Wireless physical layer security

H. Vincent Poor[a,1] and Rafael F. Schaefer[b]

[a]Department of Electrical Engineering, Princeton University, Princeton, NJ 08544; and [b]Information Theory and Applications Chair, Department of Electrical Engineering and Computer Science, Technische Universität Berlin, 10587 Berlin, Germany

This contribution is part of the special series of Inaugural Articles by members of the National Academy of Sciences elected in 2011.

Contributed by H. Vincent Poor, November 2, 2016 (sent for review June 1, 2016; reviewed by Matthieu R. Bloch and Gregory W. Wornell)

Security in wireless networks has traditionally been considered to be an issue to be addressed separately from the physical radio transmission aspects of wireless systems. However, with the emergence of new networking architectures that are not amenable to traditional methods of secure communication such as data encryption, there has been an increase in interest in the potential of the physical properties of the radio channel itself to provide communications security. Information theory provides a natural framework for the study of this issue, and there has been considerable recent research devoted to using this framework to develop a greater understanding of the fundamental ability of the so-called physical layer to provide security in wireless networks. Moreover, this approach is also suggestive in many cases of coding techniques that can approach fundamental limits in practice and of techniques for other security tasks such as authentication. This paper provides an overview of these developments.

information theory | wireless networks | security

Wireless communication is one of the most ubiquitous of modern technologies. Cellular communication alone is accessible to an estimated 5 billion people, and this is but one of an array of wireless technologies that have emerged in recent decades. Wireless networks are increasingly used for a very wide range of applications, including banking and other financial transactions, social networking, and environmental monitoring, among many others. For this reason, the security of wireless networks is of critical societal interest. Security has traditionally been implemented at the higher, logical layers of communication networks, rather than at the level of the physical transmission medium. For data confidentiality, encryption is the primary method of ensuring secrecy, a method that works well in most current situations. However, in some emerging networking architectures, issues of key management or computational complexity make the use of data encryption difficult. Examples include ad hoc networks, in which messages may pass through many intermediate terminals on the way from source to destination, and sensor or radio-frequency identification (RFID) networks such as might arise in the envisioned Internet of Things, in which the end devices are of very low complexity. For these and other reasons, there has been considerable recent interest in developing methods for secure data transmission that are based on the physical properties of the radio channel (the so-called wireless physical layer). These results are based on information theoretic characterizations of secrecy, which date to some of Claude Shannon's early work on the mathematical theory of communication (1). Whereas Shannon's work focused on symmetric key encryption systems, perhaps a more relevant development in this area was Aaron Wyner's work on the wiretap channel, which introduced the idea that secrecy can be imparted by the communication channel itself without resorting to the use of shared secret keys (2). Although not focusing on wireless networks per se, this work nevertheless lays the mathematical groundwork for the study of this issue on a much broader scale and particularly in the context of wireless networks.

For the reasons noted above, wireless physical layer security has become a major research topic in recent years, and considerable progress has been made in understanding the fundamental ability of the physical layer to support secure communications and in determining the consequent limits of this ability (3, 4). In particular, it has been shown that the two principal properties of radio transmission—namely, diffusion and superposition—can be exploited to provide data confidentiality through several mechanisms that degrade the ability of potential eavesdroppers to gain information about confidential messages. These mechanisms include the exploitation of fading, interference, and path diversity (through the use of multiple antennas), all of which also lead to potential techniques for implementation in practical wireless systems. Moreover, the random nature of wireless channels provides sources of common randomness that can be used to extract shared secret keys from the physical layer, thereby allowing more traditional methods of data protection to be applied.

This paper reviews these developments, beginning with a brief historical account of the use of information theory to characterize secrecy more generally and then discussing the main results for the principal channel models of interest in modern wireless networks. General information theoretic concepts are defined briefly as needed; these are explained in greater depth in ref. 5.

Shannon's Cipher System

Shannon was the first person who studied, in ref. 1, the problem of secure communication from an information theoretic perspective. He considered a noiseless cipher system as illustrated in Fig. 1. A transmitter (Alice) wishes to convey a message M to a legitimate receiver (Bob) while keeping it secret from an eavesdropper (Eve), who intercepts the transmission. Alice and Bob share a common secret key K that is unknown to Eve. To establish the secrecy of the message, Alice uses this key to encrypt the message M into a codeword X, which is then transmitted.

Significance

Security is a very important issue in the design and use of wireless networks. Traditional methods of providing security in such networks are impractical for some emerging types of wireless networks due to the light computational abilities of some wireless devices [such as radio-frequency identification (RFID) tags, certain sensors, etc.] or to the very large scale or loose organizational structure of some networks. Physical layer security has the potential to address these concerns by taking advantage of the fundamental ability of the physics of radio propagation to provide certain types of security. This paper provides a review of recent research in this field.

Author contributions: H.V.P. and R.F.S. designed research, performed research, and wrote the paper.

Reviewers: M.R.B., Georgia Institute of Technology; and G.W.W., Massachusetts Institute of Technology.

The authors declare no conflict of interest.

Freely available online through the PNAS open access option.

[1]To whom correspondence should be addressed. Email: poor@princeton.edu.

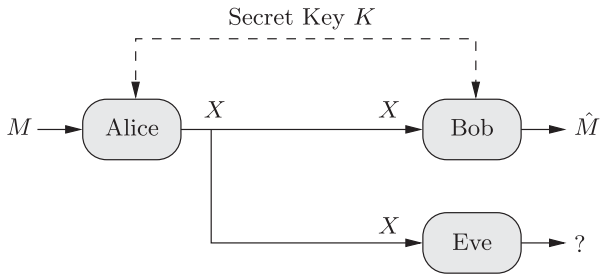

Fig. 1. Shannon's cipher system.

Accordingly, Bob uses K to decrypt the received codeword X to recover M.

A communication scheme is considered to be secure if the mutual information between the message M and the codeword X, which is overheard by Eve, is exactly zero, i.e., $I(M;X)=0$. Mutual information is defined in terms of (Shannon) entropies as $I(M;X)=H(M)-H(M|X)$, where the entropy $H(M)=-\sum p(m)\log p(m)$ describes the uncertainty about the random variable M, where $p(m)$ is the probability with which M takes on the value m, whereas the conditional entropy $H(M|X)$ describes remaining uncertainty in M after X has been observed. $I(M;X)=0$ thus implies that the uncertainty $H(M)$ about the message M is equal to the uncertainty $H(M|X)$ when the codeword X is given. In other words, the message and the codeword must be statistically independent. This condition is termed perfect secrecy and implies that the codeword X reveals no information about the message M. As a consequence, even if Eve has unbounded computational capabilities, the best strategy of Eve to infer the confidential information is to throw away the observed codeword and to simply guess the transmitted message. Shannon showed that perfect secrecy can be achieved, but only if the entropy $H(K)$ of the secret key K is at least as large as the entropy $H(M)$ of the confidential message M (1); i.e., $H(K)\geq H(M)$.

