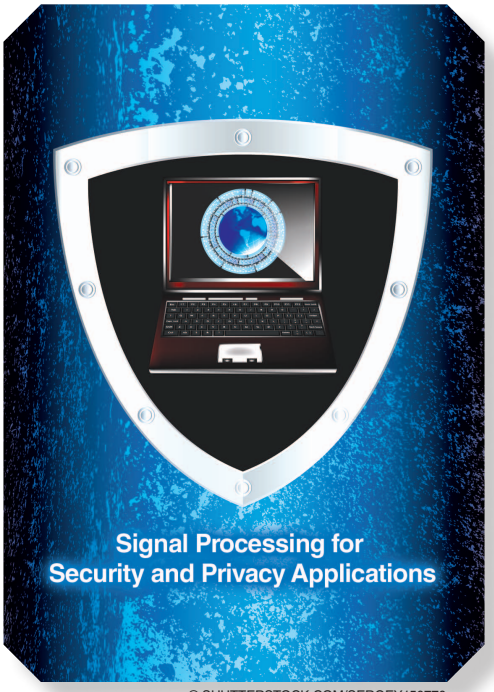
Raef Bassily, Ersen Ekrem, Xiang He, Ender Tekin, Jianwei Xie,
Matthieu R. Bloch, Sennur Ulukus, and Aylin Yener

Cooperative Security at the Physical Layer

A summary of recent advances



Wireless communications systems are particularly vulnerable to security attacks because of the inherent openness of the transmission medium. In this article, we focus on guaranteeing confidentiality against eavesdropping attacks where an unauthorized entity aims to intercept an ongoing wireless communication, and we provide a comprehensive summary of recent advances in the area of physical-layer security that guarantees confidentiality by using cooperative techniques unique to the wireless medium. These cooperative techniques consist of carefully designed coding and signaling schemes that are able to harness the properties of the physical layer and to ensure some level of information-theoretic security.

INTRODUCTION

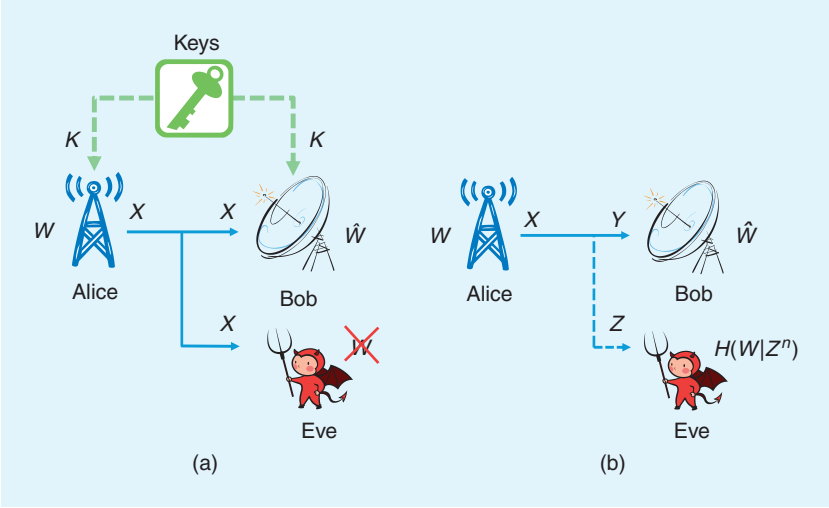
The first approach to information-theoretic security goes back to Shannon's 1949 paper [1], where he describes a special case of what is now known as the wiretap channel, in which a legitimate transmitter wishes to have secure communication with a legitimate receiver in the presence of an eavesdropper. Shannon's model considers noiseless bit-pipes between these three entities, which is to say that the observations of the legitimate receiver and the eavesdropper are identical and requires an information-theoretic level of security, meaning that the eavesdropper's observation should not leak any information about the transmitted message. In this setup, Shannon shows that the legitimate parties can achieve information-theoretically secure communications provided they share secret keys; see Figure 1(a). Denoting the message as W and the secret key as K, Shannon's one-time pad approach requires the legitimate transmitter to send $X = W \oplus K$, which both the legitimate receiver and the eavesdropper receive. The legitimate receiver further XORs the received signal with the key K to retrieve the message W. Shannon showed that, if each key is uniform and used only once, hence the name one-time pad, then the signal X leaks no information about the message W to the eavesdropper, as it is statistically independent of the message. Unfortunately, the key length should then be as large as the size of the message, which is often too costly to implement efficiently.

This pessimistic conclusion has resulted in the birth of public-key cryptography, i.e.,effectively abandoning

Digital Object Identifier 10.1109/MSP.2013.2260875
Date of publication: 20 August 2013

1053-5888/13/$31.00©2013IEEE

information-theoretic security in lieu of computation-based security, which relies on computationally hard problems, such as factoring integers into prime numbers and computing discrete logarithms, which need to be computed by adversaries in a timely manner to eavesdrop successfully on the communication [2], [3]. Concurrently, Wyner has introduced the noisy wiretap channel [see Figure 1(b)], where both links from the legitimate transmitter to the legitimate receiver and the eavesdropper are noisy and the eavesdropper gets a degraded version of the legitimate receiver's observation [4]. For this model, Wyner has determined the secrecy capacity, defined as the supremum of communication rates to the legitimate receiver at which one can guarantee reliability and information-theoretic security against the eavesdropper. Wyner's notion of information-theoretic security relaxes Shannon's definition by requiring that $\lim_{n\to\infty}[(1/n)I(W;Z^n)]=0$, i.e., the eavesdropper's observation Z^n leaks a vanishing rate of information about the message W in the limit of large coding length n. This requirement is called weak secrecy and is often criticized because it allows the eavesdropper to gather a nonvanishing amount of information about W. Wyner's definition can be strengthened to $\lim_{n\to\infty}I(W;Z^n)=0$, i.e., requiring the eavesdropper's observation to leak a vanishing amount of information, which is known as strong secrecy. Nevertheless, both requirements are much stronger than merely requiring the eavesdropper to have nonzero probability of error, and their operational significance is that the eavesdropper is completely confused about the message and no better informed than if it were not observing any signal at all. It is worth mentioning that both strong and weak secrecy constraints result in the same secrecy capacity [5], [6].



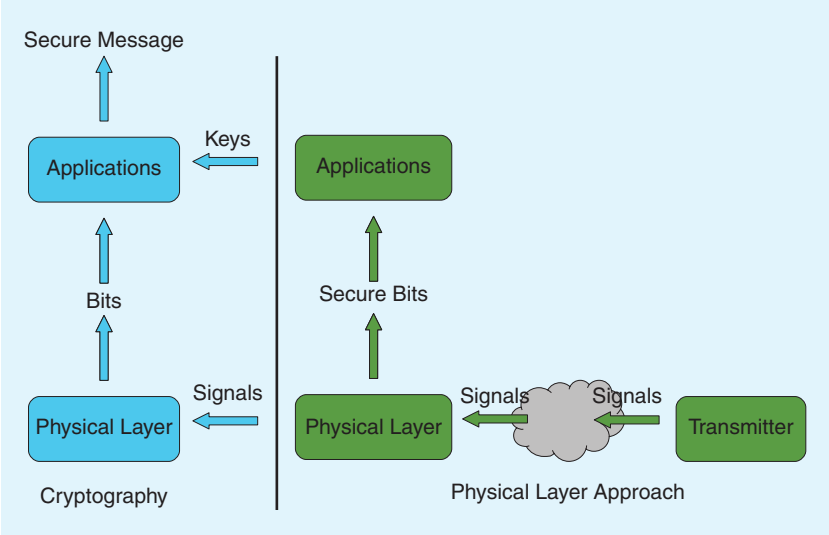
[FIG1] (a) Shannon's wiretap channel with noiseless bit-pipes and keys. (b) Wyner's wiretap channel with noisy channels.

Wyner's result has uncovered the fact that, if the eavesdropper's observation is a degraded version of the legitimate user's observation, information-theoretically secure communication between the legitimate users is possible while keeping the eavesdropper completely ignorant of the secure message, without using any secret keys. Subsequently, Csiszár and Körner have generalized Wyner's result to general, not necessarily degraded, wiretap channels [7], determining the secrecy capacity for this general wiretap channel. Their result has shown that even when the eavesdropper is not degraded with respect to the legitimate user, information-theoretically secure communication between the legitimate users is possible by exploiting the inherent randomness in the communication channel to the advantage of the legitimate users. The fundamental difference between cryptography and information-theoretic security is depicted in Figure 2: cryptography operates at higher layers of the protocol stack via encryption, while information-theoretic security operates at the physical layer by exploiting the inherent randomness in the communication channel via appropriate signaling and channel coding.

