secret-key rate adapted to the Gramian notation of the channel matrices and

$$\mathscr{B} := \left\{B \in \mathbb{C}^{L\times L} \,\middle|\, B \succeq 0 \text{ and } \mathrm{tr}(B) \leq \chi\right\}$$

is the set that corresponds to the set $\mathscr{G}$, see ⟨3.3⟩.

In order to characterize the properties of this optimization problem, we can use the properties of the MIMO secret-key rate that we discussed in the previous chapter.

⟨**5.3**⟩ **Properties (Convexity of the Problem).** According to ⟨3.4⟩, the constraint set $\mathscr{B}$ is convex. From ⟨4.36⟩, we know that $R^{\star}_K$ is a convex function of B on the set $\mathscr{B}$. Thus, we have a convex problem.

The transmitter aims to maximize the worst-case secret-key rate under a sum power constraint over all antennas, which results in a max-min optimization problem.

⟨**5.4**⟩ **Problem Formulation (Worst-Case Secret-Key Rate Maximization).** For a given channel matrix H, the worst-case secret-key rate R_{W} in ⟨5.2⟩, which was determined over the known set $\mathscr{G}$, should be maximized under a sum power constraint over all antennas at the transmitter, i.e.,

$$\max_{Q\in\mathscr{Q}} R_{\mathrm{W}}(H,Q) = \max_{Q\in\mathscr{Q}} \min_{G\in\mathscr{G}} R_K(H,G,Q),$$

where

$$\mathscr{Q} := \left\{Q \in \mathbb{C}^{L\times L} \,\middle|\, Q \succeq 0 \text{ and } \mathrm{tr}(Q) \leq P\right\}$$

is the set of all feasible transmit covariance matrices, which we have already defined in ⟨3.5⟩ for the maximization of the worst-case secrecy rate of the multi-antenna scenario. Again, we can use the Gramian matrix notation defined in ⟨2.42⟩ and the corresponding secret-key rate expression in ⟨4.35⟩ to reformulate the optimization problem:

$$\max_{Q\in\mathcal{Q}} R^{\star}_{\mathrm{W}}(A,Q) = \max_{Q\in\mathcal{Q}} \min_{B\in\mathcal{B}} R^{\star}_{K}(A,B,Q).$$

We can reduce the optimization problem in ⟨5.4⟩ to an equivalent optimization problem over the eigenvalues of Q and B.

⟨5.5⟩ Problem Formulation (Equivalent Problem). With the eigenvalue notation we introduced in ⟨3.9⟩, we can formulate the following. For a given vector a, the worst-case secret-key rate should be maximized under a sum power constraint over all antennas at the transmitter, i.e.,

$$\max_{q\in\mathcal{Q}} \widetilde{R}_{\mathrm{W}}(a,q) = \max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \widetilde{R}_{K}(a,b,q).$$

The vectors a and b contain the eigenvalues of the Gramian matrices A and B, which are derived from the channel matrices H and G, respectively. The vector q is the eigenvalue vector for the transmit covariance matrix Q. The function $\widetilde{R}_K$ with

$$\widetilde{R}_{K}(a,b,q) := \sum_{\ell=1}^{L} \left(\log_2\left(1+\rho\,(a_\ell+b_\ell)q_\ell\right) - \log_2\left(1+\rho\,b_\ell q_\ell\right)\right)$$

is a secret-key rate expression that only depends on the eigenvalues of the matrices A, B, and Q. The function $\widetilde{R}_{\mathrm{W}}$ is the worst-case secrecy rate for this case, which is defined as

$$\widetilde{R}_{\mathrm{W}}(a,q) := \min_{b\in\mathcal{B}} \widetilde{R}_{K}(a,b,q).$$

As in ⟨3.12⟩, the constraint sets for this problem are defined as

$$\mathcal{Q} := \left\{ q=(q_\ell)_{\ell=1}^{L} \in \mathbb{R}^{1\times L} \;\middle|\; q_\ell \geq 0 \text{ and } \sum_{\ell=1}^{L} q_\ell \leq P \right\} \quad \text{and}$$

$$\mathcal{B} := \left\{ b=(b_\ell)_{\ell=1}^{L} \in \mathbb{R}^{1\times L} \;\middle|\; b_\ell \geq 0 \text{ and } \sum_{\ell=1}^{L} b_\ell \leq \chi \right\}.$$

The equivalence of this optimization problem with the problem formulated in ⟨5.4⟩ is proven by a detailed and commented reformulation process, which is provided in ⟨B.4⟩ in the appendix.

The secret-key rate $\widetilde{R}_K$ of the eigenvalue problem corresponds to the secret-key rate of the multi-carrier scenario that is given in ⟨4.19⟩. Thus, we can directly apply its properties to the problem above.

⟨**5.6**⟩ **Properties (Monotonicity).** According to ⟨4.21⟩ and for all $\ell \in \{1, 2, \ldots, L\}$, the secret-key rate $\widetilde{R}_K$ in ⟨5.5⟩ is

a) monotonically increasing in a_ℓ,
b) monotonically decreasing in b_ℓ, and
c) monotonically increasing in q_ℓ.

⟨**5.7**⟩ **Properties (Convexity).** According to ⟨4.23⟩, the secret-key rate $\widetilde{R}_K$ in ⟨5.5⟩ is

a) a concave function of a,
b) a convex function of b, and
c) a concave function of q.

⟨**5.8**⟩ **Properties (Saddle-Point Problem).** In ⟨3.18⟩, we have already stated that the sets $\mathcal{Q}$ and $\mathcal{B}$ are convex. We know that the secret-key rate $\widetilde{R}_K$ is a convex function of b on the set $\mathcal{B}$. Thus, we obtain that the inner minimization problem in ⟨5.5⟩ is a convex problem. Additionally, the max-min problem in ⟨5.5⟩ is a saddle-point problem, since $\widetilde{R}_K$ is a concave function of $q \in \mathcal{Q}$ for all $b \in \mathcal{B}$ and a convex function of $b \in \mathcal{B}$ for all $q \in \mathcal{Q}$. Consequently, we can write according to (Sion, 1958):

$$\max_{q \in \mathcal{Q}} \min_{b \in \mathcal{B}} \widetilde{R}_K(a, b, q) = \min_{b \in \mathcal{B}} \max_{q \in \mathcal{Q}} \widetilde{R}_K(a, b, q).$$

⟨**5.9**⟩ **Optimal Strategy (Outer Problem).** For the maximization of the worst-case secret-key rate, the vector a, which specifies the channel from Alice to Bob, determines which components of the optimal power allocation vector q can be positive. The transmitter is only interested to allocate positive value to those components of q where the corresponding component of a is non-zero, since other terms do not contribute to a positive secret-key rate. This means that the transmitter has to take the number of receive antennas at the intended receiver into account. So far, the characterization of the optimal power allocation vector q does not differ from the characterization of the optimal strategy for the maximization of the worst-case secrecy rate in ⟨3.20⟩ and ⟨3.45⟩. But in contrast to the maximization of the worst-case secrecy rate, we do not have a minimum number of non-zero components in the optimal power allocation vector q since it is not possible to null the achievable secret-key rate with a certain vector b, see ⟨4.20⟩. Moreover, we know from ⟨5.6⟩ that the optimal power allocation vector q always uses full power P. For the worst-case secrecy rate, we have already obtained such a characterization for the adapted eigenvalue problem in ⟨3.40⟩, but not for the original problem in ⟨3.12⟩.

⟨**5.10**⟩ **Optimal Strategy (Solution of Inner Problem).** For the worst-case problem, the chosen power allocation vector q determines which components of the worst-case vector b can be positive. We can only have positive components in the worst-case vector b at positions where q is positive, since each zero in the power allocation vector nulls

the corresponding summand of the secret-key rate $\widetilde{R}_K$. For the components of b that correspond to a non-zero component of q, the optimal strategy for the inner problem can be obtained by evaluating the Karush-Kuhn-Tucker conditions, which are necessary and sufficient for this problem. This yields

$$b_\ell(\nu) = \left[-\left(\frac{1}{\rho q_\ell} + \frac{a_\ell}{2} \right) + \sqrt{\frac{a_\ell^2}{4} + a_\ell \nu} \right]^+$$

for all $\ell \in \{1, 2, \ldots, L\}$ with $q_\ell > 0$. Due to the monotonicity in all components of b, the waterfilling parameter ν with $\nu > 0$ has to be chosen such that the sum constraint of the set $\mathcal{B}$ is fulfilled with equality, i.e., $\sum_{\ell=1}^{L} b_\ell(\nu) = \chi$. Thus, we obtain a characterization of the worst-case vector b for the secret-key rate problem that is basically the same as for the secrecy rate problem. The only but essential difference is the expression we calculated for the waterfilling solution in both cases.

Regarding the number of Eve's antennas, we can draw the same conclusion as in ⟨3.21⟩ for the secrecy rate problem. If Eve has found the worst-case channel, she does not need more antennas for eavesdropping than Alice uses to transmit the message to Bob. We know from ⟨5.9⟩ that Alice adapts her transmit strategy to the number of antennas that Bob is equipped with. Hence, we can conclude again that it is sufficient if $N = \min\{L, M\}$ holds for the number of Eve's antennas.

⟨**5.11**⟩ **Optimal Strategy (Vector Ordering).** For the secrecy rate problem, we derived a result on the component ordering of the optimal vectors q and b in ⟨3.23⟩, which was based on the component ordering of the given vector a. But it is not possible to give a comparable characterization of the optimal vector component ordering for the secret-key problem in ⟨5.5⟩. Let us consider the equivalent min-max problem in ⟨5.8⟩ and study the behavior of the optimal vector q for fixed channels, which are specified by the vectors a and b. We can apply the results that we obtained for the high- and low-SNR characterization of the related multi-carrier scenario in ⟨4.28⟩ and ⟨4.29⟩. For low SNR, the optimal power allocation vector q mainly supports those components that correspond to large values of the vector a. For high SNR, the transmitter prefers components that are related to a large quotient of the values from a and b. Obviously, the ordering of the optimal vector q is not necessarily the same for the complete SNR range.

In addition to the sets defined in ⟨3.28⟩, we introduce a further constraint set, which allows us to derive bounds on the outer problem in the following.

⟨**5.12**⟩ **Notation.** With the vector $\iota := (\iota_\ell)_{\ell=1}^{L}$ and $\iota_\ell \geq 0$ for all $\ell \in \{1, 2, \ldots, L\}$, we define

$$\mathcal{Q}_\iota := \left\{ q = (q_\ell)_{\ell=1}^{L} \in \mathbb{R}^{1 \times L} \,\middle|\, 0 \leq q_\ell \leq \iota_\ell \right\}.$$

⟨**5.13**⟩ **Bounds on Outer Problem.** For the derivation of bounds on the maximized worst-case secret-key rate in ⟨5.5⟩, we can use the approach that was presented in ⟨3.27⟩ for the maximized worst-case secrecy rate. We can adapt the constraint sets by adding further constraints or relaxing the already given constraints in order to obtain upper and lower bounds on the problem. Note that we are allowed to interchange the minimization and the maximization, since we have a saddle-point problem.

⟨**5.14**⟩ **Upper Bounds.** Upper bounds can be calculated by adding further constraints to the set $\mathcal{B}$, which instead yields a set $\mathcal{B}^-$ for the inner minimization, or by relaxing the constraints of the set $\mathcal{Q}$, which provides a set $\mathcal{Q}^+$ for the outer maximization. As in ⟨3.29⟩, we can use each set $\mathcal{B}^-$ that is defined as $\mathcal{B}^- := \mathcal{B}_\beta$ with a fixed vector $\beta \in \mathcal{B}$ for the derivation of an upper bound on the problem in ⟨5.5⟩. Hence, the worst-case vector b becomes independent from the chosen transmit strategy q. Due to the monotonicity of $\widetilde{R}_K$ in each component of the vector b, the worst-case secret-key rate is then given by $\widetilde{R}_K(a, \beta, q)$ for all $q \in \mathcal{Q}$. For the outer maximization of the upper bound, we can apply the waterfilling solution in ⟨4.26⟩, which was derived for the related multi-carrier scenario, where we had fixed channel coefficients. A tight upper bound for the high-SNR regime can be obtained if all components of β are chosen to be positive, where the values are calculated according to the waterfilling solution in ⟨5.10⟩ with $\rho \to \infty$. Alternatively, an upper bound on the maximized worst-case secret-key rate can be obtained considering the equivalent min-max problem in ⟨5.8⟩. The constraints for the maximization can be relaxed by using a set $\mathcal{Q}^+$ that is defined as $\mathcal{Q}^+ := \mathcal{Q}_\iota$ with $\iota = (P)_{\ell=1}^L$. Then, the optimal transmit strategy q is independent from the previously chosen vector b. Due to the monotonicity of $\widetilde{R}_K$ in each component of the vector q, we obtain a maximized secret-key rate $\widetilde{R}_K(a, b, \iota)$ for all $b \in \mathcal{B}$, which can be minimized afterwards by applying the waterfilling solution in ⟨5.10⟩. But we cannot expect that this approach yields a tight upper bound since the sum power constraint was dramatically relaxed.

⟨**5.15**⟩ **Lower Bounds.** Lower bounds can be calculated by adding further constraints to the set $\mathcal{Q}$, which yields a set $\mathcal{Q}^-$ for the outer maximization, or by relaxing the constraints of the set $\mathcal{B}$, which provides a set $\mathcal{B}^+$ for the inner minimization. We can use each set $\mathcal{Q}^-$ that is defined as $\mathcal{Q}^- := \mathcal{Q}_\iota$ with a fixed vector $\iota \in \mathcal{Q}$ for the derivation of a lower bound. As in ⟨5.14⟩, we consider the equivalent min-max problem in ⟨5.8⟩. With the same argumentation as above, the maximized secret-key rate is $\widetilde{R}_K(a, b, \iota)$ for each $\iota \in \mathcal{Q}$, which can be minimized afterwards by applying the corresponding waterfilling solution in ⟨5.10⟩. Especially interesting are bounds that are tight for a certain SNR regime since tight upper bounds deliver not only achievable rates, but they provide also a power allocation strategy that is close to optimal. We will see in ⟨5.17⟩ that a uniform allocation of the complete power over all components of ι that correspond to a non-zero component of a yields a tight lower bound for high SNR. For low SNR, a tight lower bound is obtained by allocating the complete power to that component of ι that corresponds to the largest value in a, see ⟨5.18⟩. Alternatively, a lower bound on the maximized worst-case secret-key rate can be calculated after relaxing the constraint set $\mathcal{B}$ for the

inner minimization. Instead, we use $\mathcal{B}^+$ that is defined as $\mathcal{B}^+ := \mathcal{B}_\beta$ with $\beta = (\chi)_{\ell=1}^L$. As in ⟨5.14⟩, the worst-case secret-key rate, which is then $\widetilde{R}_K(a, \beta, q)$ for all $q \in \mathcal{Q}$, can be maximized by applying the waterfilling solution in ⟨4.26⟩. Generally, this approach will not give a tight lower bound since the sum constraint of the set $\mathcal{B}$ was relaxed too much.

⟨**5.16**⟩ **Relation to Secrecy Rates.** If we want to compare the maximized worst-case secrecy rates from ⟨3.12⟩ and ⟨3.40⟩ with the maximized worst-case secret-key rate from ⟨5.5⟩, we have to consider the corresponding rate expressions first. For a given vector a, which characterizes the channel from Alice to Bob, each vector $b \in \mathcal{B}$ for the channel to Eve, and each power allocation vector $q \in \mathcal{Q}$, we have the relation

$$\widetilde{R}_K(a, b, q) \geq \bar{R}_S(a, b, q) \geq \widetilde{R}_S(a, b, q).$$

If we consider the minimization of these rates over all $b \in \mathcal{B}$, we have to take into account that the worst-case strategies for the problems differ from each other. The relation between the rates also holds for each worst-case vector that results from any given power allocation vector $q \in \mathcal{Q}$. Although this worst-case vector minimizes the secret-key rate $\widetilde{R}_K$ for the given $q \in \mathcal{Q}$, it is generally not the worst-case vector for minimizing the secrecy rate $\bar{R}_S$, which in turn provides not necessarily the optimal strategy for minimizing the secrecy rate $\widetilde{R}_S$. This yields that the relation above can also be applied if we consider the worst-case rates for each given $q \in \mathcal{Q}$, i.e.,

$$\min_{b\in\mathcal{B}} \widetilde{R}_K(a, b, q) \geq \min_{b\in\mathcal{B}} \bar{R}_S(a, b, q) \geq \min_{b\in\mathcal{B}} \widetilde{R}_S(a, b, q).$$

With an analogous argumentation, we can compare the rates that result from the maximization of these worst-case rates over all $q \in \mathcal{Q}$. Consequently, we can write

$$\max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \widetilde{R}_K(a, b, q) \geq \max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \bar{R}_S(a, b, q) \geq \max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \widetilde{R}_S(a, b, q)$$

for any given vector a.

In order to characterize the optimal strategies for high and low SNR, we take the same approach as before and interpret $\widetilde{R}_K$ in ⟨5.5⟩ as a function of the inverse noise variance ρ for a fixed value of P.

