Perfect Secrecy in Physical Layer Network Coding Systems from Structured Interference

David A. Karpuk, *Member, IEEE,* Arsenia Chorti, *Member, IEEE*

***Abstract*—Physical layer network coding (PNC) has been proposed for next generation networks. In this contribution, we investigate PNC schemes with embedded perfect secrecy by exploiting structured interference in relay networks with two users and a single relay. In a practical scenario where both users employ finite and uniform signal input distributions, we establish upper bounds (UB) on the achievable perfect secrecy rates and make these explicit when PAM modems are used. We then describe two simple, explicit encoders that can achieve perfect secrecy rates close to these UBs with respect to an untrustworthy relay in the single antenna and single relay setting. Lastly, we generalize our system to a MIMO relay channel where the relay has more antennas than the users and study optimal precoding matrices which maintain a required secrecy constraint. Our results establish that the design of PNC transmission schemes with enhanced throughput and guaranteed data confidentiality is feasible in next generation systems.**

***Index Terms*—Physical layer network coding, achievable secrecy rate, perfect secrecy, signal space alignment**

I. Introduction

RECENTLY, the ideas of network coding [1] have been extended to the wireless physical medium; notably, in [2], [3], among others, the concept of harnessing interference through structured codes was explored in the framework of physical layer network coding (PNC). These technologies can be proven instrumental in enabling the envisaged multi-fold increase in data throughput in fifth generation (5G) networks [4]. The generic PNC system model with two independent sources and one relay is depicted in Fig. 1 and assumes that communication is executed in two cycles. In the first cycle, the nodes A, referred to as Alice, and B, referred to as Bob, simultaneously transmit respective codewords to the relay node R, referred to as Ray. In the second cycle, Ray broadcasts to Alice and Bob a function of the total received signal; Alice and Bob then retrieve each other's messages by canceling off their corresponding transmissions. Depending on the transformation executed by Ray, one of the following relaying strategies can be employed: amplify-and-forward, decode-and-forward, compress-and-forward [5], or the recently introduced compute-and-forward [6] approach.

Nevertheless, despite the potential for substantial increase of the transmission rates in wireless networks, a major obstacle in the widespread deployment of PNC and generally of relay networks arises due to security concerns, i.e., the confidentiality of the exchanged data with respect to an untrustworthy relay. A straightforward approach would be employing encryption at upper layers of the communication network or encryption at the physical layer [7]. However, the management of secret keys used by crypto algorithms depends on the structure of the access network and fourth generation systems (4G) already have a key hierarchy of height five (5) for each individual end-user, while there exist multiple keys in each layer of the hierarchy [8]. Extrapolating from the experience of 4G systems, it is expected that the management of secret keys in 5G would become an even more complicated task [9]. The generation, management, and distribution of secret keys in decentralized settings, such as device-to-device PNC networks, without an infrastructure that supports key management and authentication will impose new security challenges.

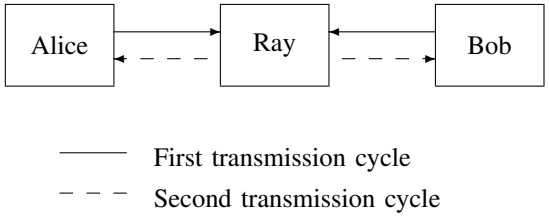

Fig. 1. Physical layer network coding (PNC) with two transmitter and one relay node.

An alternative theoretical framework for the study of data confidentiality in the physical layer of wireless networks, dubbed as physical layer security [10]–[12], has recently become a focal point of research in the wireless community. The metric of interest, referred to as the channel secrecy capacity is the supremum of transmission rates at which data can be exchanged reliably while satisfying a weak secrecy [13], [14], strong secrecy [15], or perfect secrecy constraint [16]. As an example, let X^n be the n-length encoded version of a nR-bit message transmitted by the source and let Z^n denote the passive eavesdropper's information. Weak and strong secrecy assume that the code's blocklength n becomes arbitrarily long, i.e.,

$$\lim_{n\to\infty} \frac{1}{n} I(X^n; Z^n) = 0, \text{ weak secrecy constraint, (1)}$$

$$\lim_{n\to\infty} I(X^n; Z^n) = 0, \text{ strong secrecy constraint. (2)}$$

Shannon's definition of perfect secrecy in [16] on the other

D. Karpuk is with the Department of Mathematics and Systems Analysis, Aalto University, Espoo, Finland. A. Chorti is with the Department of Computer Science and Electronic Engineering, University of Essex, Colchester, United Kingdom. emails: {david.karpuk@aalto.fi, achorti@essex.ac.uk}

D. Karpuk is supported by Academy of Finland Postdoctoral grant 268364.

hand explicitly assumes a finite blocklength, that is,

$$I(X;Z) = 0, \text{ perfect secrecy constraint.} \tag{3}$$

The first study of weak secrecy in relay channels with confidential messages has appeared in [17] while further analyses followed [18], [19]; these contributions established that the secrecy capacity of one-way relay channels is zero, unless the source-destination channel is better than the source-relay channel. In essence, relay topologies of practical interest in which the link to the relay is better than the direct link were shown to be inherently insecure. Due to this limiting result, subsequent work focused entirely on cooperative relay channels with trustworthy relays, [20]–[23] to cite but a few.

However, unlike one-way relay networks, systems employing network coding can on the other hand benefit from the simultaneity of transmissions to an untrustworthy relay to achieve data confidentiality as noted in [24]. In essence, the structured interference observed by the relay can be exploited to achieve strong secrecy in the wireless transmissions [25], [26]. In [26]–[29] the role of interference in achieving strong secrecy was demonstrated using lattice encoders; however [27] and [28] rely on the use of random dithering and good nested lattice codes in arbitrarily high dimensions. In the wiretap channel studied in [29] the superposition of the interference to the data was viewed as a modulo addition operation, i.e., the superposition was assumed to take place in the code space and not in the signal space.

In the present study, PNC networks in which Ray can observe superpositions in the signal space (real sums of signals transmitted by Alice and Bob as opposed to modulo sums in the code space) are investigated in the presence of synchronization errors assuming all nodes employ M-ary pulse amplitude modulation (M-PAM) transceivers; this *realistic* scenario is fundamentally more demanding than previously investigated settings [23], and arguably more practical than the schemes of [27], [28].

To separate the problem of secrecy from error correction, we first restrict to a noiseless channel where we evaluate upper bounds (UBs) on the achievable perfect secrecy rates, make these explicit in the case of PAM modems, and investigate the effect of synchronization errors on secrecy. The proposed secret encoders in the single-input single-output (SISO) setting allow Ray to obtain estimates of linear combinations of the transmitted PAM symbols but not to retrieve any of the secret bits they carry, thus achieving perfect secrecy, i.e., *zero information leakage per PAM symbol*. Finally, our system model is extended to the multiple-input multiple-output (MIMO) case in which we study optimal precoding matrices which achieve the required signal alignment at the relay, while preserving secrecy. Our study differs from earlier work on interference alignment for secrecy [30], [31], [32] and interference alignment for the MIMO channel [33] in that the required secrecy conditions demand equality of *matrices* rather than just of the *subspaces* generated by their columns.

The paper is organized as follows. In Section II the SISO system model is presented and we propose upper bounds (UBs) on the achievable perfect secrecy rates of the noiseless SISO system given finite constellations. In Section III we provide explicit formulas for these bounds in the case of PAM modems, demonstrate that the user with the smaller PAM constellation can transmit no secret bits without knowledge of the other user's symbol, and further discuss the impact of synchronization errors on the upper bounds. In Section IV two explicit encoders achieving perfect secrecy are constructed, the first assuming no cooperation between the users, and the second assuming that the user of the smaller constellation knows the signal transmitted by the other user. The achievable rates in both approaches are shown to be close to the upper bound. In Section V we generalize our setup to a noisy MIMO channel in which the users and the relay have multiple antennas, and study optimal precoding matrices. Finally in Section VI the conclusions of this contribution are drawn and future directions of the work are discussed.

II. Secure PNC System Model

Communication between Alice and Bob with the help of Ray takes place in two cycles as depicted in Fig. 1. In what follows, we use the subscript A to denote quantities and variables (source symbols, codewords, etc.) corresponding to Alice and the subscript B for those belonging to Bob. All channel coefficients and encoding/decoding algorithms are public, i.e., known by Alice, Bob, and Ray. Lower case letters denote realizations of respective random variables that are represented with the corresponding upper case letters, e.g., x denotes a realization of the random variable X with probability mass function (pmf) $p_X(x)$. The corresponding script letter $\mathcal{X}$ denotes the *support* of X, that is, the set of all x for which $p_X(x)$ is non-zero.

We assume that Alice and Bob's source symbols (secret messages) are drawn from discrete alphabets. Under an average power constraint, the use of Gaussian encoders has been demonstrated to achieve the secrecy capacity of the interference channel [34]. However when transmission is constrained by a joint amplitude-variance constraint[1] it has been shown that the capacity is on the contrary achieved by employing codebooks of finite size; a recent extension of these results in the wiretap channel has shown that this holds true for the secrecy capacity as well [35]. Due to this reason, in the following we exclusively operate under the assumption that all codebooks have finite size.

We start by examining the scenario in which all nodes have single antennas while the multi-antenna case will be covered in a later section. In the present work we separate the design of secrecy encoders from error-correction encoding. The reason we propose this approach is that in the noiseless PNC setting it is possible to achieve perfect secrecy without introducing *any delay*, i.e., secrecy is achieved on a per-symbol basis. Additionally, the proposed schemes do not rely on the existence of noise to increase the equivocation at Ray but rather on structured interference, i.e. the structure of the pmf modeling the observation at Ray. While a realistic system would of course employ some form of error-correction, we omit an outer error-correcting code from our system model

[1]Under this realistic assumption the amplitude of the transmitted signals is bounded, as in all actual communication systems.