The secrecy capacity for a general wiretap channel is given by

$$C_s = \max_{V\to X\to Y,Z} I(V;Y) - I(V;Z), \tag{1}$$

where the mapping from V, the message carrying signal, to X, the channel input, is called channel prefixing. When the wiretap



[FIG2] The difference between cryptographic and information-theoretic approaches to communication security.

channel is degraded, i.e., the channel input X, Bob's channel output Y and Eve's channel output Z satisfy the Markov chain $X \to Y \to Z$, there is no need for channel prefixing, and $V = X$ selection is optimal [7], and the secrecy capacity reduces to

$$C_s = \max_X I(X;Y) - I(X;Z). \tag{2}$$

Equations (1) and (2) show that secrecy is a relative concept, involving the difference of rates going to Bob and Eve. The secrecy capacity in (2) is achieved with what is known as stochastic encoding, where every message is associated with multiple codewords to confuse the eavesdropper. With the message rate C_s and confusion rate $I(X;Z)$, Bob is able to decode both the secure message and the confusion message, since his channel can resolve combined messages at rates up to $I(X;Y)$; on the other hand, all messages look equally likely to Eve because her channel's resolvability is limited to $I(X;Z)$. Channel prefixing in (1) shows another aspect of relativeness of the concept of secrecy. From the data processing inequality, using a prefixed channel reduces both the useful rate from $I(X;Y)$ to $I(V;Y)$ and the leakage rate from $I(X;Z)$ to $I(V;Z)$. However, a careful selection of V may increase the difference in (1), by decreasing $I(X;Z)$ relatively more than $I(X;Y)$, hence the need to use channel prefixing, in general. For the Gaussian wiretap channel, which models a nonfading wireless communication channel, a Gaussian channel input maximizes both mutual information terms as well as the difference of the mutual information terms in (2), and hence the secrecy capacity equals the difference of the channel capacities of the legitimate link C_B and the eavesdropping link C_E [8]. Assuming $C_B \geq C_E$,

$$C_s = C_B - C_E = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_B^2}\right) - \frac{1}{2}\log\left(1 + \frac{P}{\sigma_E^2}\right). \tag{3}$$

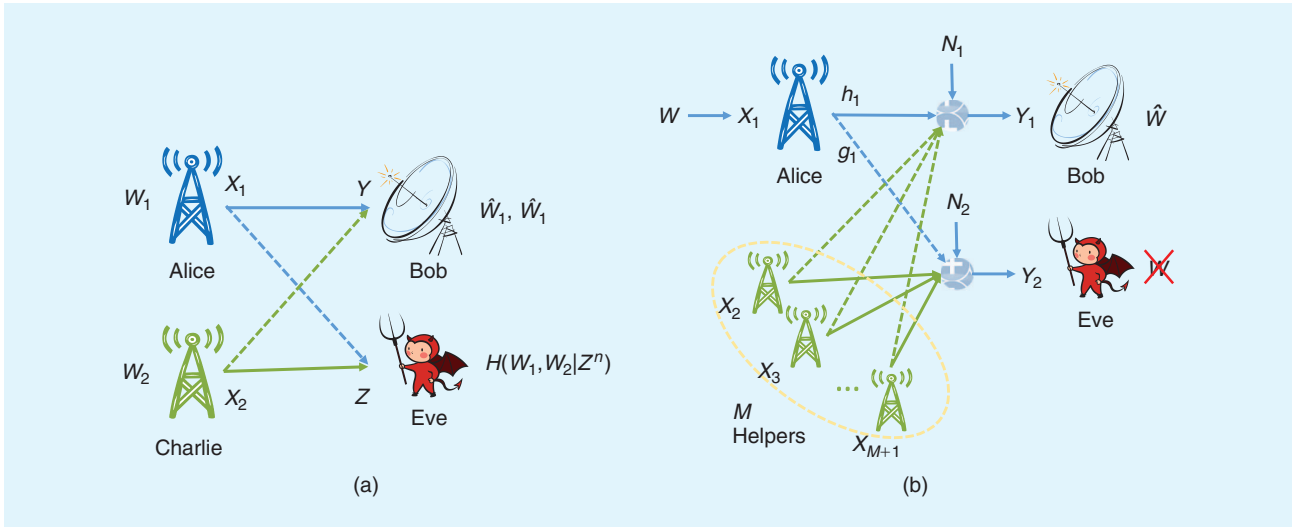
We note, for future reference, that the secrecy capacity in (3) does not scale with the transmit power P of the legitimate transmitter. That is, as P goes to infinity, C_s converges to a constant. The cost of providing information-theoretic secrecy is often measured in terms of secure degrees of freedom (s.d.o.f.), defined as the ratio of the secure communication rate R_s to $(1/2)\log P$ in the limit of infinitely large P, i.e., s.d.o.f. $= \lim_{P\to\infty}[(R_s/(1/2)\log P)]$, relative to its counterpart, the degrees of freedom, i.e., the same asymptotic behavior of rate without the secrecy constraint. Thus, we observe that the Gaussian wiretap channel incurs a severe penalty for secrecy, having reduced its degrees of freedom from one to zero for secrecy.

A crucial assumption behind the wiretap channel model, which is also used throughout this article, is the knowledge of the eavesdropper's channel statistics, i.e., the probability distribution of the eavesdropper's channel. In that respect, we restrict ourselves to "honest-but-curious" eavesdroppers, who abide by the protocols and do not attempt to jam or tamper with the transmission. More sophisticated eavesdroppers may inject signals into the communication channel [9] and/or tamper with the statistics of the communication channel by altering their own effective channels by moving around [10]. Nevertheless, the coding techniques presented hereafter play a key role in generalizing the models to more adversarial situations [10]–[12]. While we will not consider such models in this article, we will consider the effects of knowledge of the instantaneous realization of the channel gains at the legitimate transmitters via an alignment example [13] in the section "Cooperative Jamming by Alignment." In the following sections, we will overview major cooperative secrecy techniques developed for the physical layer. Our emphasis will be on presenting their basic rationale and operating principles. We refer the reader to the papers where they were originally proposed and to the subsequent papers where they were extended and applied to different scenarios for detailed performance evaluations and comparisons, e.g., [12] and [14]–[25]. In addition, for clarity and brevity, we will not discuss in detail some of the implementation challenges specific to cooperative schemes, whether they incorporate secrecy constraints or not, such as challenges related to self-interference cancellation in full-duplex relaying/jamming operations. We refer the reader to the growing body of theoretical and experimental research in this area, e.g., [26] and [27].

A FURTHER INTERPRETATION OF THIS PHENOMENON IS THAT BY TRANSMITTING SIGNALS, INDEPENDENT TRANSMITTERS CAN INJECT ADDITIONAL RANDOMNESS INTO THE CHANNEL, WHICH MAY BE DESIGNED TO FAVOR THE LEGITIMATE USERS.

COOPERATIVE JAMMING BY GAUSSIAN NOISE

In a network of transmitters and receivers, if reliability is the only concern, then to maximize the achievable reliable rate of a given transmitter-receiver pair, all other independent transmitters must remain silent as the signals they transmit will only cause interference at the receiver. However, when security is an added concern, independent transmitters can improve the secrecy rate of a given transmit-receiver pair by transmitting signals. This phenomenon was first discovered in [28] and further developed in [14] and [29]; in these works, the term cooperative jamming was coined to describe such collaborative approaches to secrecy at the physical layer of a multiuser system. One interpretation of this phenomenon has to do with the relative nature of secure communications and the fact that the achievable throughput in secrecy is equal to the difference in the rates of the legitimate channel, and the eavesdropper's channel, similar to (3). When a sender transmits signals that are independent of the intended message, these signals create interference for both the legitimate receiver and the eavesdropper, limiting both of their decoding capabilities, and reducing both of their reliable decoding rates. However, the net effect of this jamming may be an increase in



[FIG3] **(a) A multiple access wiretap channel. (b) A wiretap channel with *M* helpers.**

the difference of the rates and hence an increase in the achievable secrecy rate between the legitimate pair. In other words, while any independent transmission jams the legitimate receiver and the eavesdropper simultaneously, this may yield a net gain for the legitimate users.

Cooperative jamming [14], [28], [29] was originally proposed for a multiple access wiretap channel [30], where multiple legitimate users wish to have simultaneous secure communications with an intended receiver in the presence of an eavesdropper; for instance, Figure 3(a) shows a two-user multiple access wiretap channel where Alice and Charlie wish to have simultaneous secure communication with Bob over a multiple access channel in the presence of Eve. In this context, it was noted that to maximize the sum secrecy rate of the system, a user (Charlie) who has a stronger channel to the eavesdropper (Eve) than to the intended receiver (Bob) should cease sending message carrying signals and instead help by sending independent identically distributed (i.i.d.) Gaussian noise signals. Since Charlie has a stronger channel gain to Eve than to Bob, his jamming is more detrimental to Eve than Bob, thus increasing Alice's achievable secrecy rate.

Cooperative jamming can also be interpreted based on the potential necessity of channel prefixing in secure communications [31]. In channel prefixing, the channel input becomes a random function of the message carrying signal via the Markov chain $V \to X \to Y, Z$. In a Gaussian channel, we can choose the channel input X as a noisy version of the message carrying signal, for instance as $X = V + U$, where V and U are independent and Gaussian. In this case, U is an additional independent signal that is inserted into the channel in addition to the message carrying signal V. The purpose of U is to further confuse the eavesdropper by jamming her. In one extreme when $V = 0$, the entire transmitted signal becomes a jamming signal, $X = U$, which does not carry any messages.

