Jamming Based on an Ephemeral Key to Obtain Everlasting Security in Wireless Environments

Azadeh Sheikholeslami, *Student Member, IEEE*, Dennis Goeckel, *Fellow, IEEE*, and Hossein Pishro-Nik, *Member, IEEE*

***Abstract*—Secure communication over a wiretap channel is considered in the disadvantaged wireless environment, where the eavesdropper channel is (possibly much) better than the main channel. We present a method to exploit inherent vulnerabilities of the eavesdroppers receiver to obtain everlasting secrecy. Based on an ephemeral cryptographic key pre-shared between the transmitter Alice and the intended recipient Bob, a random jamming signal is added to each symbol. Bob can subtract the jamming signal before recording the signal, while the eavesdropper Eve is forced to perform these non-commutative operations in the opposite order. Thus, information-theoretic secrecy can be obtained, hence achieving the goal of converting the vulnerable "cheap" cryptographic secret key bits into "valuable" information-theoretic (i.e., everlasting) secure bits. We evaluate the achievable secrecy rates for different settings, and show that, even when the eavesdropper has perfect access to the output of the transmitter (albeit through an imperfect analog-to-digital converter), the method can still achieve a positive secrecy rate. Next we consider a wideband system, where Alice and Bob perform frequency hopping in addition to adding the random jamming to the signal, and we show the utility of such an approach even in the face of substantial eavesdropper hardware capabilities.**

***Index Terms*—Everlasting secrecy, secure wireless communication, A/D conversion, jamming, frequency hopping.**

I. Introduction

THE usual approach to provide secrecy is encryption of the message. Such cryptographic approaches rely on the assumption that the eavesdropper does not have access to the key, and the computational capabilities of the eavesdropper are limited [2]. However, if the eavesdropper can somehow obtain the key in the future, or the cryptographic system is broken, the secret message can be obtained from the recorded clean cipher [3], which is not acceptable in many applications requiring everlasting secrecy.

The desire for everlasting security motivates considering information-theoretic security methods, where the eavesdropper is unable to extract any information about the message from the received signal. Wyner showed that, for a discrete memoryless wiretap channel, if the eavesdropper's channel is degraded with respect to the main channel, adding randomness to the codebook allows a positive secrecy rate to be achieved [4]. This idea was extended to the more general case of a wiretap channel with a "more noisy" or "less capable" eavesdropper [5]. Hence, in order to obtain a positive secrecy rate in a one-way communication system, having an advantage for the main channel with respect to the eavesdropper's channel is essential. However, in wireless systems, guaranteeing such an advantage is not always possible, as an eavesdropper that is close to the transmitter or with a directional antenna can obtain a very high signal-to-noise ratio. Furthermore, the location and channel state information of a passive eavesdropper is usually not known to the legitimate nodes, making it difficult to pick the secrecy rate to employ. Recently, approaches based on the cooperative jamming scheme of [6] and [7], which try to build an advantage for the legitimate nodes over the eavesdropper, have been considered extensively in the literature [8]–[13]. However, these approaches require either multiple antennas, helper nodes, and/or fading and therefore are not robust across all operating environments envisioned for wireless networks. Other approaches to obtain information-theoretic security when such an advantage does not exist are schemes based on "public discussion" [14], which utilize two-way communication channels and a public authenticated channel. However, public discussion schemes result in low secrecy rates in scenarios of interest (as discussed in detail in [15]), and the technique proposed here can be used in conjunction with public discussion approaches when two-way communication is possible.

In this work, we exploit *current* hardware limitations of the eavesdropper to achieve everlasting security. Prior work in this area includes the "bounded storage model" of Cachin and Maurer [16]. However, it is difficult to plan on memory size limitations at the eavesdropper, since not only do memories improve rapidly as described by the well-known Moore's Law [17], but they also can be stacked arbitrarily subject only to (very) large space limitations. Our approach, first presented in [18] and further developed in [15], rather than exploiting limitations of the memory in the receiver back-end, exploits the limitations of the analog-to-digital converter (A/D) in the receiver front-end, where the technology progresses slowly, and unlike memory, stacking cannot be done arbitrarily due to jitter considerations. Also, from a long-term perspective, there is a fundamental bound on the ability to perform A/D conversion [19], with some authors postulating that current technology is

Manuscript received October 27, 2014; revised February 6, 2015 and May 22, 2015; accepted June 16, 2015. Date of publication June 22, 2015; date of current version November 9, 2015. This work was supported by the National Science Foundation under Grants CIF-1249275 and CIF-1421957. This work was presented in part at the 2014 Asilomar Conference on Signals, Systems, and Computers [1]. The associate editor coordinating the review of this paper and approving it for publication was R. Zhang.

The authors are with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA 01002 USA (e-mail: sheikholesla@ecs.umass.edu; goeckel@ecs.umass.edu; pishro@ecs.umass.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2015.2448074

close to that limit [20], [21]. Hence, we exploit the receiver analog-to-digital conversion processing effect on the received signal to obtain everlasting security. A rapid random power modulation instance of this approach was investigated in [15] and [18], where the transmitter Alice modulates the signal by two vastly different power levels. The intended recipient Bob, since he knows the key, can adapt to the power modulation before his A/D, while the eavesdropper Eve fails to do such and, for a restricted set of attacker modes, information-theoretic security is obtained. However, the power modulation scheme is susceptible to being broken by an eavesdropper with a more sophisticated receiver than that assumed in [15], as discussed in [15] and shown explicitly here in Section II.

Hence, here we consider a different method to obtain everlasting secrecy. First, recall that, at moderate-to-high signal-to-noise ratios (SNRs), increasing the transmit power leads to very small gains in the secrecy rate, as it makes the received signal not only stronger at Bob, but also at Eve. So, consider using excess power in a different manner. Suppose that Alice employs her cryptographically-secure key bits to select a jamming signal to add to the transmitted signal. Since Bob knows the key, he can cancel the jamming signal before his A/D; on the other hand, Eve must store the signal and try to cancel the jamming signal from the recorded signal at the output of her A/D after she obtains the key.[1] However, the jamming signal is designed such that Eve has already lost the information she would need to recover the secret message, even if she obtains the key immediately after the transmission. In particular, we present numerical results to investigate the number of cryptographic key bits needed to obtain positive secrecy rates and demonstrate the secrecy rates that can be obtained in disadvantaged environments.

Next, we consider a wideband system that additionally can employ spread-spectrum in the form of frequency hopping to further enhance everlasting secrecy. At first glance, one might think that the eavesdropper can easily thwart such an enhancement by utilizing a wideband receiver that can process all of the frequencies that the transmitter uses. However, because of the limitations in the aperture jitter of A/Ds, the implementation of an A/D with both a high sampling frequency and high resolution is not feasible. Thus, Eve faces a difficult tradeoff. If Eve employs a high resolution A/D, she will lose any information outside her bandwidth. On the other hand, if she employs an A/D with large bandwidth, the resolution of her A/D will be lower, making her receiver vulnerable to the random jamming employed by Alice, per above.

The rest of the paper is organized as follows. Section II describes the system model and the difficult challenges faced. The random jamming approach for secrecy, its analysis and numerical results for the narrowband case are presented in Section III. In Section IV, wideband systems are considered. The method of Section IV is discussed in Section V. Conclusion and ideas for future work are presented in Section VI.