⟨**5.17**⟩ **High-SNR Performance.** For the high-SNR regime, we calculate the limit for the secret-key rate $\widetilde{R}_K$, which is

$$\lim_{\rho\to\infty} \widetilde{R}_K(a, b, q) = \lim_{\rho\to\infty} \sum_{\ell=1}^{L} \log_2 \left(\frac{1 + \rho\,(a_\ell + b_\ell) q_\ell}{1 + \rho\, b_\ell q_\ell} \right) = \sum_{\ell\in\mathcal{L}} \log_2 \left(1 + \frac{a_\ell}{b_\ell} \right),$$

where

$$\mathcal{L} := \{\ell \in \{1, 2, \ldots, L\} \,|\, q_\ell > 0\}$$

is the set of vector components that is used for the transmission to Bob, which we have already defined in ⟨3.31⟩. Note that this limit corresponds to the high-SNR limit in ⟨4.28⟩, which we obtained for the related multi-carrier problem. In principle, we can state the same as for the high-SNR limit of the maximized worst-case secrecy rate in ⟨3.31⟩. In order to ensure that this limit exists, the worst-case vector b has to be chosen such that it has positive values at all positions that correspond to a positive value in the power allocation vector q. Optimally, it has only positive values at the same positions as q, i.e., $b_\ell > 0$ holds for all $\ell \in \mathcal{L}$, whereas $b_\ell = 0$ holds for all $\ell \notin \mathcal{L}$. The difference between both problems are the values that are optimally assigned to those non-zero components. For the secret-key rate problem, the optimal strategy for the worst-case vector b in ⟨5.10⟩ converges to[11]

$$b_\ell(\nu) = -\frac{a_\ell}{2} + \sqrt{\frac{a_\ell^2}{4} + a_\ell \nu} = \frac{a_\ell}{2}\left(\sqrt{1 + \frac{4\nu}{a_\ell}} - 1\right)$$

for all $\ell \in \mathcal{L}$, which is always positive for $\nu > 0$. Thus, it is always possible to obtain positive values for all components in $b \in \mathcal{L}$ independently of the given a. Consequently, we know that the limit above always exists. We see that the maximum of this worst-case high-SNR limit is not directly influenced by the values of the power allocation vector q. It is only relevant which components are chosen for the transmission. Thus, the remaining problem can be formulated as

$$\max_{\mathcal{L}} \sum_{\ell \in \mathcal{L}} \log_2\left(1 + \frac{2}{\sqrt{1 + \frac{4\nu}{a_\ell}} - 1}\right).$$

We observe that each rate summand above is positive if we assume $\nu > 0$. From this, we can conclude that the optimal strategy that maximizes the worst-case secret-key rate limit in the high-SNR regime is to allocate non-zero power to all components of q that correspond to positive values in a. For instance, this could be a uniform allocation of the power P over these components. This is in contrast to the maximization of the worst-case secrecy rate limit for high SNR in ⟨3.32⟩, where it was not necessarily optimal to use all components of q. Note that we obtained a similar result in ⟨3.49⟩ for the maximization of the high-SNR limit of the adapted worst-case secrecy rate problem.

⟨**5.18**⟩ **Low-SNR Performance.** From the results of the related multi-carrier scenario in ⟨4.29⟩, we can see that the limit of the secret-key rate $\widetilde{R}_K$ in the low-SNR regime is

$$\lim_{\rho \to 0} \widetilde{R}_K(a, b, q) = 0.$$

[11] For the formulation of the right-hand side, we have to assume that $a_\ell > 0$ holds for all $\ell \in \mathcal{L}$, which is guaranteed if we consider the optimal power allocation q according to ⟨5.9⟩, since the transmitter is only interested in allocating power to components of q that can contribute to a positive secret-key rate.

The linear Taylor series representation of $\widetilde{R}_K$ at the point $\rho = 0$ is

$$T_{\widetilde{R}_K}(\rho; 0) = \frac{1}{\ln 2} \sum_{\ell \in \mathcal{L}} a_\ell \, q_\ell \, \rho$$

with $\mathcal{L}$ as defined in ⟨5.17⟩. We observe that the increase of the secret-key rate in the low-SNR regime is independent from the vector b, which characterizes the eavesdropper channel. It is only influenced by the vector a, which characterizes the main channel to the intended receiver, and the power allocation vector q, which is chosen by the transmitter. Thus, the minimization of the linear Taylor series coefficient over all feasible channels to the eavesdropper is not relevant. We only have to consider the maximization of this expression over all power allocation vectors $q \in \mathcal{Q}$. Consequently, we obtain the same characterization of the optimal strategy as in ⟨4.29⟩ for the related multi-carrier scenario. The transmitter assigns full power to that component of q that corresponds to the largest value in the vector a. This strategy completely differs from the maximization of the worst-case secrecy rate in the low-SNR regime, which was studied in ⟨3.32⟩ and ⟨3.50⟩, where the transmitter generally intended to use more than one vector component.

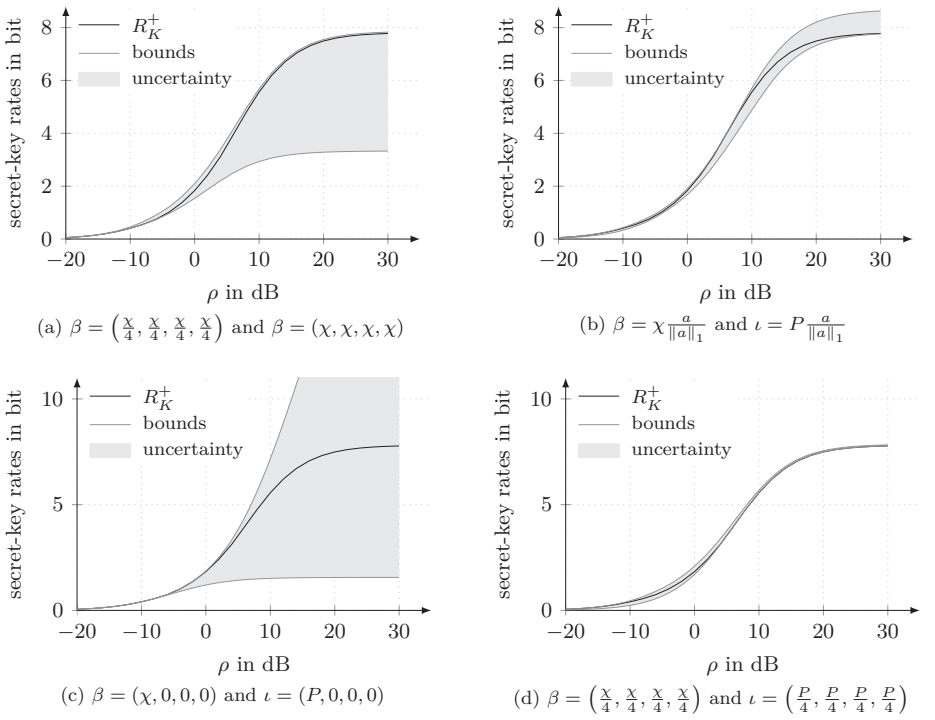
⟨**5.19**⟩ **Comparison of Secrecy and Secret-Key Rates.** In order to establish a relatively fair comparison between the approaches we discussed in the context of our worst-case studies, we calculate again a rate R_T^+, which does not only consider the achievable secret-key rate, but also takes the subsequent data transmission into account, which is necessary for this approach. As in ⟨4.30⟩, the combined rate is calculated as

$$R_T^+ := \vartheta \, R_K^+ \quad \text{with}$$
$$\vartheta := \frac{R^+}{R^+ + R_K^+}.$$

The rate comparison factor ϑ is determined by the maximized worst-case secret-key rate R_K^+ and the maximized transmission rate R^+. The latter is equivalent to the maximized transmission rate R^+ of the multi-carrier scenario, which was given in ⟨4.30⟩.

⟨**5.20**⟩ **Illustration (Bounds).** For the illustration of the results on the maximized worst-case secret-key rate, we continue the example in ⟨3.33⟩, where we discussed the results we obtained for the maximized worst-case secrecy rate. Hence, we consider a scenario with $L = M = N = 4$ antennas for each user, where the channel between Alice and Bob is characterized by $a = (3.9, 1.5, 1.0, 0.6)$ and the transmit power constraint is specified by $P = 1$. For the norm constraint on the channel from Alice to Eve, we assume again $\chi = 2$.

Figure 5.1 shows upper and lower bounds that were derived for the maximized worst-case secret-key rate of this scenario. The area between the upper and lower bounds illustrates the remaining uncertainty about the exact value of the maximized worst-case secret-key rate, which is denoted by R_K^+ and included in the diagrams for comparison. Strictly



(a) $\beta = \left(\frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}\right)$ and $\beta = (\chi, \chi, \chi, \chi)$

(b) $\beta = \chi \frac{a}{\|a\|_1}$ and $\iota = P \frac{a}{\|a\|_1}$

(c) $\beta = (\chi, 0, 0, 0)$ and $\iota = (P, 0, 0, 0)$

(d) $\beta = \left(\frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}\right)$ and $\iota = \left(\frac{P}{4}, \frac{P}{4}, \frac{P}{4}, \frac{P}{4}\right)$

Figure 5.1: Upper and lower bounds on the maximized worst-case secret-key rate R_K^+ and the remaining uncertainty regions between the bounds.

speaking, it is an approximation, which was determined by an exhaustive search[12] over all possible power allocation vectors q using a step size of 0.010 for each component.

For (a), the upper and lower bound were derived by manipulating the inner minimization according to ⟨3.27⟩. For the derivation of the upper bound, we can use each vector $\beta \in \mathcal{B}$. For the diagramm in (a), we choose $\beta = \left(\frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}, \frac{\chi}{4}\right)$, which yields a relatively good upper bound for high SNR, although β is not the high-SNR worst-case vector according to ⟨5.17⟩. The lower bound was parametrized by $\beta = (\chi, \chi, \chi, \chi)$, which cannot provide a

[12] We have already used this approach for determining the maximized worst-case secrecy rates in Chapter 3 and consequently applied it also to this problem. It is also possible to alternatively use a method that was presented by Nedić and Ozdaglar (2009), which exploits the saddle-point property of the problem. This method allows the computation of approximate saddle points with a finite number of iterations and a constant step size.

good lower bound in general since the sum constraint on the channel to Eve was relaxed too much, see ⟨5.18⟩. But it is the strictest vector we can use if we try to derive a lower bound by adapting the constraint for the inner minimization. Thus, we will further change the constraint set for the outer maximization for the derivation of upper bounds, whereas we maintain the approach of manipulating the inner minimization for the calculation of lower bounds.

The illustration in (b) shows the bounds that result from scaled versions of the parameter vector a. We observe that this results in an acceptable uncertainty over the complete SNR range. Obviously, the chosen parameter vector β significantly differs from the worst-case vector that was derived in ⟨5.17⟩. Consequently, the upper bound tends to a high-SNR limit that is greater than the limit of the maximized worst-case secret-key rate, i.e., it is not tight for high SNR. But we know from ⟨5.17⟩ that the given parameter vector ι is a relatively good choice for the lower bound since a power allocation vector whose components are all non-zero yields a tight lower bound for high SNR.

In (c), we exemplarily see the bounds that we obtain by concentrating the sum constraint values P and χ on the first components of the corresponding vectors. Clearly, these parameter vectors cannot be good for high SNR, but they provide tight bounds in the low-SNR regime. According to ⟨5.18⟩, it is optimal there to allocate full power to that component of q that corresponds to the largest value in a independently of the vector b. The resulting worst-case vector is consequently given by assigning χ to the corresponding component of b, see ⟨5.10⟩. Thus, we obtain the same parameter combination for the upper and lower bound, resulting from the given vectors $\beta = (\chi, 0, 0, 0)$ and $\iota = (P, 0, 0, 0)$, respectively.

The bounds that are derived by a uniform allocation over all four vector components are shown in (d). Obviously, these parametrizations yield bounds that are very close to optimal over the complete SNR range. Especially for high SNR, we know that it is optimal for both strategy vectors to use non-zero values for all components.

The illustration in Figure 5.2 (a) shows the minimum upper and maximum lower bounds we found by evaluating a certain number of upper and lower bounds for the example above over the complete SNR range. In addition to the bounds from Figure 5.1, we also considered further bounds that were derived from uniform allocations over a varied number of non-zero vector components as in Figure 3.5. We see that the remaining uncertainty is relatively small, which provides us nearly the exact value of the maximized worst-case secret-key rate over the complete SNR range. Furthermore, the power allocation vectors that were used for the derivation of the lower bound provide a good approximation for the optimal transmit strategy for the problem in ⟨5.5⟩. In Figure 5.2 (b), we illustrate the minimum upper and maximum lower bounds for a slightly changed scenario, where we used the same specification for the channel from Alice to Bob as before, but allowed a significantly better eavesdropper channel by choosing $\chi = 5$ for the channel constraint. We observe the same behavior as before for $\chi = 2$. By simply calculating some upper and lower bounds, we obtain a relatively good approximation of the maximized worst-case

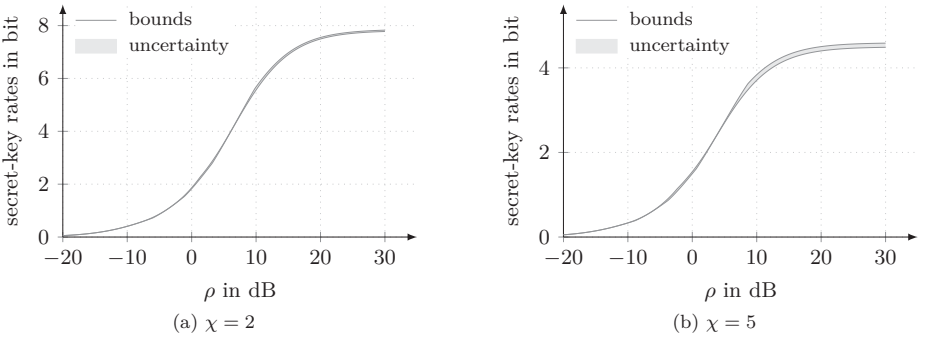
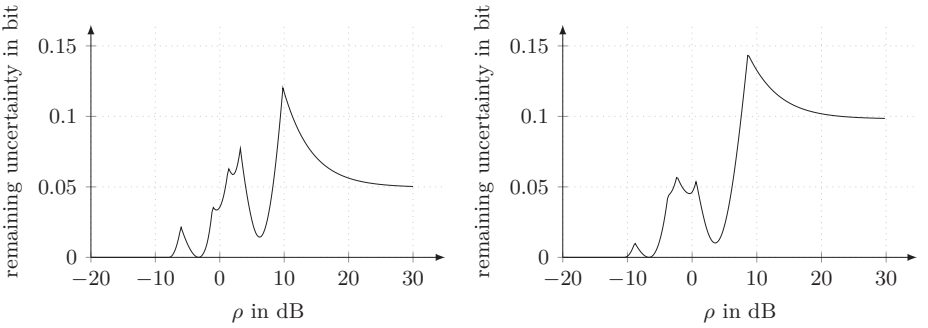


Figure 5.2: Minimum upper and maximum lower bounds on the maximized worst-case secret-key rate R_K^+ and the remaining uncertainty regions between the bounds.

secret-key rate over the complete SNR. Although there remains a small gap between the bounds for high SNR, we obtain a good estimation of the optimized rate since we know that a tight lower bound for this range was included in the calculation of these final bounds. The absolute values of the remaining uncertainty between the bounds in Figure 5.2 are shown in Figure 5.3. The peaks in the curves are located at positions where we have intersections of the originally evaluated bounds. For high SNR, we see that the remaining uncertainty tends to about 0.05 bit and 0.10 bit for the example with $\chi = 2$ and $\chi = 5$, respectively. In both cases, the largest values do not exceed 0.15 bit.

⟨**5.21**⟩ **Illustration (High- and Low-SNR Behavior).** Figure 5.4 illustrates the high- and low-SNR behavior of the maximized worst-case secret-key rate R_K^+ of the problem in ⟨5.5⟩. The low-SNR approximation in (a) results from ⟨5.18⟩. Its value is only determined by the largest component of the vector a, which characterizes the channel from Alice to Bob, and the transmit power constraint P, but independent from the eavesdropper channel and its constraint. The optimal power allocation vector allocates full power to the first vector component, which corresponds to the largest component of the vector a. The worst-case vector that results from ⟨5.10⟩ for the secret-key rate is given by $b = (\chi, 0, 0, 0)$. In (b), it can be observed that the maximized worst-case secret-key rate R_K^+ converges to the limit that was calculated with a power allocation that uses all components of the vector q. The corresponding worst-case vector for high SNR can be calculated according to ⟨5.17⟩.

⟨**5.22**⟩ **Illustration (Optimal Strategies).** Figure 5.5 shows the values of the optimal vectors and the resulting secret-key rate summands for selected SNR values, which allows us to analyze the predicted low- and high-SNR behavior in detail. In (a) and (b), which provide the optimal vectors for $\rho = -20$ dB and -10 dB, we see that the transmitter concentrates the available power in the first component of q. From the discussion in



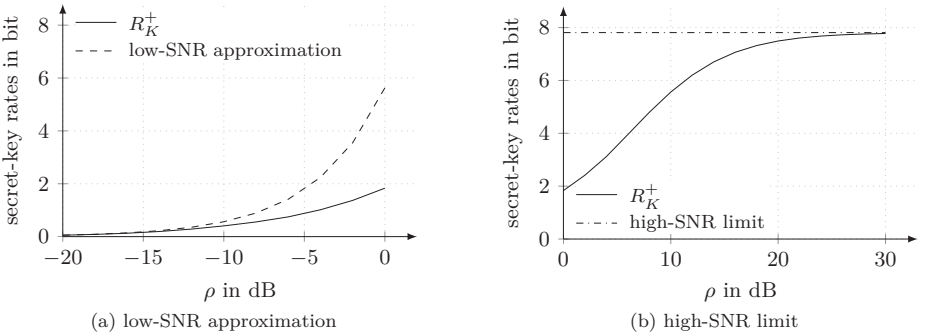
(a) $\chi = 2$ (b) $\chi = 5$

Figure 5.3: Absolute values of the remaining uncertainty between the bounds in Figure 5.2.