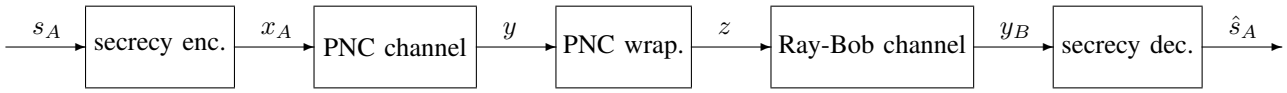

Fig. 2. Encoder for perfect secrecy in PNC systems: Alice encodes a secret message s_A into a codeword x_A using a secrecy encoder. Bob decodes the transmission from Ray to obtain an estimate $\hat{s}_A$ of the secret message transmitted by Alice.

for brevity. Alternatively, one is free to assume that the secret symbols in our system model are the output of some powerful error-correcting code (e.g. turbo or LDPC code); the results herein would remain identical.

A. First Transmission Cycle

We consider finite alphabets $\mathcal{S}_A$, $\mathcal{S}_B$ of secret messages to be transmitted by Alice and Bob, respectively, according to the pmfs of random variables S_A, S_B. The secret messages are encoded in codewords belonging to finite constellations $\mathcal{X}_A$, $\mathcal{X}_B \subset \mathbf{C}$ as follows. We set $M_A = |\mathcal{X}_A|$, $M_B = |\mathcal{X}_B|$, and $m_A = \log_2 M_A$, $m_B = \log_2 M_B$.

Encoding proceeds by first defining labeling functions

$$b_A : \mathcal{X}_A \to \mathcal{S}_A \cup \{\varepsilon\} \tag{4}$$

$$b_B : \mathcal{X}_B \to \mathcal{S}_B \cup \{\varepsilon\} \tag{5}$$

where ε represents the empty string. We assume that b_A and b_B are surjective onto $\mathcal{S}_A$ and $\mathcal{S}_B$, respectively, so that every potential secret message is encoded in some constellation point. For any $s_A \in \mathcal{S}_A \cup \{\varepsilon\}$ we set $b_A^{-1}(s_A) = \{x_A \mid b_A(x_A) = s_A\}$ and similarly for any $s_B \in \mathcal{S}_B \cup \{\varepsilon\}$. The above labeling functions define probabilistic encoding functions φ_A, φ_B as follows. For $s_A \in \mathcal{S}_A \cup \{\varepsilon\}$ we define $\varphi_A(s_A)$ to be uniformly distributed over the set $b_A^{-1}(s_A)$, and φ_B is defined analogously. Thus to transmit $s_A \in \mathcal{S}_A \cup \{\varepsilon\}$, Alice chooses from $b_A^{-1}(s_A)$ uniformly at random and transmits the chosen x_A. Identical remarks apply to Bob. As such, we have random variables X_A and X_B which model the frequency with which symbols x_A and x_B are transmitted.

Assuming perfect synchronization at Alice and Bob, Ray's observation is modeled by

$$Y = h_A X_A + h_B X_B + W_R = X_R + W_R \tag{6}$$

where h_A (respectively h_B) is the channel (fading) coefficient in the link from Alice (Bob) to Ray, $X_R = h_A X_A + h_B X_B$, and W_R is the noise at Ray, a complex circularly symmetric zero-mean Gaussian random variable with variance σ_R^2.

B. Second Transmission Cycle

In the second cycle of the communication, Ray wraps the PNC observation y using a mapping $f : \mathcal{Y} \to \mathcal{Z}$ (e.g., possible options for this mapping include "compress-and-forward" and "compute-and-forward"). We assume that f is invertible given either x_A or x_B, that is, that Alice can recover y from z given that she knows x_A, and similarly for Bob. An obvious choice is to select $\mathcal{Z} = \mathcal{Y}$ and have f be the identity function, i.e., Ray forwards exactly what he receives.

Finally, Ray transmits $z = f(y)$ to Alice and Bob, whose observations are modeled by

$$Y_A = \tilde{h}_A Z + W_A, \tag{7}$$

$$Y_B = \tilde{h}_B Z + W_B, \tag{8}$$

where $\tilde{h}_A$ (respectively $\tilde{h}_B$) is the channel (fading) coefficient from Ray to Alice (Ray to Bob), and W_A (W_B) is the noise at Alice (Bob), a complex circularly symmetric zero-mean Gaussian random variable with variance σ_A^2 (σ_B^2).

Given some observation $y_A \in \mathcal{Y}_A$ at Alice, she estimates Bob's transmitted secret message s_B as follows. From y_A she applies some maximum-likelihood (ML) decoding algorithm to produce an ML estimate $\hat{z}$ of z from equation (7). With knowledge of x_A, she can invert the wrapping function f to produce an estimate $\hat{y}$ of Ray's observation. With knowledge of h_A and x_A, she then produces an ML estimate of $\hat{x}_B$ from $\hat{y} - h_A x_A$, and decodes Bob's secret message by computing $\hat{s}_B = b_B(\hat{x}_B)$. Bob estimates Alice's transmitted secret message in an identical manner.

C. Perfect Secrecy and an Upper Bound on the Secrecy Rate

Perfect secrecy can be achieved with respect to Ray if the mutual information between Ray's observation and the secret source symbols is zero, i.e.,

$$I(Y; S_A) = 0, \text{ perfect secrecy condition for Alice} \tag{9}$$

$$I(Y; S_B) = 0, \text{ perfect secrecy condition for Bob.} \tag{10}$$

The input and output random variables in the PNC system model form respective Markov chains $S_A \to X_A \to X_R \to Y$ and $S_B \to X_B \to X_R \to Y$. As a result, due to the data processing inequality, to satisfy conditions (9) and (10) it suffices to show that

$$I(X_R; S_A) = 0, \text{ sufficient condition for (9),} \tag{11}$$

$$I(X_R; S_B) = 0, \text{ sufficient condition for (10).} \tag{12}$$

Given some fixed encoder and assuming equations (11) and (12) are satisfied, we denote by R_A^s and R_B^s the corresponding secrecy rates[2]. Loose upper bounds on R_A^s and R_B^s are imposed by the capacity in the link Alice-Ray-Bob, i.e., $R_A^s \leq I(X_A; Y_B | X_B)$ and $R_B^s \leq I(X_B; Y_A | X_A)$. The following proposition imposes an alternative upper bound on the secrecy rates, based on Ray's inherent inability to decode the corresponding secret messages.

[2]As the messages are delivered over two transmission cycles, one should potentially multiply all rates and bounds by $\frac{1}{2}$; however we omit this factor for clarity as it does not affect the nature of our results.

Proposition 1: Suppose that conditions (9) and (10) are satisfied. Then the perfect secrecy rates are bounded by $R_A^s \le \widehat{R}_A^s$ and $R_B^s \le \widehat{R}_B^s$, where

$$\widehat{R}_A^s = I(X_A;Y_B|X_B) - I(X_A;Y) + \delta_A \tag{13}$$

$$\widehat{R}_B^s = I(X_B;Y_A|X_A) - I(X_B;Y) + \delta_B. \tag{14}$$

with $\delta_A = H(X_A|Y_B,X_B)$ and $\delta_B = H(X_B|Y_A,X_A)$.

Proof: We will only prove the inequality $R_A^s \le \widehat{R}_A^s$, as the proof of $R_B^s \le \widehat{R}_B^s$ is completely analogous. Since we demand perfect secrecy, the transmission rate is upper bounded by Ray's equivocation, i.e., $R_A^s \le H(S_A) = H(S_A|Y)$. Moreover, $H(X_A|X_B) = H(X_A)$ since X_A and X_B are independent. Therefore,

$$\begin{aligned}
R_A^s &\le H(S_A|Y) \\
&= H(S_A,X_A|Y) - H(X_A|Y,S_A) \\
&= H(X_A|Y) + H(S_A|X_A,Y) - H(X_A|Y,S_A) \\
&= H(X_A|Y) - H(X_A|Y,S_A) \\
&\le H(X_A|Y) \\
&= H(X_A|Y) - H(X_A) + H(X_A) + \delta_A - \delta_A \\
&= H(X_A|X_B) - H(X_A|Y_B,X_B) - I(X_A;Y) + \delta_A \\
&= I(X_A;Y_B|X_B) - I(X_A;Y) + \delta_A
\end{aligned} \tag{15}$$

and the proposition follows. ∎

Intuitively, the difference $I(X_A;Y_B|X_B) - I(X_A;Y)$ measures Ray's equivocation with respect to X_A. On the other hand, the term δ_A measures Bob's failure to decode Alice's secret messages. By Fano's inequality δ_A can be made small when error correction is employed, while in the noiseless scenario $\delta_A = \delta_B = 0$.

III. Upper Bounds in the Noiseless Scenario

Throughout this section and the next we assume that

(i) the random variables X_A and X_B are uniform, and
(ii) all channels are fixed and invertible.

When channel state information is globally available, we assume that Alice and Bob employ channel precoders, denoted respectively by g_A and g_B, such that

$$h_A g_A = h_B g_B \tag{16}$$

so that Ray observes

$$y = h_A g_A x_A + h_B g_B x_B + w_R = h_A g_A (x_A + x_B) + w_R. \tag{17}$$

Ray now attempts to recover the sum $x_A + x_B$. The secrecy of our proposed encoders depends only on the structure of the sum $x_A + x_B$, so we set $\sigma_R^2 = 0$ in the next two sections. In this noiseless environment, Ray can post-multiply the received signal in (17) by $(h_A g_A)^{-1}$ to recover $x_A + x_B$ exactly. Similarly, the Ray-Alice and Ray-Bob channels are assumed noiseless. We summarize by adding a third assumption:

(iii) All channel gains are equal to unity and all noise sources are zero, that is, $h_A = h_B = \tilde{h}_A = \tilde{h}_B = 1$ and $\sigma_A^2 = \sigma_B^2 = \sigma_R^2 = 0$.

While (iii) may seem unrealistic, we are rather interested in the achievable perfect secrecy rates based solely on the structure of the sum $x_A + x_B$ itself. Thus while the presence of noise and fading can have a deteriorating effect on Alice and Bob's secrecy rates, removing assumption (iii) will not affect perfect secrecy relative to Ray. More precisely, provided that (16) is satisfied, our encoding schemes will guarantee that the secrecy conditions (11) and (12) are satisfied regardless of the value of σ_R^2. Hence assumption (iii) streamlines exposition and emphasizes the fact that we are not relying on a degraded channel to provide secrecy.