[1] Recall that the storage of an analog signal, which is equivalent to an analog delay line, is one of the greatest and longstanding challenges of analog signal processing.

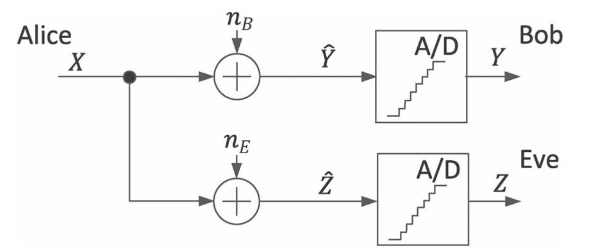

Fig. 1. Wiretap channel with receiver analog-to-digital (A/D) converters shown.

II. System Model

A. System Model

We consider a wiretap channel, which consists of a transmitter, Alice, a legitimate receiver, Bob, and an eavesdropper, Eve. The eavesdropper is assumed to be passive, i.e., it does not attempt to actively prevent (e.g., via jamming) the legitimate nodes to receive the message. Thus, the location and channel state information of the eavesdropper is assumed to be unknown to the legitimate nodes.

We assume that either a very short initial key is pre-shared between Alice and Bob, or they share an initial cryptographic key using a key agreement method like Diffie-Hellman [22] (through four phases of public communication). By employing a cryptographic stream-cipher generation method, this initial key is used to obtain a long key sequence. Several methods to generate secure stream-ciphers are available. For instance, a secure cryptographic scheme like AES with 128 bits of initial key can be used in the counter mode to generate 2^{38} bits of stream-cipher [23, Chapter 5]. Since we are using cryptographic approaches to perform key expansion and perhaps to exchange an initial key, we should assume that the computational power of Eve during message transmission is not unlimited. However, unlike cryptography, our system design is such that the key is only employed ephemerally, and thus even if (pessimistically) the full key is handed to Eve after completion of transmission, she can not obtain enough information to recover the message. Hence, our method is not vulnerable to threats against cryptographic schemes, like future key leakage or future advances in the computational power of Eve.

We consider a one-way communication system with an additive white Gaussian noise (AWGN) channel between Alice and each of Bob and Eve, and we include variations of the path-loss in the noise variance. Hence, the signal that Bob receives is:

$$\hat{Y} = X + n_B,$$

where X denotes the current code symbol, and n_B is the noise of Bob's channel, $n_B \sim \mathcal{N}(0, \sigma_B^2)$. The signal that Eve receives is:

$$\hat{Z} = X + n_E,$$

where $n_E \sim \mathcal{N}(0, \sigma_E^2)$ is the noise of Eve's channel (Fig. 1). We consider line-of-sight communication; however, the scheme works similarly on fading channels with a different calculation for the secrecy rate.

The effect of the A/D on the received signal (quantization error) is modeled by both a quantization noise, which is due to the limitation in the size of each quantization level, and missed symbols due to the quantizer's overflow. The quantization noise in this case is (approximately) uniformly distributed [24, Section 5], so we will assume it is uniformly distributed throughout the paper. For a b-bit quantizer (2^b gray levels) over the full dynamic range $[-r, r]$, two adjacent quantization levels are spaced by $\delta = 2r/2^b$, and thus the quantization noise is uniformly distributed over an interval of length δ. Throughout this paper, the quantization noise of Bob's A/D is denoted by n_{qB}, and the quantization noise of Eve's A/D is denoted by n_{qE}. Quantizer overflow happens when the amplitude of the received signal is greater than the quantizer's dynamic range. We assume that Alice knows an upper bound on Eve's current A/D conversion ability (without any assumption on Eve's future A/D conversion capabilities).

For a stationary memoryless wiretap channel any secrecy rate,

$$R_s < \max_{X \to YZ} [I(X;Y) - I(X;Z)] \tag{1}$$

is achievable [25]. We assume that X is taken from a standard Gaussian codebook where each entry has variance P, i.e., $X \sim \mathcal{N}(0, P)$. While using the Gaussian codebook is optimal for AWGN channels, it is not optimal in our model as we consider the quantization errors (the uniformly distributed quantization noise and overflows); hence, our results indicate achievable rates but not upper bounds.

B. Power Modulation Approach [15], [18]

Our goal is to use the cheap (and numerous) cryptographically secure bits of the key stream in Section II-A to obtain "expensive" information-theoretic secret bits at the legitimate receiver. As a first step, in [15], [18], we considered a rapid power modulation instance of this approach, where the transmitted signal is modulated by two vastly different power levels A_1 and A_2 at the transmitter. Since Bob knows the key, he can undo the effect of the power modulation before his A/D, putting his signal in the appropriate range for analog-to-digital conversion, while Eve must compromise between larger quantization noise and more A/D overflows. Consequently, she will lose information she needs to recover the message, and information-theoretic security is obtained. However, a clear risk of the approach of [15], [18] is a sophisticated eavesdropper with multiple A/Ds. Suppose that Eve has two A/Ds, and she uses them in parallel with a gain in front of each A/D such that each gain cancels the effect of one of the gains that Alice uses to modulate the secret message; thus, she records Z_1 and Z_2 as shown in Fig. 2. Even if Eve does not know A_1 and A_2, it is easy for her to estimate A_1 and A_2 during transmission from the received signal. For example, Eve can use a random small gain and a random large gain. With the small gain, she tracks symbols for which her A/D overflows and finds the optimum small gain, and with the large gain, she tracks symbols with small amplitude and finds the optimum large gain. After completion of the transmission, if Eve obtains the key as we assume, she can use it to retain for each channel use only the element of $\{Z_1, Z_2\}$ from the branch of her receiver properly matched to the transmission gain. In the disadvantaged

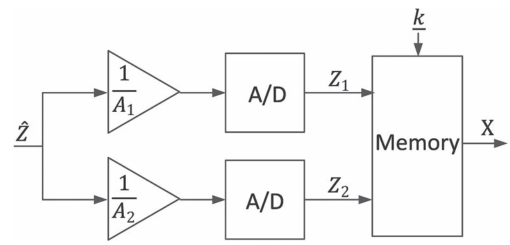

Fig. 2. Eve with a sophisticated receiver. To break the power modulation approach of [15] and [18], she can record Z_1 and Z_2 and decode them later—when she obtains the key, the encryption system is broken, or she has access to an unlimited computational power—to obtain the secret message.

