IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 8, 2017, accepted November 6, 2017, date of publication November 9, 2017,
date of current version November 28, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2771760

Channel-Aware Randomized Encryption and Channel Estimation Attack

JINHO CHOI
School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea
jchoi0114@gist.ac.kr

This work was supported in part by the Institute for Information and communications Technology Promotion under Grant funded by the Korea government (MSIT) under Grant 2017-0-00413 and in part by the Streamlined IoT Communications by Physical Layer Device Identification)

ABSTRACT In this paper, we study the channel-aware (CA) randomization for a simple physical-layer encryption scheme and show that the probability of successful attack becomes very low by CA randomization when the known plain-text attack is carried out. As CA randomization becomes vulnerable to the channel estimation attack, its impact on the performance is investigated in terms of the average number of known elements of a key subsequence when the known plain-text attack is performed together with the channel estimation attack.

INDEX TERMS Physical-layer security, randomized encryption, physical-layer encryption.

I. INTRODUCTION

Physical-layer security (PLS) is to exploit transmission channels for secure communications based on information-theoretic approaches [1]. In [2]–[4], for various wiretap channels, the secrecy capacity or rate, which is the maximum data rate with perfect secrecy [5], has been studied. Channel coding plays a crucial role in PLS to achieve the secrecy rate [6], [7] and various approaches are proposed with existing codes, e.g., [8], [9].

In [10], PLS is considered for encryption and it is shown that PLS can help improve the security of encryption. For secure transmissions in wireless sensor networks (WSNs), the notion of PLS is applied to a simple encryption scheme that is well-suited to sensors of limited computing power and energy in [11]. In [12], the randomization in the physical layer is employed to improve the security of a stream cipher in a multiuser system. In general, the approaches in [10]–[12] are different from conventional randomized encryption schemes [13], [14] as the randomization is carried out in the physical layer. In addition, in [11] and [12], encryption is considered in the physical layer to take into account channel conditions. For convenience, this kind of approach is referred to as physical-layer encryption in this paper in order to differentiate conventional encryption approaches that are implemented in a higher layer (e.g., transportation layer) [15]. As discussed in [16], in WSNs or the Internet of Things (IoT), since sensors or IoT devices have limited computing power, physical-layer encryption can be an attractive solution as it can provide reasonably secure transmissions with simple low-complexity ciphers (such as stream ciphers) in the physical layer.

It is noteworthy that there are also different approaches for physical-layer encryption based on compressive sensing (CS) [17], [18]. In [19] and [20],CS encryption (studied in [21], [22]) is considered in the physical layer to exploit different channel conditions of a legitimate receiver and an adversary.

In this paper, we consider a physical-layer encryption approach that is based on channel-aware (CA) randomization in a multicarrier system. Throughout the paper, it is assumed that a legitimate transmitter, called Alice, and a legitimate receiver, called Bob, know the channel state information (CSI) from Alice to Bob. The knowledge of partial CSI is exploited for randomization in physical-layer encryption. In particular, we consider CA randomization for encryption with a stream cipher [15], which is a lightweight cryptographic scheme and could be easily implemented using simple hardware (this makes stream ciphers attractive for sensors and IoT devices). The impact of CA randomization on the performance of the known plain-text attack [15] is studied. To see the performance, we consider the probability of successful attack. From this, we could see how CA randomization can improve the robustness of a lightweight cryptographic scheme against attacks in a multicarrier system.

Since Eve can be easily confused by CA randomization when she does not have Bob's CSI, she would try to estimate Bob's CSI by approaching Bob. Thus, we study this

attack and show the impact of correlation of channels on the performance.

It is noteworthy that although the CA randomization in this paper uses random signals, it differs from the approaches that use artificial noise to increase the secrecy rate [23]–[25]. The main purpose of the CA randomization is to induce randomness in encryption to confuse Eve, while Bob can recover a secret message using known CSI that can be seen as a shared secret key between Alice and Bob. Thus, the random signals in this paper should have the same[1] statistical properties as the secret signals. Furthermore, the performance measure in this paper is not the secrecy rate, but the probability of successful attack (for a given attack method), because CA randomized physical-layer encryption does not achieve perfect secrecy.