A further interpretation of this phenomenon is that by transmitting signals, independent transmitters can inject additional randomness into the channel, which may be designed to favor the legitimate users. While the original cooperative jamming in [14], [28], and [29] was done by using i.i.d. Gaussian signals over a multiple access channel, the concept of cooperative jamming is much more widely applicable and, in fact, has become an integral part of achievable schemes in many multiuser extensions of the wiretap channel, as will be discussed in the sequel. In addition, the manner in which jamming can be implemented is not restricted to i.i.d. Gaussian signals, and several more effective cooperative jamming mechanisms have been discovered, including cooperative jamming based on structured signals [23], [32] and cooperative jamming with interference alignment [13], [33]–[35], as will be discussed in the sequel.

It is worth mentioning that a related concept called noise forwarding was proposed in [36] for the Gaussian relay channel. In this approach, a helper relay terminal, effectively a cooperative jammer, transmits additional randomness in the form of randomly chosen (noninformation carrying) codewords from a known codebook instead of transmitting i.i.d. Gaussian noise signals, thus taking over the responsibility of generating randomness from the original transmitter. The major difference between cooperative jamming with Gaussian noise and noise forwarding is that, in the latter, by choosing the rates appropriately, the legitimate user can be enabled to decode the confusion signal, hence receiving a clean information-carrying signal whereas the eavesdropper's channel remains jammed; while in the former, both legitimate and eavesdropping links are jammed simultaneously. These strategies can outperform one another depending on the channel conditions. Both strategies have been used to extend the concept of multiuser secrecy to networks of relays in [21].

While it was originally devised for a multiple access channel, as illustrated in Figure 3(b), the concept of cooperative jamming naturally extends to multiuser and multiantenna system. By denoting by $\mathbf{h} = (h_2, \ldots, h_{M+1})$ the vector of channel gains to Bob, $\mathbf{g} = (g_2, \ldots, g_{M+1})$ the vector of channel gains to Eve, and by $\mathbf{x} = (x_2, \ldots, x_{M+1})$ the vector of jamming signals emitted by

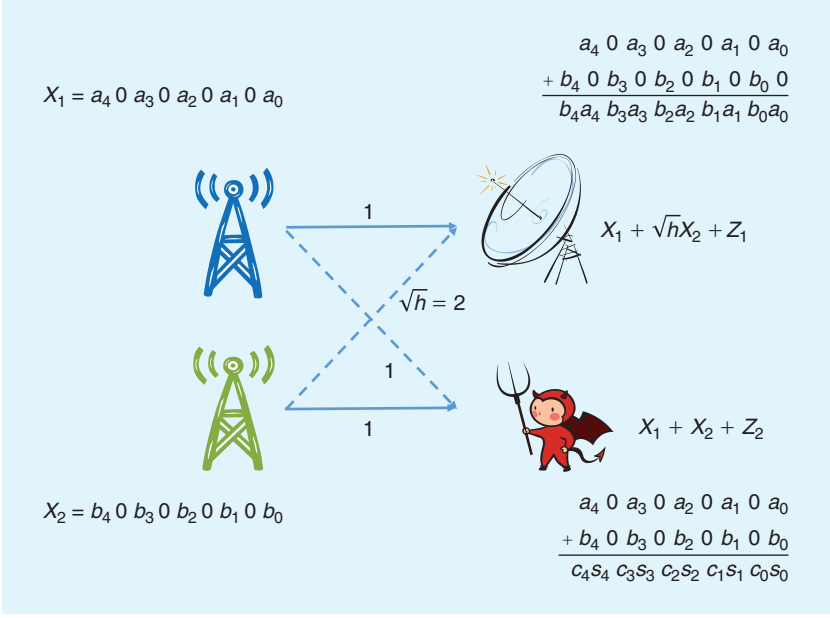
the helpers, achievable rates with i.i.d. Gaussian helper signals, are of the form

$$R_s = \frac{1}{2}\log\left(1+\frac{h_1^2 P}{\sigma_B^2+\mathbf{h}^T\mathbf{Q}\mathbf{h}}\right)-\frac{1}{2}\log\left(1+\frac{g_1^2 P}{\sigma_E^2+\mathbf{g}^T\mathbf{Q}\mathbf{g}}\right), \quad (4)$$

where $\mathbf{Q}$ is the covariance matrix of $\mathbf{x}$. For the case of multiple independent helpers, all of the transmitted helper signals need to be independent, implying that the covariance matrix $\mathbf{Q}$ must be diagonal. In this case, the denominators will reduce to sum of powers of the helpers multiplied by squared channel gains plus the power of the ambient Gaussian noise. On the other hand, for the case of a multiple-antenna helper, x_i can be arbitrarily correlated, and we will be free to choose $\mathbf{Q}$ to maximize the achievable secrecy rate. In this case, we may choose $\mathbf{Q}$ orthogonal to $\mathbf{h}$ and eliminate the cooperative jamming signal from the legitimate receiver's channel output. However, an optimal $\mathbf{Q}$ will balance minimizing interference at Bob and maximizing interference at Eve and will aim to maximize the difference of the log terms in (4). Further, (4) illustrates the interplay between signaling and coding for security at the physical layer. On the one hand, appropriate signaling, e.g., through the choice of the powers and direction of cooperative jamming signals, gives an advantage to the legitimate receiver over the eavesdropper; on the other hand, coding (i.e., stochastic encoding) translates this advantage into a secure communication rate. Consequently, multiantenna processing techniques that aim at controlling direction and strengths of signals can play an important role [12], [15], [19], [37]. However, in general, coding and signaling must be jointly designed to achieve a desired level of information-theoretic security.

COOPERATIVE JAMMING BY STRUCTURED CODES

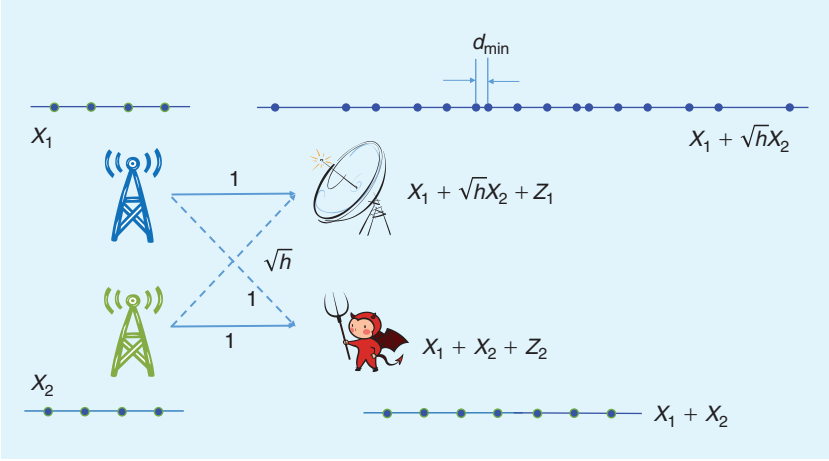
Although transmitting i.i.d. Gaussian noise is arguably a convenient signaling strategy to limit the reception capability of the eavesdropper, it could also hurt the intended receiver and result in zero s.d.o.f. as noted earlier. References [23] and [32] have proposed to let the jammer send signals with certain structure and found that it improved the achievable secrecy rate for channel models where the jamming signals could not be nulled out at the intended receiver. One such example is shown in Figure 4, in which the transmitter sends X_1 while the cooperative jammer sends X_2. Let Z_1 and Z_2 denote the real zero-mean additive Gaussian channel noise observed by the intended receiver and the eavesdropper, respectively. We assume $Z_i, i = 1, 2$ has unit variance. The intended receiver observes $X_1 + 2X_2 + Z_1$. The eavesdropper receives $X_1 + X_2 + Z_2$. An achievable secrecy rate for this channel model is $\max\{\max_{\Pr(X_1)\Pr(X_2)} I(X_1; X_1 + 2X_2 + Z_1) - I(X_1; X_1 + X_2 + Z_2), 0\}$. If $\Pr(X_1)$ and $\Pr(X_2)$ are chosen to be Gaussian, then the achieved secrecy rate is zero because the jamming signal hurts the intended receiver more than it harms the eavesdropper. However, as shown in Figure 4, if X_1 and X_2 have certain structure, so that they are aligned at the eavesdropper but remain separable at the intended receiver, a positive secrecy rate is in fact achievable. This is done as follows: let the binary representation of X_1 and X_2 be $a_L, 0, a_{L-1}, 0, \ldots, 0, a_0$ and $b_L, 0, b_{L-1}, 0, \ldots, 0, b_0$, respectively, where a_is and b_is are binary bits. The signal component in the observation made by the intended receiver, $X_1 + 2X_2$, is then given by $b_L, a_L, b_{L-1}, a_{L-1}, \ldots, b_0, a_0$, from which the intended receiver can extract the value of $a_L, a_{L-1}, \ldots, a_0$, except for a couple of least significant bits which may be corrupted by Z_1. On the other hand, X_1 and X_2 are perfectly aligned at the eavesdropper's end in terms of the position of the zeros. Let $s_i = a_i + b_i \bmod 2$, and c_i be the carrier of $a_i + b_i$. Then the eavesdropper observes $c_L, s_L, c_{L-1}, s_{L-1}, \ldots, c_0, s_0$. Ignoring the effect of channel noise Z_2, we observe that the eavesdropper knows the value of a_i only when $a_i = b_i$, which happens with probability 0.5. Therefore, each a_i could support a secrecy rate of 0.5 bit per channel use. Let R_s denote the secrecy rate achieved. Then with this scheme, we have shown that $R_s > 0$ and $\lim_{L\to\infty}(R_s/L) = 0.5$.