Finally, we note that although channel inversion is impractical in Rayleigh environments, it can be employed whenever a line of sight (LOS) exists between either transmitter and Ray, i.e., whenever a Rician, a Nakagami-m or other large scale fading channel model [36] is applicable. We will return to the question of designing optimal precoders g_A and g_B in the presence of noise in Section V.

A. An Upper Bound on the Achievable Perfect Secrecy Rates

In the noiseless setting with unit channel gains, the set of all possible observations at Ray is

$$\mathcal{Y} = \mathcal{X}_R = \{x_A + x_B \mid x_A \in \mathcal{X}_A,\ x_B \in \mathcal{X}_B\} \tag{18}$$

which comes with an addition function

$$\psi : \mathcal{X}_A \times \mathcal{X}_B \to \mathcal{Y}, \quad \psi(x_A,x_B) = x_A + x_B. \tag{19}$$

Crucial to our analysis are the sets

$$\psi^{-1}(y) = \{(x_A,x_B) \mid y = x_A + x_B\}. \tag{20}$$

The pmf of Y is given by the convolution of the pmfs of X_A and X_B, which is clearly seen to be

$$p_Y(y) = \sum_{\substack{x_A,x_B \\ x_A+x_B=y}} p_{X_A}(x_A)p_{X_B}(x_B) = \frac{|\psi^{-1}(y)|}{M_A M_B}. \tag{21}$$

The following proposition gives a compact, intuitive upper bound on the achievable secrecy rates $\widehat{R}_A^s$ and $\widehat{R}_B^s$.

Proposition 2: In the noiseless scenario $\widehat{R}_A^s$ and $\widehat{R}_B^s$ are equal. Furthermore, denoting $\widehat{R}^s = \widehat{R}_A^s = \widehat{R}_B^s$, we have

$$\widehat{R}^s = \frac{1}{M_A M_B} \sum_{y\in\mathcal{Y}} |\psi^{-1}(y)| \log_2 |\psi^{-1}(y)| \tag{22}$$

Proof: See Appendix A. ∎

In the noiseless scenario we therefore simply define $\widehat{R}^s$ to be *the* perfect secrecy rate UB. Intuitively, for a given $y \in \mathcal{Y}$, $\log_2|\psi^{-1}(y)|$ measures equivocation at Ray in bits, and therefore controls the total number of secret bits that Alice and Bob can transmit when Ray observes y. However, Alice and Bob do not necessarily a priori know the value of y. We will return to this point in Section IV.

B. An Upper Bound on the Achievable Perfect Secrecy Rates for PAM Modems

Let us now study a familiar scenario in which $\mathcal{X}_A$ and $\mathcal{X}_B$ are, respectively, M_A- and M_B-PAM constellations, so that X_A is the uniform distribution on

$$\mathcal{X}_A = \{-(M_A-1), -(M_A-3), \ldots, M_A-3, M_A-1\} \tag{23}$$

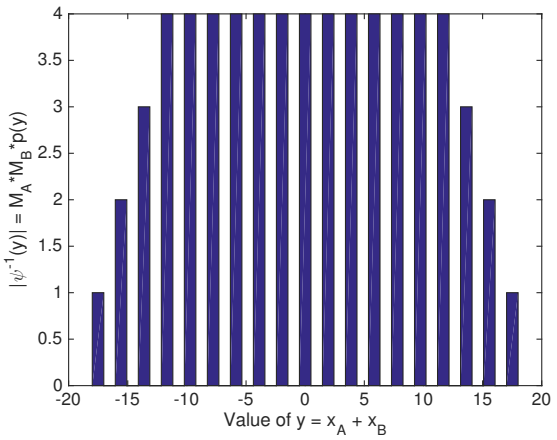

Fig. 3. The pmf of Ray's observation $y = x_A + x_B$ in the noiseless scenario with channel gains $h_A = h_B = 1$. Here Alice employs a 4-PAM modulator and Bob a 16-PAM modulator.

and similarly for X_B. Throughout this section we assume that $M_B \geq M_A$.

Proposition 3: In the noiseless setting with unit channel gains when Alice and Bob employ M_A-PAM and M_B-PAM modulators with $M_B \geq M_A$, we have

$$|\psi^{-1}(y)| = \begin{cases} 0 & y \text{ odd or } |y| \geq M_B + M_A, \\ \frac{M_B + M_A - |y|}{2} & M_B - M_A + 2 \leq |y| \leq M_B + M_A - 2, \\ M_A & |y| \leq M_B - M_A. \end{cases}$$

Proof: This is a straightforward calculation and is therefore omitted. ∎

The above proposition in conjunction with (21) allows us to explicitly describe Ray's pmf $p_Y(y)$. In Fig. 3 we plot the values of $|\psi^{-1}(y)|$ for $M_A = 4$ and $M_B = 16$.

Theorem 1: In the noiseless setting with unit channel gains when Alice and Bob employ M_A-PAM and M_B-PAM modulators with $M_B \geq M_A$, we have

$$\widehat{R}^s = m_A \frac{M_B - M_A + 1}{M_B} + \frac{2}{M_A M_B} \sum_{a=1}^{M_A - 1} a \log_2(a). \quad (24)$$

In particular, for fixed M_A we have $\lim_{M_B \to \infty} \widehat{R}^s = m_A$.

Proof: See Appendix B. ∎

While Theorem 1 provides an explicit upper bound on R_A^s and R_B^s when Alice and Bob employ PAM modems, the following proposition shows that given the current encoder description, the user with the smaller constellation can transmit no secret bits.

Proposition 4: Suppose that Alice and Bob employ PAM modems with $M_B \geq M_A$. Then $R_A^s = 0$. In particular, if $M_A = M_B$ then $R_A^s = R_B^s = 0$.

Proof: Let us pick some $x_A \in \mathcal{X}_A$ with $s_A = b_A(x_A)$ and $s_A \neq \varepsilon$. That is, we pick some constellation point x_A which encodes a genuine secret message. Now set $x_B = -x_A$, and $x'_B = M_B - M_A + 2 - x_A$ if $x_A > 0$ and $x'_B = -(M_B - M_A + 2) - x_A$ if $x_A < 0$. One can check easily that the assumption $M_B \geq M_A$ guarantees that x_B and x'_B are well-defined points in $\mathcal{X}_B$. Let $y = x_A + x_B = 0$ and $y' = x_A + x'_B$. Using Proposition 3, one sees easily that

$$|\psi^{-1}(y)| = M_A \quad \text{and} \quad |\psi^{-1}(y')| = M_A - 1. \quad (25)$$

The perfect secrecy condition $I(S_A; Y) = 0$ implies that $p(s_A|y) = p(s_A) = p(s_A|y')$. From the above two equations, it is clear that we can write

$$p(s_A|y) = \frac{k}{M_A}, \quad p(s_A|y') = \frac{k'}{M_A - 1} \quad (26)$$

for some positive integers k, k', neither of which is zero. From $p(s_A|y) = p(s_A|y')$ we arrive at $\frac{k}{M_A} = \frac{k'}{M_A - 1}$, or equivalently $(k - k')M_A = k$. This implies that M_A divides k, which is only possible if $M_A = k$ and hence $p(s_A) = p(s_A|y) = 1$. The proposition follows. ∎

While the above proposition shows that it is impossible for Alice to transmit secret bits, the same is not true of Bob, as there exist points $x_B \in \mathcal{X}_B$ for which $|\psi^{-1}(x_A + x_B)| = M_A$ for all $x_A \in \mathcal{X}_A$. Thus the above result is specific to the smaller of the two constellations.

C. Effect of Time Synchronization Errors on the Upper Bounds

One of the main issues in PNC networks is that the assumption of perfect time synchronization is too optimistic. In this subsection we investigate the effect of time synchronization on $\widehat{R}_A^s$ and $\widehat{R}_B^s$ when Alice and Bob employ M-PAM modulators. In this case the analog signals transmitted by Alice and Bob, denoted by $t_A(t)$, and $t_B(t)$ respectively, can be expressed as:

$$t_A(t) = \sum_{l=-\infty}^{\infty} x_A(l) \cos(2\pi f t) g(t - lT - \delta T_A), \quad (27)$$

$$t_B(t) = \sum_{l=-\infty}^{\infty} x_B(l) \cos(2\pi f t) g(t - lT - \delta T_B), \quad (28)$$

where T is the symbol period, δT_A and δT_B denote the synchronization errors at Alice and Bob respectively and are assumed to be uniformly distributed in the range $[0, T]$ and $g(t)$ denotes the transmitter filter (commonly implemented as a raised cosine filter). Here for simplicity we assume that the transmitter filter is a simple rectangular window of length equal to the symbol period T. Neglecting all other noise sources and assuming that Ray employs a matched filter receiver implemented as a standard correlator receiver, Ray's observation $y(l)$ during the l-th symbol can be expressed as

$$\begin{aligned} y(l) &= \frac{2}{T} \int_{-\delta T_A}^{0} x_A(l-1) \cos^2(2\pi f t) dt \\ &+ \frac{2}{T} \int_{0}^{T - \delta T_A} x_A(l) \cos^2(2\pi f t) dt \\ &+ \frac{2}{T} \int_{-\delta T_B}^{0} x_B(l-1) \cos^2(2\pi f t) dt \\ &+ \frac{2}{T} \int_{0}^{T - \delta T_B} x_B(l) \cos^2(2\pi f t) dt \\ &= (1-\alpha) x_A(l) + (1-\beta) x_B(l) + \alpha x_A(l-1) \\ &+ \beta x_B(l-1), \end{aligned} \quad (29)$$

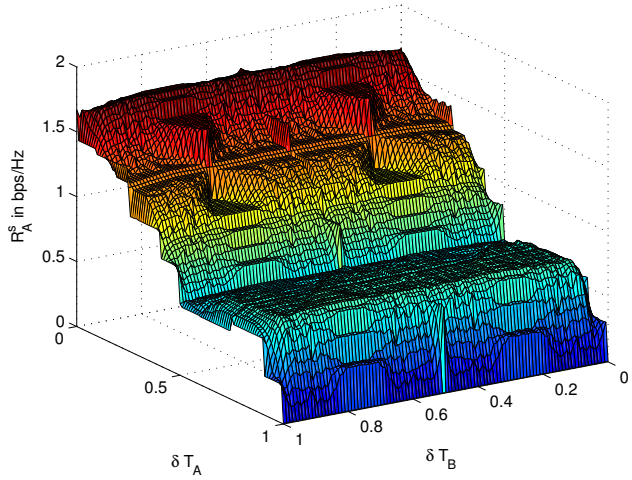

Fig. 4. Numerical evaluation of $\widehat{R}_A^s$ in the presence of time synchronization errors denoted by δT_A and δT_B. The symbol period is normalized to unity $T = 1$, and we set $M_A = 4$ and $M_B = 8$. In the evaluation of $\widehat{R}_A^s$ we assume that all the history in X_B is available.