⟨5.18⟩, it follows that this is the optimal power allocation vector for low SNR. The only non-zero component of the resulting worst-case channel is the first vector component, which takes the value χ. Note that this behavior does not change with a variation of the constraint value χ for the eavesdropper channel, even if χ exceeds the largest value in a. This is in contrast to both secrecy rate problems in Chapter 3, where the optimal strategies for low SNR were influenced by this parameter.

With increasing SNR, Alice distributes the available power over more and more components of the vector q. For high SNR, she finally uses all components of the power allocation vector for the transmission to Bob. If we compare the results for $\rho = 10$ dB, 20 dB and 30 dB, which are shown in (d), (e), and (f), we see that the transmitter chooses a uniform allocation of the available power over all four components of q. The resulting worst-case vectors slightly differ from each other since the waterfilling result from ⟨5.10⟩ is not only influenced by the vectors a and q, but also from the inverse noise variance ρ. We can observe that the worst-case vector b converges to the vector that is specified in ⟨5.17⟩ with growing SNR.

⟨**5.23**⟩ **Illustration (Variation of Channel Constraint).** We continue the example above by analyzing the influence of the parameter χ, which constrains the quality of the channel from Alice to Eve. Figure 5.6 shows that the maximized worst-case secret-key rate R_K^+ is reduced by an increase of the parameter χ, which corresponds to a more "powerful" eavesdropper channel. The diagram in (a) allows us to compare the maximized worst-case secret-key rates with the achievable rate of a transmission without secrecy constraints, which is represented by $\chi = 0$. The illustration in (b) focuses on the comparison of the maximized worst-case secret-key rates for various values of χ. In the low-SNR regime, the differences between the curves are not significant since the low-SNR increase of all rates is determined by the largest value of the vector a independently of the quality of



(a) low-SNR approximation (b) high-SNR limit

Figure 5.4: The maximized worst-case secret-key rate R_K^+ with its low-SNR approximation and its high-SNR limit.

the eavesdropper channel. This behavior is in contrast to the low-SNR performance we observed for the maximized secrecy rate in Figure 3.11, where a growing channel constraint parameter clearly decreased the achievable rate also for low SNR. With increasing SNR, the maximized worst-case secret-key rates converge to their individual high-SNR limits according to ⟨5.17⟩, which are obviously influenced by the value of the parameter χ. In (b), we can observe that we obtain positive values for the maximized worst-case secret-key rates even if the eavesdropper channel is better than the main channel to the intended receiver. We have already discussed this behavior for the basic scenario with fixed channel gains in ⟨4.16⟩.

⟨5.24⟩ Illustration (Comparison of Secrecy and Secret-Key Rates). We proceed with the example above in order to compare the key generation approach with the direct secret transmission of the data as discussed in Chapter 3. Figure 5.7 shows a comparison of the maximized worst-case secrecy rate $\bar{R}_S^+$ of the adapted problem in ⟨3.40⟩, the maximized secret-key rate R_K^+ of the problem in ⟨5.5⟩, and the combined rate R_T^+, which is calculated according to ⟨5.19⟩ in order to allow a relatively fair comparison of $\bar{R}_S^+$ and R_K^+ by additionally considering the subsequent data transmission with rate R^+ in the key generation approach. These rates are illustrated in (a) and (b) for $\chi = 2$ and $\chi = 5$, respectively. In principle, we can observe the same behavior of the rates as in ⟨4.17⟩, where we discussed the rate comparison for the basic scenario with fixed channel gains. If the eavesdropper channel is assumed to be comparably bad, the gap between the maximized worst-case secrecy rate $\bar{R}_S^+$ and the maximized secret-key rate R_K^+ is comparably small, although R_K^+ is always greater than $\bar{R}_S^+$, see ⟨5.16⟩. Thus, the additional effort for transmitting the encrypted information after the key generation significantly affects the combined rate that is achievable for the key generation approach. Consequently, we observe in (a) for $\chi = 2$ that the direct transmission of the data with rate $\bar{R}_S^+$ is superior

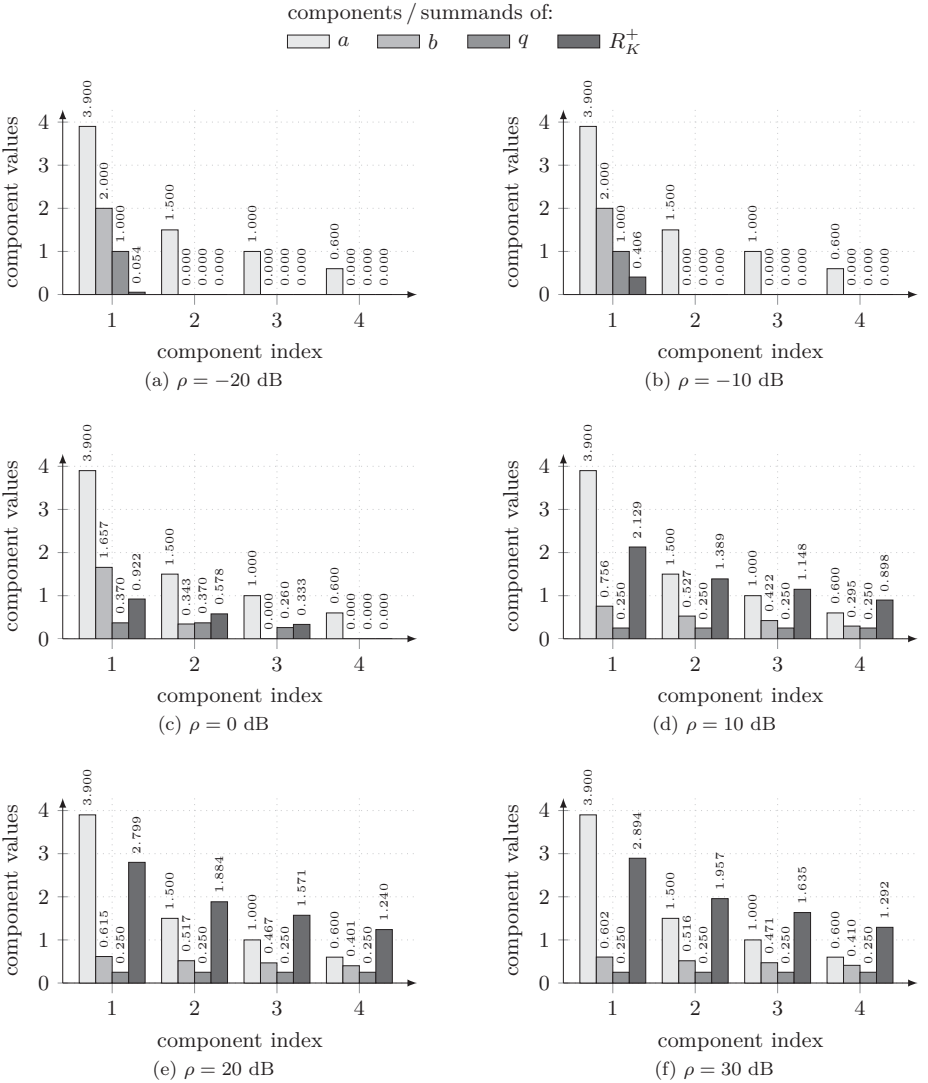
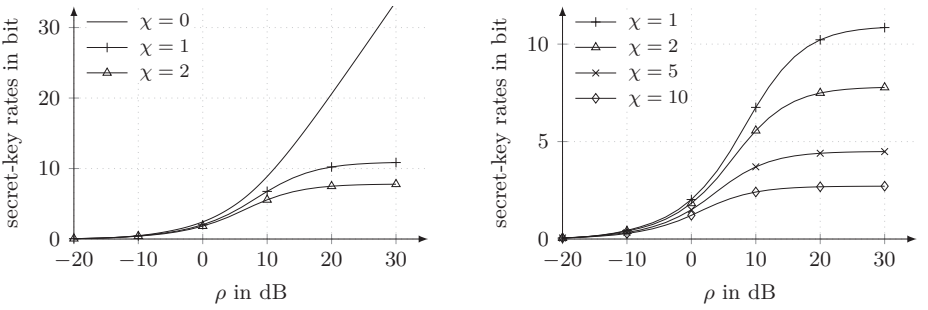


Figure 5.5: Optimal vectors corresponding to the maximized worst-case secret-key rate R_K^+ for selected SNR values.



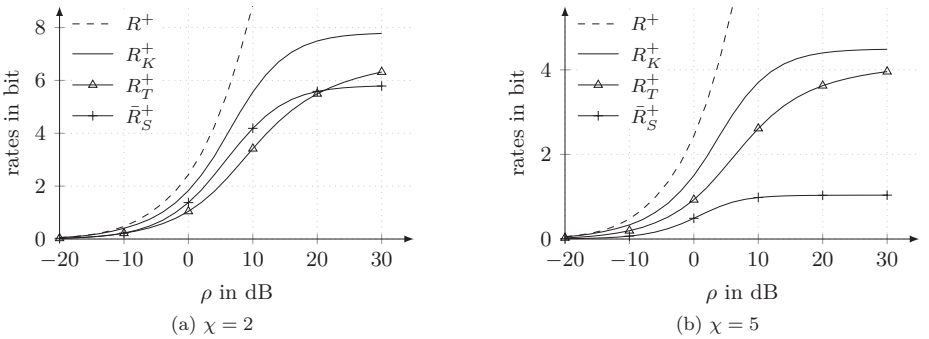
(a) comparison with / without secrecy constraints

(b) influence of channel constraint parameter χ

Figure 5.6: The maximized worst-case secret-key rate R_K^+ for various values of the constraint parameter χ for the channel from Alice to Eve.

to the key generation approach for low and medium SNR. If ρ exceeds about 22 dB, the advantage of the key generation approach becomes more and more evident. For high SNR, the combined rate R_T^+ finally converges to the maximized secret-key rate R_K^+. With a better eavesdropper channel, which is associated with larger gaps between the maximized worst-case rates $\bar{R}_S^+$ and R_K^+, Alice can more benefit from the key generation approach, although the achievable rates are generally decreased. In (b), we observe for $\chi = 5$ that the key generation approach is completely superior to the direct transmission with rate $\bar{R}_S^+$ in the simulated SNR range from $\rho = -20$ dB to 30 dB. If the constraint on the eavesdropper channel is further relaxed, such that Eve is allowed to have a better channel than Bob, only the key generation approach is suitable for a secret transmission to Bob since the maximized worst-case secrecy rates are zero in this case.

⟨**5.25**⟩ **Special Case (Multiple-Input Single-Output Scenario).** We continue the MISO scenario in ⟨3.56⟩, where Bob has only one antenna, whereas we do not formulate any constraint on the numbers of antennas that Alice and Eve are equipped with. As described in ⟨3.56⟩, the channel to Bob reduces to a (row) vector h, whose Gramian matrix $A = h^{\mathrm{H}}h$ consequently has rank one. The only non-zero eigenvalue of this matrix is $a_1 > 0$. Thus, only the first components of the optimal power allocation vector q and the worst-case vector b are non-zero, and we clearly obtain $q_1 = P$ and $b_1 = \chi$. We observe that the optimal strategies for the maximized worst-case secrecy and secret-key rate are identical. Moreover, we see that the secret-key rate expression we obtain with these strategies matches the secret-key rate of the basic scenario in Section 4.1, which allows us to directly transfer all results from that section to this MISO scenario. For the comparison between the maximized worst-case secrecy and secret-key rates, we can apply the conclusions from Figure 4.3, i.e., the influence of the eavesdropper channel constraint on the preferred communication strategy directly follows from the discussion in ⟨4.17⟩.



(a) $\chi = 2$ (b) $\chi = 5$

Figure 5.7: Comparison of the maximized secrecy rate $\bar{R}_S^+$, the maximized secret-key rate R_K^+, and the combined rate R_T^+.

⟨**5.26**⟩ **Application to Multi-Carrier Scenario.** The results from this chapter can easily be transferred to the related multi-carrier scenario, which was described in ⟨3.57⟩ in the context of maximizing the worst-case secrecy rate. The secret-key rate expressions in ⟨4.19⟩ and ⟨5.5⟩ are identical, which allows us to apply all the results from this chapter to the related multi-carrier scenario without further restrictions.

⟨**5.27**⟩ **Extension to Multiple Eavesdroppers.** Although all results in this chapter were derived for a system model with only one eavesdropper, they can be applied to a scenario with multiple non-cooperating eavesdroppers as well. A strategy that ensures the secrecy of the transmitted data against the worst-case eavesdropper simultaneously guarantees the secrecy of the information against all other eavesdroppers whose channels can be characterized by the same constraint. If we want to additionally consider multiple cooperating eavesdroppers, we have to adapt the channel constraint according to ⟨3.58⟩. Then, all results of this chapter can also be applied to a scenario with cooperating eavesdroppers.

⟨**5.28**⟩ **Extension to other Constraint Sets.** In the context of the maximized worst-case secrecy rates, we have already discussed in ⟨3.59⟩ that the reformulation of the original matrix problem to an equivalent problem over the eigenvalues of the involved matrices is also feasible for other constraint sets that can be described by unitarily invariant norms. The comments in ⟨3.59⟩ can analogously be applied to the problems of this chapter.

⟨**5.29**⟩ **Trade-off between Secrecy and Maximum Rates.** In the main parts of this thesis, we have discussed the optimization of worst-case problems. An essential assumption of this approach is that a potential and passive eavesdropper can observe the worst-case channel for each chosen transmit strategy, i.e., the eavesdropper is able to adapt its

behavior to that of the transmitter and can always find the weakest point of the setting. This point of view is very pessimistic, especially regarding the maximum achievable rates, but the advantage of this approach is that it yields rates that guarantee the secrecy of the private messages, not only against the considered eavesdropper with the worst-case channel, but also against all other eavesdroppers whose channels are subject to the given constraint. From a practical point of view, it has the disadvantage that the achievable rates are possibly very low, especially in comparison with the maximum rates that are achievable without secrecy constraints, see for instance Figure 5.7. This gap between the rates with and without secrecy constraints can be decreased if it is acceptable for the system designers and users to reduce the level of secrecy that was guaranteed so far. Although higher rates can only be achieved by partly giving up our previously formulated secrecy demands, it is difficult to quantify the resulting loss of secrecy.

We will illustrate this idea for the secret-key approach that we discussed in this chapter. In ⟨1.14⟩, we introduced an average rate expression as performance measure for the key generation approach, which allowed us a relatively fair comparison with the direct-transmission approach that we presented in Chapter 3. We proposed to calculate an average rate over both phases of the key generation approach, which are the key generation itself and the data transmission phase afterwards. A fair comparison requires that we do not only focus on the maximum achievable rate for the key generation, but also incorporate the effort that is necessary for the subsequent data transmission. In the second phase, we can operate at the maximum rate that is achievable without secrecy constraints since the secrecy of the private message is ensured by encryption with the previously generated key. In ⟨1.14⟩, we stated that it is necessary that the number of key bits is not less than the number of data bits in the private message, which is a condition for perfect secrecy according to Shannon (1949). This condition was perfectly consistent with the pessimistic view of our worst-case approach. However, we can relax this constraint if we intend to achieve higher rates than before by simultaneously reducing our secrecy requirements. In this case, a multitude of modifications of the original approach is possible. The probably simplest procedure is to use an already generated key repeatedly for several transmissions or a certain amount of time. A little bit more sophisticated is the idea to calculate a new key from a previously used key for a further transmission. Although there are no restrictions for this further processing in principle, we suggest to use methods that belong to the field of privacy amplification in order to not decrease the previously obtained level of secrecy too much.

⟨**5.30**⟩ **Publication Note.** Some ideas and results discussed in this chapter have already been presented at the *Physical-Layer Security Workshop* of the *54th IEEE Global Communications Conference (GLOBECOM)* in 2011 and published in (Wolf and Jorswieck, 2011). In this paper, we applied the worst-case scenario with a deterministic model for the uncertainty about the eavesdropper channel and the approach of (Wolf and Jorswieck, 2010a) to the secret-key generation problem in the multi-antenna scenario. This publication mainly contained the idea of reformulating the original matrix problem of the MIMO scenario into a vector problem over the eigenvalues of the involved matrices, which was

the basis for ⟨5.5⟩, and the derivation of the solution of the inner (worst-case) problem as in ⟨5.10⟩. Moreover, simple upper and lower bounds were introduced, and some aspects of the high- and low-SNR behavior were discussed in this publication. Thus, it was also a basis for ⟨5.14⟩ and ⟨5.15⟩ as well as ⟨5.17⟩ and ⟨5.18⟩.

⟨**5.31**⟩ **Related Work.** In this chapter, we considered the channel-type model for secret-key generation with a multi-antenna wiretap channel. We assumed that the transmitter does not have perfect information about the eavesdropper channel. Instead, we considered a channel uncertainty that was modeled deterministically. In contrast, many recent publications study various approaches for the source-type model. This is for instance obtained when the channel between the transmitter and the intended receiver is used as a common source of randomness between the two users. The properties of this reciprocal communication channel, which are used for the key generation, can be determined if each legitimated user sends pilot signals that allow the other to estimate the channel. These channel observations can be processed afterwards in order to generate a common key that is kept perfectly secret from the eavesdropper This approach exploits the fact that an eavesdropper, which is located at a certain distance from both legitimated users, observes different channel realizations. Below, we restrict ourselves to a discussion of publications that focus on the secret-key generation with the channel-type model. For an overview of selected publications that study the key generation with the source-type model, we refer to the introduction of this thesis.