[FIG4] Cooperative jamming with structured codes.

Designing good structured codes for cooperative jamming has attracted significant interest in the last few years. Let the average transmission power of the transmitter and the cooperative jammer be P. References [23] and [32] have used layered nested lattice codes and integer lattice codes and proposed a scheme achieving nonzero s.d.o.f. for the channel model in Figure 4 for all values of the channel gain $\sqrt{h}$ except when $\sqrt{h} = 1$. In particular, the s.d.o.f. equal to 1/2 can be achieved using real interference alignment when $\sqrt{h}$ is an algebraic irrational number. Subsequently, [33] also used real interference alignment and showed

that s.d.o.f. equal to 1/2 are indeed achievable whenever $\sqrt{h}$ is any irrational number. The principle of the achievable scheme is illustrated in Figure 5. Let $C(a, Q)$ denote the set $\{-aQ, -a(Q-1), \ldots, a(Q-1), aQ\}$ for a positive integer Q and scaling factor a. Both X_1 and X_2 take values from $C(a, Q)$. The eavesdropper's observation, $X_1 + X_2$, takes values from the set $C(a, 2Q)$. It can be verified that $I(X_1; X_1 + X_2) < 1$. On the other hand, when $\sqrt{h}$ is irrational, it can be verified that $X_1 + \sqrt{h}X_2$ can take $(2Q+1)^2$ possible values, each corresponding to a unique pair (X_1, X_2). Let $d_{\min}$ denote the minimal distance between any pair of these possible values. It can be shown that one can choose a and Q such that both Q and $d_{\min}$ increase with the transmission power P. The increase of $d_{\min}$ implies that the probability of decoding errors decreases with P while the increase in Q implies that X_1 can be used to represent more bits. Using these properties, one can prove that $I(X_1; X_1 + \sqrt{h}X_2)$ also increases with P. Since $I(X_1; X_1 + X_2) < 1$, we observe that the achievable secrecy rate $\max\{0, I(X_1; X_1 + \sqrt{h}X_2) - I(X_1; X_1 + X_2)\}$ increases with P, as well. References [34] and [35] have recently provided the converse and proved that s.d.o.f. cannot exceed 1/2 for any $\sqrt{h}$, so that the performance of a scheme based on real interference alignment is optimal for almost all possible values of $\sqrt{h}$; see the next section for details.



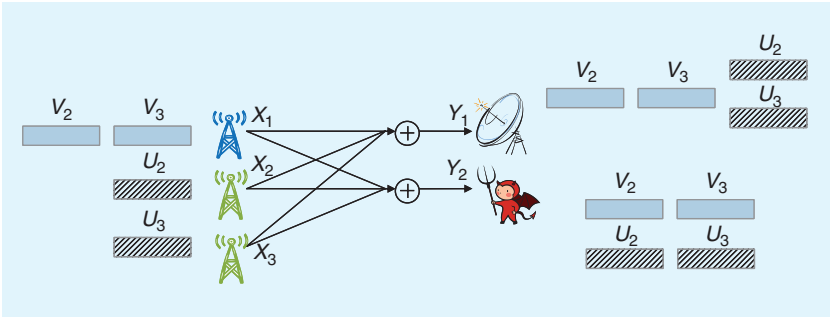
[FIG5] Real interference alignment.

COOPERATIVE JAMMING BY ALIGNMENT

As we have seen so far, cooperative jamming arises as an important tool used in achievable schemes as part of the channel prefixing procedure. In fact, it proves useful in all multiuser extensions of the wiretap channel, including the multiple access wiretap channel, relay eavesdropper channel, interference channel with confidential messages, interference channel with external eavesdroppers; see, for example, [23]. Therefore, a fundamental canonical channel structure in multiuser wiretap channels becomes the wiretap channel with helpers, i.e., cooperative jammers, which is shown in Figure 3(b). In this channel model, there is a legitimate transmitter-receiver pair, which wishes to have secure communication in the presence of an eavesdropper, and there are helpers which can transmit signals that are independent of the message. This channel model generalizes the single cooperative jammer model we have covered so far, and reduces to what we have when we focus on the individual secure rate of a single user in a multiple access wiretap channel or in an interference channel with an external eavesdropper [23], [30]. In such channels, remaining legitimate transmitters act as helpers. It also encompasses the relay eavesdropper channel with relay as the deaf helper [36].

Helper nodes can increase the secrecy rate of the legitimate pair by transmitting signals. In particular, as in the original cooperative jamming scheme, the helpers may transmit i.i.d. Gaussian signals to improve the secrecy rate of the legitimate pair [14], [28], [29]. However, such i.i.d. Gaussian cooperative jamming signals do not improve the s.d.o.f. The s.d.o.f. is still zero in this case as in the canonical Gaussian wiretap channel with no helpers. Such i.i.d. Gaussian signals maximally jam the eavesdropper but also maximally hurt the legitimate user's decoding capability. As discussed in the previous section, [23] and [38] achieved positive s.d.o.f. by using nested lattice codes in a Gaussian wiretap channel with a helper. For the Gaussian wiretap channel, with a single helper, previously, [39] and [33] achieved s.d.o.f. of 1/4 of as a symmetric individual rate on the two-user interference channel with external eavesdroppers and on the multiple access wiretap channel, respectively. Additionally, [23] and [38] achieved a s.d.o.f. of 1/2 using integer lattice codes if the channel gains are irrational algebraic numbers. Recently, [34] and [35] showed that s.d.o.f. of 1/2 can be achieved for almost all channel gains by using cooperative jamming and real interference alignment, and also provided a converse to show that, in fact, this is also an upper bound, establishing the s.d.o.f. capacity. These references also determined the s.d.o.f. for the case of M helpers to be $[M/(M+1)]$.

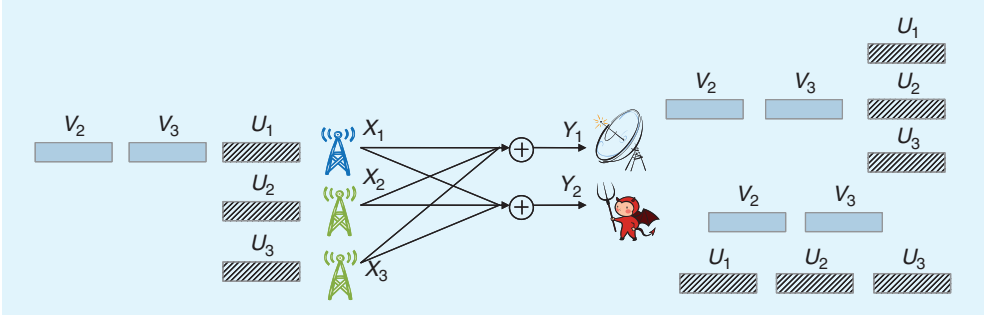
The achievable scheme that is based on structured cooperative jamming and real interference alignment is illustrated in Figure 6 for the M-helper case, when $M = 2$. The legitimate transmitter divides its message into M parts. Each helper sends a cooperative jamming signal. All of the M cooperative jamming signals are aligned in the same dimension at the legitimate receiver to occupy the smallest signal space to allow for maximum signal space that can be used by the messages. All of the M submessages are separable at the legitimate receiver because they are in different irrational dimensions. On the other hand, each cooperative jamming signal is aligned with a message signal at the eavesdropper to protect it. This alignment makes sure that the information leakage to the eavesdropper is upper bounded by a constant. Therefore, each message signal is protected by one of the cooperative jamming signals at the eavesdropper. In this achievable scheme, both the



[FIG6] An achievable scheme for the wiretap channel with *M*-helpers, based on cooperative jamming and real interference alignment.

legitimate receiver's and the eavesdropper's channel state information (CSI) are used to align message signals and cooperative jamming signals simultaneously at the legitimate receiver and the eavesdropper in the desired manner. More recently, [13] showed that s.d.o.f. of $[M/(M+1)]$ can be achieved without any eavesdropper CSI at the legitimate transmitters. This achievable scheme is illustrated in Figure 7. In this scheme, the legitimate transmitter sends M parts of the message together with one part cooperative jamming signal. This can be interpreted as the legitimate transmitter applying channel prefixing to map its message carrying signal to the channel input. All of the helpers again send cooperative jamming signals. By using only the CSI of the legitimate receiver, all of the $M+1$ cooperative jamming signals are aligned in the same dimension only at the legitimate receiver to occupy the smallest signal space. All of the message signals and cooperative jamming signals are received at random dimensions at the eavesdropper, and there is no strict alignment there. However, one extra cooperative jamming signal coming from the legitimate transmitter ensures that $M+1$ cooperative jamming signals span all of the signal space where message signals reside, limiting the decoding capability of the eavesdropper.