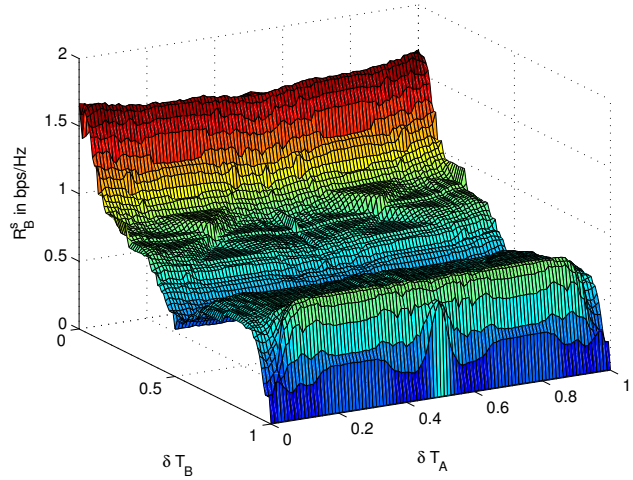

Fig. 5. Numerical evaluation of $\widehat{R}_B^s$ in the presence of time synchronization errors denoted by δT_A and δT_B. The symbol period is normalized to unity $T = 1$, and we set $M_A = 4$ and $M_B = 8$. In the evaluation of $\widehat{R}_B^s$ we assume that all the history in X_A is available.

where

$$\alpha = \frac{\sin\left(4\pi\frac{\delta T_A}{T}\right)}{4\pi} + \frac{\delta T_A}{T}, \tag{30}$$

$$\beta = \frac{\sin\left(4\pi\frac{\delta T_B}{T}\right)}{4\pi} + \frac{\delta T_B}{T}. \tag{31}$$

As a result of time synchronization errors, Alice's and Bob's symbols are misaligned when reaching Ray. We note that in this case the symmetry between $\widehat{R}_A^s$ and $\widehat{R}_B^s$ is lost due to the existence of interference that also depends on the history of the transmitted codewords (both the current l-th codeword and the previous $(l-1)$-th codeword as indicated in (29)). We investigate the effect of this misalignment by numerically evaluating $\widehat{R}_A^s$ when all the history on X_B is available and $\widehat{R}_B^s$ when all the history on X_A is available. The results are depicted in Figs. 4 and 5, respectively, when $M_A = 4$ and $M_B = 8$, averaged over $10,000$ runs. It is evident that the impact of similar synchronization errors on the smallest constellation is more acute. For relatively small synchronization errors the effect on $\widehat{R}_A^s$ is negligible; on the contrary $\widehat{R}_B^s$ is more sensitive to this effect and sharply decreases. On the other hand, as the synchronization errors increase their impact becomes increasingly important. Interestingly, due to the sinusoidal parts of α and β, there are four regions of values of $(\delta T_A, \delta T_B)$ – around the points $\left(\frac{1}{4},\frac{1}{4}\right), \left(\frac{1}{2},\frac{1}{2}\right), \left(\frac{3}{4},\frac{3}{4}\right)$ and $(1,1)$ – in which the decrease in $\widehat{R}_A^s$ and $\widehat{R}_B^s$ is more acute.

IV. Explicit Encoder Construction with PAM Modems in the Noiseless Scenario

Throughout this section we assume that Alice and Bob use PAM modems of sizes M_A and M_B, with $M_B \geq M_A$. We retain the assumptions of the previous section that all channels are noiseless and all channel gains are set to unity.

We assume in the first subsection that neither Alice nor Bob has any information about the other's symbol prior to transmission; that is, that the labeling function $b_B : \mathcal{X}_B \to \mathcal{S}_B \cup \{\varepsilon\}$ as defined in (5) (and hence, Bob's encoding function) is independent of the symbol transmitted by Alice. By Proposition 4, the same condition at Alice implies that $R_A^s = 0$, and furthermore that $R_B^s = 0$ if $M_B = M_A$. Hence we assume in Section IV-A that $M_B > M_A$ and only construct an explicit secret bit encoder at Bob in this case. We then compute the corresponding perfect secrecy rate and compare the result to the upper bound of the previous section.

In the second subsection we study Alice's achievable secrecy rate when she has knowledge of x_B prior to the transmission of this symbol by Bob. This requires a slight generalization of the system model to one where Alice's labeling function b_A can depend on both x_A and x_B. While the assumption that Alice knows Bob's signal may be unrealistic in some scenarios, one can think that in this case Bob plays the role of a helping interferer whose signal is known to Alice.

A. Explicit Encoder Construction at Bob

Under the assumption $M_B \geq M_A$, Proposition 4 guarantees that $R_A^s = 0$, and hence if $M_B = M_A$ we have by symmetry that $R_B^s = 0$ as well. Thus we make the slightly stronger assumption that $M_B > M_A$ in this subsection.

To construct our encoding function at Bob, we first define his set of secret source symbols to be $\mathcal{S}_B = \{0,1\}^{m_A}$ and S_B to be uniform on this set. We define a subset $\mathcal{X}_B^s$ of $\mathcal{X}_B$ on which Bob will transmit secret bits, by setting

$$\mathcal{X}_B^s = \{x_B \in \mathcal{X}_B \mid |x_B| \leq M_B - 2M_A - 1\}. \tag{32}$$

It follows from Proposition 3 that for all $x_B \in \mathcal{X}_B^s$ we have

$$|\psi^{-1}(x_A + x_B)| = M_A \text{ for all } x_A \in \mathcal{X}_A. \tag{33}$$

A simple computation shows that $|\mathcal{X}_B^s| = M_B - 2M_A$. Note that since M_A and M_B are powers of two, the assumption

$M_B > M_A$ is equivalent to $M_B \geq 2M_A$. Thus $\mathcal{X}_B^s$ is well-defined provided that $M_B > M_A$, but is empty in the extreme case $M_B = 2M_A$.

The set $\mathcal{X}_B^s$ is maximal in the sense that $\mathcal{X}_B^s$ is the largest subset of $\mathcal{X}_B$ on which Ray is guaranteed to experience the maximum number of bits of equivocation, namely m_A, and whose cardinality is divisible by M_A. This latter condition is necessary to maintain the assumed uniformity of the binary input distribution of secret bits.

Our bit labeling procedure for $\mathcal{X}_B$ can be described pictorially by a perfect binary tree as in Fig. 6. Each point in $\mathcal{X}_B$ is assigned in increasing order to a leaf in the perfect binary tree with M_B leaves. The edges at each level of the tree are alternately labeled with a 0 or a 1. A point x_B is then given a bit labeling $l(x_B)$ by tracing the tree downwards from the root node to the corresponding leaf, so that the bit closest to the root node is the left-most bit in the string. For the example in Fig. 6 with $M_B = 16$, we have the bit labelings $l(-5) = 0101$, $l(+7) = 1011$, etc.

We now declare the last m_A bits of all $x_B \in \mathcal{X}_B^s$ to be secret, and all other bits to be public. Thus Bob's labeling function $b_B : \mathcal{X}_B \to \mathcal{S}_B \cup \{\varepsilon\}$ is defined by

$$b_B(x_B) = \begin{cases} \text{the last } m_A \text{ bits of } l(x_B) & x_B \in \mathcal{X}_B^s \\ \varepsilon & x_B \notin \mathcal{X}_B^s \end{cases} \tag{34}$$

To transmit some $s_B \in \mathcal{S}_B \cup \{\varepsilon\}$, recall that Bob chooses uniformly from among the set $b_B^{-1}(s_B)$. Thus Bob transmits s_B with frequency $\frac{1}{M_A}\frac{|\mathcal{X}_B^s|}{|\mathcal{X}_B|}$ if $s_B \in \mathcal{S}_B$, and with frequency $1 - \frac{|\mathcal{X}_B^s|}{|\mathcal{X}_B|}$ if $s_B = \varepsilon$. It follows that each element of $\mathcal{X}_B$ is sent with frequency $\frac{1}{M_B}$, so that X_B is uniform as desired. Alice simply samples $\mathcal{X}_A$ uniformly at random.

Theorem 2: Suppose that $M_B > M_A$. Perfect secrecy is preserved given the above encoder, that is, $I(S_B; Y) = 0$. Furthermore, the secrecy rate at Bob obtained using the present strategy is given by

$$R_B^s = m_A \frac{M_B - 2M_A}{M_B} \tag{35}$$

In particular, for fixed M_A we have $\lim_{M_B \to \infty} R_B^s = m_A$.

Proof: To prove that $I(S_B; Y) = 0$, we must prove that $p(s_B|y) = p(s_B)$ whenever $p(s_B, y) > 0$. Suppose $s_B \in \mathcal{S}_B$ and that Ray observes some y such that $p(s_B, y) > 0$. Then we have that $|\psi^{-1}(y)| = M_A$ by the construction of b_B. Given that Ray observed y, define

$$\mathcal{X}_B(y) = \{x_B \mid x_A + x_B = y \text{ for some } x_A \in \mathcal{X}_A\} \tag{36}$$

to be the set of all x_B Bob could have transmitted.

First observe that $\mathcal{X}_B(y)$ necessarily consists of M_A consecutive points in $\mathcal{X}_B$. But by the construction of b_B, in any set of M_A consecutive points in $\mathcal{X}_B$ there exists at most one x_B such that $b_B(x_B) = s_B$. If $p(s_B, y) > 0$ then there exists exactly one such x_B, proving that $p(s_B|y) = \frac{1}{M_A} = p(s_B)$. Thus perfect secrecy is preserved.