Wong et al. (2009) studied the key generation approach for the channel-type model, where a fast-fading Gaussian MIMO wiretap channel was used. They extended the results of Ahlswede and Csiszár (1993) to continuous channel alphabets and evaluated the key capacity of the fast-fading MIMO wiretap channel under the assumption that neither the transmitter nor the intended receiver has any state information about the eavesdropper channel. Furthermore, they investigated the high-SNR behavior of the secret-key capacity depending on the number of antennas. They showed that the relation between the numbers of antennas at the transmitter and the eavesdropper determines whether the capacity converges to a finite limit or grows with the SNR.

The robustness of the secret-key generation is considered by Vía (2014). The author studied a Gaussian MIMO wiretap channel, where it is assumed that the transmitter does not have perfect knowledge about the eavesdropper channel. Instead, the channel was modeled by a sum of its estimation and an error matrix that is assumed to be bounded by a certain norm constraint with a fixed positive-semidefinite weighting matrix. This yields a maximization problem for the worst-case secret-key rate. Under the assumption that the eavesdropper channel is degraded with respect to the estimated worst-case channel, the problem of designing the optimal transmit covariance matrix was reformulated as a convex optimization problem. Moreover, a time-sharing approach was considered in which both users can transmit a certain fraction of the time. The author characterized the optimal transmit covariance matrix for the two special cases with a spherical uncertainty region and very large uncertainty sets.

⟨**5.32**⟩ **Summary.** In this chapter, we considered the physical-layer key generation with a MIMO wiretap channel and relaxed the assumption of perfect knowledge about the channel to the eavesdropper. The uncertainty about the eavesdropper channel was modeled by a constraint that used the Frobenius norm of this channel. For this model, we formulated two nested optimization problems. The first or inner problem was the worst-case secret-key rate problem, whose objective was to determine the worst-case channel for each chosen transmit strategy. This worst-case channel provides the eavesdropper with the maximal amount of information about the key generation process between the transmitter and the intended receiver. The second or outer problem was maximizing this worst-case secret-key rate under a transmit power constraint over all antennas. For the resulting problem, we derived an equivalent vector problem over the eigenvalues of the involved matrices. We discussed the properties of this max-min problem and showed that we have a saddle-point problem, which equivalently allows us to optimize the corresponding min-max problem. For the vector problem over the eigenvalues, we characterized the optimal strategies. We presented a waterfilling solution for the worst-case problem and derived relatively tight lower and upper bounds on the solution of the outer maximization problem. Moreover, we analyzed the behavior of the maximized worst-case secret-key rate and the corresponding optimal strategies for low and high SNR. The results of this chapter were illustrated in detail. We compared the results we obtained for the worst-case secrecy and secret-key rate and discussed similarities and differences. Finally, two special cases, the multiple-input single-output and the multi-carrier scenario, as well as possible extensions to multiple cooperating eavesdroppers and to scenarios with other constraints on the eavesdropper channel were discussed.

Part IV

Conclusion

Summary and Future Work

In this thesis, we studied how private communication between two users of a multi-antenna system can be ensured by means of the physical layer if it is assumed that the transmitter cannot have perfect information about the channel to a potential eavesdropper. The uncertainty about the eavesdropper channel was described by a deterministic model, i.e., a constraint on the quality of this channel was formulated, which corresponds to an infinite set of possible eavesdropper channels. We used a constraint on the sum of all channel gains of the multi-antenna channel between transmitter and eavesdropper, which was formulated using the Frobenius norm of this channel. In combination with a sum power constraint at the transmitter, it can be interpreted as a constraint on the overall receive power at the eavesdropper.

We discussed the problem from the perspective of the transmitter who wants to maximize the achievable rate of a reliable and secret transmission to an intended eavesdropper under a sum power constraint over all antennas and the assumption that the eavesdropper can observe the worst-case channel for each chosen transmit strategy. From this point of view, we analyzed two different approaches. One was the direct transmission of the private message to the receiver, while the reliability and secrecy of the information have to be ensured simultaneously by an appropriately chosen coding and resource allocation scheme. This yielded the study of the maximized worst-case secrecy rate. The other was an approach with two phases. First, the two legitimated users had to agree on a common key, which should be completely unknown to the eavesdropper. Afterwards, the transmitter can ensure the secrecy of the information by encryption. Thus, the subsequent transmission has only to guarantee the reliability of this encrypted information. This approach was analyzed by determining and discussing the maximized worst-case secret-key rate. We also established a fair comparison between both approaches by not only evaluating the maximized worst-case secret-key rate for the key generation, but also considering the additional effort, i.e., time and power, for the subsequent transmission of the encrypted information.

For both approaches, it was shown that the matrix problem can be reduced to an equivalent problem over the eigenvalues of the involved matrices. It was proven that the eigenvectors of the optimal transmit covariance matrix and the optimal Gramian matrix that characterizes the channel to the eavesdropper are determined by the eigenvectors of the Gramian matrix that describes the channel to the intended receiver. For both problems, we derived the corresponding worst-case channels, which can be characterized by waterfilling solutions, for each previously chosen transmit strategy. The optimal transmit strategies were characterized in terms of the number of positive components in the power

allocation vector, their ordering, and possible value ranges. We showed how relatively tight upper and lower bounds on the maximized worst-case rates can be derived. The lower bounds provided a accurate approximation of the optimal transmit power allocation, whereas the upper bounds, which often were close to the lower bounds, ensured that the strategy that was derived from the lower bound was close to optimal.

For the maximization of the worst-case secrecy rate, we considered two different transmitter structures. In addition to the original transmitter with only one joint encoder, we proposed an adapted transmitter structure, where the characteristics of the reformulated optimization problem were exploited by first parallelizing the data stream and encoding it with a set of parallel encoders afterwards. We showed that this adapted transmitter structure can yield higher rates for high SNR, especially if the eavesdropper is allowed to have a relatively good channel. Moreover, it turned out for these cases that full transmit power is not optimal if the original transmitter structure is used. For the maximization of the worst-case secrecy rate with the adapted transmitter structure and the maximization of the worst-case secret-key rate, we showed that the considered max-min problems are saddle-point problems, which can be equivalently written as min-max problems.

We showed that all rates converge to finite limits for high SNR, which results from the fact that we formulated no restriction on the maximum number of eavesdropping antennas, which allowed the eavesdropper to have more antennas than the transmitter, in order to have a real worst-case scenario. Consequently, the transmitter can always significantly reduce the sum transmit power if the noise power is low enough, nearly without any rate loss. Furthermore, we showed that the rate increase for low SNR is determined by the parameters of both channels if the maximized worst-case secrecy rate is considered, whereas only the channel to the intended receiver is relevant if the maximized worst-case secret-key rate is studied, i.e., the latter has the same low-SNR rate increase as the transmission rate in a system without secrecy constraints.

The comparison of both approaches showed that the key generation approach always yields higher rates than the direct-transmission approach. However, if the subsequent data transmission is considered in addition to the key generation, this approach loses its general superiority. It was shown that relatively bad eavesdropper channels or low SNR are advantageous for the direct transmission of the information, whereas comparably good eavesdropper channels or high SNR support the key generation approach. If the eavesdropper is allowed to have a better channel than the intended receiver, a direct transmission of the information is no longer possible. Then, only the key generation approach can yield positive rates.

Finally, we showed that our analysis can also be applied to related multi-carrier scenarios, to scenarios with multiple eavesdroppers, even if they cooperate, and to problems that are constrained by other unitarily invariant norms. For other norm constraints, it can also be applied to derive lower and upper bounds on the corresponding problems.

From the results we obtained, interesting topics for future work arise. It would be interesting to extend our approach such that the estimation error for the channel to the intended receiver is additionally included in the analysis. We could introduce the assumption that the channel estimation error can be upper-bounded by a certain value. Thus, the maximization of the worst-case would result in a max-min problem, where the joint minimization is carried out over the constraint sets that were formulated for both channels. This means that the transmitter tries to find the optimal transmit strategy under the assumption that the corresponding worst-case error occurs for the channel estimation to the intended receiver, whereas the eavesdropper can simultaneously observe the worst-case channel, which would provide him the maximum information about the private message or the secret key.

Furthermore, we suggest to investigate how the approach of this thesis can be applied to scenarios where the constraints are not formulated by unitarily invariant conditions. The equivalence of all matrix norms enables to upper- and lower-bound an arbitrary matrix norm by another matrix norm, which could be chosen such that it is unitarily invariant. Thus, we could at least derive upper and lower bounds on the optimized rates in these cases by using appropriate sub- and supersets of the given constraint sets, which can be described by unitarily invariant norms. For some practically relevant constraints, it could be evaluated how tight these upper and lower bounds are in order to conclude how good this approximation can be.

Additionally, the resulting eigenvalue problems could be evaluated for other constraints that can be formulated on the transmit power as well as the main and eavesdropper channel. The corresponding worst-case strategies could be characterized, which in turn would allow to derive optimal transmit strategies under the previously formulated worst-case assumptions.

Moreover, there are still open questions for the scenarios that were analyzed within this thesis and that are worth to be further studied. It would be interesting to completely analyze and understand the performance of relatively simple transmit strategies for the whole SNR range and not only for asymptotically low and high SNR. Such strategies could be for instance the uniform distribution of the available power over all components of the power allocation vector or the concentration of the complete power in only one component of this vector. This analysis would comprise the evaluation of the rate loss that results from these strategies compared to the optimal strategies that were characterized in this thesis.

Another idea would be to fix the maximum number of eavesdropper antennas to a value that is less than the number of antennas that the legitimated users have for transmission and reception. Note that this approach would not result in a transmission in the null space of the eavesdropper channel since the worst-case problem was considered as the inner problem with the underlying assumption that the eavesdropper can "react" on the previously chosen transmit strategy. In this context, it could be evaluated how the optimal strategies for the outer and the inner problem differ from those that were derived within

this thesis. As a consequence, we would observe that the rates will no longer converge to finite limits for high SNR. In this case, a discussion of the secure degrees of freedom would make sense.

Furthermore, the comparison between the two different approaches could be improved by additionally considering the effort that is necessary for the public communication in the key-agreement approach. Thus, an appropriate model has to be chosen for the analysis of the public communication channel, which allows a combination with the performance measures we discussed so far.

Another open point concerns the proof of the concavity of the secret-key rate with respect to the transmit covariance matrix. We pointed out that the proof in (Liang et al., 2009, Lemma C.1) cannot be generally applied to our secret-key rate expression without any further assumptions or modifications. This proof requires the existence of the inverse of a matrix that establishes a relation between the Gramian matrices that result from the matrices of both multi-antenna channels. But this relation matrix does not necessarily have full rank, since its rank is determined by the numbers of antennas that are chosen for the transmitter, the intended receiver, and the eavesdropper. Thus, it would be helpful to find a proof that works without the inverse or that can ensure that such an inverse definitely exists.

Appendix

A Mathematical Background

A.1 The $[\cdot]^+$ Function

In this section, we present and discuss the properties of the $[\cdot]^+$ function.

⟨**A.1**⟩ **Basic Properties.** We introduce some basic properties of the function

$$[\cdot]^+ : \quad \mathbb{R} \to \mathbb{R}, \quad x \mapsto [x]^+ := \max\{x, 0\} = \begin{cases} x & \text{for } x > 0 \\ 0 & \text{for } x \leq 0 \end{cases}.$$

For all $x, y \in \mathbb{R}$ and $a \geq 0$,

$$[a\,x]^+ = a\,[x]^+, \tag{A.1}$$

$$[x+y]^+ \leq [x]^+ + [y]^+, \quad \text{and} \tag{A.2}$$

$$x > y \;\text{ or }\; x \geq y \;\Rightarrow\; [x]^+ \geq [y]^+. \tag{A.3}$$

Note that a strict inequality on the left-hand side of the last line does not imply a strict inequality on the right-hand side.

⟨**A.2**⟩ **Monotonicity and Convexity.** If the $[\cdot]^+$ function is applied to a real-valued monotonic or convex function f with domain $\mathcal{X} \subseteq \mathbb{R}$, the following properties hold:

a) If the function f is (strictly) monotonically increasing on the set $\mathcal{S} \subseteq \mathcal{X}$, the function $[f]^+$ is monotonically increasing on $\mathcal{S}$, which follows directly from property (A.3). This statement can be equivalently formulated for a (strictly) monotonically decreasing function.

b) If the function f is (strictly) convex on the convex set $\mathcal{S} \subseteq \mathcal{X}$, the function $[f]^+$ is convex on $\mathcal{S}$. This can be shown according to the definition of a convex function. For all $x, y \in \mathcal{S}$ and for all $\lambda \in [0, 1]$,

$$\begin{aligned} [\underbrace{f(\lambda\,x + (1-\lambda)\,y)}_{\leq \lambda\,f(x) + (1-\lambda)\,f(y)}]^+ &\leq [\lambda\,f(x) + (1-\lambda)\,f(y)]^+ && \text{(A.4)} \\ &\leq [\lambda\,f(x)]^+ + [(1-\lambda)\,f(y)]^+ && \text{(A.5)} \\ &= \lambda\,[f(x)]^+ + (1-\lambda)\,[f(y)]^+, && \text{(A.6)} \end{aligned}$$

where (A.4) follows from the convexity of f and (A.3), whereas (A.5) and (A.6) are direct consequences of (A.2) and (A.1), respectively. Note that there is no equivalent formulation for a (strictly) concave function f.

⟨**A.3**⟩ **Maximum, Minimum, and Limit.** Let f be a real-valued function with domain $\mathcal{X} \subseteq \mathbb{R}^n$ for $n \in \mathbb{N}$. If we apply the $[\cdot]^+$ function to the function f and search for the maximum of this concatenated function on a certain set $\mathcal{S} \subseteq \mathcal{X}$, we can equivalently search for the maximum of the function f on $\mathcal{S}$ and apply the $[\cdot]^+$ function afterwards, since we can write

$$\max_{x\in\mathcal{S}} [f(x)]^+ = \max_{x\in\mathcal{S}} \begin{cases} f(x) & \text{for } f(x) > 0 \\ 0 & \text{for } f(x) \leq 0 \end{cases} = \begin{cases} \max\limits_{x\in\mathcal{S}} f(x) & \text{for } \max\limits_{x\in\mathcal{S}} f(x) > 0 \\ 0 & \text{for } \max\limits_{x\in\mathcal{S}} f(x) \leq 0 \end{cases} = \left[\max_{x\in\mathcal{S}} f(x) \right]^+ .$$

This analogously holds for the minimization over a certain set and the calculation of the limit of f as x approaches a certain value.

A.2 Equalities and Inequalities

This section provides some equalities and inequalities that are relevant for derivations in this thesis.

⟨**A.4**⟩ **Max-Min Inequality.** We have

$$\sup_{z\in\mathcal{Z}} \inf_{w\in\mathcal{W}} f(w,z) \leq \inf_{w\in\mathcal{W}} \sup_{z\in\mathcal{Z}} f(w,z)$$

for any $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}$ and any $\mathcal{W} \in \mathbb{R}^n$ and $\mathcal{Z} \in \mathbb{R}^m$. For instance, this inequality can be found in (Boyd and Vandenberghe, 2004, (5.46) in Section 5.4.1).

⟨**A.5**⟩ **Rearrangement Inequality.** For arbitrary real numbers $a_1 \geq a_2 \geq \ldots \geq a_n$ and $b_1 \geq b_2 \geq \ldots \geq b_n$, we have

$$\sum_{i=1}^{n} a_i b_{n+1-i} \leq \sum_{i=1}^{n} a_i \, (b\Pi)_i \leq \sum_{i=1}^{n} a_i b_i,$$

where Π can be any permutation matrix from the set $\mathbb{P}_n$, which is the set of all permutation matrices of size $n \times n$. This inequality and the corresponding proof were given by Hardy et al. (1952, Section 10.2).

⟨**A.6**⟩ **Hadamard's Inequality.** If $A = (a_{ij})_{i,j=1}^n \in \mathbb{C}^{n\times n}$ is positive-semidefinite, then

$$\det(A) \leq \prod_{i=1}^{n} a_{ii}.$$

Furthermore, when A is positive definite, then the equality holds if and only if A is diagonal. For instance, this inequality can be found in (Horn and Johnson, 1985, Theorem 7.8.1) or (Cover and Thomas, 1988, Theorem 3).

⟨**A.7**⟩ **Sylvester's Determinant Theorem.** If A and B are matrices of size $m \times n$ and $n \times m$ respectively, then $\det(I_m + AB) = \det(I_n + BA)$, where I_n is the identity matrix of order n. For instance, this relation can be found in (Harville, 1997, Corollary 18.1.2).

⟨**A.8**⟩ **Determinant of the Sum of Positive-Semidefinite Matrices.** Let A and B be positive-semidefinite $n \times n$ matrices with eigenvalues $a_1 \geq a_2 \geq \ldots \geq a_n \geq 0$ and $b_1 \geq b_2 \geq \ldots \geq b_n \geq 0$, respectively. Then

$$\prod_{i=1}^{n}(a_i + b_i) \leq \det(A + B) \leq \prod_{i=1}^{n}(a_i + b_{n+1-i}).$$

These bounds were derived by Fiedler (1971), who also derived similar bounds for the more general case with arbitrary Hermitian matrices in the same publication. In the corresponding proof, Fiedler used the following equalities

$$\min_{\Pi \in \mathbb{P}_n} \prod_{i=1}^{n}(a_i + (b\Pi)_i) = \prod_{i=1}^{n}(a_i + b_i) \quad \text{and} \quad \max_{\Pi \in \mathbb{P}_n} \prod_{i=1}^{n}(a_i + (b\Pi)_i) = \prod_{i=1}^{n}(a_i + b_{n+1-i}),$$

where Π is a permutation matrix of size $n \times n$ and $\mathbb{P}_n$ is the set of all permutation matrices of size $n \times n$. The (row) vector b is defined as $b := (b_i)_{i=1}^{n}$. As direct consequence of these equalities, we obtain

$$\max_{\Pi \in \mathbb{P}_n} \prod_{i=1}^{n}(1 + a_i\,(b\Pi)_i) = \prod_{i=1}^{n}(1 + a_i\,b_i) \quad \text{and} \quad \min_{\Pi \in \mathbb{P}_n} \prod_{i=1}^{n}(1 + a_i\,(b\Pi)_i) = \prod_{i=1}^{n}(1 + a_i\,b_{n+1-i}).$$

These equations can be proven by mathematical induction. The proof follows the idea of the proof of the rearrangement inequality, see (Hardy et al., 1952, Section 10.2).

