# Physical Layer Security vs. Network Layer Secrecy: Who Wins on the Untrusted Two-Way Relay Channel?

Johannes Richter*, Elke Franz†, Sabrina Gerbracht*, Stefan Pfennig†, and Eduard A. Jorswieck*
*Dep. of Electrical Engineering and Information Technology / Communications Laboratory
†Dep. of Computer Science / Privacy and Data Security
Technische Universität Dresden, 01062 Dresden, Germany
Email: {johannes.richter, elke.franz, sabrina.gerbracht, stefan.pfennig, eduard.jorswieck}@tu-dresden.de

***Abstract*—We consider the problem of secure communications in a Gaussian two-way relay network where two nodes exchange confidential messages only via an untrusted relay. The relay is assumed to be honest but curious, i.e., an eavesdropper that conforms to the system rules and applies the intended relaying scheme. We analyze the achievable secrecy rates by applying network coding on the physical layer or the network layer and compare the results in terms of complexity, overhead, and efficiency. Further, we discuss the advantages and disadvantages of the respective approaches.**

***Index Terms*—Secure network coding, compute-and-forward, bidirectional untrusted relay channel**

## I. Introduction

Nowadays, the world is connected over networks and communications are easily overheard. Protecting the confidentiality of communication in networks is therefore an important topic. Based on the assumption that an attacker has access to a limited number of links only, a network coding scheme protecting confidentiality was proposed in [1]. However, if the attacker can observe more links or even nodes, he might be able to decode the data and, hence, security measures have to be integrated.

End-to-end encryption of the data on the network layer will prevent information leakage to an attacker. Despite this basic method, various approaches for ensuring the confidentiality of network coding schemes have been proposed [2] that promise to save costs in comparison to end-to-end encryption.

Another approach to secure data transmission is based on information theoretic security: Already Shannon studied the notion of perfect secrecy in his seminal paper [3] for the case in which an eavesdropper has direct access to the codeword sent. Almost thirty years later, the theoretical basis for an information-theoretic approach was laid first by Wyner [4] and then by Csiszár and Körner [5], who proved in two seminal papers that codes for channels exist which guarantee both reliability and a prescribed degree of data confidentiality. The extension to continuous input and output alphabets was developed in [6]. It took more than another twenty years before transceiver structures are available to support these wiretap setups. Extensive analysis and designs have been conducted, parts of their results are reported in [7], [8], [9] and recent tutorial papers [10], [11].

In contrast to traditional wireless communication structures where one receiver focuses on the detection and decoding of one transmit signal treating interfering signals as noise, in physical layer network coding [12], the receiver exploits the interference as a useful part of the signal, e.g., in a linear combination of two or more transmit signals. It has been early observed that decoding a linear combination of source messages at one node does not automatically allow this node to decode each message individually [13]. Compute-and-forward network coding together with strong physical-layer security based on universal hash functions has been investigated in [14]. Kashyap et al. provided an achievable power-rate region with perfect secrecy in [15], where they applied compute-and-forward to the Gaussian two-way relay channel.

Within this paper, we compare approaches on the physical and network layer and discuss advantages and disadvantages of these approaches. We focus on the achievable secrecy rates but discuss also complexity, overhead, and efficiency.

### A. Notation

Let $\log^+(x) \triangleq \max\{0, \log(x)\}$. We denote by $x'$ the transpose of vector $x$ and by $\mathbb{F}_q$ the field of size $q$. A $d$-dimensional lattice $\Lambda \subset \mathbb{R}^d$ is an algebraic group under addition with generator matrix $G \in \mathbb{R}^{d\times d}$, i.e., $\Lambda = \{Gz : z \in \mathbb{Z}^d\}$. A lattice quantizer is a mapping $Q_\Lambda : \mathbb{R}^d \to \Lambda$ that maps a point $x$ to the nearest lattice point in Euclidean distance, i.e., $Q_\Lambda(x) = \arg\min_{\lambda\in\Lambda} \|x-\lambda\|$. Let the modulo operation with respect to the lattice $\Lambda$ be defined as $[x] \bmod \Lambda = x - Q_\Lambda(x)$.