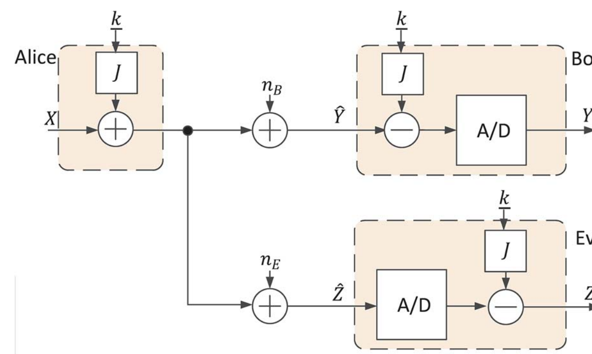

Fig. 3. Bob and Eve both receive the superposition of the message and the random jamming signal. Bob uses the key sequence to cancel the effect of the jammer on his signal before the analog-to-digital conversion, while Eve has to wait to obtain the key after completion of transmission and cancel the effect of the jammer after her A/D.

wireless scenario, Eve's recorded signal then contains more information than Bob's about the transmitted message from Alice, and thus the desired everlasting secrecy is compromised. This problem seems to be resolvable by using many gains instead of just two gains, as posited in [15]. However, the signal X is Gaussian distributed and thus the amplitude of the signal, regardless of gain, is concentrated around zero. This gives Eve an advantage in designing the quantization levels of her A/D versus the scheme proposed here, and, pragmatically, makes the specification of Eve's optimal A/D and thus the achievable rate of such a scheme intractable. Since our goal is to design a scheme that is provably secure, this latter deficiency should not be underrated. In the next section, a new approach to utilize the key bits to obtain everlasting secrecy in the case of an eavesdropper with sophisticated hardware is presented.

III. Random Jamming for Secrecy

In this paper, we propose adding random jamming with large variation to the signal to obtain secrecy (Fig. 3). Suppose that Alice employs her cryptographically-secure key bits to select a signal from a uniform discrete distribution to add to the transmitted signal. Now, since Bob knows the key, he can simply subtract off the jamming signal and continue normal decoding with an A/D converter well-matched to the span of the signal. However, Eve does not have knowledge of the key and thus has difficulty matching the span of her A/D to the received signal. If she does not change the span of her A/D, she will lose information due to overflows. On the other hand, if she increases the span of her A/D to contain all of the received signal, the width of each quantization level will increase and thus she will lose information due to higher quantization noise. As before, we assume that the key is handed to Eve as soon as transmission is complete, and obviously Eve could simply subtract the jamming signal off of her *recorded* samples in memory. But, as before, a nonlinear operation (the analog-to-digital converter) has processed the signal, hence allowing the possibility of information-theoretic secrecy *even when the secret key is handed to Eve immediately after the transmission.*[2] Indeed, with her poorly matched A/D, Eve will not have recorded a reasonable version of the signal and we will see that information-theoretic security can be obtained. In this case, one countermeasure for Eve would be to employ parallel receiver branches, each with a different fixed voltage offset; however, this is precisely a higher-resolution A/D over a larger span and thus is captured by the standard A/D model and technology trend lines. In this paper, we will show that, through such a scheme, "cheap" cryptographically-secure key bits can be used to greatly increase the transmission rate of the desired "expensive" information-theoretic secure bits.

A. Analysis

Suppose that Eve has a b_e bit A/D and she sets the span of the A/D to $2l\sigma$ to cover $[-l\sigma, l\sigma]$, where l is a constant that maximizes $I(X;Z)$, and $\sigma = \sqrt{P}$ is the standard deviation of the transmitted signal X. Now, suppose that Alice adds a random jamming signal J to X based on the pre-shared key between Alice and Bob (Fig. 3). In particular, J follows a discrete uniform distribution with 2^k levels between $-c$ and c, where k is the number of key bits per jamming symbol, and c (maximum amplitude of the jamming signal) is an arbitrary constant. In order to maximize the degradation of Eve's A/D, Alice should maximize c. Thus, given that k key bits per jamming symbol is available at Alice, the relationship between k and c is:

$$(2^k - 1) \times 2l\sigma = 2c.$$

On the other hand, Eve, in order to maximize $I(X;Z)$, expands the span of her A/D to $2nl\sigma$, where $n = 2^m$ is an arbitrary constant that maximizes $I(X;Z)$. Hence, the new resolution of Eve's A/D will be

$$\delta'_e = \frac{2l\sigma n}{2^{b_e}} = \frac{2l\sigma}{2^{b_e-m}}.$$

Since the jamming signal is uniformly distributed, if Eve does not change the span of her A/D, she will miss a fraction $\frac{2^k-2^m}{2^k}$ of the information due to her A/D overflows, and will gain only a fraction $\frac{2^m}{2^k}$ of the information. The best strategy for Eve is to choose a m that maximizes the mutual information between X and Z. When the channel between Alice and Eve is noiseless, by using the approach of [26, Pg. 251] for analyzing high resolution quantizers ($\delta'_E \ll 1$),

$$\begin{aligned} I(X;Z) &= \frac{2^m}{2^k}\left(H(Z) - H(Z|X)\right) \\ &\approx \frac{2^m}{2^k}\left(h(\hat{Z}) - \log\left(\delta'_E\right)\right) \\ &= \frac{2^m}{2^k}\left(h(X) - \log\left(\frac{2l\sigma}{2^{b_e-m}}\right)\right) \\ &= \frac{2^m}{2^k}\left(\log\left(\sigma\sqrt{2\pi e}\right) - \log(2l\sigma) + b_e - m\right) \\ &= \frac{2^m}{2^k}\left(\log\left(\sqrt{\frac{\pi e}{2l^2}}\right) + b_e - m\right) \end{aligned}$$

From [15] the optimum value for l is $l=2.5$. Hence, for $m < b_e - 1.2$, $I(X:Z)$ is strictly increasing in m and thus the maximum mutual information between Alice and Eve is obtained when m is maximum, i.e., $m=k$. This means that the best strategy for Eve is to enlarge the span of her A/D to avoid overflows. In the numerical results section we will show that $m = k$ maximizes $I(X;Z)$ even when δ'_E is not very small. Hence, in the remainder of this section, we assume the dynamic range of Eve's A/D is $2^{k+1}l\sigma$, and thus no A/D overflow happens.

Now, we calculate the exact achievable secrecy rate. From (1), in order to calculate the achievable secrecy rates, $I(X;Y)$ and $I(X;Z)$ are needed. We only show the calculations for the latter here, as $I(X;Y)$ can be obtained in a similar way. The mutual information between X and Z can be written as,

$$\begin{aligned} I(X;Z) &= h(Z) - h(Z|X) \\ &= \int_{-l\sigma}^{l\sigma} -f_Z(z)\log\left(f_Z(z)\right)dz \\ &\quad - \int_{-\infty}^{\infty} f_X(x)\int_{-l\sigma}^{l\sigma} -f_{Z|X=x}(z)\log\left(f_{Z|X=x}(z)\right)dzdx, \end{aligned} \tag{2}$$

Hence, we need to calculate the probability density functions (pdf) of Z and $Z|X=x$. The signal at the input of Eve's receiver is $\hat{Z}=J+X+n_E$. Suppose that after analog-to-digital conversion, Eve can somehow obtain the key and cancel the effect of the jamming signal. Hence, the eventual signal that Eve obtains is: $Z=X+n_E+n_{qE}$. For simplicity of presentation, we define the random variable Z' as $Z'=X+n_E$. Since $X\sim\mathcal{N}(0,P)$ and $n_e\sim\mathcal{N}(0,\sigma_e^2)$, Z' follows a normal distribution with zero mean and variance $P+\sigma_E^2$. Hence, the probability density function of Z is,

$$\begin{aligned} f_Z(z) &= f_{Z'}(z) * f_{n_{qE}}(z) \\ &= \frac{1}{\delta'_E}\int_{-l\sigma}^{l\sigma} f_{Z'}(s)U_{[-\delta'_E/2,\delta'_E/2]}(z-s)ds \\ &= \frac{1}{\delta'_E}\int_{\max(-l\sigma,z-\delta'_E/2)}^{\min(l\sigma,z+\delta'_E/2)} f_{Z'}(s)ds \\ &= \frac{1}{\delta'_E}\left[Q\left(\frac{\max\left(-l\sigma,z-\delta'_E/2\right)}{\sqrt{P+\sigma_E^2}}\right) - Q\left(\frac{\min\left(l\sigma,z+\delta'_E/2\right)}{\sqrt{P+\sigma_E^2}}\right)\right], \end{aligned} \tag{3}$$

where $U_{[a,b]}(.)$ is the rectangle function on $[a,b]$, i.e., the value of the function is 1 on the interval $[a,b]$ and is zero elsewhere.