As Bob transmits m_A secret bits uniformly at random whenever $x_B \in \mathcal{X}_B^s$ and no secret bits otherwise, his secrecy rate is given by

$$R_B^s = m_A \frac{|\mathcal{X}_B^s|}{|\mathcal{X}_B|} \tag{37}$$

which is easily seen to be equal to the stated quantity. ■

Note that for $s_B \in \mathcal{S}_B$ we used the fact that $p(s_B) = \frac{1}{M_A}$ in the theorem, while Bob actually transmits this bit string with the smaller frequency $\frac{1}{M_A}\frac{|\mathcal{X}_B^s|}{|\mathcal{X}_B|}$. This apparent discrepancy is due to the fact that for the purposes of measuring secrecy with respect to Ray, we are not concerned with the resulting distribution on $\mathcal{S}_B \cup \{\varepsilon\}$ since secrecy is not relevant when Bob transmits the empty secret string ε. Put another way, Ray can possibly obtain non-trivial information about whether or not $s_B \in \mathcal{S}_B$, but provided that $s_B \in \mathcal{S}_B$ the above encoder guarantees perfect secrecy.

To encode queues of public and secret bits, Bob begins at the root node of the tree and travels downwards, encoding public bits until he hits a node all of whose descending edges correspond to secret bits. He then switches to his queue of secret bits and begins encoding those, until the constellation point to be sent is completely determined.

Example 1: Let us set $M_A = 4$ and $M_B = 16$, and suppose that Bob wishes to transmit the public and secret (respectively) bit queues

$$\mathcal{Q}_B^p = 10110101, \quad \mathcal{Q}_B^s = 1111 \tag{38}$$

He begins by encoding the left-most bits in $\mathcal{Q}_B^p$, namely 10, at which point the first two bits in $\mathcal{Q}_B^s$ (namely 11) determine the final decision in the tree. The first constellation point to be sent is therefore $x_B = +7$, corresponding to the bit string 1011. He continues in this way, finally determining the symbols for transmission to be

$$\begin{aligned} 1011 &\to +7 \quad = x_B(1) \\ 1101 &\to +11 \quad = x_B(2) \\ 0111 &\to -1 \quad = x_B(3) \end{aligned} \tag{39}$$

where $x_B(i)$ is sent during the i^{th} time instance. ■

Let us study the effectiveness of this scheme by comparing R_B^s to the upper bound $\widehat{R}^s$. We define

$$\Delta_B = |\widehat{R}^s - R_B^s|, \quad \epsilon_B = \Delta_B / \widehat{R}_B^s \tag{40}$$

to measure the absolute and relative failure of R_B^s to obtain the upper bound. In Fig. 7 we measure Δ_B for various values of $M_B \geq 4M_A$, and do the same for ϵ_B in Fig. 8. As one can see from the plots, we have $\Delta_B \to 0$ and $\epsilon_B \to 0$ as $M_B \to \infty$ and M_A stays fixed. Indeed, this is easily provable using the explicit expressions for R_B^s and $\widehat{R}^s$. We see from Fig. 7 that when $M_B = 4M_A$, for example, the gap Δ_B increases with M_B, but that the relative gap ϵ_B is approximately constant with increasing M_B and $M_A = M_B/4$.

B. Explicit Encoder Construction at Alice with Side Information

In this subsection we generalize our system model slightly to allow Alice to have prior knowledge of the symbol x_B transmitted by Bob. While this may not be realistic in some practical scenarios, we have seen by Proposition 4 that given no knowledge of Bob's symbol, Alice's perfect secrecy rate is zero when both employ PAM modems with $M_B \geq M_A$.

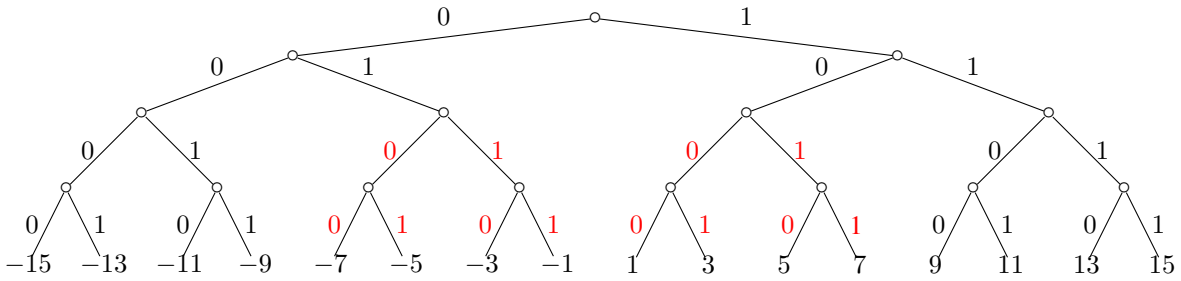

Fig. 6. Secret bit encoder at Bob for $M_A = 4$ and $M_B = 16$, where secret bits are denoted in red and public bits in black. Bob transmits m_A secret bits on the subset $\mathcal{X}_B^s = \{-7, \ldots, +7\}$ of $\mathcal{X}_B$.

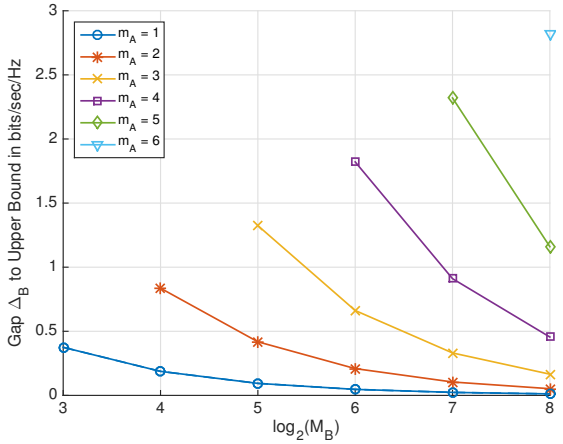

Fig. 7. The gap $\Delta_B = |\widehat{R}^s - R_B^s|$ between Bob's secrecy rate given the encoding scheme of Section IV-A and the upper bound $\widehat{R}^s$, as a function of M_B for various values of $M_B \geq 4M_A$.

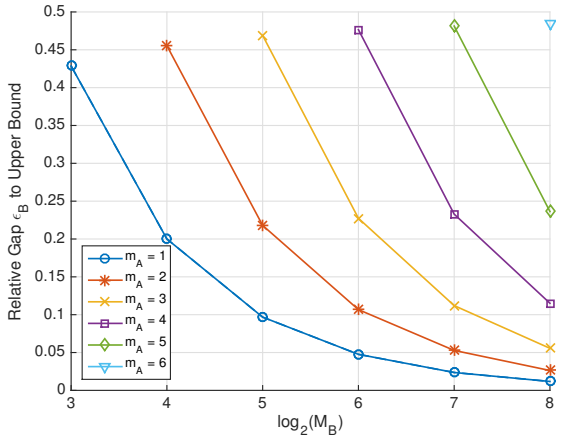

Fig. 8. The relative gap $\epsilon_B = |\widehat{R}^s - R_B^s|/\widehat{R}^s$ between Bob's secrecy rate given the encoding scheme of Section IV-A and the upper bound $\widehat{R}^s$, as a function of M_B for various values of $M_B \geq 4M_A$.

In what follows we let $\mathcal{S}_A = \{0,1\}^{m_A}$ and S_A be the uniform random variable on this set. We define Alice's bit labeling by a function

$$b_A : \mathcal{X}_A \times \mathcal{X}_B \to \mathcal{S}_A \cup \{\varepsilon\} \tag{41}$$

where $\mathcal{X}_A$ and $\mathcal{X}_B$ are M_A-PAM and M_B-PAM constellations, respectively. Here the value $s_A = b_A(x_A, x_B)$ should be interpreted as the secret symbol encoded in x_A, provided that Bob transmits x_B.

x_A \ x_B	-7	-5	-3	-1	$+1$	$+3$	$+5$	$+7$
$+3$	00	00	00	00	00	ε	ε	ε
$+1$	ε	01	01	01	01	01	ε	ε
-1	ε	ε	11	11	11	11	11	ε
-3	ε	ε	ε	10	10	10	10	10

Fig. 9. The bit labeling $b_A : \mathcal{X}_A \times \mathcal{X}_B \to \{0,1\}^{m_A} \cup \{\varepsilon\}$ for $M_A = 4$ and $M_B = 8$. Secret bits are depicted in red, and are transmitted exactly when $|\psi^{-1}(x_A + x_B)| = M_A$.

The encoder is similar to the one proposed in the previous subsection. Alice labels each of her points x_A with a unique bit string $l(x_A) \in \{0,1\}^{m_A}$ of length m_A. Given a symbol x_B to be transmitted by Bob, we define b_A by

$$b_A(x_A, x_B) = \begin{cases} l(x_A) & \text{if } |\psi^{-1}(x_A + x_B)| = M_A \\ \varepsilon & \text{otherwise} \end{cases} \tag{42}$$

In other words, for a given x_B all of the bits encoded in x_A are secret provided that $|\psi^{-1}(x_A + x_B)| = M_A$; otherwise Alice transmits no secret bits. We depict the labeling b_A in the case of $M_A = 4$ and $M_B = 8$ in Fig. 9.

Given some secret message s_A to be transmitted and prior information about the codeword x_B to be transmitted by Bob, Alice picks the unique x_A such that $l(x_A) = s_A$. If $|\psi^{-1}(x_A + x_B)| = M_A$, then she transmits x_A and therefore sends the secret message s_A to Bob. If $|\psi^{-1}(x_A + x_B)| < M_A$, she then picks some $x'_A \neq x_A$ uniformly at random and transmits this x'_A, sending the empty string ε to Bob. It follows from the uniformity of S_A and X_B that X_A is uniform as well.

Theorem 3: Suppose that $M_B \geq M_A$. Perfect secrecy is preserved given the above encoder, that is, $I(S_A; Y) = 0$. Furthermore, the secrecy rate at Alice obtained using the present strategy is given by

$$R_A^s = m_A \frac{M_B - M_A + 1}{M_B}. \tag{43}$$

In particular, for fixed M_A we have $\lim_{M_B \to \infty} R_A^s = m_A$.