## II. System Model

We investigate the two-way relay-channel with half-duplex nodes as depicted in Figure 1. The links are additive white Gaussian noise (AWGN) channels with fading coefficients $g_1$ and $g_2$. Each node has an average transmit power constraint $E\|s\|^2 \leq P$. Nodes 1 and 2 have messages for each other but

This work is supported by the German Research Foundation (DFG) in the Collaborative Research Center 912 "Highly Adaptive Energy-Efficient Computing."

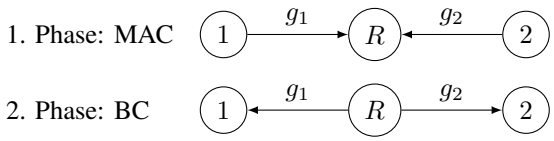


Figure 1. Two-Way Relay-Channel.

have no direct connection. They transmit messages with the help of a relay in two phases. The relay applies compute-and-forward (CF) [16]. In the first phase the channel is a multiple access channel (MAC), i.e., the relay receives a superposition of both signals from nodes 1 and 2 and tries to decode a linear combination of the original messages. In the second phase, we have a broadcast channel (BC), i.e., the linear combination is encoded with a capacity achieving code and sent to both nodes simultaneously.

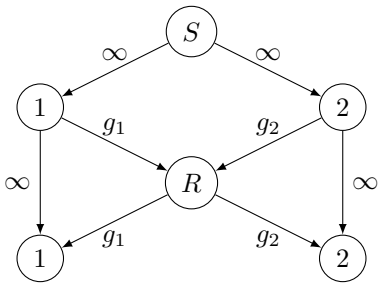


Figure 2. Two-Way Relay-Channel modeled as butterfly network.

Equivalently, the two-way relay-channel in Figure 1 can be modeled as a butterfly network with a single virtual source node as depicted in Figure 2. In order to model the source nodes from the two-way relay channel, the two source nodes 1 and 2 are fed by the virtual source node $S$ over links of infinite capacity. Both source nodes send their signals over the channels $g_1$ and $g_2$ to the relay, which corresponds to the MAC phase in the two-way relay-channel. In order to model the knowledge of the own sent message at the destination nodes 1 and 2, which are in the case of the two-way relay-channel identical to the source nodes 1 and 2, we have an infinite capacity link from source 1 to destination 1 and from source 2 to destination 2. The relay transmits over the channels $g_1$ and $g_2$ the linear combination of the messages. This corresponds to the BC phase in the two-way relay-channel.

**Remark 1.** This butterfly model is more convenient for the approaches on the network layer than the two-way relay-channel, as the chosen approaches only support intra-flow communication, which originates from a single source node.

## III. Physical Layer

### A. Transmission Scheme

We consider compute-and-forward at the relay as introduced in [16]. Thereby, each message is encoded using a nested lattice code [12], [17], [18].

In the first phase, the relay receives the signal

$$y_r = g_1 s_1 + g_2 s_2 + z_r, \tag{1}$$

where $g_1, g_2$ are the fading coefficients, $s_1, s_2$ are the signal vectors sent by the source nodes, and $z_r \sim \mathcal{N}(0, I_d)$ is additive white Gaussian noise. Using the compute-and-forward framework, the relay can decode an equation or linear combination of the original lattice points,

$$v = [a_1 s_1 + a_2 s_2] \bmod \Lambda, \tag{2}$$

for some coefficients $(a_1, a_2) \in \mathbb{Z}^2$.

**Remark 2.** Aside from the coefficient vectors $a = (1, 0)$ and $a = (0, 1)$, the relay can obtain the single messages if the transmission rates are low enough to be able to decode several linear independent linear combinations.