[2]We put the previous phrase in italics so that the reader does not confuse the proposed approach with a number of schemes in the information-theoretic secrecy literature that look similar, but must presume that the key (or secret) on which the jamming sequence is based is kept secret from Eve forever.

The random variable Z' given $X = x$ has a Gaussian distribution with mean x and variance σ_E. Thus, the probability density function of $Z|X = x$ is,

$$\begin{aligned} f_{Z|X=x}(z) &= f_{Z'|X=x}(z) * f_{n_{qE}}(z) \\ &= \frac{1}{\delta'_E} \int_{\max(-l\sigma, z-\delta'_E/2)}^{\min(l\sigma, z+\delta'_E/2)} f_{Z'|X=x}(s) ds \\ &= \frac{1}{\delta'_E} \left[Q\left(\frac{\max\left(-l\sigma, z-\frac{\delta'_E}{2}\right) - x}{\sigma_E} \right) \right. \\ &\quad \left. - Q\left(\frac{\min\left(l\sigma, z+\frac{\delta'_E}{2}\right) - x}{\sigma_E} \right) \right] \end{aligned} \tag{4}$$

Hence, $I(X; Z)$ can be calculated by substituting (3) and (4) in (2). Similarly, $I(X; Y)$ can be calculated by substituting Z with Y, σ_E with σ_B, and δ'_E with δ_B (where δ_B is the resolution of Bob's A/D) in (2), (3), and (4). The achievable secrecy rate can be found by substituting these expressions for the mutual information into $R_s = I(X; Y) - I(X; Z)$.

In the case that the channel between Alice and Eve is noiseless (e.g., Eve picks up the transmitter), $I(X; Z)$ can be obtained from (2) through the evaluation of $h(Z)$ and $h(Z|X)$ given that the channel noise is zero. $h(Z)$ can be found by setting $\sigma_E^2 = 0$ in (3), and $h(Z|X)$ can be obtained as,

$$\begin{aligned} h(Z|X) &= \int_{-\infty}^{\infty} h(Z|X = x) f_X(x) dx \\ &= \int_{-\infty}^{\infty} h(X + n_{qE}|X = x) f_X(x) dx \\ &= \int_{-\infty}^{\infty} h(n_{qE}) f_X(x) dx = \log\left(\delta'_E\right) \end{aligned} \tag{5}$$

Numerical results are presented in the next section.

B. Numerical Results

In this section, we first show that $I(X; Z)$ is maximized when Eve sets the span of her A/D to avoid overflow, and then we study the achievable secrecy rates of the proposed method for various scenarios. In order to maximize the mutual information ($I(X; Y)$ or $I(X; Z)$), we set the quantization range by $l = 2.5$ [15]. Since $I(X; Z)$ is an intricate function of the span of Eve's A/D (m) and the number of key bits employed per jamming symbol (k), we find the maximum of this function numerically. In Fig. 4, $I(X; Z)$ versus the span of Eve's A/D m and the number of key bits k when Eve employs a $b_E = 20$ bit A/D is shown. It can be seen that the value of $I(X; Z)$ for various numbers of key bits per jamming symbol is maximized when $m = k$. Thus, Eve will set the dynamic range of her A/D to $2^{k+1} l\sigma$ to avoid overflow.

In order to see how many cryptographic key bits per symbol are needed to achieve secrecy, the curves of achievable secrecy rates versus the number of key bits per jamming symbol, for various qualities of Eve's A/D, are shown in Fig. 5. In this figure, the transmitter power $P = E[X^2] = 1$, which does not include the jamming power (Note that we will consider a total power constraint below in Fig. 8). Although the quality of

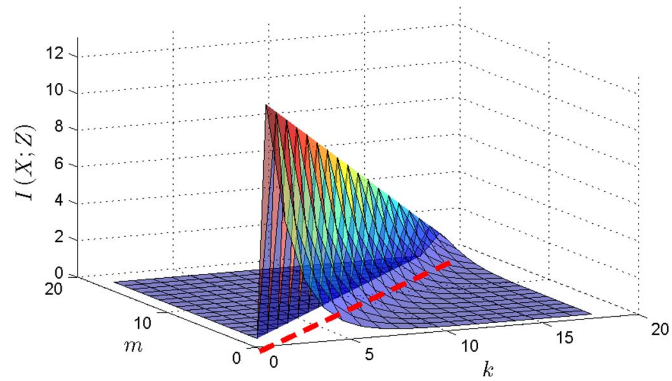

Fig. 4. $I(X; Z)$ versus k (the number of key bits per jamming symbol) and m (the span of Eve's A/D) when Eve has a $b_e = 20$ bit A/D. Observe that the mutual information is maximized when $m = k$ (the red dashed line). Thus, Eve will set the span of her A/D to $2^{k+1} l\sigma$.

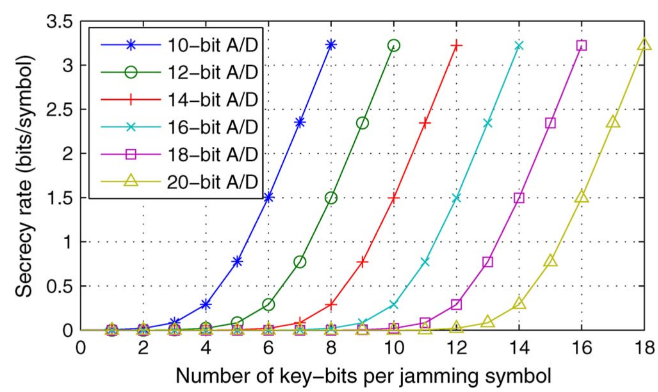

Fig. 5. Achievable secrecy rates versus the number of key bits when Bob employs a 10-bit A/D and Eve employs A/D's of various quality. $P = 1$, $l = 2.5$, and the signal-to-noise ratio of each of Eve's channel and Bob's channel is 30 dB.

each of Bob's and Eve's channel is the same with a signal-to-noise ratio of 30 dB, and thus the secrecy capacity of the corresponding wiretap channel is zero, positive secrecy rates are achieved through the proposed method. Further, even in the case that Eve has an A/D of much better quality than Bob's A/D (or she has stacked multiple A/Ds of the same quality as Bob's A/D until limited by clock jitter), by utilizing more key bits per jamming symbol, which are cheap cryptographic bits and can be obtained at little cost [15], positive secrecy rates (i.e., expensive information-theoretically secure bits) can be obtained. The achievable secrecy rates versus the signal-to-noise ratio of Eve's channel (SNR_E) for various numbers of key bits per jamming symbol, when the SNR of Bob's channel is 60 dB, are depicted in Fig. 6. It can be seen that, even in disadvantaged environments where the quality of Eve's channel is better than the quality of Bob's channel, a positive secrecy rate can be achieved. In Fig. 7, we look at the extreme case that Eve is able to receive exactly what Alice transmits (e.g., the adversary is able to pick up the transmitter's radio and hook directly to the antenna), but the channel between Alice and Bob is noisy and hence no other classical technique[3] is effective. Finally, the secrecy rate versus the number of key

[3] Quantum-cryptography techniques [27] are exempt from this.