Assuming the message and the secret key to be sequences of binary numbers, perfect secrecy is achieved by the so-called one-time pad approach (6), where the codeword is simply the binary addition [exclusive or (XOR) operation] of the message and the secret key; i.e., $X=M\oplus K$. This idea extends beyond the binary case and the result holds in a much more general setting, which is known as the crypto lemma (7).

The observation that Alice and Bob must share a secret key of the same length as the message they want to exchange seems discouraging at first. But this mainly stems from the fact that the communication channel is assumed to be noiseless so that Eve observes exactly the same as Bob. However, the physical layer especially in wireless communication systems is anything but noiseless. In the following we will see that this imperfection of the communication channel can be explicitly exploited to establish secrecy by physical layer methods without the need of a shared secret key.

Wyner's Wiretap Channel

The wiretap channel was introduced by Wyner (2) and its communication task is similar to Shannon's cipher system: Alice wants to transmit a confidential message to Bob while keeping it secret from Eve. The wiretap channel generalizes the previous scenario by considering noisy communication channels as shown in Fig. 2. However, no secret key is available to the legitimate users.

Accordingly, the objective is now twofold: Alice must encode the message M into a codeword X^n of length n such that Bob, having received Y^n, can reliably recover the message; i.e.,

$$\mathbb{P}\{\hat{M}\neq M\}\underset{n\to\infty}{\longrightarrow}0.$$

Note that a codeword of length n makes use of the channel n times; i.e., $X^n=(X_1,...,X_n)$, where X_i is sent in the ith channel use. Similarly, $Y^n=(Y_1,...,Y_n)$ and $Z^n=(Z_1,...,Z_n)$ describe corresponding channel outputs at the legitimate receiver and eavesdropper, respectively.

At the same time, the message must be kept secret from Eve. An issue then is how to specify secrecy in this setting, which is discussed next.

Secrecy Criterion. Shannon's cipher system considered the criterion of perfect secrecy. This is a very stringent criterion as it requires strict statistical independence between the message M and the channel output Z^n at Eve. In particular, when the communication channel is noisy, this is hard to realize and it is reasonable to relax the criterion by requiring statistical independence only asymptotically in the block length n.

Having in mind that the channel output at Eve should not reveal any information about the confidential message, Wyner defined secrecy in terms of equivocation, or conditional entropy (2). Specifically, he required that the conditional entropy $\frac{1}{n}H(M|Z^n)\approx\frac{1}{n}H(M)$ so that the knowledge of the channel output Z^n does not decrease the uncertainty rate about the message M; in other words, it does not provide any information about M. This criterion is known as weak secrecy and is often equivalently written in terms of mutual information as

$$\frac{1}{n}I(M;Z^n)\underset{n\to\infty}{\longrightarrow}0.$$

This quantity describes the information leaked about M to Eve in terms of a rate due to the normalization by the block length n. This definition of secrecy has its vulnerabilities (8) and can be strengthened by dropping the division by n to

$$I(M;Z^n)\underset{n\to\infty}{\longrightarrow}0.$$

This condition is termed strong secrecy and the intuition is to have the total amount of information leaked to Eve vanish as $n\to\infty$. Strong secrecy for the wiretap channel was first considered in refs. 9 and 10. Recently, different approaches to achieve strong secrecy were presented in refs. 11–15. One might question whether this definition for secrecy is meaningful. And indeed, strong secrecy ensures that the decoding error approaches one exponentially fast for any decoding strategy Eve may use (16). This demonstrates the usefulness of the strong secrecy criterion and establishes a desirable and practically relevant operational meaning.

Recently, this criterion was further strengthened by considering semantic security (17). Here, Eve is not only not able to decode the transmitted message, but also not able to obtain any information about it at all.

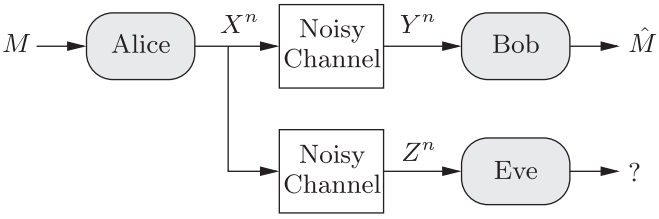

Fig. 2. Wyner's wiretap channel.

Secrecy Capacity. Recall that Alice must encode the message into a codeword such that it is useful for Bob to recover the transmitted message (reliability) and at the same time the same codeword is useless for Eve (security). These two requirements seem to be conflicting and it is not obvious that it is possible to achieve both simultaneously.

Surprisingly, it is indeed possible and the so-called secrecy capacity characterizes the maximal rate at which both requirements are met. For discrete memoryless channels, for which the relation between the transmitted input and received output symbols at each independent channel use can be described by a conditional probability distribution of the channel output given the channel input, Wyner established the secrecy capacity in ref. 2 for the case of degraded channels, i.e., channels for which $X - Y - Z$ form a Markov chain, which means that X and Z are statistically independent conditioned on Y. This result was subsequently generalized by Csiszár and Körner to the general, nondegraded case in ref. 18.

The secrecy capacity of the discrete memoryless wiretap channel is given by

$$C_S = \max_{V-X-(Y,Z)} \big(I(V;Y) - I(V;Z)\big), \qquad [1]$$

where the maximization is over all random variables V and X such that the Markov chain relationship $V - X - (Y, Z)$ is satisfied. (The prefixed V introduces artificial noise into the system and serves to make the eavesdropper channel noisier. This is known as channel prefixing.) Intuitively, the mutual information term $I(V;Y)$ represents the channel quality of the legitimate link and describes the rate at which Alice can reliably transmit to Bob. Accordingly, the term $I(V;Z)$ represents the channel quality of the eavesdropper link and the maximum transmission rate is penalized exactly by this quantity. Another important observation is that to have a positive secrecy capacity, the channel to Bob has to be "less noisy" than the channel to Eve; i.e., $I(V;Y) > I(V;Z)$ for some V. This means Alice and Bob must have an advantage over Eve at the physical layer itself.

The crucial idea for achieving the secrecy capacity is the following: Instead of using all of the available resources for message transmission, a certain part of them are used for randomization by adding "dummy" messages unknown to Bob and Eve. Specifically, for each confidential message Alice wants to transmit, there are multiple valid codewords and a stochastic encoder chooses one of them uniformly at random. The key idea is now to choose the randomization rate for each confidential message roughly as $I(V;Z)$, i.e., according to Eve's channel quality. Thus, Eve will be saturated with the useless information carried by the dummy variables, leaving no remaining resources for decoding the confidential message itself (19). Because the channel quality to Bob supports reliable transmission roughly at rate $I(V;Y)$, the remaining rate available for secure transmission of the confidential message is $I(V;Y) - I(V;Z)$ as Bob usually has to decode both the confidential message and the dummy variables to recover the correct message.