The decoding is successful, if the transmission rates of the source nodes are below the computation rate [16, Th. 2]

$$R_{CF} = \max_a \frac{1}{2} \log_2^+ \left( \left( \|a\|^2 - \frac{(g'a)^2 P}{1 + P\|g\|^2} \right)^{-1} \right), \tag{3}$$

where $g = (g_1, g_2)'$ and $a = (a_1, a_2)'$. The relay encodes $v$ with a capacity achieving code and transmits the codeword to destination nodes 1 and 2 simultaneously. Both destination nodes can decode the linear combination sent by the relay, subtract their own messages and get the message sent by the other source node or pass the decoded linear combination to higher layers.

**Proposition 1** (Achievable Rate Region)**.** *The achievable rate region for the two-way relay channel with compute-and-forward is given by*

$$R_1 \leq R_{CF}, \quad R_2 \leq R_{CF}, \tag{4}$$

*where $R_1$ and $R_2$ are the transmission rates of nodes 1 and 2, respectively.*

**Remark 3.** The resulting rate region combines the constraints from both phases and is given by

$$R_1 \leq \min\left\{R_{CF}, \tfrac{1}{2}\log_2(1 + Pg_1^2), \tfrac{1}{2}\log_2(1 + Pg_2^2)\right\}, \tag{5}$$
$$R_2 \leq \min\left\{R_{CF}, \tfrac{1}{2}\log_2(1 + Pg_1^2), \tfrac{1}{2}\log_2(1 + Pg_2^2)\right\}. \tag{6}$$

We can remove the min-function because the computation rate will not be larger than the single user rates. Otherwise, it would contradict the definition of the capacity of the point-to-point channel. The proof of the computation rate and the achievable rate region can be found in [16].

### B. Secrecy

In practice, it happens often that a transmission between two nodes has to use a relay that cannot be trusted. Therefore, the messages have to be encoded at the transmitter such that the relay cannot decode the messages separately. Assuming that the relay is an honest but curious eavesdropper, we use a compute-and-forward based approach to secure the messages, which was introduced in [19]. Nodes 1 and 2 use nested lattice codes with a course lattice $\Lambda$, a binning lattice $\Lambda_B$, and a fine lattice $\Lambda_F$, which build a chain $\Lambda \subset \Lambda_B \subset \Lambda_F$. Due to the additional binning lattice $\Lambda_B$, this procedure corresponds to a common binning strategy [9] with the lattice points in $\Lambda_B$

defining the bins. Points in $\Lambda_F$ are added randomly to confuse the eavesdropper, i.e., the relay, and provide the required secrecy. This results in the following achievable secrecy rate region.

**Proposition 2** (Achievable Secrecy Rate Region [19, Th. 1])**.** *Consider a two-way relay-channel with fading coefficients $g_1$ and $g_2$ which are grouped to a vector $g = (g_1, g_2)'$. Each node has an average transmit power constraint $E\|s\|^2 \leq P$ and the noise at each node is assumed to be i.i.d. normally distributed, $\mathcal{N}(0, I_d)$. Then an achievable secrecy rate region is given by*

$$R_1 + R_2 \leq 2R_{CF} - \tfrac{1}{2}\log_2(1 + Pg_1^2 + Pg_2^2) \qquad (7)$$

*where*

$$R_{CF} = \max_{\substack{a_1 \neq 0 \\ a_2 \neq 0}} \frac{1}{2}\log_2^+\left(\left(\|a\|^2 - \frac{(g'a)^2 P}{1 + P\|g\|^2}\right)^{-1}\right). \qquad (8)$$

The proof can be found in [19].

## IV. Network Layer

### A. Basic Assumptions

In addition to the previously presented secure compute-and-forward scheme on the physical layer, we want to take a look on available alternative approaches on the network layer.