The rest of the paper is organized as follows. In Section II, we present a CA randomized physical-layer encryption method in a multicarrier system. An effective attack that is based on the channel estimation is studied and the performance analysis is carried out in Section III. Numerical results are presented in Section IV. Finally, the paper is concluded with some remarks in Section V.

Notation: Matrices and vectors are denoted by upper- and lower-case boldface letters, respectively. The superscripts T and H denote the transpose and complex conjugate transpose, respectively. For a vector $\mathbf{a}$, diag($\mathbf{a}$) is the diagonal matrix with the diagonal elements from $\mathbf{a}$. For a matrix $\mathbf{X}$ (a vector $\mathbf{x}$), $[\mathbf{X}]_n$ ($[\mathbf{x}]_n$) represents the nth column (element, resp.). If $\mathcal{A}$ is a set of indices, $[\mathbf{x}]_{\mathcal{A}}$ is a subvector of $\mathbf{x}$ obtained by taking the corresponding elements. $\mathbb{E}[\cdot]$ denotes the statistical expectation. $\mathcal{CN}(\mathbf{a}, \mathbf{R})$ represents the distribution of circularly symmetric complex Gaussian (CSCG) random vectors with mean vector $\mathbf{a}$ and covariance matrix $\mathbf{R}$.

II. CA RANDOMIZED PHYSICAL-LAYER ENCRYPTION

A. SYSTEM MODEL AND ASSUMPTIONS

Suppose that there is a pair of legitimate transmitter and receiver, called Alice and Bob, respectively, and an adversary (or an eavesdropper), called Eve. We consider a multicarrier system for secure transmissions from Alice to Bob with L subcarriers over a wideband channel. Suppose that Alice transmits a block of signal symbols over L subcarriers, which is denoted by $\mathbf{s} \in \mathbb{C}^{L\times 1}$. Then, the received signal at Bob is given by

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{n}, \tag{1}$$

where $\mathbf{n} \sim \mathcal{CN}(0, N_0\mathbf{I})$ is the background noise vector and $\mathbf{H} = \text{diag}(H_0, \ldots, H_{L-1})$ is a diagonal (frequency-domain) channel matrix. Here, H_l denotes the channel coefficient over the lth subcarrier from Alice to Bob.

Similarly, the received signal at Eve is given by

$$\mathbf{z} = \mathbf{G}\mathbf{s} + \mathbf{w}, \tag{2}$$

where $\mathbf{w} \sim \mathcal{CN}(0, N_0\mathbf{I})$ is the background noise vector and $\mathbf{G} = \text{diag}(G_0, \ldots, G_{L-1})$ is a diagonal (frequency-domain) channel matrix. Here, G_l represents the channel coefficient over the lth subcarrier from Alice to Eve. We consider the following assumption throughout the paper.

A1) The channel coefficients in the frequency domain[2] are

$$H_l \sim \mathcal{CN}(0, \sigma_H^2) \text{ and } G_l \sim \mathcal{CN}(0, \sigma_G^2). \tag{3}$$

In addition, H_l and G_l are independent.

Let $\alpha_l = |H_l|^2$ and $\beta_l = |G_l|^2$. We also assume time division duplexing (TDD) mode for CA secure transmissions [16], [19], [26]. Bob can transmit a pilot signal to allow Alice to estimate Bob's CSI, $\mathbf{H}$. In addition, Alice sends a pilot signal to Bob so that Bob can estimate his CSI, $\mathbf{H}$. Note that due to the pilot signal from Alice, Eve can also estimate her CSI, $\mathbf{G}$. Therefore, throughout the paper, we assume that both Alice and Bob know $\mathbf{H}$, but not $\mathbf{G}$, and Eve knows $\mathbf{G}$, but not $\mathbf{H}$.