Secure Communication over Wireless Channels

In this section, the information theoretic approaches to security discussed above for discrete memoryless channels are extended to models for physical wireless channels. Wireless physical layer security is one of the key applications of these concepts, as a signal broadcast over a wireless medium is not only received by its intended receiver but also easily eavesdropped upon by nonlegitimate receivers. As we have noted above, the imperfection of the wireless medium will help establish security by exploiting the noisy channel.

Gaussian Wiretap Channels. The Gaussian wiretap channel is the most basic model for a wireless channel, having linear time-invariant multiplicative links corrupted by additive white Gaussian noise. When Alice transmits a signal X_i, the received signals $Y_{B,i}$ at Bob and $Y_{E,i}$ at Eve at channel use i can then be expressed as

$$Y_{B,i} = h_B X_i + N_{B,i} \quad \text{and} \quad Y_{E,i} = h_E X_i + N_{E,i}, \qquad [2]$$

where h_B and h_E are the channel gains between Alice and Bob and between Alice and Eve, respectively, and $N_{B,i}$ and $N_{E,i}$ are additive white Gaussian noises, independent of the transmitted signals, with zero means and variances σ_B^2 and σ_E^2, respectively. Here, white noise refers to a random process that is independent from channel use to channel use.

Considering an average transmit power constraint of P, the secrecy capacity of the Gaussian wiretap channel was established in ref. 20 and is given by

$$C_S = \frac{1}{2}\log\Big(1 + \frac{P|h_B|^2}{\sigma_B^2}\Big) - \frac{1}{2}\log\Big(1 + \frac{P|h_E|^2}{\sigma_E^2}\Big).$$

The secrecy-capacity–achieving strategy is to transmit with full power P and to choose the input signals according to a Gaussian distribution. This latter choice is by no means obvious, as Gaussian input maximizes the information flow to Bob, but at the same time also to Eve. Interestingly, the secrecy capacity in this case turns out to be equal to the difference between the main channel's Shannon capacity and the eavesdropper channel's Shannon capacity. From this it follows immediately that secure communication is possible if and only if Bob has a better channel than Eve in the sense that the signal-to-noise ratio of the main channel must be larger than that of the eavesdropper channel; i.e., $|h_B|^2/\sigma_B^2 > |h_E|^2/\sigma_E^2$. We return to this point later.

Multiantenna Wiretap Channels. Systems with multiple transmit and receive antennas, so-called multiple-input multiple-output (MIMO) systems, can improve the performance of wireless transmission significantly and hence form the basis of most modern high-capacity wireless systems. Thus, the MIMO wiretap channel is particularly of interest. Accordingly, Alice, Bob, and Eve are assumed to have multiple transmit and receive antennas, respectively. Note that a multiantenna eavesdropper can also be interpreted as multiple single-antenna eavesdroppers that cooperate.

When Alice transmits a vector-valued signal $\boldsymbol{X}_i$, the received vector-valued signals $\boldsymbol{Y}_{B,i}$ at Bob and $\boldsymbol{Y}_{E,i}$ at Eve can be expressed as

$$\boldsymbol{Y}_{B,i} = \boldsymbol{H}_B\boldsymbol{X}_i + \boldsymbol{N}_{B,i} \quad \text{and} \quad \boldsymbol{Y}_{E,i} = \boldsymbol{H}_E\boldsymbol{X}_i + \boldsymbol{N}_{E,i},$$

where $\boldsymbol{H}_B$ and $\boldsymbol{H}_E$ are matrices containing multiplicative channel gains, and $\boldsymbol{N}_{B,i}$ and $\boldsymbol{N}_{E,i}$ are independent (of each other and for different values of i) additive Gaussian noise vectors at Bob and Eve with zero means and identity covariance matrices. The transmission is subject to an average transmit power constraint $tr(\boldsymbol{Q}) \le P$ with $\boldsymbol{Q} = \mathbb{E}[\boldsymbol{X}_i\boldsymbol{X}_i^T]$ being the covariance matrix of the transmitted signal.

The secrecy capacity of the MIMO Gaussian wiretap channel was established in refs. 21 and 22 and is given by

$$C_S = \max_{tr(\boldsymbol{Q})\le P} \left(\frac{1}{2}\log\det\Big(\boldsymbol{I} + \boldsymbol{H}_B\boldsymbol{Q}\boldsymbol{H}_B^T\Big) - \frac{1}{2}\log\det\Big(\boldsymbol{I} + \boldsymbol{H}_E\boldsymbol{Q}\boldsymbol{H}_E^T\Big)\right). \qquad [3]$$

Similarly to the scalar case, capacity is achieved by transmitting with full power P and by choosing Gaussian-distributed input symbols. Although, in principle, the secrecy capacity of the MIMO wiretap channel is given by the above relation, it remains to find the optimal transmit covariance matrix $\boldsymbol{Q}$ that maximizes the rate in **[3]**. Analytically, this is a nontrivial task as

the corresponding optimization problem is nonconvex in general. Accordingly, the optimal transmit covariance matrix has been characterized only for certain special cases. For example, the optimal transmit strategy is known for the general matrix power constraint $\boldsymbol{Q} \preccurlyeq \boldsymbol{S}$ with $\boldsymbol{S} \succcurlyeq \boldsymbol{0}$ being a positive semidefinite matrix (23), full-rank channels, or isotropic eavesdroppers (24).

A scenario that is completely understood is the multiple-input single-output wiretap channel, in which Alice has multiple transmit antennas, Bob has a single receive antenna only, and Eve may have multiple receive antennas. In this case, the optimal transmit covariance matrix is known in closed form (21). Denoting the channel to Bob by the vector $\boldsymbol{h}_B$ and that to Eve by the matrix $\boldsymbol{H}_E$, the solution of the secrecy rate maximization problem in **[3]** is

$$C_S = \frac{1}{2} \log \left(\lambda_{\max}(\boldsymbol{I} + P\boldsymbol{h}_B\boldsymbol{h}_B^T, \boldsymbol{I} + P\boldsymbol{H}_E^T\boldsymbol{H}_E) \right),$$

with $\lambda_{\max}$ the largest generalized eigenvalue of the two matrices $\boldsymbol{I} + P\boldsymbol{h}_B\boldsymbol{h}_B^T$ and $\boldsymbol{I} + P\boldsymbol{H}_E^T\boldsymbol{H}_E$. The optimal transmit strategy achieving the secrecy capacity is to form a beam in the direction of the generalized eigenvector corresponding to $\lambda_{\max}$.