Proof: For $y \in \mathcal{Y}$ we set

$$\mathcal{X}_A(y) = \{x_A \mid x_A + x_B = y \text{ for some } x_B \in \mathcal{X}_B\}. \tag{44}$$

Given some $s_A \in \mathcal{S}_A$ such that $p(s_A, y) > 0$, then $|\psi^{-1}(y)| = M_A$ as Alice only transmits secret bits if she knows Ray will

experience the maximal amount of entropy. Thus $\mathcal{X}_A(y) = \mathcal{X}_A$ whenever Alice transmits secret bits. Since every $x_A \in \mathcal{X}_A$ is assigned a unique bit string, it follows easily that $p(s_A|y) = \frac{1}{M_A} = p(s_A)$ and hence we have perfect secrecy.

To calculate the rate, we need to calculate the number of pairs (x_A, x_B) for which $|\psi^{-1}(x_A + x_B)| = M_A$. For a fixed x_A, one can compute easily using Proposition 3 that this number is $M_B - M_A + 1$, thus the total number of such pairs is $M_A M_B - M_A^2 + M_A$. The total number of all pairs (x_A, x_B) is of course $M_A M_B$, from which we calculate the secrecy rate to be

$$R_A^s = m_A \frac{M_A M_B - M_A^2 + M_A}{M_A M_B} \tag{45}$$

which is equal to the quantity stated in the theorem. ■

As before, note that Ray will know whether or not Alice transmitted secret bits, based on the value of $|\psi^{-1}(y)|$ which is, of course, available to Ray. But provided that Alice transmits secret bits, Ray will have no information about the specific transmitted bit string.

Example 2: Suppose that we set $M_A = 4$ and $M_B = 8$, and use the encoder depicted in Fig. 9. Let us suppose that Alice wishes to transmit the queue

$$\mathcal{Q}_A^s = 1011 \tag{46}$$

of secret bits, and that she knows in advance that $x_B(1) = +7$, $x_B(2) = -5$, and $x_B(3) = +5$. She begins at the two left-most bits in the queue, namely the secret message 10. Noting that $l(-3) = 10$ and that $|\psi^{-1}(-3+7)| = M_A$, she sends the symbol $x_A(1) = -3$, which encodes 10.

Now consider the second two bits in Alice's queue, namely 11. Since $l(-1) = 11$ she must transmit the point $x_A = -1$ to send this secret bit string. But since $x_B(2) = -5$ and $|\psi^{-1}(-1-5)| < M_A$, she instead selects $x_A(2)$ uniformly at random from the other elements of $\mathcal{X}_A$ during this time instance, and waits to transmit 11.

During the third time instance, Alice sees that $x_B(3) = +5$ and that $|\psi^{-1}(-1+5)| = M_A$, so she sends $x_A(3) = -1$ which for the given value of x_B encodes the final two secret bits 11 in her queue. ■

To study the effectiveness of our encoding scheme, we as before set

$$\Delta_A = |\widehat{R}^s - R_A^s| = \frac{2}{M_A M_B} \sum_{a=1}^{M_A - 1} a \log_2(a) \tag{47}$$

and $\epsilon_A = \Delta_A / \widehat{R}^s$ to measure the absolute and relative failure of R_A^s to achieve the upper bound. We plot Δ_A in Fig. 10 and ϵ_A in Fig. 11, as a function of M_B for various values of M_A. As with the previous encoding scheme, both Δ_A and ϵ_A approach 0 for fixed M_A and increasing M_B.

V. Generalization to the MIMO Relay Channel

This section removes the noiseless assumption and simultaneously generalizes to a MIMO channel in which Alice and Bob each have N antennas and Ray has $M \geq N$ antennas. We assume that Alice and Bob employ one of the encoders discussed in Section IV. Having fixed a secrecy encoder, it

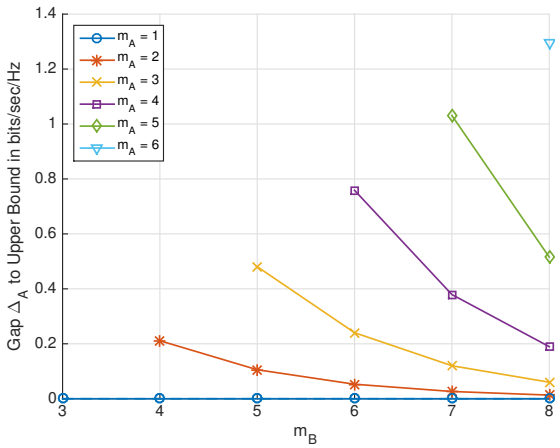

Fig. 10. The gap $\Delta_A = |\widehat{R}^s - R_A^s|$ between Alice's secrecy rate given the encoding scheme of Section IV-B and the upper bound $\widehat{R}^s$, as a function of M_B for various values of $M_B \geq 4M_A$.

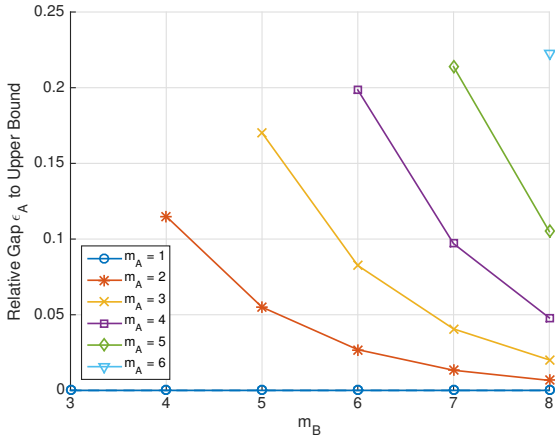

Fig. 11. The relative gap $\epsilon_A = |\widehat{R}^s - R_A^s| / \widehat{R}^s$ between Alice's secrecy rate given the encoding scheme of Section IV-B and the upper bound $\widehat{R}^s$, as a function of M_B for various values of $M_B \geq 4M_A$.

is crucial to the success of Alice and Bob's transmission that Ray decode the sum $x_A + x_B$ of their symbols correctly, a point we now address by studying optimal precoding matrices at Alice and Bob.

Let us denote the channel matrices Alice to Ray and Bob to Ray by H_A, $H_B \in \mathbf{C}^{M \times N}$, respectively, and the channel matrices from Ray to Alice and Ray to Bob, respectively, by $\tilde{H}_A$ and $\tilde{H}_B \in \mathbf{C}^{N \times M}$. We assume all matrices are selected from a continuous distribution and are therefore full-rank with probability 1.

Let $d \leq N$ and suppose Alice and Bob wish to transmit realizations of length d random vectors X_A and X_B of codewords. They employ linear precoders G_A, $G_B \in \mathbf{C}^{N \times d}$, so that Ray observes

$$Y = H_A G_A X_A + H_B G_B X_B + W_R \tag{48}$$

where W_R is a length M vector of additive noise, with entries i.i.d. zero-mean circularly symmetric complex Gaussian and variance σ_R^2 per complex dimension. To guarantee that Ray only observes sums of information symbols, Alice and Bob

then must construct G_A and G_B to satisfy

$$H_A G_A = H_B G_B \tag{49}$$

so that given a realization of (48) Ray observes

$$y = H_A G_A (x_A + x_B) + w_R \tag{50}$$

from which he attempts to decode the sum $x_A + x_B$. Hence condition (49) is crucial to employing the secrecy encoders of the previous section.

We further impose power constraints on Alice and Bob by first defining their average per-symbol power by

$$P_A = \mathbf{E}|x_{A,i}|^2, \quad P_B = \mathbf{E}|x_{B,i}|^2 \tag{51}$$

where $x_A = (x_{A,1}, \ldots, x_{A,d})^T$ and $x_{A,i} \in \mathcal{X}_A$, and similarly for $x_{B,i}$. To maintain this constraint after precoding we impose the conditions

$$||G_A||_F^2 \leq N, \quad ||G_B||_F^2 \leq N. \tag{52}$$

Here we recall that $||A||_F^2$ denotes the squared Frobenius norm of a matrix A, defined by $\sum_i \sigma_i^2$, where σ_i are the singular values of A. Note that assuming (49) and (51), and after appropriate scaling of the channel matrices H_A and H_B, we have that the average power of the received signal at Ray is $P_R = P_A + P_B$.

A. Degrees of Freedom

It is well-known and not hard to show (see [32], [37], [38]) that the *degrees of freedom* d of interference-free transmit dimensions available to both Alice and Bob is bounded by $d \leq (2N - M)^+$, and that every d satisfying this inequality admits an interference-free transmission scheme. Let us recall briefly how such schemes are constructed. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be the column spans of H_A and H_B, respectively, so that $\dim \mathcal{H}_A \cap \mathcal{H}_B = (2N - M)^+$. If $d \leq (2N - M)^+$ then Alice and Bob decide on a d-dimensional subspace $\mathcal{S}$ of this intersection, and then choose $N \times d$ precoding matrices G_A, G_B such that $\operatorname{colspan} H_A G_A = \operatorname{colspan} H_B G_B = \mathcal{S}$. In a similar manner, $d \leq (2N - M)^+$ guarantees that Ray can transmit his PNC codewords back to Alice and Bob without the loss of any signal dimensions.

To ensure successful encoding and decoding which maximizes the degrees of freedom, we therefore restrict to d, M, and N satisfying $1 \leq d = 2N - M$ from now on.

B. The Dimension of the Space of Precoders

In this subsection we compute the dimension of the space of all G_A and G_B satisfying the secrecy constraint (49) and the power constraint (52). The dimension of this space measures the number of independent parameters when choosing precoding matrices, and determines the difficulty of optimizing the precoders numerically. To be mathematically precise, 'dimension' here means 'dimension as a real manifold', but we omit the mathematical technicalities in favor of exposition.

If G_A and G_B are any precoders such that $||G_A||_F^2 < N$ and $||G_B||_F^2 < N$, then we can always improve the performance of the system by multiplying both precoders by a constant so that either $||G_A||_F^2 = N$ or $||G_B||_F^2 = N$. So from now on we assume that one of the inequalities in (52) is an equality. On the other hand, the probability that both inequalities are actually equalities, e.g. that both precoders can be chosen to maximize both Alice and Bob's transmit power and satisfy (49), is zero.