Note that as in [26], the estimation of CSI is imperfect due to the presence of background noise and the CSI estimation error has to be taken into account. However, we do not consider the CSI estimation error in this paper. In particular, for a tractable analysis of the channel estimation attack in Section III, we will assume that the CSI is perfectly estimated (while the impact of the CSI estimation error might be considered for future research).

B. CA RANDOMIZED ENCRYPTION

Alice can transmit signals through a subset of the subcarriers of the power gains greater than or equal to τ. Here, τ is positive and a design parameter. The resulting CA scheme relies on the partial CSI, which is defined as

$$D_l = \mathbb{1}(\alpha_l \geq \tau), \tag{4}$$

where $\mathbb{1}(S)$ is the indicator function that becomes 1 if the statement S is true and 0 otherwise. For convenience, we also define

$$\mathcal{I} = \{l \,|\, D_l = 1\} = \{l \,|\, \alpha_l \geq \tau\}. \tag{5}$$

Alice transmits a secret message over $\mathcal{I}$ and random signals over $\mathcal{I}^c$, where $\mathcal{I}^c$ represents the complement set of $\mathcal{I}$. Since Bob knows $\mathcal{I}$ from $\mathbf{H}$, he can choose the signals transmitted through $\mathcal{I}$ and discard the random signals transmitted through $\mathcal{I}^c$. On the other hand, Eve does not exactly know $\mathcal{I}$. Thus, since she has to consider the signals through all the subcarriers and due to random signals, she may have an incorrect message. A similar CA randomization approach (with interleaving according to the channel gains) is used in [26]. Note that the CA randomization based on the partial CSI in (4) is an indirect approach to extract the secret-key from CSI as opposed to direct approaches, e.g. [27]. Since only one-bit quantization is used as in (4), it might be robust against the CSI estimation error, although the CSI estimation

[1]For example, if the secret signals are independent binary random variables, the random signals are also independent binary random variables.

[2]The channel coefficients in the frequency domain, H_l's, can be correlated. However, if the subset of subcarriers with sufficient frequency spacing is used, the corresponding H_l's can be assumed to independent.

error[3] is not considered in this paper. In this subsection, CA randomization is applied to a simple cipher for physical-layer encryption as follows.

Let $\mathbf{m} = [m_0 \ \ldots \ m_{M-1}]$ denote the secret message or plain-text to Bob, where $M = |\mathcal{I}|$. In addition, let

$$\alpha_{m(0)} \geq \ldots \geq \alpha_{m(L-1)}, \tag{6}$$

where $m(l)$ denotes the index of the subcarrier whose channel gain is the lth largest. Clearly, we have $\mathcal{I} = \{m(0), \ldots, m(M-1)\}$. We consider a randomized physical-layer encryption method that uses Bob's CSI, $\mathbf{H}$, or CA randomized encryption, which is denoted by

$$\mathbf{c} = \mathcal{E}(\mathbf{m}, \mathbf{H}), \tag{7}$$

where $\mathbf{c}$ is the cipher-text of length L. In this section, we consider the following encryption method:

$$\mathcal{E}(\mathbf{m}, \mathbf{H}) = [\mathbf{m}\ \mathbf{r}]\mathbf{P}_{\mathbf{H}}, \tag{8}$$

where $\mathbf{r}$ of size $1 \times (L-M)$ is a random bit sequence and $\mathbf{P}_{\mathbf{H}}$ is a permutation matrix that depends on $\mathbf{H}$, which is given by

$$[\mathbf{P}_{\mathbf{H}}]_{m,l} = \begin{cases} 1, & \text{if } m = m(l); \\ 0, & \text{o.w.;} \end{cases}$$

Note that $\mathcal{E}(\cdot, \cdot)$ can be seen as a homophonic encoder [28] with the random bit sequence, $\mathbf{r}$. The statistical properties of $\mathbf{r}$ should be the same as those of $\mathbf{m}$ so that Eve cannot exploit any statistical differences to find $\mathbf{m}$.