Partial Channel State Information. The previous discussions have in common that knowledge of the gains of all channels (including those to eavesdroppers) is available to the legitimate users. This condition is termed perfect channel state information (CSI) and such idealized communication assumptions allow one to obtain important insights and to develop an understanding of the fundamental principles of wireless physical layer security. However, due to the nature of the wireless channel, but also due to practical limitations such as inaccurate channel state estimation or limited feedback schemes, practical systems always have to deal with limited CSI. In particular, perfect eavesdropper CSI is questionable unless the eavesdroppers are otherwise legitimate network participants, as malevolent eavesdroppers will not provide any information about their channels or may even jam or otherwise influence the legitimate channel. A survey on secure communication under channel uncertainty and adversarial attacks can be found in ref. 25.

A realistic model for the unpredictable nature of the wireless channel and the imperfections of practical implementations is to assume that the actual realization of the channel gains is unknown to Alice and Bob but is known to lie in an uncertainty set of possible channels. This is the concept of compound channels and it accordingly requires reliability and secrecy for all possible channel realizations in this uncertainty set. Such a guaranteed performance criterion is particularly relevant for the transmission of confidential information that must be kept secret regardless of the actual channel conditions.

The compound wiretap channel has been studied, for example, in refs. 16, 26, and 27. In this scenario, the legitimate channel and eavesdropper channel are not known, but belong to uncertainty sets $\mathcal{H}_B$ and $\mathcal{H}_E$. Such channels can be studied abstractly, but there are also useful concrete versions of possible uncertainty sets. For example, due to limited channel estimation capability, the true channel to Bob might be considered to be in a certain neighborhood of its estimated version. Accordingly, a reasonable uncertainty set is given by a (spherical) set

$$\mathcal{H}_B = \left\{ \boldsymbol{H}_B : \boldsymbol{H}_B = \boldsymbol{H}_0 + \Delta\boldsymbol{H}, \|\Delta\boldsymbol{H}\|_2 \leq \epsilon \right\} \qquad \textbf{[4]}$$

with $\| \cdot \|_2$ the spectral norm. Then, ϵ describes the maximum estimation error $\Delta\boldsymbol{H}$ around the estimated channel $\boldsymbol{H}_0$. Another uncertainty model is to assume that the received channel gain for the eavesdropper is limited; i.e.,

$$\mathcal{H}_E = \left\{ \boldsymbol{H}_E : \|\boldsymbol{H}_E\|_2 \leq \epsilon \right\}. \qquad \textbf{[5]}$$

Here, $\|\boldsymbol{H}_E\|_2$ corresponds to the largest channel gain, which is thus assumed to not exceed ϵ. Such an uncertainty set models, for example, the scenario in which an eavesdropper cannot approach the transmitter beyond a minimum protection distance. All such scenarios are covered by the concept of compound channels.

Assuming **[4]** and **[5]** to be the uncertainty sets for Bob's and Eve's channels yields a compound wiretap channel that reflects two practically relevant points: First, Eve's desire is to be confidential so that only minimal CSI is available to Alice. It might be known only that Eve is beyond a certain protection distance, as noted above. And second, Bob on the other hand wants to maximize the rate and, accordingly, is willing to share his CSI with Alice. However, due to practical limitations only a channel estimate is available, resulting in additive uncertainty. This model is studied in ref. 27.

Determining the secrecy capacity of the compound wiretap channel is a challenging task and it is known only for certain special cases. For degraded channels, i.e., for which each potential eavesdropper channel realization is a degraded version of all possible legitimate channel realizations, the secrecy capacity has been established for refs. 16 and 26 for discrete memoryless channels and in ref. 26 for MIMO Gaussian channels. The compound MIMO wiretap channel above with uncertainty sets **[4]** and **[5]** is not degraded and is one of the few examples for which the secrecy capacity has been established for the nondegraded case:

$$C_S = \max_{tr(\boldsymbol{Q}) \leq P} \left(\min_{\boldsymbol{H}_B \in \mathcal{H}_B} \frac{1}{2} \log\det\left(\boldsymbol{I} + \boldsymbol{H}_B\boldsymbol{Q}\boldsymbol{H}_B^T\right) - \max_{\boldsymbol{H}_E \in \mathcal{H}_E} \frac{1}{2} \log\det\left(\boldsymbol{I} + \boldsymbol{H}_E\boldsymbol{Q}\boldsymbol{H}_E^T\right) \right).$$

The analysis reveals the characteristic structure of secure communication under channel uncertainty. The maximum transmission rate is limited by the worst channel to Bob and by the best channel to Eve. This result confirms the intuition that for guaranteeing reliable and secure communication, one has to be prepared for the worst channel conditions. This result further shows how the performance degrades because of channel uncertainty.

Fading Wiretap Channels. In the above discussion, the channel has been considered to be fixed during the entire duration of transmission. In particular, for the previously discussed Gaussian wiretap channel, the multiplicative channel gains h_B and h_E in **[2]** are constant. For wireless channels this is rarely the case because multipath propagation and interference usually result in changing communication conditions, particularly for mobile networks. This phenomenon is known as fading. In such an environment, the input–output relations of the channels are typically modeled as

$$Y_{B,i} = h_{B,i}X_i + N_{B,i} \quad \text{and} \quad Y_{E,i} = h_{E,i}X_i + N_{E,i},$$

where all $h_{B,i}$, $h_{E,i}$, $N_{B,i}$, and $N_{E,i}$ are mutually independent. Here, $h_{B,i}$ and $h_{E,i}$ are fading coefficients that characterize the communication conditions at channel use i. The input signal is subject to an average power constraint $\frac{1}{n}\sum_{i=1}^n \mathbb{E}[X_i^2] \leq P$ and the noise processes, which are independent from channel use to channel use, are Gaussian with zero means and variances σ_B^2 and σ_E^2 respectively, as before.

For ergodic fading channels, the fading coefficients are independent and identically distributed and are allowed to change from channel use to channel use. Thus, Alice, Bob, and Eve might experience a different fading state for each channel use. Assuming that all terminals have perfect CSI about the current fading state, so-called instantaneous CSI, the ergodic secrecy capacity has been studied in ref. 28 and is given as

$$C_S = \max_{\mathbb{E}_A[\gamma] \leq P} \mathbb{E}_A \left[\frac{1}{2} \log\left(1 + \frac{\gamma|h_B|^2}{\sigma_B^2}\right) - \frac{1}{2} \log\left(1 + \frac{\gamma|h_E|^2}{\sigma_E^2}\right) \right]$$

with γ the power allocation (to be explained below) and

$$A = \left\{ (h_B, h_E) : \frac{|h_B|^2}{\sigma_B^2} > \frac{|h_E|^2}{\sigma_E^2} \right\} \quad [6]$$

so that the expectation is taken over all fading realizations in which Bob experiences a better channel in terms of signal-to-noise ratio than Eve; i.e., $\mathbb{E}_A[\cdot]$ denotes the expectation over all $(h_B, h_E) \in A$.