A practical implementation of network coding (Practical Network Coding, PNC) on the network layer has been introduced by Chou et al. in [20]. PNC bases on Random Linear Network Coding (RLNC) [21], i.e., forwarding nodes randomly select the coefficients for computing the combined data packets. In the following we summarize only the parameters that have to be considered for the comparison. For a more detailed description of PNC, we refer to [20].

The source node splits data to be sent into packets $x_i$ of $m$ symbols $x_{i,j} \in \mathbb{F}_q$, amends each packet by a global encoding vector (GEV) to allow for a decentralized solution, and organizes the packets into matrices called generations. A generation comprises $h$ data packets; only packets of one and the same generation can be combined during network coding (intra-session network coding). The GEV consists of $h$ symbols $\beta_{i,j} \in \mathbb{F}_q$. Hence, the data packets to be sent have the following structure:

$$x_i = (\beta_{i,1}, \beta_{i,2}, ..., \beta_{i,h}, x_{i,1}, x_{i,2}, ..., x_{i,m}).$$

### B. Approaches for Enforcing Confidentiality

To ensure confidentiality of the data to be sent, the attacker must not be able to decode the original data. This goal can be achieved by end-to-end encryption of the data to be sent. However, methods tailored to network coding can require less encryption and decryption effort. An overview on various approaches for securing network coding against eavesdroppers can be found in [2]. Within this article, we focus on approaches that utilize cryptographic primitives. The cryptographic methods proposed so far either suggest to protect the GEV or to apply a simple and cost-effective operation to the data packets before sending them. For our comparison, we selected the two following approaches, as these approaches do not require the packets to be decoded at the relay. Therefore, CF can be applied on the physical layer.

Ensuring confidentiality by encrypting the encoding coefficients, which are randomly selected by the source node (locked coefficients), was proposed in [24]. Additionally, the packets are amended by a further GEV, which functions in the normal network coding manner (unlocked coefficients). The destination nodes decode the packets using the unlocked coefficients, decrypt the locked coefficients, and decode the data packets by means of the decrypted coefficients. The security of this protocol named SPOC (Secure Practical Network Coding) was investigated in [22].

Instead of protecting the GEV, permuting all symbols of the data packets before sending them (P-Coding) was suggested in [23]). The permutation only changes the sequence of the symbols, so that the forwarding nodes can compute linear combinations as usual. After applying the inverse permutation, the destination nodes can decode the data.

## V. Comparison of the Approaches

### A. Assumptions

There are various issues that complicate a comparison of approaches working at physical layer and network layer. At physical layer, transmission rates and channel uses are important parameters. Data processing at higher layers is usually not considered. At network layer, we are talking about the transmission of data packets of a certain size. We assume that the lower layers ensure the transmission of the sequences of bytes over the insecure channels (physical layer is a "bit-pipe"). Even if we focus on one layer, processing at the other layers is necessary. Further, more aspects have to be considered for a fair comparison, e.g., the type of achieved security and computational complexity.

Consequently, the comparison of approaches working at these different layers is not at all straightforward. As a starting point, we evaluate the overhead implied by the different approaches, i.e., the possible relative payload.

For the calculation of the payload, we do not consider the GEV for the network layer approaches since we can assume the coefficients $\beta_{i,j}$ to be 1 in case of the butterfly network. Please note that the encrypted GEV is part of the data packets for SPOC, i.e., it reduces the payload per packet.

For similar reasons, we neglect the payload caused by the distribution of the CF coefficients $a$ for the approach on the physical layer.

### B. Payload of Network Layer Schemes

The payload per data packet depends on the symbol size $q$, on the packet size $n$, and on the generation size $h$. For both approaches, it is not necessary to increase the symbol size so that we assume $q = 2^8$ according to [20]. Since we do not consider the GEV, SPOC achieves an absolute payload of $L_{\text{abs}} = n - h\frac{\lceil \text{ld } q \rceil}{8}$ and a relative payload of $L = \frac{L_{\text{abs}}}{n}$ per packet. In contrast, P-Coding provides an absolute payload of $L_{\text{abs}} = n$ and therefore a relative payload of $L = \frac{n}{n} = 1$.