At Bob, if $\mathbf{c}$ is available, $\mathbf{m}$ can be found by the following decryption method:

$$\mathcal{D}(\mathbf{c}, \mathbf{H}) = \left[\mathbf{c}\mathbf{P}_{\mathbf{H}}^{-1}\right]\begin{bmatrix}\mathbf{I} \\ \mathbf{0}\end{bmatrix}. \tag{9}$$

That is, when $\mathbf{c} = \mathcal{E}(\mathbf{m}, \mathbf{H})$, we can readily show that

$$\hat{\mathbf{m}} = \mathcal{D}(\mathbf{c}, \mathbf{H}) = ([\mathbf{m}\ \mathbf{r}]\mathbf{P}_{\mathbf{H}})\,\mathbf{P}_{\mathbf{H}}^{-1}\begin{bmatrix}\mathbf{I} \\ \mathbf{0}\end{bmatrix} = \mathbf{m}.$$

For simplicity, in this section, we consider the following binary phase shift keying (BPSK) mapping to transmit $\mathbf{c}$:

$$\mathcal{S}(b) = \sqrt{P}(1 - 2\,b), \ b \in \{0, 1\}.$$

Then, $\mathbf{c}$ becomes $\mathbf{s} = [s_0 \ \ldots \ s_{L-1}]^{\mathrm{T}}$ in (1) and (2), where

$$s_l = \mathcal{S}(c_l \oplus x_l). \tag{10}$$

Here, $\mathbf{x} = [x_0 \ \ldots \ x_{L-1}]$, where $x_l \in \{0, 1\}$, represents a subsequence of a key sequence obtained by a pseudorandom number (PN) generator.

III. CHANNEL ESTIMATION ATTACK

In this section, we focus on the performance of a known plain-text attack to estimate the key sequence of the CA randomized encryption scheme in Subsection II-B.

[3]The impact of CSI estimation error on permutation error or mismatch between Alice and Bob can be found in [26], where it is shown that the probability of permutation mismatch is negligible at a high signal-to-noise ratio (SNR).

A. KNOWN PLAIN-TEXT ATTACK

In this subsection, we discuss the known plain-text attack by Eve to find the key sequence. In this attack, we assume that Eve knows a message, $\mathbf{m}$, and M. With known message $\mathbf{m}$ and her received signal, $\mathbf{z}$, Eve can attempt to find $\mathbf{x}$.

If a PN generator is used with an initial vector, $\mathbf{x}$ becomes a subsequence of a PN sequence with a finite period. When Eve knows the structure of the PN generator, she might be able to determine the initial vector with some subsequences using correlation attacks [29], [30]. Thus, one successful attack (which provides M known elements of $\mathbf{x}$) may be enough for Eve to determine the initial vector and subsequently the key sequence. If the length of the initial vector is much longer than M, Eve needs more than one successful attack. In any case, in order to understand the level of security under the known plain-text attack, we are interested in finding the probability of successful attack, where the event of successful attack is defined as that Eve can correctly know M elements of $\mathbf{x}$ from $(\mathbf{m}, \mathbf{z})$ without knowing Bob's CSI, $\mathbf{H}$.

As mentioned earlier, we assume that Eve knows M, i.e., the length of the secret message. Thus, Eve is to choose M received signals from $\mathbf{z}$. For convenience, denote by $\mathcal{M}$ the index set of M selected received signals. Consider an index, say $\bar{l}$. If the $\bar{l}$th received signal, $z_{\bar{l}}$, corresponds to one of $\mathbf{m}$ and a decision is correctly carried out, Eve can perform the following operation:

$$s_{\bar{l}} \oplus c_{\bar{l}} = (c_{\bar{l}} \oplus x_{\bar{l}}) \oplus c_{\bar{l}} = x_{\bar{l}},$$