The key idea behind this result is that the instantaneous CSI allows one to decompose the fading channel into a set of parallel and time-invariant channels. Now, each fading realization corresponds to a particular wiretap channel and it remains to determine the optimal power allocation γ between all these parallel wiretap channels. Obviously, power is allocated only to those fading realizations in which Bob experiences a better channel than Eve [6]. The fading wiretap channel has been intensively discussed in refs. 28–30. In ref. 31 a layered decoding and secrecy approach is discussed, which adapts to the channel quality without requiring perfect CSI.

Having a closer look at the secrecy capacity of the (static) wiretap channel and the fading wiretap channel, one observes the following. Whereas for the (static) wiretap channel secure communication is possible only if Bob has a better channel than Eve, i.e., $|h_B|^2/\sigma_B^2 > |h_E|^2/\sigma_E^2$, for the fading wiretap channel it suffices to have $\mathbb{P}\{|h_B|^2/\sigma_B^2 > |h_E|^2/\sigma_E^2\} > 0$ to have a positive secrecy capacity. Thus, interestingly, fading is actually beneficial for communicating confidential information. Even if Eve's channel is better than Bob's on average, the ergodic secrecy capacity is positive, because whenever Bob experiences a better channel than Eve instantaneously (which will happen infinitely often), this fading realization can be exploited for secure communication.

Physical Layer Security in Wireless Networks

There has been considerable effort in extending and generalizing concepts and results for the wiretap channel to more complex multiuser scenarios as well. We briefly discuss the practically relevant models of the broadcast channel, multiple access channel, interference channel, and relay channel. These channels give insight into the properties of more complex networks.

Broadcast Channel. The broadcast channel describes the communication scenario in which one sender transmits information to several receivers. For example, this channel describes the downlink phase of a cellular communication system in which a base station transmits data to several mobile users.

The broadcast channel with confidential messages models the communication scenario in which one transmitter Alice transmits a common message M_0 to two receivers Bob 1 and Bob 2 and a confidential message M_1 to one receiver, say Bob 1, which must be kept secret from the other one. Thus, Bob 2 is a legitimate receiver for the common message M_0 and, at the same time, an eavesdropper for the confidential message M_1. This scenario models situations, for example, in which some (basic) content is multicast while other (premium) content is unicast. It was introduced by Csiszár and Körner (18) and is depicted in Fig. 3. Here, instead of a single secrecy capacity, we have a region of possible reliable rates R_0 for the common message and secrecy rates

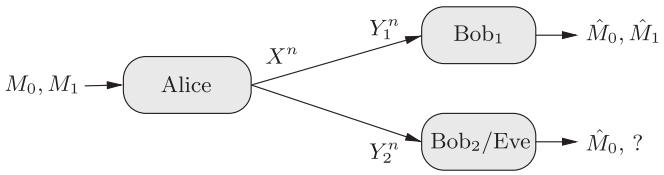

Fig. 3. Broadcast channel with confidential messages.

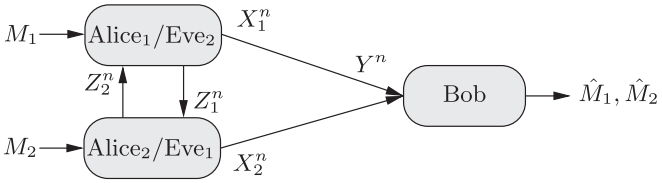

Fig. 4. Multiple-access channel with confidential messages.

R_1 for the confidential message. The secrecy capacity region has been established and is given by all rate pairs (R_0, R_1) that satisfy

$$R_0 \le \min\{I(U; Y_1), I(U; Y_2)\}$$
$$R_1 \le I(V; Y_1|U) - I(V; Z|U)$$

for random variables $U - V - X - (Y_1, Y_2)$. The basic coding idea for achieving this rate region is based on a combination of superposition coding and wiretap coding. The common message M_0 designated for both receivers is encoded first and represented by the auxiliary random variable U. As M_0 must be decoded at both receivers, the corresponding rate is limited by the weaker of the channel qualities to Bob 1, i.e., $I(U; Y_1)$, and to Bob 2, i.e., $I(U; Y_2)$. Then, superimposed on that, the confidential message M_1 is encoded in V according to the same principle as for the wiretap channel discussed above. Accordingly, the confidential rate is limited by a similar difference of both channel qualities but conditioned on U because the common message is known at both receivers.

In a similar way to that for the wiretap channel, the broadcast channel with confidential messages has been subsequently extended into several directions as well, including MIMO Gaussian channels (32), channels with partial CSI (33), and fading channels (28).

Multiple-Access Channel. The multiple-access channel is the counterpart to the broadcast channel: Multiple senders transmit information to a single receiver. An example of where this occurs is in the uplink phase of a cellular system in which several mobile users transmit data to a base station.

In a multiple-access channel with confidential messages two senders Alice 1 and Alice 2 transmit confidential messages M_1 and M_2 to a single receiver Bob. Each transmitter overhears the transmission of the other one so that Alice 1 and Alice 2 must send their confidential messages such that they are decodable by Bob but leak no information to the other transmitter. This situation is visualized in Fig. 4. Again, we have a region of secret rates for the two users' messages. Inner and outer bounds on this region have been derived in ref. 34, although the secrecy capacity region itself remains unknown.

A slightly different setting is given by the multiple-access wiretap channel in which both transmitters are trustworthy but their communication must be secured from an external eavesdropper. This situation has been studied, for example, in refs. 35 and 36. Similar to the multiple-access channel with confidential messages the secrecy capacity region is unknown and only inner and outer bounds have been established so far.

Interference Channel. The interference channel describes the communication scenario in which multiple transmitter–receiver pairs interfere with each other. Each sender is interested only in transmitting information to its designated receiver. However, due to the open nature of the wireless medium, the transmitted signals are received not only by the intended receivers but also by the other users.

The interference channel with confidential messages considers two transmitters Alice 1 and Alice 2 who wish to transmit their confidential messages M_1 and M_2 to their respective receivers

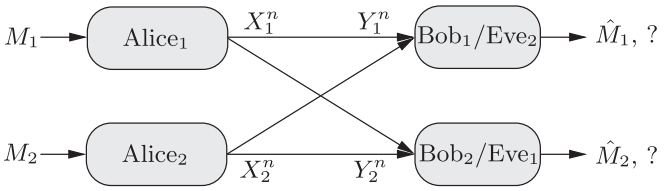

Fig. 5. Interference channel with confidential messages.