Finally, these ideas of using cooperative jamming signals and alignment can be used in other network structures to determine exact sum s.d.o.f. Reference [35] shows that the exact sum s.d.o.f. of a two-user interference channel with confidential messages is 2/3 and the exact sum s.d.o.f. of a K-user multiple access wiretap channel is $[K(K-1)/K(K-1)+1]$, giving 2/3 for the two-user case.



[FIG7] The achievable scheme for the wiretap channel with *M*-helpers, based on cooperative jamming and real interference alignment, without eavesdropper CSI.

EXPLICIT CODES FOR COOPERATIVE JAMMING

While the fundamental limits of cooperative jamming and the related signal processing techniques are now reasonably well understood, much less is known about the design of explicit and low-complexity codes that are required to achieve the performance predicted by information theory. Nevertheless, recent works on coding for the wiretap channel have highlighted the usefulness of low-density parity-check (LDPC) codes [40], [41] and polar codes [42] to provide information-theoretic secrecy. In this section, we discuss how such constructions extend to cooperative physical-layer security by discussing codes for cooperative jamming.

For brevity and clarity, we consider the two-user multiple access wiretap channel illustrated in Figure 3(a), in which the legitimate users Alice and Charlie wish to transmit secret messages W_1 and W_2, respectively. We also ignore reliability and solely focus on the design of codes that provide secrecy. The messages are encoded into codewords of length n, denoted by X_1^n and X_2^n, respectively, while the eavesdropper observes the symbol-wise interference Z^n of the codewords through a memoryless channel with transition probabilities $p_{Z|X_1X_2}$; in other words, the eavesdropper obtains signals through a multiple access channel. The objective of the legitimate receivers is to design codewords whose interference is detrimental to the eavesdropper, hence the objective is to achieve the opposite result of traditional coding for the multiple access channel.

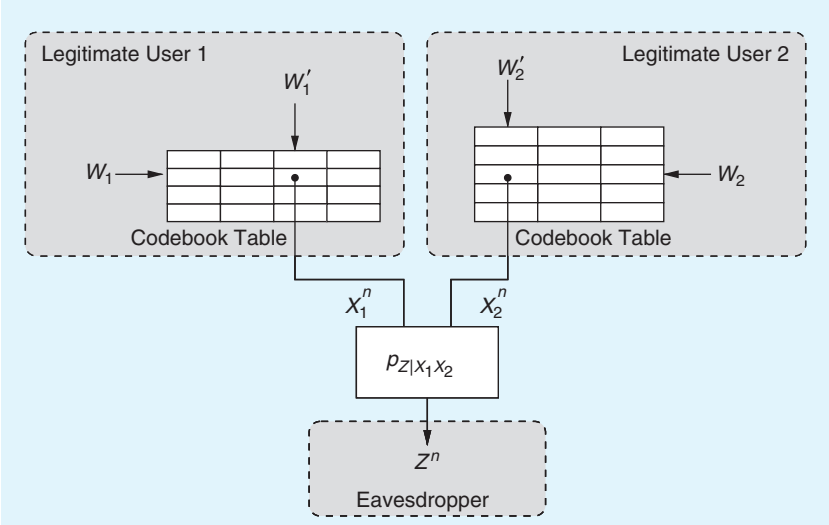
As illustrated in Figure 8, the key ingredients that enable cooperative security are the use of nested codes together with randomization in the encoding process, i.e., stochastic encoding, at both legitimate users. The codeword X_1^n transmitted by the first legitimate user is determined not only by the secret message W_1, but also by an auxiliary message W_1' chosen uniformly at random. Similarly, the codeword X_2^n transmitted by the second legitimate user is determined by the secret message W_2 and an auxiliary message W_2'. One can therefore think of the codebook of each user as the union of nested subcodebooks, each indexed by a different secret message. In Figure 8, subcodebooks consist of the lines of the codebook tables. The main challenge is then to find explicit techniques to construct the codebooks and the subcodebooks. We describe next two design philosophies that can be used to obtain explicit codes.

1) Secrecy from capacity-achieving codes for the multiple access channel: This first design philosophy is based on the observation that the mutual information

rate $[(1/n)/(I(W_1, W_2; Z^n))]$ can be upper bounded as [14], [43]

$$\frac{1}{n} I(W_1, W_2; Z^n) \leq C_{\text{MAC}} - R_1' - R_2' + O(P_e), \tag{5}$$

where C_{MAC} denotes the capacity of the multiple access channel $p_{Z|X_1X_2}$, $R_1' = [(1/n)/(H(W_1'))]$ is the rate of the subcodebooks for User 1, $R_2' = [(1/n)/(H(W_2'))]$ is the rate of the subcodebooks for User 2, and P_e denotes the probability of decoding error of auxiliary messages over the same multiple access channel. Therefore, a sufficient condition to guarantee secrecy is to use subcodebooks such that $R_1' + R_2' \approx C_{\text{MAC}}$ and $P_e \approx 0$, i.e., subcodebooks that are capacity achieving for the multiple access channel. In general, finding capacity-achieving codes for arbitrary channels is challenging, but the capacity-approaching properties of spatially coupled LDPC codes for the multiple access channel provide a partial solution. By appropriately puncturing spatially coupled LDPC codes for the multiple access channel [44], one can obtain the multiple subcodebooks required to guarantee secrecy, and show that information rates as low as 10^{-3} are leaked to the eavesdropper [44]. Note, however, that such a construction only guarantees that the eavesdropper obtains a negligible rate of information.



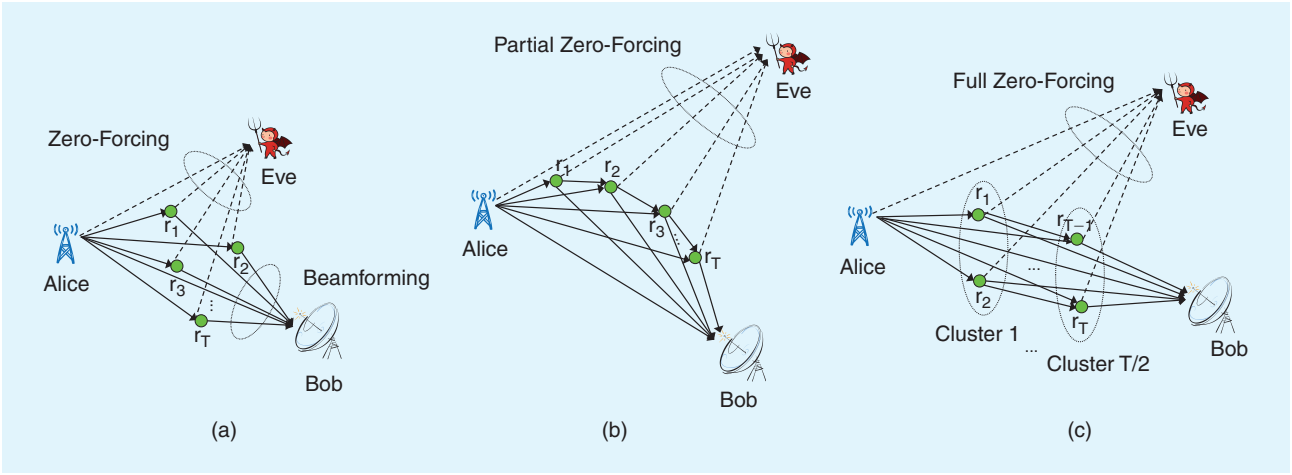
[FIG8] Coding for cooperative jamming. Each legitimate user randomizes his encoding with auxiliary messages.

2) Secrecy from channel resolvability codes for the multiple access channel: A second design philosophy is to understand the mutual information $I(W_1, W_2; Z^n)$ as a Kullback–Leibler divergence and to upper bound it as [45] $I(W_1, W_2; Z^n) \leq \sum_{m_1,m_2} p(m_1, m_2)\, \mathbb{D}\,(p_{Z^n|W_1=m_1,W_2=m_2} \| q_{Z^n})$, where q_{Z^n} is some arbitrary distribution of the eavesdropper's observations and $p_{Z^n|W_1=m_1,W_2=m_2}$ is the distribution of the observations induced by the subcodebooks indexed by m_1 and m_2. Therefore, a sufficient condition to ensure secrecy is to use subcodebooks that always generate the same distribution q_{Z^n}. Codebooks that induce a specific distribution at the output of a multiple access channel are known in information theory as multiple access channel resolvability codes. Few channel resolvability codes are known but, in the case of symmetric channel, polar codes can be used to induce a uniform distribution [42]. Hence, by puncturing polar codes for symmetric multiple access channels, one therefore obtains the subcodebooks of a cooperative jamming code. Although such a code ensures that the eavesdropper obtains negligible information, which is a stronger guarantee that the previous approach, symmetric multiple access channels are not suitable models for wireless channels, which presently limits the range of applications.