Proof. In his proof of the main result, Fiedler (1971) formulated a hint how the equalities above can be proven. For a better understanding, a more detailed version of this proof is provided below. We exemplarily show the proof for the upper bound. The same steps can be applied to prove the lower bound.

Notation: We define

$$Y_k(b\Pi) := \prod_{i=1}^{n}(1 + a_i\,(b\Pi)_i) \quad \text{and} \quad Z_k := \prod_{i=1}^{n}(1 + a_i\,b_i).$$

Base Clause: For a clear insight, we discuss the cases for $k = 1, 2, 3$.

For $k = 1$, there is only one possible permutation. We get

$$Y_1(b_1) = (1 + a_1\,b_1) = Z_1.$$

For $k = 2$, there are only two permutations (b_1, b_2) and (b_2, b_1), which leads to

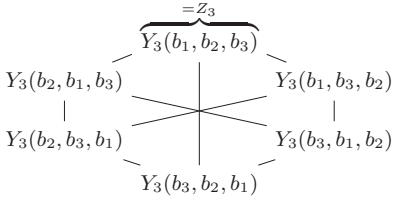
$$Y_2(b_2, b_1) = (1 + a_1\, b_2)\,(1 + a_2\, b_1) \leq (1 + a_1\, b_1)\,(1 + a_2\, b_2) = Y_2(b_1, b_2) = Z_2$$

due to

$$\begin{aligned} & (1 + a_1\, b_2)\,(1 + a_2\, b_1) \leq (1 + a_1\, b_1)\,(1 + a_2\, b_2) \\ \Leftrightarrow \quad & a_2\, b_1 + a_1\, b_2 \leq a_2\, b_2 + a_1\, b_1 \\ \Leftrightarrow \quad & (a_1 - a_2)\,(b_2 - b_1) \leq 0, \end{aligned}$$

which obviously is true, since we assumed $a_1 \geq a_2$ and $b_1 \geq b_2$.

For $k = 3$, we can use the result from the case $k = 2$ to compare all possible permuations as follows. For each vector $b\Pi$, we can compare the resulting product Y_3 with all other products calculated with a vector that differs from $b\Pi$ only by the interchange of two components. This leads to a partial order, which we illustrate by the following Hasse diagram.



Induction Step: Let us assume that $Y_k(b\Pi) \leq Z_k$ holds for all permutations $\Pi \in \mathbb{P}_k$. Now, we take an arbitrary vector $b\bar{\Pi}$ with $\bar{\Pi} \in \mathbb{P}_{k+1}$ and assume $(b\bar{\Pi})_{k+1} = b_\ell$ and $(b\bar{\Pi})_j = b_{k+1}$ with $j, \ell \in \{1, 2, \ldots, k\}$, i.e., b_{k+1} can be found at the j-th position, whereas b_ℓ was permuted to the last position of the vector. Due to the ordering of the vector b, we have $b_\ell \geq b_{k+1}$. We calculate

$$\begin{aligned} Y_{k+1}(b\bar{\Pi}) &= (1 + a_1\,(b\bar{\Pi})_1) \ldots (1 + a_j\, b_{k+1}) \ldots (1 + a_k\,(b\bar{\Pi})_k)\,(1 + a_{k+1}\, b_\ell) \\ &\leq (1 + a_1\,(b\bar{\Pi})_1) \ldots (1 + a_j\, b_\ell) \ldots (1 + a_k\,(b\bar{\Pi})_k)\,(1 + a_{k+1}\, b_{k+1}) \\ &= Y_k((b\bar{\Pi})_1, \ldots, (b\bar{\Pi})_{j-1}, b_\ell, (b\bar{\Pi})_{j+1}, \ldots, (b\bar{\Pi})_k)\,(1 + a_{k+1}\, b_{k+1}) \\ &\leq Z_k\,(1 + a_{k+1}\, b_{k+1}) = Z_{k+1}. \end{aligned}$$

The first inequality comes from the interchange of b_ℓ and b_{k+1}, which does not decrease the product as shown for the case $k = 2$. The second inequality directly follows from the induction hypothesis.

Consequently, we have shown that $Y_k(b\Pi) \leq Z_k$ and $Y_k(b) = Z_k$ for all $\Pi \in \mathbb{P}_k$ and $k \in 1, 2, \ldots, n$ with $n \in \mathbb{N}$. □

B Additional Material

B.1 Proofs for Propositions in Chapter 3

⟨**B.1**⟩ **Detailed Proof for ⟨3.12⟩.** The proof comprises four parts. In each part, we present a chain of equations and the corresponding explanations for the manipulations afterwards. The main reformulation steps, which are contained in the second and third part of the proof, are inspired by Telatar (1995), who used such an approach to derive the expression for the capacity of multi-antenna Gaussian channels.

Notation: We write the eigenvalue decomposition of the matrices A, B, and Q as

$$A = U\Delta_a U^{\mathrm{H}}, \quad B = V\Delta_b V^{\mathrm{H}}, \quad \text{and} \quad Q = W\Delta_q W^{\mathrm{H}}.$$

The matrices Δ_a, Δ_b, and Δ_q are diagonal matrices whose main diagonal entries are the eigenvalues of the matrices A, B, and Q, respectively. The matrices U, V, and W are unitary matrices whose columns can be identified with the corresponding eigenvectors of the matrices A, B, and Q, respectively.

First Part: Sylvester's determinant theorem can provide various equivalent expressions for the secrecy rate $R_S^\star$ in ⟨2.43⟩. We start with the following notation:

$$R_S^\star(A,B,Q) = \left[\log_2 \det\left(I_L + \rho\, A^{\frac{1}{2}} Q A^{\frac{1}{2}}\right) - \log_2 \det\left(I_L + \rho\, Q^{\frac{1}{2}} B Q^{\frac{1}{2}}\right)\right]^+$$

and reformulate the problem in ⟨3.6⟩ into

$$\begin{aligned}
&\max_{Q\in\mathscr{Q}} \min_{B\in\mathscr{B}} \left[\log_2 \det\left(I_L + \rho\, A^{\frac{1}{2}} Q A^{\frac{1}{2}}\right) - \log_2 \det\left(I_L + \rho\, Q^{\frac{1}{2}} B Q^{\frac{1}{2}}\right)\right]^+ \\
&\overset{(1)}{=} \left[\max_{Q\in\mathscr{Q}} \min_{B\in\mathscr{B}} \left(\log_2 \det\left(I_L + \rho\, A^{\frac{1}{2}} Q A^{\frac{1}{2}}\right) - \log_2 \det\left(I_L + \rho\, Q^{\frac{1}{2}} B Q^{\frac{1}{2}}\right)\right)\right]^+ \\
&\overset{(2)}{=} \left[\max_{Q\in\mathscr{Q}} \left(\log_2 \det\left(I_L + \rho\, A^{\frac{1}{2}} Q A^{\frac{1}{2}}\right) - \max_{B\in\mathscr{B}} \log_2 \det\left(I_L + \rho\, Q^{\frac{1}{2}} B Q^{\frac{1}{2}}\right)\right)\right]^+.
\end{aligned}$$

Explanations:

(1) The properties of the $[\cdot]^+$ function allow us to interchange the maximization over $\mathscr{Q}$ and the minimization over $\mathscr{B}$ with the $[\cdot]^+$ operation.

(2) The first term is not a function of B. Thus, the minimization of the difference of both terms can be reduced to a maximization of the second term.

Second Part: The maximization of the second term above can be equivalently reformulated as follows:

$$\begin{aligned}
&\max_{B\in\mathscr{B}} \log_2 \det\left(I_L + \rho\, Q^{\frac{1}{2}} B Q^{\frac{1}{2}}\right)\\
&\overset{(1)}{=} \max_{B\in\mathscr{B}} \log_2 \det\left(I_L + \rho\, \underbrace{W\Delta_q^{\frac{1}{2}}}\, \underbrace{W^{\mathrm{H}} B W \Delta_q^{\frac{1}{2}} W^{\mathrm{H}}}\right)\\
&\overset{(2)}{=} \max_{B\in\mathscr{B}} \log_2 \det\left(I_L + \rho\, W^{\mathrm{H}} B W \Delta_q^{\frac{1}{2}} W^{\mathrm{H}} W \Delta_q^{\frac{1}{2}}\right)\\
&\overset{(3)}{=} \max_{B\in\mathscr{B}} \log_2 \det\left(I_L + \rho\, W^{\mathrm{H}} B W \Delta_q\right)\\
&\overset{(4)}{=} \max_{\substack{\Delta_b\in\mathscr{B}\\ \Delta_b \text{ diagonal}}} \max_{V\in\mathbb{U}_L} \log_2 \det\left(I_L + \rho\, W^{\mathrm{H}} V \Delta_b V^{\mathrm{H}} W \Delta_q\right)\\
&\overset{(5)}{=} \max_{\substack{\Delta_b\in\mathscr{B}\\ \Delta_b \text{ diagonal}}} \log_2 \left(\max_{V\in\mathbb{U}_L} \det\left(I_L + \rho\, W^{\mathrm{H}} V \Delta_b V^{\mathrm{H}} W \Delta_q\right)\right)\\
&\overset{(6)}{=} \max_{\substack{\Delta_b\in\mathscr{B}\\ \Delta_b \text{ diagonal}}} \log_2 \det\left(I_L + \rho\, \Delta_b \Delta_q\right).
\end{aligned}$$

Explanations:

(1) We use the eigenvalue decomposition of the matrix Q according to $\langle 3.9 \rangle$, which is $Q = W\Delta_q W^{\mathrm{H}}$, and insert $Q^{\frac{1}{2}} = W\Delta_q^{\frac{1}{2}} W^{\mathrm{H}}$.

(2) Sylvester's determinant theorem allows us to interchange the position of the matrices $W\Delta_q^{\frac{1}{2}}$ and $W^{\mathrm{H}} B W \Delta_q^{\frac{1}{2}} W^{\mathrm{H}}$ inside the determinant.

(3) The matrix W is a unitary matrix, i.e., we have $W^{\mathrm{H}} W = I_L$. Hence, we obtain $\Delta_q^{\frac{1}{2}} W^{\mathrm{H}} W \Delta_q^{\frac{1}{2}} = \Delta_q$.

(4) We apply the eigenvalue decomposition of the matrix B according to $\langle 3.9 \rangle$, which is $B = V\Delta_b V^{\mathrm{H}}$. Accordingly, we write the maximization over $B \in \mathscr{B}$ as a (nested) maximization over the eigenvalues and eigenvectors of B. The constraint sets have to be adapted: The eigenvalue matrix Δ_b has to be diagonal and has to fulfill the constraints specified by the set $\mathscr{B}$. The eigenvector matrix V has to be a unitary matrix, which we write as $V \in \mathbb{U}_L$, where $\mathbb{U}_L$ is the set of all unitary matrices of dimension $L \times L$.

(5) The monotonicity of the logarithm enables the interchange of the maximization and the $\log_2$ function.

(6) From Hadamard's inequality, we know that the determinant of a positive-semidefinite matrix is upper-bounded by the product of its diagonal elements. For a positive definite matrix, this upper bound can be achieved if and only if the matrix is diagonal. Thus, the optimal solution for the maximization over the eigenvectors of B is to choose $V = W$, which leads to $W^{\mathrm{H}} V = V^{\mathrm{H}} W = I_L$ and ensures that the positive definite

matrix $I_L + \rho W^{\mathrm{H}} V \Delta_b V^{\mathrm{H}} W \Delta_q$ is diagonal. For a diagonal matrix, the product over its diagonal entries is equivalent to its determinant.

Third Part: We continue with the equivalent reformulation of the outer maximization from the first part applying the result from the second part. We use the same approach as above:

$$
\begin{aligned}
&\max_{Q \in \mathscr{Q}} \left(\log_2 \det \left(I_L + \rho A^{\frac{1}{2}} Q A^{\frac{1}{2}} \right) - \max_{B \in \mathscr{B}} \log_2 \det \left(I_L + \rho Q^{\frac{1}{2}} B Q^{\frac{1}{2}} \right) \right) \\
&\overset{(1)}{=} \max_{\substack{Q \in \mathscr{Q} \\ Q = W \Delta_q W^{\mathrm{H}}}} \left(\log_2 \det \left(I_L + \rho A^{\frac{1}{2}} Q A^{\frac{1}{2}} \right) - \max_{\substack{\Delta_b \in \mathscr{B} \\ \Delta_b \text{ diagonal}}} \log_2 \det \left(I_L + \rho \Delta_b \Delta_q \right) \right) \\
&\overset{(2)}{=} \max_{\substack{Q \in \mathscr{Q} \\ Q = W \Delta_q W^{\mathrm{H}}}} \left(\log_2 \det \left(I_L + \rho \underbrace{U \Delta_a^{\frac{1}{2}} U^{\mathrm{H}} Q U}_{\Delta_a^{\frac{1}{2}}} \underbrace{\Delta_a^{\frac{1}{2}} U^{\mathrm{H}}}_{} \right) - \max_{\substack{\Delta_b \in \mathscr{B} \\ \Delta_b \text{ diagonal}}} \log_2 \det \left(I_L + \rho \Delta_b \Delta_q \right) \right) \\
&\overset{(3)}{=} \max_{\substack{Q \in \mathscr{Q} \\ Q = W \Delta_q W^{\mathrm{H}}}} \left(\log_2 \det \left(I_L + \rho \Delta_a^{\frac{1}{2}} U^{\mathrm{H}} U \Delta_a^{\frac{1}{2}} U^{\mathrm{H}} Q U \right) - \max_{\substack{\Delta_b \in \mathscr{B} \\ \Delta_b \text{ diagonal}}} \log_2 \det \left(I_L + \rho \Delta_b \Delta_q \right) \right) \\
&\overset{(4)}{=} \max_{\substack{Q \in \mathscr{Q} \\ Q = W \Delta_q W^{\mathrm{H}}}} \left(\log_2 \det \left(I_L + \rho \Delta_a U^{\mathrm{H}} Q U \right) - \max_{\substack{\Delta_b \in \mathscr{B} \\ \Delta_b \text{ diagonal}}} \log_2 \det \left(I_L + \rho \Delta_b \Delta_q \right) \right) \\
&\overset{(5)}{=} \max_{\substack{\Delta_q \in \mathscr{Q} \\ \Delta_q \text{ diagonal}}} \max_{W \in \mathbb{U}_L} \left(\log_2 \det \left(I_L + \rho \Delta_a U^{\mathrm{H}} W \Delta_q W^{\mathrm{H}} U \right) - \max_{\substack{\Delta_b \in \mathscr{B} \\ \Delta_b \text{ diagonal}}} \log_2 \det \left(I_L + \rho \Delta_b \Delta_q \right) \right) \\
&\overset{(6)}{=} \max_{\substack{\Delta_q \in \mathscr{Q} \\ \Delta_q \text{ diagonal}}} \left(\log_2 \left(\max_{W \in \mathbb{U}_L} \det \left(I_L + \rho \Delta_a U^{\mathrm{H}} W \Delta_q W^{\mathrm{H}} U \right) \right) - \max_{\substack{\Delta_b \in \mathscr{B} \\ \Delta_b \text{ diagonal}}} \log_2 \det \left(I_L + \rho \Delta_b \Delta_q \right) \right) \\
&\overset{(7)}{=} \max_{\substack{\Delta_q \in \mathscr{Q} \\ \Delta_q \text{ diagonal}}} \left(\log_2 \det \left(I_L + \rho \Delta_a \Delta_q \right) - \max_{\substack{\Delta_b \in \mathscr{B} \\ \Delta_b \text{ diagonal}}} \log_2 \det \left(I_L + \rho \Delta_b \Delta_q \right) \right).
\end{aligned}
$$

Explanations:

(1) We replace the second term by the result of the second part and add the constraint that the eigenvalue decomposition of Q is written as $Q = W \Delta_q W^{\mathrm{H}}$ in order to have a formal connection between the notation in the first and second term.

(2) We use the eigenvalue decomposition of the matrix A according to $\langle 3.9 \rangle$, which is $A = U \Delta_a U^{\mathrm{H}}$, and insert $A^{\frac{1}{2}} = U \Delta_a^{\frac{1}{2}} U^{\mathrm{H}}$.

(3) Sylvester's determinant theorem allows us to interchange the position of the matrices $U \Delta_a^{\frac{1}{2}} U^{\mathrm{H}} Q U$ and $\Delta_a^{\frac{1}{2}} U^{\mathrm{H}}$ inside the determinant of the first term.

(4) The matrix U is a unitary matrix, i.e., we have $U^{\mathrm{H}} U = I_L$. Hence, we obtain $\Delta_a^{\frac{1}{2}} U^{\mathrm{H}} U \Delta_a^{\frac{1}{2}} = \Delta_a$.