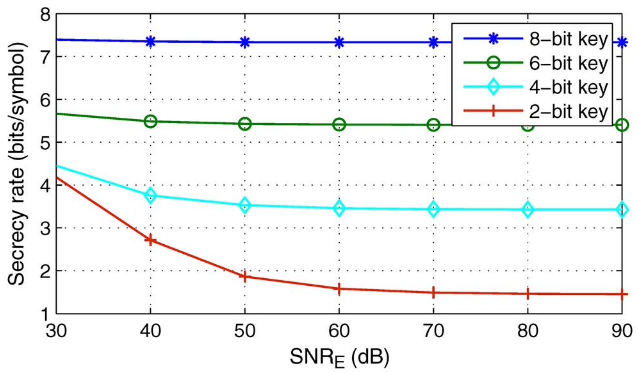

Fig. 6. Achievable secrecy rates versus the signal-to-noise ratio of Eve's channel (SNR_E) for various numbers of key bits per jamming symbol, when the SNR of Bob's channel is 60 dB. $P = 1$, $l = 2.5$, and both Bob and Eve use 10-bit A/Ds. Even when the quality of Eve's channel is much better than that of Bob's channel, positive secrecy rates can be achieved.

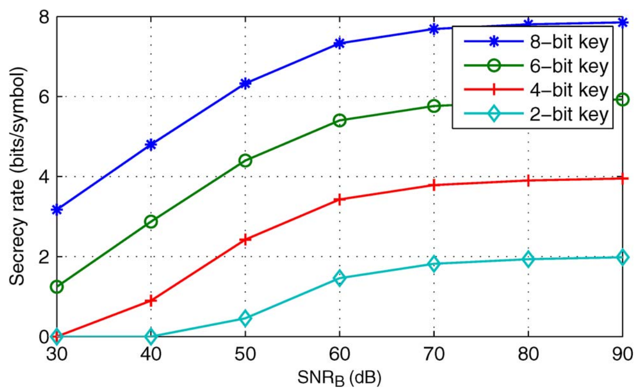

Fig. 7. Achievable secrecy rates versus signal-to-noise ratio of Bob's channel, for various numbers of key bits per jamming symbol, when Eve's channel is noiseless, i.e., Eve has perfect access to what the transmitter sends and thus no other classical technique is effective. $P = 1$, $l = 2.5$, and both Bob and Eve use 10-bit A/Ds.

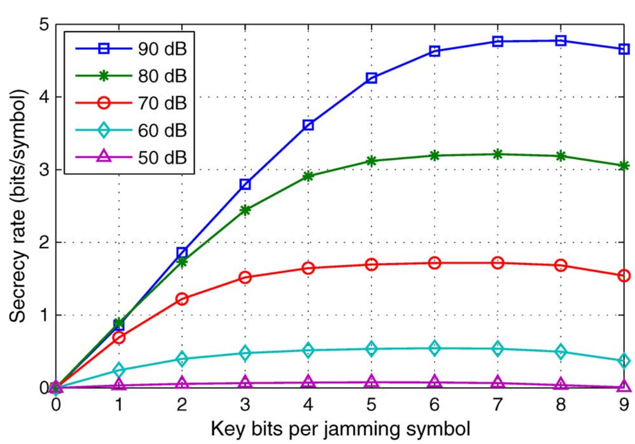

Fig. 8. Secrecy rate versus the number of key bits per jamming symbol (k) for various values of the total SNR, when $P + P_J = 1$, Bob and Eve each have a 10-bit A/D, and the quality of both channels is the same.

bitsper jamming symbol (k) for a total power constraint is shown in Fig. 8. The total power $P + P_J = 1$, Bob and Eve each have a 10-bit A/D, and both channels have the same quality. When $k = 0$, there is no jamming and all of the power is allocated to the signal; thus, the secrecy rate is zero. As the number of key bits (and hence the power allocated to the jamming signal) increases, the secrecy rate increases, until eventually, as the power allocated to the portion of the signal containing the message becomes very small, it tapers at high jamming powers.

IV. Wideband Channels

Frequency hopping is a spread spectrum technique that divides the entire available frequency band into sub-channels, such that at each time instance the signal is being sent over one sub-channel according to an entry in a pre-specified hopping pattern. When Alice and Bob have access to a wideband channel, they can utilize frequency hopping using the cryptographic key described in Section II-A to obtain information-theoretic secrecy. Alice sends a narrow-band signal with bandwidth W in a (large) frequency band of span F by employing a narrowband slot centered at a frequency f_c. The center frequency f_c for each symbol is chosen based on the key from a uniform ensemble of frequencies in the interval $[-F/2 + W/2, F/2 - W/2]$. Since Bob knows the key, he can tune his receiver to the correct frequency slot. Eve, since she does not know the key during the time of transmission, does not know the correct frequency slot and thus she is forced to either risk missing symbols that are out of her bandwidth or expand the bandwidth of her receiver. As we will explain in Section V, it is not feasible for a receiver to have a large bandwidth and a high resolution A/D simultaneously. Hence, by using the random jamming scheme of Section III in conjunction with frequency hopping, we can prevent an eavesdropper from obtaining the message.

Let Z_B be the total additive noise, including both channel and quantization noise, at Bob's receiver and Z_E be the total additive noise at Eve's receiver. In the case of band-limited channels, since each of Z_B and Z_E is a superposition of a Gaussian noise (channel) and a uniform noise (quantization), the capacity of Bob's channel and Eve's channel cannot be found directly. Fortunately, upper and lower bounds on the capacity of a band-limited channel with independent additive noise are available [28], [29]. For a channel with bandwidth W, for a signal power of P and total additive noise Z with power N, the capacity C lies between bounds,

$$W \log\left(\frac{P+N}{N}\right) \leq C \leq W \log\left(\frac{P+N}{\mathcal{E}_Z}\right), \tag{6}$$

where $\mathcal{E}_Z$ is the *entropy power* of Z. Suppose Z is a superposition of Gaussian noise G and uniform noise U. Since G and U are zero-mean independent random variables,

$$N = E[Z^2] = Var(G) + Var(U) = \sigma^2 + \frac{\delta^2}{12}. \tag{7}$$

The entropy power for a random variable Z is defined as,

$$\mathcal{E}_Z = \frac{1}{2\pi e} 2^{2h(Z)},$$

where $h(Z)$ is the differential entropy of Z. Here, the entropy power of Z cannot be easily calculated. Hence, we use the convolution inequality of entropy powers to find an upper bound on $\mathcal{E}_Z$. The convolution inequality of entropy powers states that the entropy power of the sum of two independent random variables is greater than or equal to the sum of the entropy powers of the summands [28], [30]. Thus,

$$\begin{aligned}\mathcal{E}_Z &\geq \mathcal{E}_G + \mathcal{E}_U \\ &= Var(G) + \frac{6}{\pi e} Var(U) \\ &= \sigma^2 + \frac{\delta^2}{2\pi e}.\end{aligned} \tag{8}$$