Bob 1 and Bob 2. Because both transmissions interfere with each other, each transmitter must encode and transmit its message in such a way that it is kept secure from the counterpart receiver. This is shown in Fig. 5. Inner and outer bounds on the secrecy capacity region for this channel have been established in refs. 37 and 38.

A different communication scenario is given by the cognitive interference channel with one common and one confidential message. Here, the common message is known to both transmitters and must be conveyed to both receivers whereas the confidential message is known only at one transmitter and must be conveyed to its respective receiver, keeping the other receiver ignorant of it. Unlike the other interference scenarios, the secrecy capacity region is known in this case (39).

Relay Channel. The aim of a relay is to support the communication between a transmitter and a receiver. Relays are used, for example, for coverage and range extension or to increase the maximal transmission rate.

The relay channel with confidential messages considers the scenario in which the sender Alice wishes to transmit a confidential message to receiver Bob. The transmission is supported by an untrusted relay so that Alice must encode and transmit the message in such a way that the relay is able to help the communication, but does not get any information about the message. This has been studied in refs. 40 and 41.

The relay channel with an external eavesdropper differs from the previous scenario by having a trusted relay, but the confidential transmission must be secured against an external eavesdropper. This situation is considered in ref. 42.

Secret-Key Generation

In the previous discussions we saw how information theoretic approaches can be used to secure a confidential message transmission over a wireless channel. We now discuss how these information theoretic approaches can be used to generate secret keys based on public discussion and subsequently with the help of wireless channels. Surveys of the use of the wireless physical layer for secret-key generation can be found in refs. 43 and 44.

Public Discussion. Secret-key generation using public discussion was first considered simultaneously by Ahlswede and Csiszár (45) and Maurer (46). In this setting the two terminals Alice and Bob observe correlated versions Y_A^n and Y_B^n of a common random source. Based on these observations both terminals want to agree on the same secret key; i.e., $\mathbb{P}\{K_A \neq K_B\} \to 0$ as $n \to \infty$, where K_A and K_B are secret keys generated at Alice and Bob, respectively. To do so, they are allowed to exchange unlimited information (in multiple iterations) via a noiseless public channel. However, this channel is eavesdropped upon so that whatever is exchanged via public discussion must not reveal any information about the secret key itself. This condition is modeled similarly to the wiretap channel by adopting a strong secrecy criterion,

$$I(\Phi; K_A, K_B) \underset{n\to\infty}{\longrightarrow} 0,$$

where Φ denotes the public discussion over the public channel. In other words, the secret key must be independent of the public discussion. This scenario is shown in Fig. 6.

The aim is now to determine the secret-key capacity, which characterizes the maximal rate at which secret keys can be generated. In refs. 45 and 46 it has been shown that for the case of unlimited public communication, the secret-key capacity is

$$C_K = I(Y_A; Y_B). \quad \textbf{[7]}$$

Moreover, it has been shown that this rate can be achieved by a single one-way communication from Alice to Bob.

The crucial idea for generating a uniformly distributed secret key of rate **[7]** is based on Slepian–Wolf coding (5) and can be outlined as follows. All sequences Y_A^n that can be observed by, say, Alice are divided into bins, with each one containing $2^{nI(Y_A;Y_B)}$ sequences. Now, when Alice observes Y_A^n, she sets the secret key to the index of the particular sequence and sends only the bin index (but not the index of the sequence itself) over the noiseless channel to Bob. Based on the Slepian–Wolf coding idea, having observed Y_B^n this bin index is sufficient for Bob to infer the other observation Y_A^n. Thus, Bob is able to choose the same secret key as Alice. As the bin index and the sequence index are independent, no information about the secret key is leaked to Eve.

In the previous model, Eve was able to eavesdrop upon the public communication only over the noisy channel. This has been extended by allowing Eve to further observe its own correlated observation Y_E^n of the common random source as depicted in Fig. 6. Whereas for the previous scenario the secret-key capacity is known, this is no longer the case when Eve has observed her own realization. Only upper and lower bounds on the secret-key capacity C_K are known: $I(Y_A; Y_B) - \min\{I(Y_A; Y_E), I(Y_B; Y_E)\} \leq C_K \leq \min\{I(Y_A; Y_B), I(Y_A; Y_B|Y_E)\}$. Although arbitrary information exchange between Alice and Bob is allowed in principle, the lower bound is achieved by a one-way communication from Alice to Bob or Bob to Alice only. Comparing this rate with the rate in **[7]**, it can be interpreted as the maximum secret-key rate $I(Y_A; Y_B)$ that can be generated minus some information leakage $\min\{I(Y_A; Y_E), I(Y_B; Y_E)\}$ to Eve. This reveals the same structure as that for the secrecy capacity of the wiretap channel in **[1]**. However, it is possible to control whether information is leaked from Alice, $I(Y_A; Y_E)$, or from Bob, $I(Y_B; Y_E)$.

In the above setting, the public communication was unlimited in the sense that no restrictions on the corresponding communication rate have been made. In practical applications, however, there might be such restrictions that then result in a certain degradation in secret-key capacity (47).

Wireless Channels. Now we extend the previous discussion on secret-key generation based on public discussion to the practi-

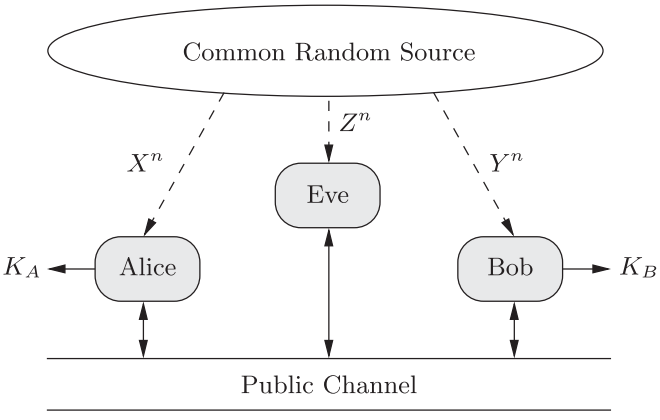

Fig. 6. Secret-key generation.

cally relevant case of wireless channels. We will see that wireless channels themselves can serve as sources of common randomness, making previous concepts applicable (43, 48, 49).

The scenario is the same: Two terminals Alice and Bob want to generate a secret key, keeping an eavesdropper Eve in the dark. Both terminals can transmit over a wireless fading channel and can further use a noiseless public channel for public discussion. Eve overhears the transmissions over the wireless channel and also eavesdrops upon the public discussion. The crucial idea is to exploit the reciprocity of the wireless channel to obtain correlated observations of the common fading channel. Then the key can be generated as discussed above.