(5) We insert the eigenvalue decomposition of the matrix Q. Accordingly, we write the maximization over $Q \in \mathscr{Q}$ as a (nested) maximization over the eigenvalues and

eigenvectors of Q. The constraint sets have to be adapted: The eigenvalue matrix Δ_q has to be diagonal and fulfill the constraints specified by the set $\mathscr{Q}$. The eigenvector matrix W has to be a unitary matrix, which we write as $W \in \mathbb{U}_L$, where $\mathbb{U}_L$ is the set of all unitary matrices of dimension $L \times L$ as specified above.

(6) The second term is not a function of W. Thus, the maximization of the difference of both terms can be reduced to a maximization of the first term. Furthermore, the monotonicity of the logarithm enables the interchange of this maximization and the $\log_2$ function in the first term.

(7) Again, Hadamard's inequality is applied. It yields the optimal solution for the maximization over the eigenvectors of Q, which is to choose $W = U$ leading to $U^{\mathrm{H}}W = W^{\mathrm{H}}U = I_L$ and ensuring that the positive definite matrix $I_L + \rho\,\Delta_a U^{\mathrm{H}} W \Delta_q W^{\mathrm{H}} U$ is diagonal. Again, we write the product over the diagonal entries as determinant of this diagonal matrix.

Fourth Part: With the result of the third part, we can reformulate the complete problem from the first part and obtain:

$$
\begin{aligned}
&\left[\max_{Q\in\mathscr{Q}}\left(\log_2\det\left(I_L+\rho\,A^{\frac{1}{2}}QA^{\frac{1}{2}}\right)-\max_{B\in\mathscr{B}}\log_2\det\left(I_L+\rho\,Q^{\frac{1}{2}}BQ^{\frac{1}{2}}\right)\right)\right]^+\\
&\overset{(1)}{=}\left[\max_{\substack{\Delta_q\in\mathscr{Q}\\ \Delta_q\text{ diagonal}}}\left(\log_2\det\left(I_L+\rho\,\Delta_a\Delta_q\right)-\max_{\substack{\Delta_b\in\mathscr{B}\\ \Delta_b\text{ diagonal}}}\log_2\det\left(I_L+\rho\,\Delta_b\Delta_q\right)\right)\right]^+\\
&\overset{(2)}{=}\left[\max_{q\in\mathcal{Q}}\left(\log_2\prod_{\ell=1}^{L}\left(1+\rho\,a_\ell q_\ell\right)-\max_{b\in\mathcal{B}}\log_2\prod_{\ell=1}^{L}\left(1+\rho\,b_\ell q_\ell\right)\right)\right]^+\\
&\overset{(3)}{=}\left[\max_{q\in\mathcal{Q}}\left(\sum_{\ell=1}^{L}\log_2\left(1+\rho\,a_\ell q_\ell\right)-\max_{b\in\mathcal{B}}\sum_{\ell=1}^{L}\log_2\left(1+\rho\,b_\ell q_\ell\right)\right)\right]^+\\
&\overset{(4)}{=}\left[\max_{q\in\mathcal{Q}}\min_{b\in\mathcal{B}}\left(\sum_{\ell=1}^{L}\log_2\left(1+\rho\,a_\ell q_\ell\right)-\sum_{\ell=1}^{L}\log_2\left(1+\rho\,b_\ell q_\ell\right)\right)\right]^+\\
&\overset{(5)}{=}\max_{q\in\mathcal{Q}}\min_{b\in\mathcal{B}}\left[\sum_{\ell=1}^{L}\left(\log_2\left(1+\rho\,a_\ell q_\ell\right)-\log_2\left(1+\rho\,b_\ell q_\ell\right)\right)\right]^+.
\end{aligned}
$$

Explanations:

(1) We combine the results of the first and third part.

(2) We calculate the determinants of the diagonal matrices, which are the products of their diagonal entries. We use the vector notation for the eigenvalues of the matrices A, B, and Q, which was introduced in ⟨3.9⟩ as a, b, and q, and adapt the constraint sets to this vector notation, which leads to the sets $\mathcal{Q}$ and $\mathcal{B}$ defined in ⟨3.12⟩.

(3) The logarithm of a product is equivalent to the sum of the logarithmized terms.

(4) Since the first term does not depend on b, we can equivalently write the maximization of the second term as minimization of the difference.

(5) Finally, we combine both sums and interchange again the $[\cdot]^+$ operation with the maximization over $\mathcal{Q}$ and the minimization over $\mathcal{B}$ exploiting the properties of the $[\cdot]^+$ function.

⟨B.2⟩ Detailed Proof for ⟨3.23⟩. For the proof, we introduce the following notation: We write $a\downarrow$ with $a \in \mathbb{R}^{1\times L}$, i.e., a is a row vector of length L, if the components of this vector are sorted in descending order, i.e., $a_1 \geq a_2 \geq \ldots \geq a_L$. Now, we consider the optimization problem in ⟨3.12⟩. Each vector $q \in \mathcal{Q}$ can be equivalently written as $q = \lambda\Pi_q$ with $\lambda \in \mathcal{Q}$, $\lambda\downarrow$, and $\Pi_q \in \mathbb{P}_L$, where λ is the (row) vector of length L that contains the components of q in descending order, Π_q is a permutation matrix of size $L \times L$, and $\mathbb{P}_L$ is the set of all permutation matrices of size $L \times L$. This also holds for each vector $b \in \mathcal{B}$: We can write $b = \beta\Pi_b$ with $\beta \in \mathcal{B}$, $\beta\downarrow$, and $\Pi_b \in \mathbb{P}_L$. With ⟨3.22⟩, we derive the permutation matrices Π_q and Π_b, which are optimal for problem ⟨3.12⟩. We start with an equivalent expression of ⟨3.12⟩, which was derived in the fourth part of the corresponding proof in ⟨B.1⟩:

$$
\begin{aligned}
&\left[\max_{q\in\mathcal{Q}}\left(\sum_{\ell=1}^{L}\log_2\left(1+\rho\, a_\ell q_\ell\right)-\max_{b\in\mathcal{B}}\sum_{\ell=1}^{L}\log_2\left(1+\rho\, b_\ell q_\ell\right)\right)\right]^+\\
&\overset{(1)}{=}\left[\max_{\substack{\lambda\in\mathcal{Q}\\ \lambda\downarrow}}\max_{\Pi_q\in\mathbb{P}_L}\left(\sum_{\ell=1}^{L}\log_2\left(1+\rho\, a_\ell(\lambda\Pi_q)_\ell\right)-\max_{\substack{\beta\in\mathcal{B}\\ \beta\downarrow}}\max_{\Pi_b\in\mathbb{P}_L}\sum_{\ell=1}^{L}\log_2\left(1+\rho\,(\beta\Pi_b)_\ell(\lambda\Pi_q)_\ell\right)\right)\right]^+\\
&\overset{(2)}{=}\left[\max_{\substack{\lambda\in\mathcal{Q}\\ \lambda\downarrow}}\max_{\Pi_q\in\mathbb{P}_L}\left(\sum_{\ell=1}^{L}\log_2\left(1+\rho\, a_\ell(\lambda\Pi_q)_\ell\right)-\max_{\substack{\beta\in\mathcal{B}\\ \beta\downarrow}}\sum_{\ell=1}^{L}\log_2\left(1+\rho\,(\beta\Pi_q)_\ell(\lambda\Pi_q)_\ell\right)\right)\right]^+\\
&\overset{(3)}{=}\left[\max_{\substack{\lambda\in\mathcal{Q}\\ \lambda\downarrow}}\left(\max_{\Pi_q\in\mathbb{P}_L}\sum_{\ell=1}^{L}\log_2\left(1+\rho\, a_\ell(\lambda\Pi_q)_\ell\right)-\max_{\substack{\beta\in\mathcal{B}\\ \beta\downarrow}}\sum_{\ell=1}^{L}\log_2\left(1+\rho\,(\beta\Pi_q)_\ell(\lambda\Pi_q)_\ell\right)\right)\right]^+\\
&\overset{(4)}{=}\left[\max_{\substack{\lambda\in\mathcal{Q}\\ \lambda\downarrow}}\left(\sum_{\ell=1}^{L}\log_2\left(1+\rho\, a_\ell\lambda_\ell\right)-\max_{\substack{\beta\in\mathcal{B}\\ \beta\downarrow}}\sum_{\ell=1}^{L}\log_2\left(1+\rho\,\beta_\ell\lambda_\ell\right)\right)\right]^+.
\end{aligned}
$$

Explanations:

(1) We insert $q = \lambda\Pi_q$ and $b = \beta\Pi_b$ and write each maximization as two (nested) maximizations over the set of all ordered vectors and the set of all permutation matrices.

(2) From ⟨A.8⟩, we obtain that the optimal vector b, which maximizes the sum in the second term, adopts the ordering of the vector q, i.e., the maximization over all $\Pi_b \in \mathbb{P}_L$ yields $\Pi_b = \Pi_q$.

(3) The value of the second term is independent from the chosen permutation matrix Π_q. Consequently, we only have to consider the first term for the maximization over all $\Pi_q \in \mathbb{P}_L$.
(4) From ⟨A.8⟩, we know that the sum in the first term is maximized if we choose the same ordering for a and q, i.e., the maximization over all $\Pi_q \in \mathbb{P}_L$ is achieved by $\Pi_q = I_L$.

From this analysis, we can conclude that the vectors q and b that are optimal for ⟨3.12⟩ adopt the ordering of the vector a.

⟨B.3⟩ Derivation for ⟨3.32⟩. We study the optimization of the low-SNR approximation of the secrecy rate $\widetilde{R}_S$ in ⟨3.32⟩ under the assumption that the components of the vector a are sorted in descending order as formulated in ⟨3.22⟩. For convenience, we reduce the max-min problem to the relevant part of this approximation, i.e., we omit the outer $[\cdot]^+$ function, the factor ρ, and the positive constant $\frac{1}{\ln 2}$ below. The remaining problem can be reformulated as follows:

$$
\begin{aligned}
&\max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \left(\sum_{\ell=1}^{L} (a_\ell - b_\ell)\, q_\ell \right) \\
&= \max_{q\in\mathcal{Q}} \min_{b\in\mathcal{B}} \left(\sum_{\ell=1}^{L} a_\ell\, q_\ell - \sum_{\ell=1}^{L} b_\ell\, q_\ell \right) \\
&\overset{(1)}{=} \max_{q\in\mathcal{Q}} \left(\sum_{\ell=1}^{L} a_\ell\, q_\ell - \max_{b\in\mathcal{B}} \sum_{\ell=1}^{L} b_\ell\, q_\ell \right) \\
&\overset{(2)}{=} \max_{q\in\mathcal{Q}} \left(\sum_{\ell=1}^{L} a_\ell\, q_\ell - \chi \max_{\ell=1,2,\ldots,L} \{q_\ell\} \right) \\
&\overset{(3)}{=} \max_{\substack{\lambda\in\mathcal{Q}\\ \lambda\downarrow}} \max_{\Pi_q\in\mathbb{P}_L} \left(\sum_{\ell=1}^{L} a_\ell\, (\lambda\Pi_q)_\ell - \chi\lambda_1 \right) \\
&\overset{(4)}{=} \max_{\substack{\lambda\in\mathcal{Q}\\ \lambda\downarrow}} \left(\max_{\Pi_q\in\mathbb{P}_L} \left(\sum_{\ell=1}^{L} a_\ell\, (\lambda\Pi_q)_\ell \right) - \chi\lambda_1 \right) \\
&\overset{(5)}{=} \max_{\substack{\lambda\in\mathcal{Q}\\ \lambda\downarrow}} \left(\left(\sum_{\ell=1}^{L} a_\ell\, \lambda_\ell \right) - \chi\lambda_1 \right) \\
&\overset{(6)}{=} \max_{L'} \left\{ \max_{\substack{\lambda\in\mathcal{Q}\\ \lambda\downarrow\\ \lambda_{L'+1}=\lambda_{L'+2}=\ldots=\lambda_L=0}} \left(\left(\sum_{\ell=1}^{L} a_\ell\, \lambda_\ell \right) - \chi\lambda_1 \right) \right\} \quad \text{with} \quad L' \in \{1, 2, \ldots, L\}.
\end{aligned}
$$

Explanations:

(1) The first term is not a function of b. Thus, the minimization of the difference of both terms can be reduced to a maximization of the second term.

(2) The maximum value of the second term is achieved by allocating χ to that component of b that corresponds to the largest value in q. All other components of b are consequently set to zero.

(3) We apply the notation for the ordering of vector components, which we have already introduced in $\langle$B.2$\rangle$. We insert $q = \lambda \Pi_q$ and write the maximization over $q \in \mathcal{Q}$ as a (nested) maximization over the set of all ordered vectors $\lambda \in \mathcal{Q}$ and the set of all permutation matrices. For the second term, we observe that the largest component of the vector q is always represented by λ_1 now.

(4) Since the ordering of the vector components is not relevant for the second term, we can equivalently apply the maximization over all permutation matrices to the first term only.

(5) From the rearrangement inequality follows that the maximum value of the first term that results from the optimization over all permutation matrices is achieved by choosing the same order for a and q, i.e., λ is optimal for this problem.

(6) We split the maximization over all sorted vectors $\lambda \in \mathcal{Q}$ into a nested maximization, where the outer problems iterates over the number of positive components in the vector λ, and the inner problem identifies the resulting maximum value for this certain number of positive vector components.

For convenience, we define

$$R(\lambda) := \left(\sum_{\ell=1}^{L} a_\ell \, \lambda_\ell \right) - \chi \lambda_1 \quad \text{and}$$
$$\mathcal{M}_{L'} := \{ \lambda \in \mathcal{Q} \,|\, \lambda_\downarrow \text{ and } \lambda_{L'+1} = \lambda_{L'+2} = \ldots = \lambda_L = 0 \} \, .$$

We focus on the inner maximization problem, which can be written as $\max_{\lambda \in \mathcal{M}_{L'}} R(\lambda)$ now, for an increasing number $L' \in \{1, 2, \ldots, L\}$:

- For $L' = 1$, we obtain

$$\max_{\lambda \in \mathcal{M}_1} R(\lambda) = (a_1 - \chi) \, P =: R_1$$

since it is clearly optimal to allocate full power to the only positive component of λ.

- We observe that $\max_{\lambda \in \mathcal{M}_2} R(\lambda) > R_1$ holds if and only if $a_2 > (a_1 - \chi)$. Then, we find

$$\max_{\lambda \in \mathcal{M}_2} R(\lambda) = (a_1 + a_2 - \chi) \, \tfrac{P}{2} =: R_2$$

since it is optimal to allocate the largest possible value to λ_2 such that $\lambda_1 \geq \lambda_2$ and the power constraint is fulfilled with equality, i.e., we set $\lambda_1 = \lambda_2 = \frac{P}{2}$. Otherwise,

we know that R_1 is the maximum value for all $L' \in \{1, 2, \ldots, L\}$, since we cannot obtain a larger contribution by allocating power to any other component of the vector λ, since the components of a are sorted in descending order.

- Similarly, we see that $\max_{\lambda \in \mathcal{M}_3} R(\lambda) > R_2$ holds if and only if $a_3 > \frac{1}{2}(a_1 + a_2 - \chi)$. Then it is optimal to allocate the largest possible value to λ_3 such that $\lambda_1 \geq \lambda_2 \geq \lambda_3$ and the power constraint is fulfilled with equality, i.e., we set $\lambda_1 = \lambda_2 = \lambda_3 = \frac{P}{3}$. Otherwise, we know that we cannot achieve a larger value than before by allocating power to any other component of the vector λ, due to the ordering of a.

This can analogously be continued until $L' = L$ is achieved. The procedure described above corresponds to the remaining optimization problem, which was formulated in ⟨3.32⟩.

B.2 Proofs for Propositions in Chapter 5

⟨B.4⟩ Detailed Proof for ⟨5.5⟩. We start by introducing some additional notation. Then, we present the main idea of the proof. Finally, we show the reformulation process in detail.

Notation: We use the eigenvalue decomposition of the matrices A, B, and Q that we have already introduced in ⟨B.1⟩:

$$A = U \Delta_a U^{\mathrm{H}}, \quad B = V \Delta_b V^{\mathrm{H}}, \quad \text{and} \quad Q = W \Delta_q W^{\mathrm{H}}$$

with the diagonal matrices Δ_a, Δ_b, and Δ_q and the unitary matrices U, V, and W, which contain the eigenvalues and eigenvectors of the matrices above.

With this notation, we can define the sets $\mathscr{Q}^-$ and $\mathscr{B}^-$ with $\mathscr{Q}^- \subset \mathscr{Q}$ and $\mathscr{B}^- \subset \mathscr{B}$ by

$$\begin{aligned} \mathscr{Q}^- &:= \left\{ Q \in \mathbb{C}^{L \times L} \,\middle|\, Q = U \Delta_q U^{\mathrm{H}},\ Q \succeq 0 \text{ and } \operatorname{tr}(Q) \leq P \right\} \quad \text{and} \\ \mathscr{B}^- &:= \left\{ B \in \mathbb{C}^{L \times L} \,\middle|\, B = W \Delta_b W^{\mathrm{H}},\ B \succeq 0 \text{ and } \operatorname{tr}(B) \leq \chi \right\}. \end{aligned}$$

The sets $\mathscr{Q}^-$ and $\mathscr{B}^-$ are derived from the sets $\mathscr{Q}$ and $\mathscr{B}$ by adding a further constraint on the eigenvectors of the matrices Q and B, respectively. In the definition of $\mathscr{Q}^-$, it is additionally required that the matrix Q has the same eigenvectors as the matrix A, whereas the matrix B is constrained to have the same eigenvectors as the matrix Q by the definition of $\mathscr{B}^-$.