which provides an element of $\mathbf{x}$. The probability that Eve can make an incorrect decision provided that $\bar{l}$ corresponds to one of $\mathbf{m}$ is [31]

$$\begin{aligned}\theta &= \Pr(|z_{\bar{l}} - G_{\bar{l}}\sqrt{P}|^2 < |z_{\bar{l}} - G_{\bar{l}}(-\sqrt{P})|^2 \mid s_{\bar{l}} = -\sqrt{P}) \\ &= \mathbb{E}\left[\mathcal{Q}\left(\sqrt{\frac{2P|G_l|^2}{N_0}}\right)\right] \\ &= \frac{1}{2}\left(1 - \sqrt{\frac{\gamma_{\mathrm{E}}}{1+\gamma_{\mathrm{E}}}}\right),\end{aligned} \tag{11}$$

where $\gamma_{\mathrm{E}} = \frac{\sigma_G^2 P}{N_0}$, θ is the (conditional) error probability (provided that the selected index $\bar{l} \in \mathcal{I}$), and $\mathcal{Q}(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$. Thus, if Eve knows all the indices corresponding to $\mathbf{m}$ (which is possible when $\mathbf{P}_{\mathbf{H}}$ or Bob's CSI is available at Eve), the probability of successful attack, which is denoted by P_{SA}, becomes $P_{\mathrm{SA}} = (1-\theta)^M$. In other words, if γ_{E} is sufficiently high, Eve can expect a very high P_{SA}.

On the other hand, if $\bar{l}$ does not correspond to any of $\mathbf{m}$, Eve may have a random bit. Thus, if Eve cannot choose any index correctly, the probability of successful attack becomes $\left(\frac{1}{2}\right)^M = 2^{-M}$. Taking into account all possible combinations, we can find the probability of successful attack as follows.

Lemma 1: The probability of successful attack is given by

$$P_{SA} = \left(\frac{1}{2} + \left(\frac{1}{2} - \theta\right)\delta\right)^{\delta L}, \tag{12}$$

where $\delta = \frac{M}{L}$.

Proof: See Appendix A. ∎

In (12), for a fixed δ, P_{SA} can decrease exponentially with L, which implies that the probability of successful attack can be very low in a multicarrier system with large L, which becomes additional secrecy gain of a wider bandwidth system.

Note that although the successful attack can provide M elements of $\mathbf{x}$, their locations in $\mathbf{x}$ are unknown. Thus, Eve has to consider all possible combinations to determine correct locations, which would increase the computational cost at Eve. In addition, the probability of successful attack in (12) can increase if more pairs of known plain-text and its corresponding received signal are available under the same CSI. In particular, for independent known plain-text, the probability of successful attack with J pairs of known plain-text and its corresponding received signal would be $1-(1-P_{\mathrm{SA}})^J \approx JP_{\mathrm{SA}}$. In general, however, since the CSI is time-varying, the variation of CSI can limit the number of pairs, J. Thus, the overall probability of successful attack would be not be high if P_{SA} is sufficiently low and J is not too large.

Since a closed-form expression for the probability of successful attack is found as in (12), M can be decided to make the known plain-text attack more difficult (or to lower the probability of successful attack).

Lemma 2: There exists a unique minimum of $P_{SA}(M)$ *as it is a log-convex function of* M *(here,* $P_{SA}(M)$ *is used to emphasize that* P_{SA} *in* (12) *is a function of* M*). The minimum point lies between* 0 *and* L *if* $\theta < \frac{1}{4}$.

Proof: See Appendix B. ∎

According to Lemma 2, we can see that there is an optimal value of M that minimizes the probability of successful attack, and with a sufficiently low value of θ, the optimal value of M would lie between 0 and L. If L is very large, we may use a convex optimization technique to find the optimal value of M. However, if L is small, a linear search can be used.