Proposition 5: Fix N and M such that $M/2 < N \leq M$, let $d = 2N - M$, and let $H_A, H_B \in \mathbf{C}^{M \times N}$ be generic full-rank matrices. Consider the matrix equation $H_A G_A = H_B G_B$ for some variable matrices $G_A, G_B \in \mathbf{C}^{N \times d}$ such that $||G_A||_F^2 \leq N$ or $||G_B||_F^2 \leq N$, and that exactly one of these inequalities is an equality. Then

$$\dim_{\mathbf{R}} \mathcal{P} = 2(d^2 - 1). \tag{53}$$

where $\dim_{\mathbf{R}}$ denotes dimension as a real manifold and $\mathcal{P}$ is the space of all such G_A, G_B satisfying the above conditions.

Proof: As a real Euclidean space, the dimension of the space of all pairs $G_A, G_B \in \mathbf{C}^{N \times d}$ is $4Nd$. Accounting for both real and imaginary parts, the equation $H_A G_A - H_B G_B = 0$ defines $2Md$ linear equations in the entries of G_A, G_B, all of which are independent by the assumptions that H_A and H_B are generic and full-rank. Furthermore, suppose without loss of generality that $||G_A||_F^2 = N$. This single additional quadratic equation further reduces the dimension of the total space by two. Putting this all together gives us $\dim_{\mathbf{R}} \mathcal{P} = 4Nd - 2Md - 2 = 2(d^2 - 1)$ as claimed. ∎

Thus when the degrees of freedom of the system is maximized, we have $\dim \mathcal{P} = 2(d^2 - 1)$ dimensions to optimize over when constructing optimal precoders. When $(M, N) = (3, 2)$ or $(5, 3)$, for example, the dimension of $\mathcal{P}$ is zero and thus $\mathcal{P}$ consists of only isolated points, meaning that additional steepest descent optimization cannot improve system performance.

C. Optimizing Precoders at Alice and Bob

While the previous section addressed the difficulty of optimizing precoders, in this subsection we address exactly what objective functions should be optimized. Successful transmission between Alice and Bob requires Ray to accurately detect the sum $x_A + x_B$. That is, assuming the secrecy constraint $H_A G_A = H_B G_B$ is satisfied, G_A and G_B should then be designed to maximize the mutual information at Ray. We see that the task at hand is the following optimization problem:

$$\begin{aligned} \underset{G_A, G_B}{\text{maximize}} \quad & I(Y; X_A + X_B) \\ \text{subject to} \quad & \begin{cases} \max\{||G_A||_F^2, ||G_B||_F^2\} \leq N \\ H_A G_B = H_B G_B \end{cases} \end{aligned} \tag{54}$$

where $Y = H_A G_A X_A + H_B G_B X_B + W_R$ as before. Notice that the constraints exactly describe the space $\mathcal{P}$ of all precoders studied in Proposition 5.

It is important to note that the goal of the above optimization problem is not to increase the secrecy rate for either Alice or Bob, as the protocols of the previous section have already fixed this quantity. Rather, we seek to increase the overall data rate of the total received signal at Ray, subject to the secrecy constraints.

1) Zero-forcing precoders: A straightforward zero-forcing scheme which satisfies the power and secrecy constraints of (54) is the following. Let $\begin{bmatrix} E_A \\ -E_B \end{bmatrix}$ be a $2N \times d$ matrix whose columns form a basis of the right nullspace of the $M \times 2N$ block matrix $[H_A \ H_B]$. Now set

$$G_A = \sqrt{N}E_A/\gamma, \quad G_B = \sqrt{N}E_B/\gamma \\ \gamma = \max\{||E_A||_F, ||E_B||_F\} \tag{55}$$

and it follows immediately that $H_AG_A = H_BG_B$ as desired. When $N = M = d$, we can take $G_A = \sqrt{N}H_A^{-1}/\gamma$ and $G_B = \sqrt{N}H_B^{-1}/\gamma$, where $\gamma = \max\{||H_A^{-1}||_F, ||H_B^{-1}||_F\}$.

Every pair G_A, G_B of precoding matrices satisfying the secrecy and power constraint can be constructed via the above process. However, for certain parameters of M and N, one can further optimize some initial zero-forcing scheme.

2) Relaxation using the gap approximation: As an attempt at an improvement on the above scheme, let us suppose that the power and secrecy constraints of (54) are satisfied and use the gap approximation to approximate $I(Y; X_A + X_B)$ by the channel capacity:

$$C_{(H_A,H_B)} \approx I(Y; X_A + X_B) + \Gamma \tag{56}$$

where Γ is a constant. By a well-known formula [39], the channel capacity (for fixed H_A, H_B) is then

$$C_{(H_A,H_B)} = \log_2 \det\left(I_M + \frac{P_A + P_B}{\sigma_R^2} H_A G_A G_A^\dagger H_A^\dagger\right) \tag{57}$$

The relaxation of the optimization problem at hand is then to maximize $C_{(H_A,H_B)}$ over all pairs (G_A, G_B) subject to the same constraints of (54). At first glance H_B and G_B are absent from this expression, but recall that we have already assumed that $H_AG_A = H_BG_B$.

To optimize (57) numerically, one performs steepest descent as follows. Let $G = \begin{bmatrix} G_A \\ G_B \end{bmatrix}$, so that the task is to optimize over all possible G satisfying the power and secrecy constraints. The constraints of (54) restrict the set of all possible G to a bounded region of $\mathcal{N} = \text{null}\begin{bmatrix} H_A & -H_B \end{bmatrix}$. One performs steepest descent on the coordinates of G as normal, but after every iteration replaces G with the projection $\text{Proj}_{\mathcal{N}}G$ and scales both blocks of G to satisfy the power constraint of (54). We omit further details.

In Fig. 12 we plot the channel capacity (57). Here the "zero-forcing" precoders were found according to (55). The "gap approximation" precoders were then numerically optimized according to (57), and results were averaged over 10^3 pairs (H_A, H_B) of channel matrices. The entries of H_A and H_B were drawn from i.i.d. complex zero-mean circularly symmetric Gaussian distributions with variance $1/M$.

The most notable feature of Fig. 12 is that further optimization improves the precoding schemes for $(M, N) = (3, 3)$ and $(4, 3)$ quite a bit, but offers no improvement for the other two cases. This is explained by Proposition 5, since only for these parameters is $\dim_{\mathbf{R}} \mathcal{P} = 2(d^2 - 1) > 0$. Secondly, the performance of the gap approximation precoder for $(M, N) = (4, 3)$ is better than that of the zero-forcing precoder for $(M, N) = (3, 3)$, even though the second scheme offers an additional degree of freedom. Hence at the practical, finite SNR regimes of interest, specific precoding matrices may have more impact on capacity than the degrees of freedom.

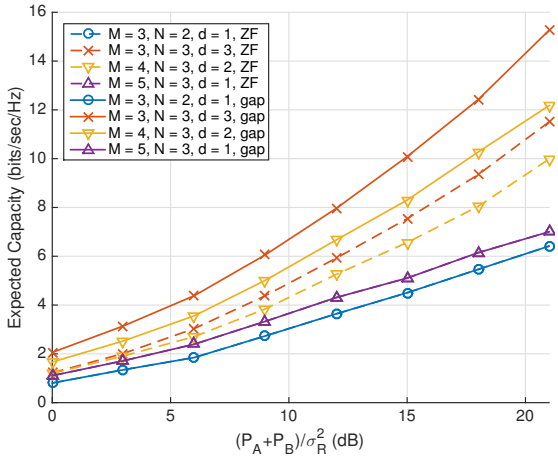

Fig. 12. The expected ergodic capacity $\mathbf{E}_{(H_A,H_B)}C_{(H_A,H_B)}$ as computed by (57) for randomly chosen zero-forcing precoders of (55), and those which have been further optimized using the gap approximation (57) of the mutual information $I(Y; X_A + X_B)$.

VI. Conclusions and Future Work

We have studied the potential for perfect secrecy in a single-relay network with two users. Given finite, uniform input distributions, we have calculated upper bounds for the perfect secrecy rates under the assumptions that one user does or does not have information about the other user's signal, made these upper bounds explicit for PAM modems, and discussed the impact of synchronization errors on secrecy. Two schemes that achieve perfect secrecy were presented using standard M-PAM modulators, one which assumes no cooperation between the users, and one which assumes the user with the smaller constellation knows the other user's signal. Gaps to the relevant upper bounds were shown to be small, especially asymptotically as the size of the larger constellation increases. The system was generalized to a MIMO setting, and precoding matrices maintaining the required secrecy constraints were studied. Finally, the potential for lattice encoders, alternative power allocation schemes, and applications to larger relay networks will be examined in the future.

Appendix

A. Proof of Proposition 2

Proof: We first show that the UBs in the noiseless scenario are given by

$$\widehat{R}_A^s = m_A - I(Y; X_A), \quad \widehat{R}_B^s = m_B - I(Y; X_B). \tag{58}$$

To see this note that in the noiseless scenario, the assumptions of Section II guarantee that $I(Y_B; X_A|X_B) = m_A$, as Alice's symbol is perfectly recoverable given Bob's observation. Furthermore, the noiseless assumption guarantees that $H(X_A|Y_B, X_B) = 0$, and thus (58) for $\widehat{R}_A^s$ follows directly by substitution into (13). The result for Bob follows by symmetry.