When Alice transmits a signal X_A over the wireless channel, the received signals Y_B at Bob and Y_E at Eve are

$$Y_B = h_{AB}X_A + N_B \quad \text{and} \quad Y_E = h_{AE}X_A + N_E$$

with h_{AB} and h_{AE} the channel gains between Alice and Bob and Eve, respectively. N_A and N_B are additive Gaussian noise terms with zero means and variances σ^2. Alternatively, when Bob transmits a signal X_B, the received signals Y_A at Alice and Y_E at Eve are $Y_A = h_{BA}X_B + N_A$ and $Y_E = h_{BE}X_B + N_E$.

If both transmissions happen in the same frequency band and within the coherence time of the channel, it is reasonable to assume that the channel between Alice and Bob is reciprocal; i.e., $h_{AB} = h_{BA}$. Even if the channel is not perfectly reciprocal, it suffices to obtain correlated versions that are useful for the following secret-key generation process. Moreover, as Eve's location is assumed to be different from Alice's and Bob's, the transmitted signals experience different transmission conditions, resulting in channel observations h_{AE} and h_{BE} at Eve that are independent of h_{AB} and h_{BA}.

In a first phase, Alice and Bob send training signals that allow each terminal to estimate its channel $\tilde{h}_{AB}$ and $\tilde{h}_{BA}$. If the training symbols are sent within the channel coherence time T, Alice and Bob are able to obtain correlated versions of the common channel gain. This allows both terminals to use the same protocol: They can agree on a secret key by using the correlated versions of the common channel gain and by using the public channel for exchanging information based on Slepian–Wolf coding. Then a secret key of rate

$$R_K = \frac{1}{T} I(\tilde{h}_{AB}; \tilde{h}_{BA}) = \frac{1}{2T} \log\left(1 + \frac{\sigma_1^4 P^2 T^2}{4(\sigma^4 + \sigma^2\sigma_1^2 PT)}\right) \quad [8]$$

can be generated. The expression [8] reveals that the secret-key rate depends on the transmit power P as well as the coherence time T of the channel. As expected, with increasing power P the secret-key rate increases as well. However, with increasing coherence time T the secret-key rate decreases and approaches zero. Thus, from a secrecy perspective, a rapidly varying channel is beneficial whereas a slowly varying channel or a channel that is almost constant results in a low key rate.

Conclusion

In this paper, we have reviewed recent research in the field of wireless physical layer security, which exploits the physical properties of radio channels, notably diffusion and superposition, to provide security in wireless data transmission. By using an information theoretic formalism, we have seen that, in all of the principal channel models of wireless networking, the physical layer can in principle support reliable data transmission with perfect secrecy under realistic conditions. Note that a common theme of these results is a reliance on accurate channel modeling. Although this is a common approach in the design and analysis of communication systems, it nevertheless means that robustness to the model used is a factor that needs to be considered in practice. We have discussed this issue in the context of channel state information, but it is in general an important issue for further research.

Although we have focused here primarily on the fundamental issue of secrecy capacity, practical issues such as code design (50), authentication (51), and medium access control (52) have been considered in this context as well. Moreover, these basic ideas have been applied in other settings, such as optical communication (53, 54) and situations with adversarial attacks (25), and in other application areas, such as biometric identification systems (55, 56) and smart electricity grids (57).

ACKNOWLEDGMENTS. This work was supported in part by the US National Science Foundation under Grants CMMI-1435778 and ECCS-1647198 and in part by the German Research Foundation under Grant WY 151/2-1.

1. Shannon CE (1949) Communication theory of secrecy systems. *Bell Syst Tech J* 28: 656–715.
2. Wyner AD (1975) The wire-tap channel. *Bell Syst Tech J* 54:1355–1387.
3. Liang Y, Poor HV, Shamai (Shitz) S (2009) Information theoretic security. *Foundation and Trends in Communications and Information Theory* 5:355–580.
4. Bloch M, Barros J (2011) *Physical-Layer Security: From Information Theory to Security Engineering* (Cambridge Univ Press, Cambridge, UK).
5. Cover TM, Thomas JA (2006) *Elements of Information Theory* (Wiley-Interscience, Hoboken, NJ).
6. Vernam GS (1926) Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Trans Am Inst Electr Eng* XLV:295–301.
7. Forney GD, Jr (2003) On the role of MMSE estimation in approaching the information-theoretic limits of linear Gaussian channels: Shannon meets Wiener. *Proceedings of the 41st Allerton Conference on Communication, Control, and Computing* (IEEE, Piscataway, NJ), pp 430–439.
8. Maurer UM (1994) The strong secret key rate of discrete random triples. *Communication and Cryptography – Two Sides of One Tapestry*, eds Blahut RE, Costello DJ, Maurer U, Mittelholzer T (Springer, Boston), pp 271–285.
9. Csiszár I (1996) Almost independence and secrecy capacity. *Probl Peredachi Inf* 32: 48–57.
10. Maurer U, Wolf S (2000) Information-theoretic key agreement: From weak to strong secrecy for free. *Proceedings of EUROCRYPT 2000 on Advances in Cryptography*, Lecture Notes in Computer Science, ed Preneel B (Springer, Berlin), Vol 1807, pp 351–368.
11. Bloch MR, Laneman JN (2013) Strong secrecy from channel resolvability. *IEEE Trans Inf Theory* 59:8077–8098.
12. Devetak I (2005) The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans Inf Theory* 51:44–55.
13. Han TS, Endo H, Sasaki M (2014) Reliability and secrecy functions of the wiretap channel under cost constraint. *IEEE Trans Inf Theory* 60:6819–6843.
14. Hayashi M (2006) General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel. *IEEE Trans Inf Theory* 52:1562–1575.
15. Hou J, Kramer G (2014) Effective secrecy: Reliability, confusion, and stealth. *Proceedings of the IEEE International Symposium on Information Theory* (IEEE, New York), pp 601–605.
16. Bjelaković I, Boche H, Sommerfeld J (2013) Secrecy results for compound wiretap channels. *Probl Inf Transm* 49:73–98.
17. Bellaire M, Tessaro S, Vardy A (2012) A cryptographic treatment of the wiretap channel. *Proceedings of Advances in Cryptology (CRYPTO)*, eds Safavi-Naini R, Canetti R (Springer, Berlin), pp 1–31.
18. Csiszár I, Körner J (1978) Broadcast channels with confidential messages. *IEEE Trans Inf Theory* 24:339–348.
19. Massey JL (1983) A simplified treatment of Wyner's wire-tap channel. *Proceedings of the 21st Allerton Conference on Communication, Control and Computing* (IEEE, Piscataway, NJ), pp 268–276.
20. Leung-Yan-Cheong SK, Hellman ME (1978) The Gaussian wire-tap channel. *IEEE Trans Inf Theory* 24:451–456.
21. Khisti A, Wornell GW (2010) Secure transmission with multiple antennas I: The MISOME wiretap channel/Part II: The MIMOME wiretap channel. *IEEE Trans Inf Theory* 56:5515–5532.
22. Oggier F, Hassibi B (2011) The secrecy capacity of the MIMO wiretap channel. *IEEE Trans Inf Theory* 57:4961–4972.
23. Bustin R, Liu R, Poor HV, Shamai(Shitz) S (2009) An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel. *EURASIP J Wirel Commun Netw* 2009:370970.
24. Loyka S, Charalambous CD (2013) Further results on optimal signaling over secure MIMO channels. *Proceedings of the IEEE International Symposium on Information Theory* (IEEE, Piscataway, NJ), pp 2019–2023.
25. Schaefer RF, Boche H, Poor HV (2015) Secure communication under channel uncertainty and adversarial attacks. *Proc IEEE* 103:1796–1813.