B. CHANNEL ESTIMATION ATTACK

As shown in Subsection III-A, if CA randomization is employed, the probability of successful attack of the known plain-text attack, becomes negligible. To overcome this problem, Eve can consider the channel estimation attack. In this section, we study the channel estimation attack that can mitigate CA randomization to improve the performance of the known plain-text attack.

1) CORRELATION ANALYSIS OF CHANNEL ESTIMATION ATTACK

In the frequency-domain, we can have

$$G_l = \rho H_l + U_l, \tag{13}$$

where ρ is constant (which is the unnormalized correlation coefficient) and U_l is an independent CSCG random variable. In addition to **A1**, we consider the following assumption.

A2) $U_l \sim \mathcal{CN}(0, \sigma_U^2)$ is independent of H_l.

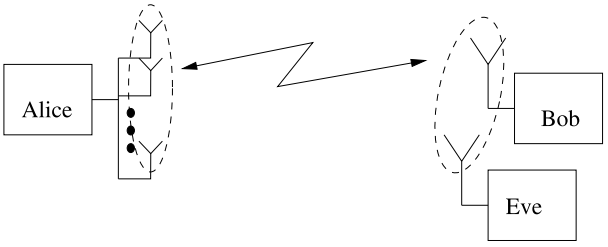


FIGURE 1. For effective channel estimation attack, Eve may approach Bob rather than Alice when Alice uses multiple antennas.

Under **A2**, from (13), σ_G^2 becomes

$$\sigma_G^2 = |\rho|^2\sigma_H^2 + \sigma_U^2 \tag{14}$$

and the correlation coefficient between G_l and H_l is given by

$$\rho_{G,H} = \frac{\mathbb{E}[G_l H_l^*]}{\sigma_G\sigma_H} = \frac{\rho\sigma_H^2}{\sigma_G\sigma_H}. \tag{15}$$

In general, Eve wants to have a large correlation coefficient and a large channel gain to mitigate CA randomization by precisely estimating H_l from G_l. To this end, Eve can approach Alice so that $\sigma_G^2 \gg \sigma_H^2$ and $|\rho_{G,H}| \to 1$. In order to avoid this problem, Alice can physically prevent anybody from approaching her. Alternatively, Alice can use multiple antennas (with sufficient spacing) so that Eve's channel can be correlated with only one of multiple antennas. In this case, Eve may choose to approach Bob[4] as illustrated in Fig. 1.

If Eve is close to Bob, we expect that the distance between Alice and Eve is similar to that between Alice and Bob and the average channel power gain at Eve is similar to that at Bob. Thus, we can assume that $\sigma_G^2 = \sigma_H^2$ or $\gamma_{\mathrm{E}} = \gamma_{\mathrm{B}}$. Consequently, Eve may not be able to enjoy both higher SNR (than Bob's SNR) and high correlation simultaneously. If $\sigma_G^2 = \sigma_H^2$, it can be shown that

$$\begin{aligned}\rho_{G,H} &= \rho\\ \sigma_U^2 &= \sigma_H^2(1-|\rho|^2).\end{aligned}$$

From this, we may modify **A2** as follows:

A2a) $U_l \sim \mathcal{CN}(0, \sigma_U^2)$ is independent of H_l and $\sigma_U^2 = \sigma_H^2(1-|\rho|^2)$ (or $\sigma_H^2 = \sigma_G^2$).

Under (13), Eve can attempt to estimate H_l for given G_l. To this end, the conditional probability density function (pdf) of H_l for given G_l, $f(H_l \mid G_l)$, can be considered. Under **A1** and **A2**, from (13), it can be seen that H_l is a conditional CSCG random variable for given G_l. Thus, from [32], the conditional mean becomes the minimum mean squared error (MMSE) estimate of H_l for given G_l, which is given by

$$\begin{aligned}\hat{H}_l &= \mathbb{E}[H_l \mid G_l] = \frac{\mathbb{E}[H_l G_l^*]}{\mathbb{E}[|G_l|^2]}G_l\\ &= \psi\rho^* G_l,\end{aligned} \tag{16}$$