COOPERATION IN NETWORKS OF RELAYS

In this section, we consider a network of cooperating partners and allow for passive as well as active cooperation. In particular, we have a legitimate transmitter and a legitimate receiver wanting to have secure communication in the presence of an eavesdropper. In addition, we have a network of N relays, who are willing to help the legitimate pair. Here, we divide the possible ways in which trusted nodes can help the legitimate pair into two: passive (deaf) cooperation, where the cooperating partner either does not hear the transmitted signal from the legitimate transmitter or even if it hears it, ignores it. Cooperative jamming and noise forwarding concepts we have discussed so far fall into this category. Active cooperation, where the cooperating party explicitly utilizes its overheard information to reinforce the message carrying signal in the air by transmitting signals correlated with it. For clarity, we restrict our attention to cooperation schemes with relays employing decode-and-forward (DAF), although other relaying schemes are also possible.

In [21], for the case of a single deaf helper, necessary conditions for each of cooperative jamming with Gaussian noise and noise forwarding to yield a secrecy rate higher than the secrecy capacity of the underlying Gaussian wiretap channel are obtained. In particular, the following conclusion is reached: Depending on the relative location of a helping node with respect to the destination and the eavesdropper, a helping node may either be a useful cooperative jammer or a useful noise forwarder but not both at the same time, or it may not be useful at all as a deaf helper. Another problem with significant practical importance is the problem of relay selection in multiple relay networks in the secrecy context. For example, [16] proposes a scheme that enables an opportunistic selection of two relays to increase security where one relay uses DAF strategy while the other uses cooperative jamming strategy. In [17], again the idea of employing cooperative jammers in a multiple relay network to improve security is adopted, where the eavesdroppers may collude. Reference [21] considers applying both cooperative jamming and noise forwarding strategies in multiple relay networks to improve the secrecy rates that were achieved when



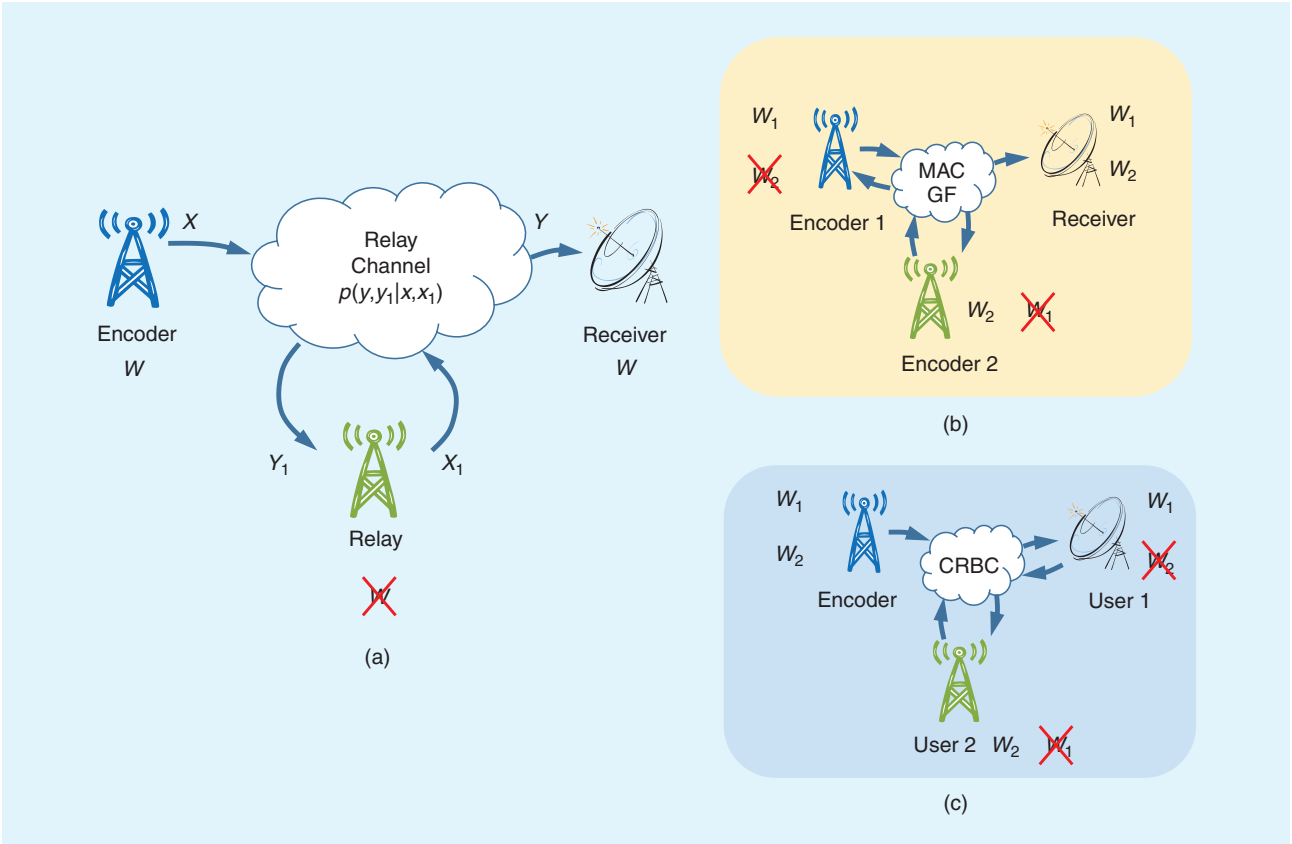
[FIG9] **(a) Multiple relay single-hop strategy. (b) Multiple relay *T*-hop strategy. (c) Multiple relay (*T*/2)-hop strategy.**

only cooperative jamming with Gaussian noise is used. The objective is to select a set of K, $K \leq N$, relays that act as the best deaf helpers. In the special case of $K = 1$, the optimal strategy is obvious and requires $O(N)$ computations. The general relay selection problem, i.e., the case where $K > 1$, has exponential computational complexity; [21] proposed a suboptimal multiple deaf helper selection strategy, which selects at most K relays over at most K selection stages in which the source and the relays negotiate to identify the deaf helpers to be selected one by one in a greedy fashion.

The second mode of cooperation for secrecy we consider is the active mode of cooperation in which a relay listens to the source transmissions and uses its observation to improve the achievable secrecy rate. This model with a single relay is developed in [36]. Reference [22] considers DAF-based cooperation for secrecy in multiple relay networks and proposes three different strategies based on DAF with zero-forcing (DF/ZF). In the first strategy, all the relays decode the source message at the same time, then perform beamforming by transmitting scaled versions of the same signal to the destination; see Figure 9(a). In this strategy, all the relays' signal components can be eliminated from the eavesdropper's observation, i.e., full zero-forcing can be achieved. Although this strategy is simple and allows for full zero-forcing, it has an obvious drawback, which is that the relays which are far from the source could possibly create a bottleneck that limits the achievable rate. To overcome this drawback, in the second strategy, the relays are ordered with respect to their distances from the source and they perform DAF in a multihop fashion [see Figure 9(b)], i.e., the closest relay decodes the source message first, forwards it (with the help of the source) to the second closest relay, and so forth until it reaches the destination. Thus, if the total number of the relays is T, then the transmission of each message block is done in T hops. This strategy overcomes the bottleneck drawback of the first strategy. However, given that all the relays transmit fresh information in every transmission block, only half of the relays' signal components can be forced to zero at the eavesdropper. That is, only partial zero-forcing is possible in this strategy. To achieve full zero-forcing in the second strategy, one needs to set half of the relays' signal components to zero. Based on this observation, the (*T*/2)-hop third strategy combines the advantages of the two aforementioned strategies in an efficient way. That is, the achievable rate is not limited by the worst source-relay channel as in the first strategy, yet we can eliminate all the relays' signals from the eavesdropper's observation. In this strategy, the relays are ordered with respect to their distances from the source and then grouped into clusters of two relays per cluster. The source transmits the message to the relays in the first cluster (closest to the source), which decode the message and forward it (with the help of the source) to the relays in the second cluster and so on so forth until the message is forwarded to the destination; see Figure 9(c). The relays in each clusters do not have any direct communication among them. By properly adjusting the signal coefficients at the relays, one can zero-force all the relays' signals at the eavesdropper. Hence, in typical situations, this strategy provides a reasonable compromise between the first two strategies.

SECRECY AGAINST COOPERATING PARTNERS

So far, we have described the methods by which cooperative behavior of the legitimate parties can provide and improve secrecy of the system, mainly cooperative jamming. In this section, we consider a different paradigm and study the interactions arising between cooperation and secrecy in channel models where the potential cooperating partners (helpers) are also potential eavesdroppers. In these models, all nodes are active participants of a network and are motivated to improve each others' rates; however, they would also like to keep their own messages as confidential as possible. Hence, in these models, each user eavesdrops despite helping the other user. That is, the users are untrusted but unmalicious, usually called honest-but-curious parties. Such communication scenarios have practical applications. For instance, a transmitter can broadcast distinct contents intended for different receivers.