From (6) and (7), the capacity of Bob's channel can be lower bounded as:

$$\begin{aligned}C_B &\geq W \log\left(\frac{P + N_B}{N_B}\right) \\ &= W \log\left(\frac{P + \sigma_B^2 + \frac{\delta_B^2}{12}}{\sigma_B^2 + \frac{\delta_B^2}{12}}\right).\end{aligned} \tag{9}$$

Now consider Eve's receiver with bandwidth W_E. If $W_E < F$, since Eve does not know the hopping pattern, she will lose anything that is sent outside of the bandwidth that she is currently monitoring, i.e., she can only obtain a fraction $\frac{W_E}{F}$ of the message. If in addition to frequency hopping, Alice adds a random jamming signal to the transmitted signal, according to Section III-A Eve should increase the span of her A/D to avoid A/D overflows. Suppose k bits per jamming symbol are employed by Alice; hence, the new resolution of Eve's A/D is

$$\delta'_E = \frac{2l\sigma}{2^{b_e - k}}.$$

Using this fact and from (6), (7) and (8), an upper bound for the capacity of Eve's channel is:

$$\begin{aligned}C_E &\leq \frac{W_E}{F} W \log\left(\frac{P + N_E}{\mathcal{E}_{ZE}}\right) \\ &\leq \frac{W_E}{F} W \log\left(\frac{P + \sigma_E^2 + \frac{\delta_E'^2}{12}}{\sigma_E^2 + \frac{\delta_E'^2}{2\pi e}}\right).\end{aligned} \tag{10}$$

Thus, from (9) and (10), a lower bound on the secrecy capacity is:

$$\begin{aligned}C_s &= C_B - C_E \\ &\geq W \log\left(\frac{P + \sigma_B^2 + \frac{\delta_B^2}{12}}{\sigma_B^2 + \frac{\delta_B^2}{12}}\right) - \frac{W_E W}{F} \log\left(\frac{P + \sigma_E^2 + \frac{\delta_E'^2}{12}}{\sigma_E^2 + \frac{\delta_E'^2}{2\pi e}}\right).\end{aligned} \tag{11}$$

Hence, any secrecy rate,

$$\begin{aligned}R_s = \Bigg[& W \log\left(\frac{P + \sigma_B^2 + \frac{\delta_B^2}{12}}{\sigma_B^2 + \frac{\delta_B^2}{12}}\right) \\ & - \frac{W_E W}{F} \log\left(\frac{P + \sigma_E^2 + \frac{\delta_E'^2}{12}}{\sigma_E^2 + \frac{\delta_E'^2}{2\pi e}}\right)\Bigg]^+,\end{aligned} \tag{12}$$

is achievable. The secrecy rate versus bandwidth and resolution of Eve's receiver is shown in Fig. 9. In this example, both Bob and Eve have channels with SNR equal to 30 dB. Bob has a 20-bit A/D, $W = 100$ kHz, and transmitter span $F = 100$ MHz. In Fig. 9(a) only frequency hopping is employed, and it can be seen that by using a wideband receiver at Eve, the secrecy rate is zero. In Fig. 9(b), in addition to the frequency hopping, a random jamming signal with $k = 20$ bits per jamming symbol is added to the signal, which helps the legitimate nodes to obtain a positive secrecy rate (for this setting, the worst case rate of 2.736 bits/s/Hz is available), even when Eve uses a wideband receiver and a high resolution A/D. However, in this case the number of jamming bits needed to gain a non-zero secrecy rate is large. Furthermore, if Eve uses a wideband receiver with a very high resolution A/D, the secrecy capacity with a 20-bit A/D at Bob will be zero. In the next section, we will see that speed-resolution limitation of A/Ds helps us to obtain non-zero secrecy rates with much fewer numbers of key bits per jamming symbol, and in all feasible scenarios.

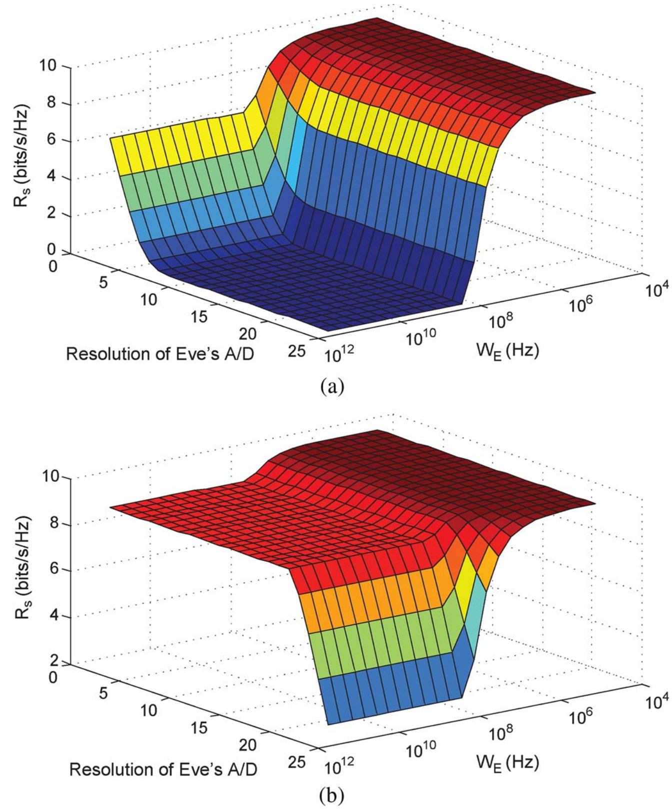

Fig. 9. Secrecy rate versus bandwidth and resolution of Eve's receiver: (a) frequency hopping, (b) frequency hopping with a 20-bit random jamming signal. Both Bob and Eve have channels of SNR equal to 30 dB. Bob has a 20-bit A/D, signal bandwidth $W = 100$ kHz, and transmitter span $F = 100$ MHz. Without random jamming, the worst case secrecy rate is zero, while with random jamming, a worst case secrecy rate of 2.736 bits/s/Hz is achievable.