SPOC assumes encryption of the originally chosen GEV by means of a symmetric encryption scheme such as AES. If we

consider only the encryption of the encoding coefficients, the length of these coefficients would be determined by the block length $l$ of the cipher. To avoid this effect, we assume that the first $l$ bytes of the data packet are encrypted.

To allow for a comparison to physical layer approaches that consider the transmission rate per channel use, we evaluate the relative payload for transmitting a certain amount of information ($B$ bytes). Structuring the data into packets and generations causes additional overhead if the data to be sent is not a multiple of the payload per generation. The ratio of information size to transmitted data size can be computed by

$$r = \frac{B}{\left\lceil \frac{\left\lceil \frac{B}{L_{\text{abs}}} \right\rceil}{h} \right\rceil nh}, \tag{9}$$

where $r \in [0, 1]$.

### C. Secrecy Rate

We define the achievable secrecy rate $R_s$ [bit/cu] as the amount of information bits that can be securely transmitted within a channel use. We focus on the achievable sum rate, i.e., the rate of the virtual node $S$ in Figure 2.

On the physical layer, the achievable secrecy sum rate is given by Proposition 2, i.e.,

$$R_s^{\text{PHY}} = 2R_{CF} - \tfrac{1}{2}\log_2(1 + Pg_1^2 + Pg_2^2). \tag{10}$$

The network layer depends on the reliable transmission on the physical layer. Therefore, the achievable secrecy sum rate is the ratio $r$ of information to transmitted data times the achievable rate on the physical layer without secrecy (Proposition 1), i.e.,

$$R_s^{\text{NET}} = 2rR_{CF}. \tag{11}$$

Since the ratio $r$ of information size to transmitted data size goes to one as the packet size $n$ goes to infinity, it is obvious that the achievable secrecy sum rate on the network layer will asymptotically approach $2R_{CF}$, i.e., the CF sum rate. Note that this is only true if the information size is large with respect to the packet size. Otherwise, the packets will not be fully filled which results in a large overhead.

For the simulations, we assume the butterfly network as introduced in Sec. II (Figure 2) with a multicast capacity of $h = 2$. Hence, generations for network layer approaches contain $h = 2$ data packets.

As an example, we choose a symmetric scenario where the channel parameters are $g = (12, 12)'$ and the transmit power for all nodes is $P = 1$ Watt. Please note that we normalized the power to noise ratio to one and put the scaling in the channel coefficients. This scenario corresponds to a more realistic parameter set of, e.g., $g = (0.8, 0.8)'$, $P/\sigma^2 = 23.52$ dB, where $\sigma^2$ is the noise power which is assumed as 1 Watt throughout this paper.

On the physical layer, we get the following computation rate by choosing the coefficients $a$ of the linear combination as $a = (1, 1)'$,

$$R_{CF} = 3.5875 \text{ bit/cu}. \tag{12}$$

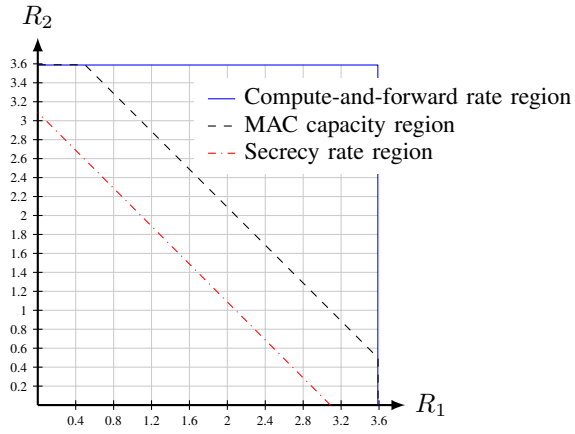


Figure 3. Achievable rate regions with different transmission schemes on the physical layer for channel coefficients $g = (12, 12)'$ and $P = 1$ Watt.