[FIG10] **(a) Relay channel. (b) MAC-GF. (c) CRBC.**

The transmitter would want each receiver to decode only the content they paid for (or subscribed to) and be unable to decode the other content they have not paid for (or not subscribed to). However, since both receivers are valid members of the transmitter's network, they have incentive to (or are required to) help each other. Similarly, there can be military, governmental, banking, or other organizational networks, where even though multiple users are valid members of a network, they may have different clearance levels with respect to the transmitted information. Also, in this scenario, users would be required to help each other but would not be allowed to decode each other's message. The main question in this context is as follows: Is there a tradeoff or a synergy between cooperation and secrecy, i.e., does cooperation cause additional leakage of information, in addition to what wireless communication channel already provides as a result of overheard information, or can cooperation improve secrecy by limiting or reversing the leakage of information?

The first work addressing this question is [46], which considered a basic three-node relay network [Figure 10(a)] from a secrecy point of view. In the model of [46], the transmitter sends a common message to both the legitimate user and the relay in addition to a confidential message directed to the legitimate receiver, which needs to be kept hidden from the relay node. Achievable schemes presented [46] rely on the DAF technique. In particular, the relay uses a partial DAF strategy where the common message and a part of the confidential message is decoded and forwarded to the receiver. The main conclusion that can be drawn from the achievable scheme in [46] is that as long as the relay node uses a DAF-type cooperation, it cannot increase the secrecy rate of the transmitter, even though it can increase its achievable rate. This conclusion is quite intuitive, because although the relay node can increase the rate of the transmitter, it cannot increase it beyond the amount that it itself can decode. Consequently, the secrecy rate, which, roughly speaking, is the difference between the rates of the receiver and the eavesdropper (relay in this case), cannot be increased if the relay node uses a DAF-type cooperation strategy.

The interaction of cooperation and secrecy in this scenario was further studied in [24] by focusing on a special class of relay channels. In this special class, there is an orthogonal link between the relay and the receiver, and the transmitter has a broadcast channel to the relay and the receiver. [24] proposed to use compress-and-forward (CAF) for this channel and analyzed its performance. From a secrecy point of view, the advantage of CAF over DAF is that in CAF, the relay does not need to decode the message, and hence, by using CAF, the relay, in addition to improving the rate of the transmitter, might also improve the secrecy rate of the transmitter. To examine this possibility in more depth, let us focus on the special class of Gaussian relay channels considered in [24]. In this channel, the receiver

observes $Y=(Y_t,Y_r)$, where $Y_t=X+Z_t$, $Y_r=bX_1+Z_r$, and $Y_1=aX+Z_1$, where Z_t, Z_r, Z_1 are independent Gaussian random variables with zero-mean and unit-variance. We also assume $E[X^2]\le P$ and $E[X_1^2]\le P$. For this channel, CAF yields the following secrecy rate:

$$R_s=\frac{1}{2}\log\left(1+P+\frac{a^2P}{1+N_c}\right)-\frac{1}{2}\log(1+a^2P), \qquad (6)$$

where $N_c=[((a^2+1)P+1)/(b^2P(P+1))]$. We can now compare the rate given in (6) with the corresponding wiretap channel, where the relay node does not transmit any signal. We first note that, in the corresponding wiretap channel, secrecy rate is zero whenever $a>1$. However, the rate in (6) can be positive even when $a>1$ if b is sufficiently large, i.e., if the relay-receiver link is strong enough. Although we considered a special class of relay channels in this example, the same conclusion holds for the general Gaussian relay channel. Here, we observed that CAF can increase the secrecy rate with respect to the underlying wiretap channel. The basic reason for this is that, using CAF, the relay node can increase the overall achievable rate of the network to levels which are not decodable at the relay node. This, in effect, increases the difference of the rates in the transmitter-relay and transmitter-receiver links, which, roughly speaking, corresponds to the secrecy rate.

SIGNAL PROCESSING TECHNIQUES AT THE PHYSICAL LAYER CAN FURTHER BE UTILIZED FOR TRANSMITTER AND RECEIVER SIDE PROCESSING/FILTERING FOR SECURITY.

It has also been shown in [47] that, in the absence of the direct link between the legitimate parties, i.e., the two-hop model, where all signals to be communicated from Alice to Bob have to flow through the untrusted relay, combination of cooperative jamming by the destination (Bob), and CAF renders communication secure from the cooperating relay. The recent reference [48] considers the case where the relay may turn malicious and manipulate signals it receives and finds that secure communication and detection of such behavior is still possible via a combination of structured codes and structured cooperative jamming.

Next, we consider more general scenarios where the cooperating partners are active users who have their own information to send as well. First, we consider the multiple access channel with generalized feedback (MAC-GF) [Figure 10(b)] where both users have their own messages to send, and they both receive feedback signals that are correlated with the message of the other user. These signals can be used to cooperate and increase the rates; however, these signals are also the basis for loss of secrecy. In this setup, each user considers the other user both as a cooperating partner and also as an eavesdropper. This channel model can be considered as a two-sided version of the relay channel, where the relaying nodes have their own messages as well. In this channel model, we can observe the implications of the actions (i.e., cooperation) of one user on the rate and secrecy of the other user, as well as on the rate and secrecy of itself. MAC-GF was studied from a secrecy point of view first in [49] and [50]. However, in their setup, the users were not allowed to cooperate. Consequently, the only effect of the feedback signals in [49] and [50] was the loss of secrecy and there was no opportunity to observe the interactions between cooperation and secrecy. This interaction was studied in [51] by allowing users to cooperate. In particular, the reference proposed an achievable scheme relying on CAF and showed that both users can have secrecy against each other by cooperating via a CAF-based cooperation scheme.

Secrecy against cooperating partners was further investigated in the cooperative relay broadcast channel (CRBC) [Figure 10(c)] where a transmitter has messages to send to two receivers over a broadcast channel, and there is a one-sided cooperation link from User 1 to User 2. In this model, User 2 will consider User 1 as a cooperating partner and also an eavesdropper, and User 1 will consider User 2 as an eavesdropper. This model is studied in [25], where a CAF-based achievable scheme is presented to show the beneficial effects of cooperation on secrecy. If User 1 does not transmit any signals, then the channel becomes a Gaussian broadcast channel, and it will be degraded in one of the directions. Consequently, in the underlying broadcast channel, both users cannot have positive secrecy rates simultaneously; only the stronger user can have a nonzero secrecy rate. We observe that if the first user sends cooperative signals using CAF, then both users can have secure communications simultaneously. In addition, if the first user is the weaker user, then it can send jamming signals to make sure that it itself achieves positive secrecy rates. In general, the first user can implement a combined strategy that combines CAF-based cooperation together with jamming to provide both users an array of possible secure rates. The main conclusion that can be drawn from [24], [25], and [51] is that there is a synergy between cooperation and secrecy: an untrusted helper can improve secrecy. However, this improvement in secrecy critically depends on the form of cooperation protocol being used. For example, since in DAF-based strategies the helper needs to decode the message, these strategies cannot improve secrecy against an untrusted helper. On the other hand, since in CAF-based strategies the untrusted helper does not need to decode the message, such strategies may improve secrecy.

CONCLUSIONS

In this article, we have provided a summary of recent advances in physical-layer security techniques for wireless communication systems where cooperating legitimate parties aid in improving the secure communication rates. A variety of canonical scenarios have been outlined, focusing on succinct results that provide fundamental insights. In particular, we have observed that cooperative jamming, where legitimate transmitters aid in improving secure rates for the system as a whole by transmitting noise or structured signals, emerges as a powerful insight to drive signal processing algorithms at the physical layer. In networks

involving multiple antennas, signal processing has been used to design secure beamforming schemes, and in multiuser and/or multiantenna networks signal processing has been used to design secure interference alignment schemes. We have also observed the merit of relays in providing secure source to destination rates via various active cooperation schemes when they are trusted parties and even when they themselves are prevented from decoding the messages they relay. In these cases, signal processing steps in toward the design of distributed cooperation and relay selection schemes. Signal processing techniques at the physical layer can further be utilized for transmitter and receiver side processing/filtering for security. In addition, signal processing can be used to bring information-theoretic approaches from the asymptotic regime to a finite block-length regime as well as in developing practically implementable algorithms. In conclusion, the design of signaling schemes and explicit code constructions for cooperative security at the physical layer thus remains a vibrant area for future research. We expect the cooperative techniques discussed in this work to continue to be useful in various settings, as well as in new models including more powerful and active adversaries.

AUTHORS

Raef Bassily (bassily@psu.edu) received the B.S. degree in electrical and computer engineering and the M.S. degree in engineering mathematics from Cairo University, Giza, Egypt, in 2003 and 2006, respectively. He received the Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park, in 2011. He was a research associate in the Department of Computer Science at the University of Maryland, College Park, from January to August 2012. Since August 2012, he has been a research associate in the Department of Computer Science and Engineering at The Pennsylvania State University. His research interests include information and coding theory, wireless communications, cryptography, physical-layer security, statistical data privacy, and machine learning.