V. Discussion

A limiting factor in the performance of A/Ds is aperture jitter, which is the uncertainty in the sampling time of the A/D. In order to better understand the relationship between the aperture jitter of an A/D and its impact on an A/D's performance, let us consider the signal-to-noise-and-distortion ratio (SNDR) of an A/D. The SNDR of an A/D is the ratio of the root mean square (rms) of the amplitude of the input signal to the rms sum of all

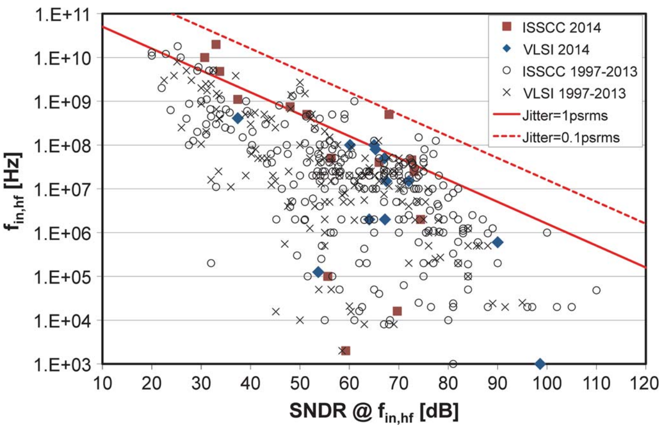

Fig. 10. Sampling frequency versus SNDR of published works from 1997 to 2014. The red lines are jitter envelopes. The solid line corresponds to 1 ps aperture jitter and the dashed line corresponds to 0.1 ps aperture jitter (courtesy of [32]).

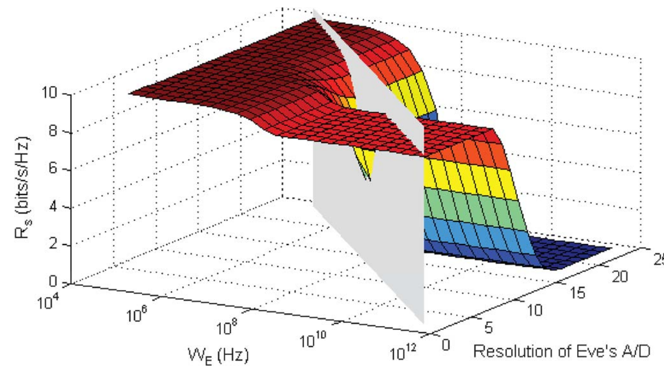

Fig. 11. Secrecy rate versus bandwidth and resolution of Eve's receiver, when a 10-bit random jamming signal is added to the transmitted signal. Both Bob and Eve have channels with SNR of 30 dB. Bob has a 20-bit A/D, $W = 100$ kHz, and transmitter bandwidth $F = 100$ MHz. The gray plane is the current technology jitter envelope (0.1 ps). The bandwidth-resolutions on the right side of the gray plane are not feasible by the current technology, and thus a worst case secrecy rate of 4.25 bits/s/Hz is available.

other spectral components. The signal-to-noise-and-distortion ratio due to the aperture jitter t_j when the input signal is sampled with frequency f_{in} is [31]:

$$\mathrm{SNDR}_j = 20\log_{10}\left(\frac{1}{2\pi f_{in} t_j}\right). \tag{13}$$

Hence, when other non-idealities (quantization noise, thermal noise, etc.) of the A/D are not considered, (13) describes the performance limit of an A/D due to the aperture jitter. The sampling rate versus SNDR for trends in the current state-of-the-art of A/Ds is shown in Fig. 10. In this figure, the performance envelope of (13) is shown by a solid red line for $t_j = 1$ ps, and a dashed red line for $t_j = 0.1$ ps. It can be seen that the best aperture jitter achieved by the current state-of-the art of A/Ds is 0.1 ps.

The relationship between SNDR and effective number of bits (ENOB) can be found by using the relationship between SNDR and number of bits for an ideal A/D,

$$\mathrm{SNDR} = 6.02\ \mathrm{ENOB} + 1.76\ \mathrm{dB} \tag{14}$$

Thus, in Fig. 10, with a change in the scaling of the horizontal axis, SNDR is equivalent to ENOB.

From the numerical results at the end of the previous section, it seems that it is always possible for Eve to use a wideband high-resolution A/D to compromise secrecy, in the same way that a larger than envisioned memory at Eve would compromise secrecy in the bounded memory model of [16], [33]–[38]. However, from the discussion above, aperture jitter is a critical limitation in the performance of A/Ds that prevents Eve from increasing the bandwidth and resolution of her A/D arbitrarily. In fact, aperture jitter restricts the product of the sampling rate and the resolution of an A/D.

In Fig. 11, the secrecy rate versus bandwidth and resolution of Eve's A/D, when a 10-bit random jamming signal is added to the transmitted signal is shown. In this figure, both Bob and Eve have channels with an SNR of 30 dB. Bob has a 20-bit A/D, a signal bandwidth $W = 100$ kHz, and a transmitter span of $F = 100$ MHz. The gray plane in this figure is the current technology jitter envelope. Assuming that the eavesdropper has access to the best A/D with current technology, the bandwidth-resolutions she can utilize are restricted to this jitter envelope, and anything beyond this envelope is not feasible. Hence, the minimum secrecy rate in this case is 4.25 bit/s/Hz. This shows that, in practice, much fewer key bits per jamming symbol are needed compared to Fig. 9(b), and, for current technology (0.1 ps jitter), the eavesdropper cannot compromise secrecy by employing a better A/D. Clearly, in this case either the aperture jitter of the eavesdropper's A/D should be known to legitimate nodes, or they should assume that the eavesdropper has access to the best current technology.

A. Aperture Jitter Evolution and Its Ultimate Limit

The best aperture jitter for A/Ds has changed from 100 ps in the 1980s to 0.1 ps in the current state of the art. This improvement of the jitter might seem unfavorable to our proposed method, as we rely on the non-ideality of the eavesdropper's A/D. Thus, if the jitter improves with the same slope, unbounded over time, it can destroy the ability to transmit messages with the proposed method at some point in the future. However, the trend of A/D jitter shows that the current state of the art was achieved in 2005, and has not changed significantly since that time. This, along with the fact that the technology scaling has changed dramatically since 2005, suggests that the performance of A/D aperture jitter is already in a state of saturation [32], [39]. Nevertheless, it is possible that the aperture jitter improves over time. Fortunately, there exists an ultimate limit on the ability to store an accurate reconstruction of an analog signal due to the Heisenberg uncertainty principle [19]–[21].

VI. Conclusion and Future Work

In this paper, we have introduced a method to convert ephemeral "cheap" cryptographic key bits to "expensive" information-theoretically secure bits to achieve everlasting security in wireless environments where the intended recipient Bob is at a disadvantage relative to the eavesdropper Eve. A random jamming signal chosen from a discrete uniform random ensemble based on a key pre-shared between the transmitter Alice and Bob is added to each transmitted symbol. The intended receiver uses the key sequence to subtract the jamming signal, while the eavesdropper Eve, in order to prevent overflows of her analog-to-digital (A/D) converter, needs to enlarge her A/D span and thus degrade the resolution of her A/D, thus resulting in information loss even if Eve is handed the key at the conclusion of transmission and is able to modify her recorded signal to attempt to remove the jamming effect. The numerical results show that this method can provide secrecy even in the case that the eavesdropper has perfect access to the output of the transmitter's radio and an A/D of much better quality than that of the intended receiver. We have also considered the case when the legitimate nodes and the eavesdropper have access to wideband channels.