Furthermore, we introduce the set

$$\mathcal{T} := \left\{ T = (t_{ij})_{i,j=1}^{L} \in \mathbb{Z}^{L \times L} \,\middle|\, t_{ii} \in \{-1, 1\} \text{ and } t_{ij} = 0 \text{ for } i \neq j \right\},$$

which describes matrices that are unitary and diagonal and whose main diagonal elements are either -1 or 1.

Main Idea: With the sets $\mathscr{Q}^-$ and $\mathscr{B}^-$, we can derive a lower and an upper bound on the max-min problem in $\langle 5.4 \rangle$. We obtain

$$\max_{Q \in \mathscr{Q}^-} \min_{B \in \mathscr{B}} R_K^\star(A,B,Q) \leq \max_{Q \in \mathscr{Q}} \min_{B \in \mathscr{B}} R_K^\star(A,B,Q) \leq \max_{Q \in \mathscr{Q}} \min_{B \in \mathscr{B}^-} R_K^\star(A,B,Q),$$

since we have $\mathscr{Q}^- \subset \mathscr{Q}$ and $\mathscr{B}^- \subset \mathscr{B}$. Note that the set $\mathscr{B}^-$ depends on the matrix Q since the matrix B is restricted to have the same eigenvectors as the previously chosen matrix Q. Nevertheless, we obtain an upper bound on the max-min problem in $\langle 5.4 \rangle$ by evaluating the right-hand side of the inequality above instead of the original problem. For each given matrix A and each $Q \in \mathscr{Q}$, we know that the minimization over the correponding set $\mathscr{B}^-$ yields a value that is greater or equal than the result that is obtained if the minimization is carried out over the set $\mathscr{B}$, since we have $\mathscr{B}^- \subset \mathscr{B}$. Clearly, this relation is preserved if we add the outer maximization over the set $\mathscr{Q}$ to both problems.

In the rest of the proof, we show that both bounds equal the eigenvalue problem in $\langle 5.5 \rangle$, i.e., the problem in $\langle 5.5 \rangle$ is equivalent to the original problem in $\langle 5.4 \rangle$.

Lower Bound: The reformulation of the lower bound comprises five parts. Each chain of equations or inequations is followed by the corresponding explanations for the manipulations afterwards.

First Part (Lower Bound): For each $Q \in \mathscr{Q}^-$, we can apply the eigenvalue decomposition notation that we introduced above and write the secret-key rate $R_K^\star$ in $\langle 4.35 \rangle$ as

$$\begin{aligned}
&R_K^\star(U\Delta_a U^{\mathrm{H}}, B, U\Delta_q U^{\mathrm{H}}) \\
&\overset{(1)}{=} \log_2 \det\Big(I_L + \rho\, \underbrace{(U\Delta_a U^{\mathrm{H}} + B)\, U\Delta_q}\, \underbrace{U^{\mathrm{H}}}\Big) - \log_2 \det\Big(I_L + \rho\, \underbrace{B\, U\Delta_q}\, \underbrace{U^{\mathrm{H}}}\Big) \\
&\overset{(2)}{=} \log_2 \det\big(I_L + \rho\, U^{\mathrm{H}}(U\Delta_a U^{\mathrm{H}} + B)\, U\Delta_q\big) - \log_2 \det\big(I_L + \rho\, U^{\mathrm{H}} B\, U\Delta_q\big) \\
&\overset{(3)}{=} \log_2 \det\big(I_L + \rho\,(\Delta_a + U^{\mathrm{H}} B\, U)\Delta_q\big) - \log_2 \det\big(I_L + \rho\, U^{\mathrm{H}} B\, U\Delta_q\big) \\
&\overset{(4)}{=} \log_2 \det\left(I_L + \rho\,(\Delta_a + B')\Delta_q\right) - \log_2 \det\left(I_L + \rho\, B'\Delta_q\right) \\
&= R_K^\star(\Delta_a, B', \Delta_q).
\end{aligned}$$

Explanations:

(1) We insert the eigenvalue decomposition of the matrices A and Q into the secret-key rate function $R_K^\star$.

(2) Sylvester's determinant theorem allows us to interchange the position of the matrix U^{H} and the other part of the matrix product inside the determinants of both terms.

(3) In the first term, we expand the matrix product. We can apply $U^{\mathrm{H}}U = I_L$, since the matrix U is a unitary matrix.

(4) We define $B' := U^{\mathrm{H}} B\, U$ and finally obtain that the secret-key rate can be expressed as $R_K^\star(\Delta_a, B', \Delta_q)$ for all $Q \in \mathscr{Q}^-$.

Second Part (Lower Bound): Now, we want to discuss the properties of the matrix B' and some other matrices that can be derived from the matrix B. In order to belong to the set $\mathscr{B}$, a matrix of dimension $L \times L$ has to be positive-semidefinite and fulfill the trace constraint. Both properties are only influenced by the eigenvalues of the matrix and not by its eigenvectors. Thus, we can write

$$B \in \mathscr{B} \quad \Leftrightarrow \quad B' := U^{\mathrm{H}} B\, U \in \mathscr{B},$$

since the multiplication with the unitary matrix U as in B' only changes the eigenvectors of the matrix B. The same argumentation holds for the matrix $TB'T$ with $T \in \mathcal{T}$, i.e.,

$$B' \in \mathscr{B} \quad \Leftrightarrow \quad TB'T \in \mathscr{B},$$

since $T \in \mathcal{T}$ is diagonal and unitary, which yields $T = T^{\mathrm{H}}$ and $TT^{\mathrm{H}} = T^{\mathrm{H}}T = TT = I_L$. Finally, we consider the matrix $\frac{1}{2}B' + \frac{1}{2}TB'T$. From $B \in \mathscr{B}$ and the equivalence relations above, we can conclude that this matrix also belongs to the set $\mathscr{B}$, i.e.,

$$B \in \mathscr{B} \quad \Rightarrow \quad \tfrac{1}{2}B' + \tfrac{1}{2}TB'T \in \mathscr{B},$$

since the positive semidefiniteness and the trace constraint, which are required in the definition of the set $\mathscr{B}$, are not influenced by this linear combination of the two matrices.

Third Part (Lower Bound): Now, we want to evaluate the secret-key rate $R_K^\star$ for the matrices $Q \in \mathscr{Q}^-$ and $TB'T \in \mathscr{B}$ with $T \in \mathcal{T}$. We start with the secret-key rate expression that we obtained at the end of the first part:

$$\begin{aligned}
&R_K^\star(\Delta_a, TB'T, \Delta_q) \\
&\overset{(1)}{=} \log_2 \det\left(I_L + \rho\,(\Delta_a + TB'T)\Delta_q\right) - \log_2 \det\left(I_L + \rho\, TB'T\Delta_q\right) \\
&\overset{(2)}{=} \log_2 \det\left(T\left(I_L + \rho\,(\Delta_a + TB'T)\Delta_q\right)T\right) - \log_2 \det\left(T\left(I_L + \rho\, TB'T\Delta_q\right)T\right) \\
&\overset{(3)}{=} \log_2 \det\left(I_L + \rho\,(\Delta_a + B')\Delta_q\right) - \log_2 \det\left(I_L + \rho\, B'\Delta_q\right) \\
&\overset{(4)}{=} R_K^\star(\Delta_a, B', \Delta_q).
\end{aligned}$$

Explanations:

(1) We simply insert the matrices into the secret-key rate expression.

(2) For both terms, we can multiply the matrix inside the determinant with T from both sides without changing the value of the determinant, since $T \in \mathcal{T}$ is unitary and diagonal, which yields $T = T^{\mathrm{H}}$.

(3) We expand the matrix products in both terms. We can interchange the position of the diagonal matrices Δ_a, Δ_q, and T if necessary and apply $TT = I_L$.

(4) We observe the following: For each matrix $B' \in \mathscr{B}$ and each $T \in \mathcal{T}$, we obtain the same value for the secret-key rate $R_K^\star$ if we use the matrix $TB'T$ instead of the matrix B'.

Fourth Part (Lower Bound): Now, we want to consider the secret-key rate $R_K^\star$ for the matrices $Q \in \mathscr{Q}^-$ and $\frac{1}{2}B' + \frac{1}{2}TB'T \in \mathscr{B}$ with $T \in \mathcal{T}$. We use again the secret-key rate expression we obtained at the end of the first part:

$$\begin{aligned} & R_K^\star(\Delta_a, \tfrac{1}{2}B' + \tfrac{1}{2}TB'T, \Delta_q) \\ & \overset{(1)}{\leq} \tfrac{1}{2}R_K^\star(\Delta_a, B', \Delta_q) + \tfrac{1}{2}R_K^\star(\Delta_a, TB'T, \Delta_q) \\ & \overset{(2)}{=} R_K^\star(\Delta_a, B', \Delta_q). \end{aligned}$$

Explanations:

(1) The inequality is a direct consequence of the convexity of $R_K^\star$ in $B \in \mathscr{B}$, see $\langle 4.36 \rangle$.

(2) From the analysis in the third part, we know that both secret-key rate expressions have the same value. Consequently, they add up as given above.

Fifth Part (Lower Bound): In the second part, we have shown that we can transform each matrix $B' \in \mathscr{B}$ into a matrix $\frac{1}{2}B' + \frac{1}{2}TB'T \in \mathscr{B}$, where we can use each matrix $T \in \mathcal{T}$. From the fourth part, we know that this transformation can only decrease the value of the corresponding secret-key rate $R_K^\star$. We are interested in minimizing the secret-key rate $R_K^\star$ for each $Q \in \mathscr{Q}^-$. With this aim, we can consequently always improve the resulting value of $R_K^\star$ by choosing a matrix $\frac{1}{2}B' + \frac{1}{2}TB'T$ instead of the matrix B'. Thus, we propose the following transformation process, which will not increase the value of the secret-key rate $R_K^\star$, for each $B_0' \in \mathscr{B}$ with $Q \in \mathscr{Q}^-$:

$$B_0' \overset{T_1}{\longmapsto} B_1' \overset{T_2}{\longmapsto} B_2' \overset{T_3}{\longmapsto} \ldots \overset{T_{L-1}}{\longmapsto} B_{L-1}'.$$

For all $\ell \in \{1, 2, \ldots, L-1\}$, the matrix $B_\ell' \in \mathscr{B}$ is given by

$$B_\ell' := \tfrac{1}{2}B_{\ell-1}' + \tfrac{1}{2}T_\ell B_{\ell-1}' T_\ell,$$

where $T_\ell \in \mathcal{T}$ is characterized by $t_{\ell\ell} = -1$ and $t_{ii} = 1$ for all $i \in \{1, 2, \ldots, L\}$ with $i \neq \ell$. The ℓ-th step of this transformation process, which calculates the matrix B_ℓ' from the matrix $B_{\ell-1}'$, nulls all elements of the ℓ-th row and ℓ-th column of the matrix $B_{\ell-1}'$ except the corresponding main diagonal element, but it does not change any other element of this matrix. Thus, we always obtain a diagonal matrix B_{L-1}' at the end of the proposed transformation process.

We draw the following conclusion: For each matrix $B_0' \in \mathscr{B}$, we can find a transformed matrix $B_{L-1}' \in \mathscr{B}$, which yields a secret-key rate $R_K^\star$ that is less or equal than the secret-key rate that can be calculated for the matrix B_0'. Furthermore, all these transformed matrices $B_{L-1}' \in \mathscr{B}$ are diagonal. Consequently, we always obtain a corresponding secret-key rate expression that only depends on the eigenvalues of the involved matrices. This yields the secret-key rate in $\langle 5.5 \rangle$ if we use the vector notation for the eigenvalues instead of the matrix notation above. The constraint sets $\mathscr{Q}^-$ and $\mathscr{B}$ correspond to the sets $\mathcal{Q}$ and $\mathcal{B}$ in $\langle 5.5 \rangle$ if we also apply this notational change. Thus, we observe that we can

calculate the lower bound on the problem in ⟨5.4⟩ equivalently by evaluating the problem in ⟨5.5⟩.

For the derivation of the lower bound, we formulated the additional constraint that the matrices A and Q have the same eigenvectors, which were specified by the unitary matrix U. In the first part of this derivation, we introduced $B' := U^{\mathrm{H}} B\, U$. If we assume that B' is diagonal, i.e., we have $B' = \Delta_b$, we see that this can be achieved by a matrix B that has the same eigenvectors as the matrices A and Q, i.e., we have $B = U \Delta_b U^{\mathrm{H}}$.

Upper Bound: The approach for the reformulation of the upper bound comprises two parts. In principle, the idea for the reformulation differs from the approach for the derivation of the lower bound above, although the first step is very similar. Again, each chain of equations or inequations is followed by the corresponding explanations for the manipulations afterwards.

First Part (Upper Bound): For each $B \in \mathscr{B}^{-}$, we can write the secret-key rate $R_K^{\star}$ in ⟨4.35⟩ with the eigenvalue decomposition notation that we introduced above as

$$
\begin{aligned}
& R_K^{\star}(A, W\Delta_b W^{\mathrm{H}}, W\Delta_q W^{\mathrm{H}}) \\
& \overset{(1)}{=} \log_2 \det\left(I_L + \rho\, W \Delta_q^{\frac{1}{2}} W^{\mathrm{H}} (A + W\Delta_b W^{\mathrm{H}})\, W \Delta_q^{\frac{1}{2}} W^{\mathrm{H}}\right) \\
& \quad - \log_2 \det\left(I_L + \rho\, W \Delta_q^{\frac{1}{2}} W^{\mathrm{H}} W \Delta_b W^{\mathrm{H}} W \Delta_q^{\frac{1}{2}} W^{\mathrm{H}}\right) \\
& \overset{(2)}{=} \log_2 \det\left(I_L + \rho\, \underbrace{W \Delta_q^{\frac{1}{2}} (W^{\mathrm{H}} A\, W + \Delta_b)\, \Delta_q^{\frac{1}{2}}}\, \underbrace{W^{\mathrm{H}}}\right) \\
& \quad - \log_2 \det\left(I_L + \rho\, \underbrace{W \Delta_q^{\frac{1}{2}} \Delta_b \Delta_q^{\frac{1}{2}}}\, \underbrace{W^{\mathrm{H}}}\right) \\
& \overset{(3)}{=} \log_2 \det\left(I_L + \rho\, \Delta_q^{\frac{1}{2}} (W^{\mathrm{H}} A\, W + \Delta_b)\, \Delta_q^{\frac{1}{2}}\right) \\
& \quad - \log_2 \det\left(I_L + \rho\, \Delta_q^{\frac{1}{2}} \Delta_b \Delta_q^{\frac{1}{2}}\right) \\
& \overset{(4)}{=} R_K^{\star}(W^{\mathrm{H}} A\, W, \Delta_b, \Delta_q).
\end{aligned}
$$

Explanations:

(1) We insert the eigenvalue decomposition of the matrices B and Q into the secret-key rate function $R_K^{\star}$.

(2) In the first term, we expand the matrix product. Additionally, we can apply $W^{\mathrm{H}} W = I_L$, since the matrix W is a unitary matrix.

(3) Sylvester's determinant theorem allows us to interchange the position of the matrix W and the other part of the matrix product inside the determinants of both terms. Afterwards, we apply $W^{\mathrm{H}} W = I_L$ again.

(4) We finally obtain that the secret-key rate can be expressed as $R_K^{\star}(W^{\mathrm{H}} A\, W, \Delta_b, \Delta_q)$ for all $B \in \mathscr{B}^{-}$.

Second Part (Upper Bound): Now, we consider the max-min problem that we introduced for the upper bound above. We reformulate this problem as follows:

$$\max_{Q\in\mathscr{Q}} \min_{B\in\mathscr{B}^-} R_K^\star(A,B,Q)$$

$$\overset{(1)}{=} \max_{\substack{\Delta_q\in\mathscr{Q} \\ \Delta_q \text{ diagonal}}} \max_{W\in\mathbb{U}_L} \min_{\substack{\Delta_b\in\mathscr{B} \\ \Delta_b \text{ diagonal}}} R_K^\star(A, W\Delta_b W^{\mathrm{H}}, W\Delta_q W^{\mathrm{H}})$$

$$\overset{(2)}{=} \max_{\substack{\Delta_q\in\mathscr{Q} \\ \Delta_q \text{ diagonal}}} \max_{W\in\mathbb{U}_L} \min_{\substack{\Delta_b\in\mathscr{B} \\ \Delta_b \text{ diagonal}}} R_K^\star(W^{\mathrm{H}} A\, W, \Delta_b, \Delta_q)$$

$$\overset{(3)}{\leq} \max_{\substack{\Delta_q\in\mathscr{Q} \\ \Delta_q,\, \Delta_b \text{ diagonal}}} \min_{\Delta_b\in\mathscr{B}} \max_{W\in\mathbb{U}_L} R_K^\star(W^{\mathrm{H}} A\, W, \Delta_b, \Delta_q)$$

$$\overset{(4)}{=} \max_{\substack{\Delta_q\in\mathscr{Q} \\ \Delta_q,\, \Delta_b \text{ diagonal}}} \min_{\Delta_b\in\mathscr{B}} \Bigg(\max_{W\in\mathbb{U}_L} \left(\log_2 \det\left(I_L + \rho\, \Delta_q^{\frac{1}{2}} (W^{\mathrm{H}} A\, W + \Delta_b)\, \Delta_q^{\frac{1}{2}}\right)\right) - \log_2 \det\left(I_L + \rho\, \Delta_q^{\frac{1}{2}} \Delta_b \Delta_q^{\frac{1}{2}}\right) \Bigg)$$

$$\overset{(5)}{=} \max_{\substack{\Delta_q\in\mathscr{Q} \\ \Delta_q,\, \Delta_b \text{ diagonal}}} \min_{\Delta_b\in\mathscr{B}} \Bigg(\log_2 \det\left(I_L + \rho\, \Delta_q^{\frac{1}{2}} (\Delta_a + \Delta_b)\, \Delta_q^{\frac{1}{2}}\right) - \log_2 \det\left(I_L + \rho\, \Delta_q^{\frac{1}{2}} \Delta_b \Delta_q^{\frac{1}{2}}\right) \Bigg).$$

Explanations:

(1) We insert the eigenvalue decomposition of the matrices Q and B. Accordingly, we write the maximization over $Q \in \mathscr{Q}$ as a (nested) maximization over the eigenvalues and eigenvectors of Q. The constraint sets are derived from the original constraint set: The eigenvalue matrix Δ_q has to be diagonal and fulfill the constraints specified by the set $\mathscr{Q}$. The eigenvector matrix W has to be a unitary matrix of dimension $L \times L$. Consequently, we write $W \in \mathbb{U}_L$. In principle, we could also write the minimization over $B \in \mathscr{B}^-$ as a (nested) minimization over the eigenvalues and eigenvectors of B. However, the eigenvectors of the matrix B have already been fixed by the definition of the set $\mathscr{B}^-$. Thus, if is sufficient to substitute the minimization over $B \in \mathscr{B}^-$ by the minimization over the eigenvalues of the matrix B. For the corresponding constraint set, we write $\Delta_b \in \mathscr{B}$, since the eigenvalue matrix has to fulfill the constraints of the original constraint set. Furthermore, it is required that Δ_b is diagonal.