Ersen Ekrem (ersen@umd.edu) received the B.S. and M.S. degrees in electrical and electronics engineering from Bogazici University, Istanbul, Turkey, in 2006 and 2007, respectively. He received his Ph.D. degree from the Department of Electrical and Computer Engineering at the University of Maryland, College Park, in August 2012. Currently, he is with Qualcomm, Santa Clara. He received the Distinguished Dissertation Fellowship from the Electrical and Computer Engineering Department at the University of Maryland, College Park, in 2012. His research interests include information theory and wireless communications.

Xiang He (hexiang129@gmail.com) received B.S. and M.S. degrees in electrical engineering from Shanghai Jiao Tong University, China, in 2003 and 2006, respectively. He received his Ph.D. degree in 2010 from the Department of Electrical Engineering at The Pennsylvania State University and joined Microsoft that same year. In 2010, he received the Melvin P. Bloom Memorial Outstanding Doctoral Research Award from the Department of Electrical Engineering at The Pennsylvania State University and the Best Paper Award of the Communication Theory Symposium at the IEEE International Conference on Communications. His research interests include information theoretic secrecy, coding theory, queuing theory, optimization techniques, distributed detection, and estimation.

Ender Tekin (tekin@psu.edu) received his B.S. degree from Bogazici University in 2000 and his M.S. and Ph.D. degrees from The Pennsylvania State University in 2001 and 2008, respectively. He is currently an associate scientist at the Smith-Kettlewell Eye Research Institute. His research interests include information theory, communications security, machine learning, and multimodal signal processing with applications in rehabilitation engineering. He has been a reviewer for various international conferences and journals and has been a Member of the IEEE since 2000.

Jianwei Xie (xiejw@umd.edu) received the B.S. and M.S. degrees in electronic engineering from Tsinghua University, Beijing, China, in 2006 and 2008, respectively. Currently, he is working toward the Ph.D. degree in the Department of Electrical and Computer engineering at the University of Maryland, College Park. He received the Distinguished Dissertation Fellowship from the Electrical and Computer Engineering Department at the University of Maryland, College Park, in 2013. His research interests include information theory and wireless communications.

Matthieu R. Bloch (matthieu.bloch@ece.gatech.edu) received the engineering degree from Supelec, France, the M.S. degree in electrical engineering from Georgia Tech in 2003, the Ph.D. degree in engineering science from the Universite de Franche-Comte, France, in 2006, and the Ph.D. degree in electrical engineering from Georgia Tech in 2008. Currently, he is an assistant professor in the School of Electrical and Computer Engineering at Georgia Tech. He is a corecipient of the 2011 Joint Paper Award of the IEEE Communications Society and IEEE Information Theory Society and a coauthor of *Physical-Layer Security: From Information Theory to Security Engineering* (Cambridge, 2011).

Sennur Ulukus (ulukus@umd.edu) received her B.S. and M.S. degrees in electrical and electronics engineering from Bilkent University, Ankara, Turkey. She received her Ph.D. degree in electrical and computer engineering from the Wireless Information Network Laboratory, Rutgers University. She is a professor of electrical and computer engineering at the University of Maryland at College Park, where she also holds a joint appointment with the Institute for Systems Research. Prior to joining University of Maryland, she was a senior technical staff member at AT&T Labs Research. Her research interests are in wireless communication theory and networking and network information theory. She received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications and the 2005 National Science Foundation CAREER Award.

Aylin Yener (yener@ee.psu.edu) has been a professor of electrical engineering at The Pennsylvania State University, University Park, since 2010. Her previous academic appointments include associate professor and assistant professor at

The Pennsylvania State University, visiting associate professor at Stanford University (sabbatical leave), and P.C. Rossin assistant professor at Lehigh University. She received her Ph.D. degree from the Wireless Information Network Laboratory, Rutgers University. Her research interests are in information theory, communication theory, and network science, with emphasis on information (theoretic) security, green communications, and fundamental performance limits of wireless networks. She received the National Science Foundation CAREER Award in 2003.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J. (before 1984)*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[3] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[4] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[5] I. Csiszar, "Almost independence and secrecy capacity," *Probl. Inform. Transmiss.*, vol. 32, no. 1, pp. 48–57, 1996.

[6] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology—EUROCRYPT 2000* (Lecture Notes in Computer Science, vol. 1807). Berlin: Springer-Verlag, 2000, pp. 351–368.

[7] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[8] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. IT-24, no. 4, pp. 451–456, July 1978.

[9] M. Medard, "Capacity of correlated jamming channel," in *Proc. 35th Annu. Allerton Conf. Commun., Contr., Comput.*, 1997.

[10] X. He and A. Yener, "Secrecy when the eavesdropper controls its channel states," in *Proc. IEEE Int. Symp. Information Theory*, 2011.

[11] X. He and A. Yener, "Providing secrecy when the eavesdropper channel is arbitrarily varying: A case for multiple antennas," in *Proc. 48th Annu. Allerton Conf. Commun., Contr., Comput.*, 2010.

[12] S. Gerbracht, C. Scheunert, and E. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inform. Forensics Sec.*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[13] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming," in *Proc. Conf. Information Sciences Systems*, 2013.

[14] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[15] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[16] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[17] S. Vasudevan, S. Adams, D. Goeckel, Z. Ding, D. Towsley, and K. K. Leung, "Secrecy in wireless relay channels through cooperative jamming," in *Proc. ACITA 2010*.

[18] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[19] S. Fakoorian and L. Swindlehurst, "Solutions for the MIMO Gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Signal Processing*, vol. 59, no. 10, pp. 5013–5022, Oct. 2011.

[20] R. Bassily and S. Ulukus, "Ergodic secret alignment," *IEEE Trans. Inform. Theory*, vol. 58, no. 3, pp. 1594–1611, Mar. 2012.

[21] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *IEEE Trans. Signal Processing*, vol. 61, no. 6, pp. 1544–1554, Mar. 2013.

[22] R. Bassily and S. Ulukus, "Secure communication in multiple relay networks through decode-and-forward strategies," *J. Commun. Netw.*, vol. 14, no. 4, pp. 352–363, Aug. 2012.

[23] X. He and A. Yener, "Providing secrecy with structured codes: Tools and applications to two-user Gaussian channels," submitted for publication.

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

[25] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inform. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.

[26] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.

[27] M. Jain, J. I. Choi, T. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha, "Practical, real-time, full duplex wireless," in *Proc. 17th Annu. Int. Conf. Mobile Computing and Networking*, 2011.

[28] E. Tekin and A. Yener, "Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy," in *Proc. 44th Annu. Allerton Conf. Commun., Contr., Comput.*, 2006.

[29] E. Tekin and A. Yener, "The multiple access wire-tap channel: Wireless secrecy and cooperative jamming," in *Proc. Information Theory and Applications Workshop*, 2007.

[30] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[31] E. Ekrem and S. Ulukus, "Cooperative secrecy in wireless communications," in *Securing Wireless Communications at the Physical Layer*, W. Trappe and R. Liu, Eds. New York: Springer-Verlag, 2009, pp. 143–172.

[32] X. He and A. Yener, "Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signaling," in *Proc. IEEE Global Telecommun. Conf.*, 2009.

[33] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure degrees-of-freedom of the multiple-access-channel," submitted for publication.

[34] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers," in *Proc. 50th Annu. Allerton Conf. Commun., Contr., Comput.*, 2012.

[35] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," submitted for publication.

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

[37] A. O. Hero, "Secure space–time communication," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.

[38] X. He, "Cooperation and information theoretic security in wireless networks," Ph.D. dissertation, Dept. Elect. Eng., Pennsylvania State Univ., University Park, PA, 2010.

[39] J. Xie and S. Ulukus, "Real interference alignment for the *K*-user Gaussian interference compound wiretap channel," in *Proc. 48th Annu. Allerton Conf. Commun., Contr., Comput.*, 2010.

[40] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channels," *IEEE Trans. Inform. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[41] V. Rathi, R. Urbanke, M. Andersson, and M. Skoglund, "Rate-equivocation optimal spatially coupled LDPC codes for the BEC wiretap channel," in *Proc. IEEE Int. Symp. Information Theory*, 2011.

[42] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inform. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[43] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[44] A. Pierrot and M. Bloch, "LDPC-based coded cooperative jamming codes," *Proc. IEEE Information Theory Workshop*, 2012.

[45] A. Pierrot and M. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Trans. Inform. Forensics Sec.*, vol. 6, no. 3, pp. 595–605, Sept. 2011.

[46] Y. Oohama, "Relay channels with confidential messages," submitted for publication.

[47] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP J. Wireless Commun. Network.*, 2009.

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

[49] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[50] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Information Theory*, 2006.

[51] E. Ekrem and S. Ulukus, "Effects of cooperation on the secrecy of multiple access channels with generalized feedback," in *Proc. Conf. Information Sciences Systems*, 2008.

[SP]