When the channel bandwidth is larger than the signal bandwidth, the legitimate nodes can use their cryptographic key bits to try to hide the location of the signal from Eve by employing a frequency hopping technique. With this extra degree of freedom, since the product of the bandwidth and the resolution of an A/D is limited by its aperture jitter, Eve will be forced to make an additional tradeoff between A/D resolution and sampling frequency. Hence, the strategy of system nodes is to use frequency hopping in conjunction with the additive random jamming method. Eve must choose to either use a high resolution A/D with small bandwidth and thus lose anything outside her bandwidth, or use a wideband A/D with low resolution and thus be susceptible to the random jamming signal. Technology trend lines and fundamental limits for A/Ds indicate this will pose a significant challenge to Eve.

REFERENCES

[1] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik, "Everlasting secrecy in disadvantaged wireless environments against sophisticated eavesdroppers," in *Proc. IEEE Asilomar*, 2014, pp. 1994–1998.

[2] D. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA: CRC Press, 2006.

[3] R. Benson, "The verona story," Nat. Security Agency Central Security Service, Washington, DC, USA, Historical Publications. [Online]. Available: www.nsa.gov

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

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

[6] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Technol. Conf.*, 2005, vol. 62, pp. 1906–1910.

[7] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proc. IEEE Military Commun. Conf.*, 2005, pp. 1501–1506.

[8] L. Lai and H. El Gamal, "Cooperative secrecy: The relay-eavesdropper channel," in *Proc. IEEE Int. Symp. Inf. Theory*, 2007, pp. 931–935.

[9] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[10] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE GLOBECOM*, 2008, pp. 1–5.

[11] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Cooperative jamming for wireless physical layer security," in *Proc. IEEE/SP Workshop Statist. Signal Process.*, 2009, pp. 417–420.

[12] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in mimo relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[13] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.

[14] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[15] A. Sheikholeslami, D. Goeckel, and H. Pishro-nik, "Everlasting secrecy by exploiting non-idealities of the eavesdroppers receiver," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1828–1839, Sep. 2013.

[16] C. Cachin and U. Maurer, "Unconditional security against memory-bounded adversaries," *Adv. Cryptology*, vol. 1294, pp. 292–306, 1997.

[17] R. Kuchibhatla, "IMFT 25-nm MLC NAND: Technology scaling barriers broken," EE Times News and Analysis, 2010.

[18] A. Sheikholeslami, D. Goeckel, and H. Pishro-nik, "Exploiting the non-commutativity of nonlinear operators for information-theoretic security in disadvantaged wireless environments," in *Proc. IEEE Allerton Conf.*, 2012, pp. 233–240.

[19] R. H. Walden, "Analog-to-digital converter survey and analysis," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 4, pp. 539–550, Apr. 1999.

[20] S. Krone and G. Fettweis, "Fundamental limits to communications with analog-to-digital conversion at the receiver," in *Proc. IEEE Workshop Signal Process. Adv. Wireless Commun.*, 2009, pp. 464–468.

[21] S. Krone and G. Fettweis, "A fundamental physical limit to data transmission and processing," *IEEE Signal Process. Lett.*, vol. 17, no. 3, pp. 305–307, Mar. 2010.

[22] E. Rescorla, "Diffie-Hellman key agreement method," RFC 2631, Internet Engineering Task Force, Jun. 1999.

[23] C. Paar andJ. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Berlin, Germany: Springer-Verlag, 2010.

[24] B. Widrow and I. Kollár, *Quantization Noise*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[25] M. Bloch and J. Laneman, "On the secrecy capacity of arbitrary wiretap channels," in *Proc. 46th Annu. Allerton Conf.*, 2008, pp. 818–825.

[26] T. Cover *et al.*, *Elements of Information Theory*. New York, NY, USA: Wiley, 2006.

[27] C. H. Bennett *et al.*, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, 1984, vol. 175, p. 8.

[28] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 623–656, Oct. 1948.

[29] S. Ihara, "On the capacity of channels with additive non-Gaussian noise," *Elsevier Inf. Control*, vol. 37, no. 1, pp. 34–39, Apr. 1978.

[30] N. M. Blachman, "The convolution inequality for entropy powers," *IEEE Trans. Inf. Theory*, vol. IT-11, no. 2, pp. 267–271, Apr. 1965.

[31] W. A. Kester, *Data Conversion Handbook*. New York, NY, USA: Newnes, 2005.

[32] B. Murmann, "ADC Performance Survey 1997–2014." [Online]. Available: http://web.stanford.edu/\ignorespacesmurmann/adcsurvey.html

[33] C. Cachin, C. Crépeau, and J. Marcil, "Oblivious transfer with a memory-bounded receiver," in *Proc. 39th Annu. Symp. Found. Comput. Sci.*, 1998, pp. 493–502.

[34] Y. Aumann and M. O. Rabin, "Information theoretically secure communication in the limited storage space model," in *Proc. Adv. Cryptology*, 1999, pp. 65–79.

[35] S. Dziembowski and U. Maurer, "Tight security proofs for the bounded-storage model," in *Proc. 34th Annu. ACM Symp. Theory Comput.*, 2002, pp. 341–350.

[36] Y. Aumann, Y. Z. Ding, and M. O. Rabin, "Everlasting security in the bounded storage model," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1668–1680, Jun. 2002.

[37] S. Dziembowski and U. Maurer, "The bare bounded-storage model: The tight bound on the storage requirement for key agreement," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2790–2792, Jun. 2008.

[38] R. Dowsley, F. Lacerda, and A. C. Nascimento, "Oblivious transfer in the bounded storage model with errors," in *Proc. IEEE ISIT*, 2014, pp. 1623–1627.

[39] B. E. Jonsson, "A/D-converter performance evolution," Converter Passion, 2012.

Azadeh Sheikholeslami received the B.Sc. degree in electrical engineering from the University of Tehran, Tehran, Iran, and the M.Sc. degree in communications engineering from Sharif University of Technology, Tehran, Iran. She is currently working toward the Ph.D. degree in electrical engineering at the University of Massachusetts, Amherst, MA, USA.

Her current research interests include network information theory and physical layer security.

Dennis Goeckel (S'89–M'92–SM'04–F'11) received the B.S. degree from Purdue University in 1992, and the M.S. and Ph.D. degrees from the University of Michigan in 1993 and 1996, respectively. Since 1996, he has been with the Electrical and Computer Engineering Department, University of Massachusetts at Amherst, where he is currently a Professor. He has been a Lilly Teaching Fellow (2000–2001) and received the University of Massachusetts Distinguished Teaching Award in 2007. He has served on the Editorial Board of a number of international journals in communications and networking: IEEE TRANSACTIONS ON NETWORKING, IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTION ON WIRELESS COMMUNICATIONS, and the IEEE TRANSACTIONS ON COMMUNICATIONS. He received the NSF CAREER Award in 1999.

Hossein Pishro-Nik received the B.S. degree from Sharif University of Technology, and the M.Sc. and Ph.D. degrees from the Georgia Institute of Technology, all in electrical and computer engineering. He is an Associate Professor of electrical and computer engineering at the University of Massachusetts, Amherst. His research interests include the mathematical analysis of communication systems, in particular, error control coding, wireless networks, and vehicular ad hoc networks. His awards include an NSF Faculty Early Career Development (CAREER) Award, an Outstanding Junior Faculty Award from UMass, and an Outstanding Graduate Research Award from the Georgia Institute of Technology.