(2) We replace the secret-key rate expression by its equivalent that we obtained as final result in the first part.

(3) The max-min inequality allows us to interchange the maximization over the eigenvector matrix W of the matrix Q and the minimization over the eigenvalue matrix Δ_b of the matrix B if the relation symbol is adapted accordingly. The outer maximization over the eigenvalue matrix Δ_q of the matrix Q does not influence the relation.

(4) We insert the expression for the secret-key rate that we obtained at the end of the

first part. Furthermore, we can apply the maximization over the eigenvector matrix W of the matrix Q to the first term only, since the second term is independent from the matrix W.

(5) We consider the maximization of the first term over the eigenvector matrix W for fixed matrices A, Δ_b, and Δ_q. From Hadamard's inequality, we know that the maximum value of the determinant of the positive-definite matrix $I_L + \rho\,\Delta_q^{\frac{1}{2}}(W^{\mathrm{H}} A\, W + \Delta_b)\,\Delta_q^{\frac{1}{2}}$ is upper-bounded by the product of its diagonal elements. This value is achieved if and only if this matrix is diagonal. We obtain such a diagonal matrix if the matrix $W^{\mathrm{H}} A\, W$ is diagonal, which in turn is achieved by setting $W = U$, i.e., the eigenvectors of the matrices A and Q have to be the same, which yields $W^{\mathrm{H}} A\, W = \Delta_a$. For a diagonal matrix, the product over its diagonal entries is equivalent to its determinant.

The remaining optimization problem is only an optimization problem over the eigenvalues of the involved matrices. If we apply the vector notation for the eigenvalues instead of the matrix notation above, we obtain the constraint sets $\mathcal{Q}$ and $\mathcal{B}$ and the secret-key rate expression in ⟨5.5⟩. Thus, we observe that we can calculate the upper bound on the problem in ⟨5.4⟩ equivalently by evaluating the problem in ⟨5.5⟩.

Conclusion: We have shown that the lower and the upper bound equal both the eigenvalue problem in ⟨5.5⟩. Thus, we can conclude that the problem in ⟨5.5⟩ is equivalent to the original problem in ⟨5.4⟩.

Bibliography

Ahlswede, Rudolph and Imre Csiszár (1993). Common Randomness in Information Theory and Cryptography—Part I: Secret Sharing. *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132.

Anand, Santhanakrishnan and Rajarathnam Chandramouli (2010). On the Location of an Eavesdropper in Multiterminal Networks. *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 148–157.

Bagherikaram, Ghadamali, Abolfazl S. Motahari, and Amir K. Khandani (2013). The Secrecy Capacity Region of the Gaussian MIMO Broadcast Channel. *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 2673–2682.

Bloch, Matthieu R. and João Barros (2011). *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press.

Bloch, Matthieu R., João Barros, Miguel R. S. Rodrigues, and Steven W. McLaughlin (2008). Wireless Information-Theoretic Security. *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534.

Boche, Holger and Rafael F. Schaefer (2013). Capacity Results and Super-Activation for Wiretap Channels With Active Wiretappers. *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1482–1496.

Boche, Holger and Rafael F. Wyrembelski (2013). Secret Key Generation using Compound Sources – Optimal Key-Rates and Communication Costs. *Proceedings of 9th International ITG Conference on Systems, Communication and Coding (SCC)*. Munich, Germany.

Boyd, Stephen and Lieven Vandenberghe (2004). *Convex Optimization*. Cambridge University Press.

Cover, Thomas M. and Joy A. Thomas (1988). Determinant Inequalities via Information Theory. *SIAM Journal on Matrix Analysis and Applications*, vol. 9, no. 3, pp. 384–392.

Cover, Thomas M. and Joy A. Thomas (2006). *Elements of Information Theory*. John Wiley & Sons.

Csiszár, Imre and János Körner (1978). Broadcast Channels with Confidential Messages. *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348.

Cumanan, Kanapathippillai, Zhiguo Ding, Bayan Sharif, Gui Yun Tian, and Kin K. Leung (2014). Secrecy Rate Optimizations for a MIMO Secrecy Channel With a Multiple-Antenna Eavesdropper. *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, pp. 1678–1690.

Diggavi, Suhas N. and Thomas M. Cover (2001). The Worst Additive Noise Under a Covariance Constraint. *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3072–3081.

Dong, Lun, Zhu Han, Athina P. Petropulu, and H. Vincent Poor (2009). Cooperative Jamming for Wireless Physical Layer Security. *Proceedings of the 15th IEEE Workshop on Statistical Signal Processing (SSP)*. Cardiff, UK.

Engelmann, Sabrina, Anne Wolf, and Eduard A. Jorswieck (2014). Precoding for Secret Key Generation in Multiple Antenna Channels with Statistical Channel State Information. *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*. Florence, Italy.

Fiedler, Miroslav (1971). Bounds for the Determinant of the Sum of Hermitian Matrices. *Proceedings of the American Mathematical Society*, vol. 30, no. 1, pp. 27–31.

Gabry, Frédéric, Ragnar Thobaben, and Mikael Skoglund (2011). Outage Performances for Amplify-and-Forward, Decode-and-Forward and Cooperative Jamming Strategies for the Wiretap Channel. *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*. Cancun, Mexico.

Gerbracht, Sabrina, Anne Wolf, and Eduard A. Jorswieck (2010). Beamforming for Fading Wiretap Channels with Partial Channel Information. *Proceedings of the International ITG Workshop on Smart Antennas (WSA)*. Bremen, Germany.

Goel, Satashu and Rohit Negi (2008). Guaranteeing Secrecy using Artificial Noise. *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189.

Gopala, Praveen K., Lifeng Lai, and Hesham El Gamal (2008). On the Secrecy Capacity of Fading Channels. *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698.

Hardy, Godfrey H., John E. Littlewood, and George Pólya (1952). *Inequalities*. Cambridge University Press.

Harville, David A. (1997). *Matrix Algebra From a Statistician's Perspective*. Springer.

Ho, Ka-Ming (Zuleita), Eduard A. Jorswieck, and Sabrina Engelmann (2013). Information Leakage Neutralization for the Multi-Antenna Non-Regenerative Relay-Assisted Multi-Carrier Interference Channel. *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1672–1686.

Horn, Roger A. and Charles R. Johnson (1985). *Matrix Analysis*. Cambridge University Press.

Huang, Jing and A. Lee Swindlehurst (2012). Robust Secure Transmission in MISO Channels Based on Worst-Case Optimization. *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1696–1707.

Jorswieck, Eduard A. (2010). Secrecy Capacity of Single- and Multi-Antenna Channels with Simple Helpers. *Proceedings of the International ITG Conference on Source and Channel Coding (SCC)*. Siegen, Germany.

Jorswieck, Eduard A. (2013). Secret Key Region in Multiple Antenna Wiretap Interference Channels with Public Discussion. *Proceedings of 9th International ITG Conference on Systems, Communication and Coding (SCC)*. Munich, Germany.

Jorswieck, Eduard A. and Sabrina Gerbracht (2009). Secrecy Rate Region of Downlink OFDM Systems: Efficient Resource Allocation. *Proceedings of the 14th International OFDM-Workshop (InOWo)*. Hamburg, Germany.

Jorswieck, Eduard A. and Rami Mochaourab (2009). Secrecy Rate Region of MISO Interference Channel: Pareto Boundary and Non-Cooperative Games. *Proceedings of the International ITG Workshop on Smart Antennas (WSA)*. Berlin, Germany.

Jorswieck, Eduard A. and Anne Wolf (2008). Resource Allocation for the Wire-tap Multicarrier Broadcast Channel. *Proceedings of the 1st International Workshop on Multiple Access Communications (MACOM)*. Saint Petersburg, Russia.

Jorswieck, Eduard A., Anne Wolf, and Sabrina Gerbracht (2010). Secrecy on the Physical Layer in Wireless Networks. Trends in Telecommunications Technologies. INTECH. Chap. 20, pp. 413–435.

Jorswieck, Eduard A., Anne Wolf, and Sabrina Engelmann (2013). Secret Key Generation from Reciprocal Spatially Correlated MIMO Channels. *Proceedings of the 56th IEEE Global Communications Conference (GLOBECOM)*. Atlanta, USA.

Jorswieck, Eduard A., Pin-Hsun Lin, Sabrina Engelmann, and Anne Wolf (2015). Secure Communications in Fast- and Slow-Fading Wiretap Channels with Partial and Statistical CSI at the Transmitter. Lecture Notes in Electrical Engineering (LNEE). Springer.

Khisti, Ashish and Gregory W. Wornell (2007). The MIMOME Channel. *Proceedings of the 45th Annual Allerton Conference on Communication, Control and Computing*. Monticello, USA.

Leung-Yan-Cheong, Sik K. and Martin E. Hellman (1978). The Gaussian Wire-Tap Channel. *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456.

Li, Jiangyuan and Athina P. Petropulu (2012). Explicit Solution of Worst-Case Secrecy Rate for MISO Wiretap Channels With Spherical Uncertainty. *IEEE Transactions on Signal Processing*, vol. 60, no. 7, pp. 3892–3895.

Li, Qiang and Wing-Kin Ma (2011). Optimal and Robust Transmit Designs for MISO Channel Secrecy by Semidefinite Programming. *IEEE Transactions on Signal Processing,* vol. 59, no. 8, pp. 3799–3812.

Li, Qiang, Mingyi Hong, Hoi-To Wai, Wing-Kin Ma, Ya-Feng Liu, and Zhi-Quan Luo (2013). An Alternating Optimization Algorithm for the MIMO Secrecy Capacity Problem under Sum Power and Per-Antenna Power Constraints. *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. Vancouver, Canada.

Li, Zang, Roy Yates, and Wade Trappe (2006). Secrecy Capacity of Independent Parallel Channels. *Proceedings of the 44th Annual Allerton Conference on Communication, Control, and Computing*. Monticello, USA.

Li, Zang, Wade Trappe, and Roy Yates (2007). Secret Communication via Multi-antenna Transmission. *Proceedings of the 41st Annual Conference on Information Sciences and Systems (CISS)*. Baltimore, USA.

Liang, Yingbin, Gerhard Kramer, H. Vincent Poor, and Shlomo Shamai (Shitz) (2007). Compound Wire-tap Channels. *Proceedings of the 45th Annual Allerton Conference on Communication, Control, and Computing*. Monticello, USA.

Liang, Yingbin, H. Vincent Poor, and Shlomo Shamai (Shitz) (2008a). Information Theoretic Security. *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580.

Liang, Yingbin, Gerhard Kramer, H. Vincent Poor, and Shlomo Shamai (Shitz) (2008b). Recent Results on Compound Wire-tap Channels. *Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. Cannes, France.

Liang, Yingbin, H. Vincent Poor, and Shlomo Shamai (Shitz) (2008c). Secure Communication Over Fading Channels. *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492.

Liang, Yingbin, Gerhard Kramer, H. Vincent Poor, and Shlomo Shamai (Shitz) (2009). Compound Wiretap Channels. *EURASIP Journal on Wireless Communications and Networking*.

Liu, Jia, Y. Thomas Hou, and Hanif D. Sherali (2009). Optimal Power Allocation for Achieving Perfect Secrecy Capacity in MIMO Wire-tap Channels. *Proceedings of the 43rd Annual Conference on Information Sciences and Systems (CISS)*. Baltimore, USA.

Liu, Ruoheng, Tie Liu, H. Vincent Poor, and Shlomo Shamai (Shitz) (2010). Multiple-Input Multiple-Output Gaussian Broadcast Channels With Confidential Messages. *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4215–4227.

Liu, Tie, Vinod M. Prabhakaran, and Sriram Vishwanath (2008). The Secrecy Capacity of a Class of Parallel Gaussian Compound Wiretap Channels. *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*. Toronto, Canada.

Maurer, Ueli M. (1990). Provably Secure Key Distribution based on Independent Channels. *Proceedings of the IEEE Information Theory Workshop (ITW)*. Veldhoven, The Netherlands.

Maurer, Ueli M. (1993). Secret-Key Agreement by Public Discussion based on Common Information. *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742.

Nedić, Angelia and Asuman Ozdaglar (2009). Subgradient Methods for Saddle-Point Problems. *Journal of Optimization Theory and Applications*, vol. 142, no. 1, pp. 205–228.

Negi, Rohit and Satashu Goel (2005). Secret Communication using Artificial Noise. *Proceedings of the Vehicular Technology Conference (VTC)*. Dallas, USA.

Oggier, Frédérique E. and Babak Hassibi (2007). The Secrecy Capacity of the MIMO Wire-tap Channel. *Proceedings of the 45th Annual Allerton Conference on Communication, Control and Computing*. Monticello, USA.

Papandreou, Nikolaos and Theodore Antonakopoulos (2008). Bit and Power Allocation in Constrained Multicarrier Systems: The Single-User Case. *EURASIP Journal on Advances in Signal Processing*.

Shafiee, Shabnam and Sennur Ulukus (2007). Achievable Rates in Gaussian MISO Channels with Secrecy Constraints. *Proceedings of the IEEE International Symposium on Information Theory*. Nice, France.

Shannon, Claude E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715.

Shi, Wei and James Ritcey (2010). Robust Beamforming for MISO Wiretap Channel by Optimizing the Worst-Case Secrecy Capacity. *Proceedings of the 44th Asilomar Conference on Signals, Systems and Computers*. Pacific Grove, USA.

Sion, Maurice (1958). On General Minimax Theorems. *Pacific Journal of Mathematics*, vol. 8, no. 1, pp. 171–176.

Telatar, I. Emre (1995). *Capacity of Multi-antenna Gaussian Channels*. Technical Memorandum, Bell Laboratories, Lucent Technologies.

Tomasin, Stefano and Eduard A. Jorswieck (2014). Pilot-based Secret Key Agreement for Reciprocal Correlated MIMOME Block Fading Channels. *Proceedings of the 57th IEEE Global Communications Conference (GLOBECOM)*. Austin, USA.

Vía, Javier (2014). Robust Secret Key Capacity for the MIMO Induced Source Model. *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. Florence, Italy.

Weingarten, Hanan, Tie Liu, Shlomo Shamai (Shitz), Yossef Steinberg, and Pramod Viswanath (2007). The Capacity Region of the Degraded MIMO Compound Broadcast Channel. *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*. Nice, France.

Wolf, Anne and Eduard A. Jorswieck (2010a). Maximization of Worst-Case Secrecy Rates in MIMO Wiretap Channels. *Proceedings of the 44th Asilomar Conference on Signals, Systems, and Computers*. Pacific Grove, USA.

Wolf, Anne and Eduard A. Jorswieck (2010b). On the Zero Forcing Optimality for Friendly Jamming in MISO Wiretap Channels. *Proceedings of the 11th IEEE International Workshop on Signal Processing Advances for Wireless Communications (SPAWC)*. Marrakech, Morocco.

Wolf, Anne and Eduard A. Jorswieck (2011). Maximization of Worst-Case Secret Key Rates in MIMO Systems with Eavesdropper. *Proceedings of the 54th IEEE Global Communications Conference (GLOBECOM)*. Houston, USA.

Wolf, Anne, Eduard A. Jorswieck, and Carsten R. Janda (2015). Worst-Case Secrecy Rates in MIMOME Systems under Input and State Constraints. *Proceedings of the 7th IEEE International Workshop on Information Forensics and Security (WIFS)*. Rome, Italy.

Wong, Tan F., Matthieu R. Bloch, and John M. Shea (2009). Secret Sharing over Fast-Fading MIMO Wiretap Channels. *EURASIP Journal on Wireless Communications and Networking*.

Wyner, Aaron D. (1975). The Wire-Tap Channel. *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387.

Xiao, Liang, Larry Greenstein, Narayan Mandayam, and Wade Trappe (2007). Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication. *Proceedings of the IEEE International Conference on Communications (ICC)*. Glasgow, UK.

Yeung, Raymond W. (2008). *Information Theory and Network Coding*. Springer.

Zhou, Xiangyun and Matthew R. McKay (2009). Physical Layer Security with Artificial Noise: Secrecy Capacity and Optimal Power Allocation. *Proceedings of the International Conference on Signal Processing and Communication Systems (ICSPCS)*. Omaha, USA.