With this computation rate, we can achieve a secrecy rate of

$$R_s^{\text{PHY}} = 3.0875 \text{ bit/cu}. \tag{13}$$

The achievable rate regions with the capacity region of the multiple access channel for comparison is given in Figure 3.

In Figure 4, the achievable secrecy sum rates for the presented approaches on the physical layer and the network layer are plotted over the packet size $n$ for an information size of $B = 100000$ bytes. The secrecy sum rates for SPOC and P-Coding are calculated according to (11). Because the relative payload of the P-Coding approach is 1, it achieves a secrecy sum rate of $2R_{CF}$ even for small packet sizes unlike the SPOC approach. For large packet sizes, not all packets will be filled completely and the achievable rate will decrease. This effect can be seen in more detail for an information size of $B = 100$ bytes in Figure 5, where the network layer schemes achieve the full secrecy sum rate of $2R_{CF}$ only for $n = \{2, 10, 50\}$. Such an effect might be seen in sensor networks where the amount of transmit data is small whereas a behavior like in Figure 4 will more likely occur in streaming applications with full buffers.

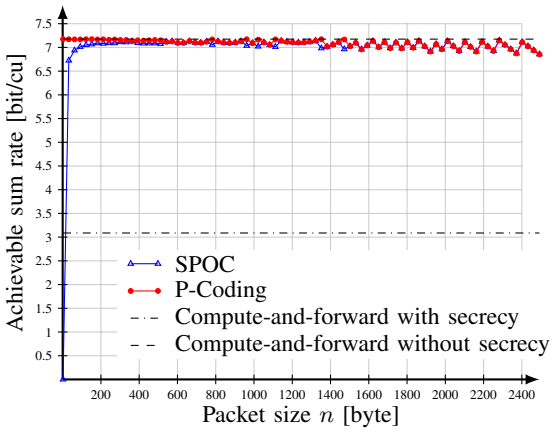


Figure 4. Achievable sum rates on physical layer and network layer with different transmission schemes for information size $B = 100000$ bytes.

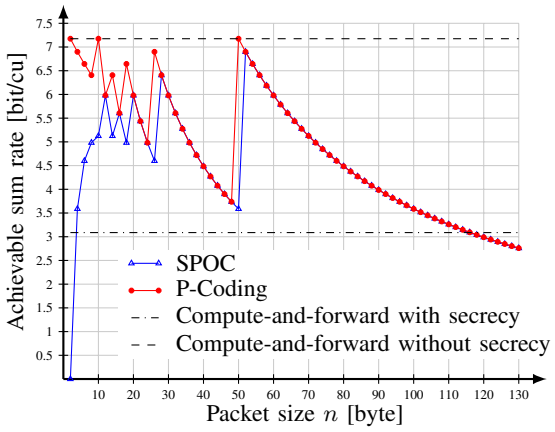


Figure 5. Achievable sum rates on physical layer and network layer with different transmission schemes for information size $B = 100$ bytes.

### D. Differences on the Layers

In this section, we want to discuss some problems that occur when trying to compare physical layer secrecy schemes to network layer confidentiality schemes. We do not aim to answer the question which approach is better. Instead we want to point out some things that need to be kept in mind, when comparing secrecy on different layers.

First of all, the definitions of secrecy differ significantly on the two layers. On the physical layer we are talking about information theoretic security, i.e., the secrecy can be measured quantitatively with regard to the statistical independence between the messages sent by the transmitter and the received signal at the eavesdropper. In our system, we have the weak secrecy criterion, i.e., the information leakage rate to the eavesdropper goes asymptotically to zero as the block length goes to infinity.

The information theoretic security of SPOC requires additional steps before encoding [22]. The authors showed that with certain pre-processing steps the mutual information between the original messages and the transmitted messages goes to zero as the field size goes to infinity. If the locked coefficients are sent over the network as suggested in [24], the security depends on the cryptographic algorithm, i.e., the whole scheme can be only computational secure. The authors of [22] assumed that this information is sent over a secret channel.