By the above it suffices to compute the mutual information $I(Y;X_A)$. We first fix a single $x_A \in \mathcal{X}_A$ and compute the marginal mutual information $I(Y;x_A)$. An easy computation reveals that the joint distribution (Y,X_A) has pmf

$$p_{Y,X_A}(y,x_A) = \frac{|\psi^{-1}(y) \cap (\{x_A\} \times \mathcal{X}_B)|}{M_A M_B} = \begin{cases} 0, & \psi^{-1}(y) \cap (\{x_A\} \times \mathcal{X}_B) = \emptyset \\ \frac{1}{M_A M_B}, & \text{otherwise} \end{cases}$$

Computing the mutual information $I(Y;x_A)$ now gives

$$\begin{aligned} I(Y;x_A) &= \sum_{y \in \mathcal{Y}} p_{Y,X_A}(y,x_A) \log_2 \left(\frac{p_{Y,X_A}(y,x_A)}{p_Y(y) p_{X_A}(x_A)} \right) \\ &= \sum_{\substack{y \in \mathcal{Y} \\ y \in x_A + \mathcal{X}_B}} \frac{1}{M_A M_B} \log_2 \frac{M_A}{|\psi^{-1}(y)|} \end{aligned} \tag{59}$$

Summing up over all x_A, we arrive at

$$\begin{aligned} I(Y;X_A) &= \sum_{x_A \in \mathcal{X}_A} I(Y;x_A) \\ &= m_A - \sum_{x_A \in \mathcal{X}_A} \sum_{\substack{y \in \mathcal{Y} \\ y \in x_A + \mathcal{X}_B}} \frac{\log_2 |\psi^{-1}(y)|}{M_A M_B} \\ &= m_A - \sum_{y \in \mathcal{Y}} \frac{|\psi^{-1}(y)|}{M_A M_B} \log_2 |\psi^{-1}(y)| \end{aligned} \tag{60}$$

where the last equality follows by grouping like summands together. An analogous calculation holds for Bob, and the proposition follows. ∎

B. Proof of Theorem 1

Proof: Define $S = \sum_{y \in \mathcal{Y}} |\psi^{-1}(y)| \log_2 |\psi^{-1}(y)|$. We can use the explicit formula for $|\psi^{-1}(y)|$ from Proposition 3 to write S as $S = F + L$ where

$$F = \sum_{\substack{y=-(M_B-M_A) \\ y \text{ even}}}^{M_B-M_A} m_A M_A$$

$$L = 2 \sum_{\substack{y=M_B-M_A+2 \\ y \text{ even}}}^{M_B+M_A-2} \frac{M_B+M_A-y}{2} \log_2 \left(\frac{M_B+M_A-y}{2} \right)$$

The number of even integers in the interval $[-(M_B - M_A), M_B - M_A]$ is exactly $M_B - M_A + 1$, and hence $F = m_A M_A (M_B - M_A + 1)$. Making the change of variables $a = \frac{M_B+M_A-y}{2}$ transforms the sum L into $L = 2\sum_{a=1}^{M_A-1} a \log_2(a)$. We can conclude the proof by recalling that $\widehat{R}^s = S/M_A M_B = (F+L)/M_A M_B$, which is easily shown to be equal to the quantity in the theorem given the above calculations. ∎

ACKNOWLEDGMENT

We would like to thank the anonymous reviewers for their useful and constructive comments that have greatly improved both the contents and the presentation of this work.

REFERENCES

[1] R. Ahlswede, C. Ning, S.-Y.R. Li, and R.W. Yeung, "Network information flow", *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Apr. 2000.

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

[3] T. Koike-Akino, P. Popovski, and V. Tarokh, "Optimized constellations for two-way wireless relaying with physical network coding", *IEEE J. Sel. Areas Commun.*, vol. 27, no. 5, pp. 773–787, June 2009.

[4] F. Boccardi, R.W. Heath, A. Lozano, T.L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G", *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 74–80, Feb. 2014.

[5] J.N. Laneman, D.N.C. Tse, and G.W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior", *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[6] B. Nazer and M. Gastpar, "Reliable physical layer network coding", *Proc. IEEE*, vol. 99, no. 3, pp. 438–460, Mar. 2011.

[7] A. Chorti, "Masked-OFDM: a physical layer encryption for future OFDM applications", in *IEEE Global Commun. Conf. Workshops (GC'WS)*, Miami, FL, Dec. 2010, pp. 1254–1258.

[8] "IEEE Std 802.15.1-2002", pp. 1–473, 2002.

[9] E. Jorswieck, L. Lai, W.-K. Ma, H.V. Poor, W. Saad, and A.L. Swindlehurst, "Guest editorial:signal processing for wireless physical layer security", *IEEE J. Sel. Areas Commun.*, vol. 9, no. 31, pp. 1657–1659, Sept. 2013.

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

[11] Y. Liang, H.V. Poor, and S. Shamai, *Information Theoretic Security*, Now Publishers, Hanover, MA, 2009.

[12] A. Chorti, C. Hollanti, J.-C. Belfiore, and H. Vincent Poor, "Physical layer security: a paradigm shift in data confidentiality", *Springer Lect. Notes Electrical Eng.*, vol. 358, pp. 1–15, 2015.

[13] A.D. Wyner, "The wire-tap channel", *Bell System Techn. J.*, vol. 54, no. 8, pp. 1385–1357, Oct. 1975.

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

[15] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification", *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 394–400, Feb. 1995.

[16] C.E. Shannon, "A mathematical theory of cryptography", *Bell System Techn. J.*, vol. 28, pp. 656–715, Oct. 1949.

[17] Y. Oohama, "Coding for relay channels with confidential messages", in *Proc. IEEE Inf. Theory Workshop (ITW)*, Cairns, Australia, Sept. 2001, pp. 87–89.

[18] Y. Oohama, "Capacity theorems for relay channels with confidential messages", in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, June 2007, pp. 926–930.

[19] X. He and A. Yener, "Cooperation with an untrusted relay: a secrecy perspective", *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[20] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy", *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sept. 2008.

[21] D. Lun, Z. Han, A.P. Petropulu, and H.V. Poor, "Improving wireless physical layer security via cooperating relays (part 2)", *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1845–1888, Mar. 2010.

[22] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks", *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 388–396, Feb. 2012.

[23] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M.R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: a summary of recent advances", *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sept. 2013.

[24] J.P. Vilela, L. Lima, and J. Barros, "Lightweight security for network coding", in *Proc. IEEE Int. Conf. Commun. (ICC)*, Beijing, China, May 2008, pp. 1750–1754.

[25] 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, Jan. 2013.

[26] S. Vatedka, N. Kashyap, and A. Thangaraj, "Secure compute-and-forward in a bidirectional relay", *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2531–2556, May 2015.

[27] X. He and A. Yener, "Providing secrecy with lattice codes", in *Forty-sixth Annual Allerton Conf.*, Allerton House, UIUC, Illinois, USA, Sep. 23-26 2008, pp. 1199–1206, IEEE.
[28] X. He and A. Yener, "Interference channels with strong secrecy", in *Forty-Seventh Annual Allerton Conf.*, Allerton House, UIUC, IL, USA, Sep. 30 - Oct. 2 2009, pp. 811–818.
[29] C. Ling, L. Luzzi, and J.-C. Belfiore, "Lattice codes achieving strong secrecy over the mod-Λ Gaussian channel", in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Boston, MA, July 2012, pp. 2306–2310.
[30] O.O. Koyluoglu, H. El Gamal, L. Lai, and H.V. Poor, "Interference alignement for secrecy", *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, June 2011.
[31] J. Xie and S. Ulukus, "Secure degrees of freedom for one-hop wireless networks", arXiv:1209.537v1 [cs.IT], 2012.
[32] Y. Tian and A. Yener, "Degrees of freedom for the MIMO multi-way relay channel", *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2495–2511, Mar. 2014.
[33] G. Bresler, D. Cartwright, and D. Tse, "Feasibility of interference alignment or the MIMO interference channel", *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5573–5586, Sept. 2014.
[34] X. Tang, L. Ruoheng, P. Spasojevict', and H.V. Poor, "Interference assisted secret communication", *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153 – 3167, May 2011.
[35] O. Ozel, *Coding and Scheduling in Energy Harvesting Communication Systems*, PhD thesis, Department of Electrical and Computer Engineering, University of Maryland, 2014, http://www.ece.umd.edu/ ulukus/papers/theses/ozel-thesis.pdf.
[36] H. Hashemi, "The indoor radio propagation channel", *Proc. IEEE*, vol. 81, no. 7, pp. 943–968, July 1993.
[37] R.S. Ganesan, T. Weber, and A. Klein, "Interference alignment in multi-user two way relay networks", in *Proc. IEEE Veh. Technol. Conf. (VTC)*, Yokohama, Japan, May 2011.
[38] Y. Tian and A. Yener, "Signal space alignment and degrees of freedom for the two-cluster multi-way relay channel", in *Proc. IEEE Int. Conf. Commun. China (ICCC)*, Beijing, China, Aug. 2012.
[39] W. Santipach and M. L. Honig, "Capacity of a multiple-antenna fading channel with a quantized precoding matrix", *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1218–1234, Mar. 2009.

David Karpuk (M'12) (born 1984, USA) received his Ph.D. degree in mathematics from the University of Maryland, College Park in 2012. His research interests include applications of algebra and number theory to communications engineering, particularly wireless communications, physical later security, interference alignment, and broadcast channels.

After receiving his Ph.D. in number theory, Karpuk joined the Algebra, Number Theory, and Applications research group at Aalto Univeresity, Finland as a postdoctoral researcher. He has been the recipient of postdoctoral research grants from the Magnus Ehrnrooth Foundation and the Academy of Finland. He also served as a visiting researcher at the University of Essex, United Kingdom during the Fall semester of 2014, and has been a reviewer for a number of international conferences and journals.

Arsenia Chorti (S'00, M'05) obtained an M.Eng. degree in EEE from the University of Patras (Greece) and a D.E.A. degree in Electronics at the University Pierre et Marie Curie - Paris VI (France). In November 2005 she obtained her Ph.D. in EE from Imperial College London (UK). She undertook post-doctoral positions at the Universities of Southampton (UK), TCU (Greece) and UCL (UK), between 2005 and 2008. She has served as a Senior Lecturer in Communications at Middlesex University (UK) from December 2008 to April 2010. Between 2010 and 2013 she was a Marie Curie IOF researcher at Princeton University (US) and ICS-FORTH (Greece). Since October 2013 she holds a Lecturer position in Communications and Networks at CSEE University Essex (UK) and is a visiting research collaborator at Princeton University. Her research interests span the areas of stochastic signal processing, communications and information theory. Dr. Chorti is a chartered engineer from the Technical Chambers of Greece since 2007.