26. Liang Y, Kramer G, Poor HV, Shamai (Shitz) S (2009) Compound wiretap channels. *EURASIP J Wirel Commun Netw* 2009:142374.
27. Schaefer RF, Loyka S (2015) The secrecy capacity of compound MIMO Gaussian channels. *IEEE Trans Inf Theory* 61:5535–5552.
28. Liang Y, Poor HV, Shamai(Shitz) S (2008) Secure communication over fading channels. *IEEE Trans Inf Theory* 54:2470–2492.
29. Gopala PK, Lai L, El Gamal H (2008) On the secrecy capacity of fading channels. *IEEE Trans Inf Theory* 54:4687–4698.
30. Khisti A, Tchamkerten A, Wornell GW (2008) Secure broadcasting over fading channels. *IEEE Trans Inf Theory* 54:2453–2469.
31. Zou S, Liang Y, Lai L, Poor HV, Shamai (Shitz) S (2015) Broadcast networks with layered decoding and layered secrecy: Theory and applications. *Proc IEEE* 10:1841–1856.
32. Ly HD, Liu T, Liang Y (2010) Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages. *IEEE Trans Inf Theory* 56:5477–5487.
33. Schaefer RF, Boche H (2014) Robust broadcasting of common and confidential messages over compound channels: Strong secrecy and decoding performance. *IEEE Trans Inf Forensics Secur* 9:1720–1732.
34. Liang Y, Poor HV (2008) Multiple-access channels with confidential messages. *IEEE Trans Inf Theory* 54:972–1002.
35. Tang X, Liu R, Spasojevic P, Poor HV (2007) Multiple access channels with generalized feedback and confidential messages. *Proceedings of the IEEE Information Theory Workshop* (IEEE, Piscataway, NJ), pp 608–613.
36. Tekin E, Yener A (2008) The Gaussian multiple access wire-tap channel. *IEEE Trans Inf Theory* 54:5747–5755.
37. Koyluoglu OO, El Gamal H, Lai L, Poor HV (2011) Interference alignment for secrecy. *IEEE Trans Inf Theory* 57:3323–3332.
38. Liu R, Maric I, Spasojevic P, Yates R (2008) Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans Inf Theory* 54:2493–2507.
39. Liang Y, Somekh-Baruch A, Poor HV, Shamai (Shitz) S, Verdú S (2009) Capacity of cognitive interference channels with and with out secrecy. *IEEE Trans Inf Theory* 55: 604–619.
40. He X, Yener A (2010) Cooperation with an untrusted relay: A secrecy perspective. *IEEE Trans Inf Theory* 56:3801–3827.
41. Oohama Y (2007) Relay channels with confidential messages. *Proceedings of the IEEE International Symposium on Information Theory* (IEEE, Piscataway, NJ), pp 926–930.
42. Lai L, El Gamal H (2008) The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans Inf Theory* 54:4005–4019.
43. Lai L, Liang Y, Poor HV, Du W (2014) Key generation from wireless channels. *Physical Layer Security in Wireless Communications*, eds Zhou X, Song L, Zhang Y (CRC, Boca Raton, FL).
44. Narayan P, Tyagi H (2016) Multiterminal secrecy by public discussion. *Foundation and Trends in Communications and Information Theory* 13:129–275.
45. Ahlswede R, Csiszár I (1993) Common randomness in information theory and cryptography-Part I: Secret sharing. *IEEE Trans Inf Theory* 39:1121–1132.
46. Maurer UM (1993) Secret key agreement by public discussion from common information. *IEEE Trans Inf Theory* 39:733–742.
47. Csiszár I, Narayan P (2000) Common randomness and secret key generation with a helper. *IEEE Trans Inf Theory* 46:344–366.
48. Wilson R, Tse D, Scholtz RA (2007) Channel identification: Secret sharing using reciprocity in ultrawideband channels. *IEEE Trans Inf Forensics Secur* 2:364–375.
49. Ye C, Mathur S, Reznik A, Trappe W, Mandayam N (2010) Information-theoretic key generation from wireless channels. *IEEE Trans Inf Forensics Secur* 5:240–254.
50. Bloch M,Hayashi M, Thangaraj A (2015) Error-control coding for physical-layer secrecy. *Proc IEEE* 103:1725–1746.
51. Lai L, El Gamal H, Poor HV (2009) Authentication over noisy channels. *IEEE Trans Inf Theory* 55:906–916.
52. Liang Y, Poor HV, Ying L (2011) Secure communications over wireless broadcast networks: Stability and utility maximization. *IEEE Trans Inf Forensics Secur* 6:682–692.
53. Guan K, Winzer PJ, Soljanin E (2012) Information-theoretic security in space-division multiplexed fiber optic networks. *Proceedings of the European Conference and Exhibition on Optical Communication* (Optical Society of America, Washington, DC), p Tu.3.C.4.
54. Song EC, Soljanin E, Cuff P, Poor HV, Guan K (2014) Rate-distortion-based physical layer secrecy in multimode fiber. *IEEE Trans Commun* 62:1080–1090.
55. Ignatenko T, Willems FMJ (2012) Biometric security from an information-theoretical perspective. *Foundations and Trends in Communications and Information Theory* 7:135–316.
56. Lai L, Ho S-W, Poor HV (2011) Privacy-security tradeoff in biometric security systems part I: Single uses case/part II: Multiple uses case. *IEEE Trans Inf Forensics Secur* 1:122–151.
57. Sankar L, Rajagopalan SR, Mohajer S, Poor HV (2013) Smart meter privacy: A theoretical framework. *IEEE Trans Smart Grid* 2:837–846.