P-Coding requires a new permutation key for each generation to prevent that a key compromise threatens the security of subsequently sent generations. Further, the encoded messages should be uniformly distributed which requires an additional pre-processing.

Both network layer approaches require a key distribution, which needs to be done securely. On the physical layer, no secret keys are necessary and therefore no additional communication overhead occurs. Another advantage of the physical layer secrecy is the lower computational complexity compared to the cryptographic operations that are needed on the network layer. However, these tasks can be done in hardware and are fast in execution.

## VI. Summary and Outlook

In this paper, we analyzed network coding under secrecy constraints in the two-way relay network. We compared different approaches on the physical layer and the network layer with the main focus on the achievable secrecy rate. We showed that network coding on the network layer can achieve higher secrecy rates if the packet size is chosen appropriately. On the other hand, physical layer network coding provides stronger secrecy with less computational complexity.

## References


[1] N. Cai and R. W. Yeung, "Secure Network Coding," in *Proc. IEEE Int. Symp. on Information Theory (ISIT)*, 2002.

[2] L. Lima, J. P. Vilela, P. F. Oliveira, and J. Barros, "Network coding security: Attacks and countermeasures," 2008. [Online]. Available: http://arxiv.org/abs/0809.1366

[3] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[4] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[6] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[7] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*, ser. Foundations and Trends in Communications and Information Theory. now publishers, 2009, vol. 5, no. 4-5, pp. 355–580.

[8] R.-H. Liu and W. Trappe, Eds., *Security Wireless Communications at the Physical Layer*. Springer, 2009.

[9] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[10] Y.-S. Shiu, S.-Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-W. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Feb. 2011.

[11] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 40–47, Jan. 2012.

[12] B. Nazer and M. Gastpar, "Reliable physical layer network coding," *Proc. IEEE*, vol. 99, no. 99, pp. 438–460, 2011.

[13] K. Lu, S. Fu, Y. Qian, and T. Zhang, "On the security performance of physical-layer network coding," in *Proc. IEEE Int. Conf. on Communications (ICC)*, 2009.

[14] X. He and A. Yener, "Strong secrecy and reliable byzantine detection in the presence of an untrusted relay," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 177–192, 2013.

[15] N. Kashyap, S. V, and A. Thangaraj, "Secure compute-and-forward in a bidirectional relay," 2012. [Online]. Available: http://arxiv.org/abs/1206.3392

[16] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, 2011.

[17] R. Zamir, "Lattices are everywhere," in *Information Theory and Applications Workshop*, 2009, pp. 392–421.

[18] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3401–3416, 2005.

[19] J. Richter, C. Scheunert, S. Engelmann, and E. A. Jorswieck, "Secrecy in the two-way relay channel with compute-and-forward," 2013. [Online]. Available: http://www.ifn.et.tu-dresden.de/~richterj/paper/Richter2013.pdf

[20] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Proc. Annual Allerton Conf. on Comm., Control, and Computing*, 2003.

[21] T. Ho, R. Koetter, M. Médard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," in *Proc. IEEE Int. Symp. on Information Theory (ISIT)*, 2003.

[22] L. Lima, J. P. Vilela, J. Barros, and M. Médard, "An information-theoretic cryptanalysis of network coding – is protecting the code enough?" in *Int. Sym. on Inf. Theory and its Applications (ISITA)*, 2008.

[23] P. Zhang, Y. Jiang, C. Lin, Y. Fan, and X. Shen, "P-Coding: Secure network coding against eavesdropping attacks," in *Proc. IEEE INFOCOMM*, 2010.

[24] J. P. Vilela, L. Lima, and J. Barros, "Lightweight security for network coding," in *Proc. IEEE Int. Conf. on Communications (ICC)*, 2008.