[4]If Bob also employs multiple receive antennas, the channel correlation, $\rho_{G,H}$, can be low. To overcome this, Eve may have multiple antennas. However, for simplicity, we only assume that Bob and Eve are equipped with single antenna in this paper.

where $\psi = \frac{\sigma_H^2}{\sigma_H^2|\rho|^2+\sigma_U^2}$. Note that under **A2a**, $\psi = 1$. At Eve, once $\hat{H}_l$ is found, she can obtain an estimate of the partial CSI of Bob as

$$\hat{D}_l = \mathbb{1}(|\hat{H}_l|^2 \geq \tau_{\rm E}) = \mathbb{1}(\hat{\alpha}_l \geq \tau_{\rm E}), \tag{17}$$

where $\hat{\alpha}_l = |\hat{H}_l|^2$ and $\tau_{\rm E}$ is a design parameter that Eve can choose to decide whether or not the lth subcarrier is used to transmit secret information from Alice to Bob using CA randomization.

Note that $\hat{\alpha}_l$ becomes an exponential random variable as both H_l and U_l are CSCG random variables. Thus, it can be shown that

$$\hat{\alpha}_l \sim f(\hat{\alpha}_l) = \frac{1}{\sigma_{\hat{H}}^2} e^{-\frac{\hat{\alpha}_l}{\sigma_{\hat{H}}^2}}, \ \hat{\alpha}_l \geq 0,$$

where $\sigma_{\hat{H}}^2 = \mathbb{E}[|\hat{H}_l|^2] = \psi^2|\rho|^2\mathbb{E}[|G_l|^2]$. We can also readily show that $\sigma_{\hat{H}}^2 = |\rho|^2\sigma_H^2$ under **A2a**.

Lemma 3: Suppose that G_l is given as (13)*. Under **A1** and **A2**, a closed-form expression for the conditional probability of $\hat{D}_l = 1$ for given $D_l = 1$ can be found as*

$$\begin{aligned} P(\tau, \tau_E) &= \Pr(\hat{D}_l = 1 \,|\, D_l = 1) = \Pr(\hat{\alpha}_l \geq \tau_E \,|\, \alpha_l \geq \tau) \\ &= e^{\bar{\tau}}\Bigg[e^{-\bar{\tau}}\mathcal{Q}_1\left(a\sqrt{\tau}, \sqrt{\nu}\right) + e^{-\frac{\nu}{2+a^2\sigma_H^2}} \\ &\quad \times \left(1 - \mathcal{Q}_1\left(\sqrt{\tau\left(\frac{2}{\sigma_H^2} + a^2\right)}, \frac{a\sqrt{\nu}}{\sqrt{\frac{2}{\sigma_H^2} + a^2}}\right)\right)\Bigg], \end{aligned} \tag{18}$$

where

$$a = \sqrt{\frac{2|\rho|^2}{\sigma_U^2}},$$
$$\nu = \frac{2\tau_E}{\sigma_U^2\psi^2|\rho|^2},$$

and $\mathcal{Q}_m(a, b)$ is the Marcum Q-function that is defined as $\mathcal{Q}_m(a, b) = \int_b^\infty x\left(\frac{x}{a}\right)^{m-1} e^{-\frac{x^2+a^2}{2}} I_{m-1}(ax)\,dx$. Here, $I_n(x)$ is the modified Bessel function of order n.

Proof: See Appendix C. ∎

2) AVERAGE NUMBER OF KNOWN ELEMENTS OF KEY SUBSEQUENCE

For convenience, let K denote the number of the elements of $\mathbf{x}$ that are chosen and all correctly decided from $\mathbf{z}$ by Eve (for a given $\tau_{\rm E}$) by the known plain-text attack. If K is sufficiently large, Eve can successfully decide the initial vector of the PN generator. Thus, for Alice and Bob, a small K is desirable so that Eve cannot find the initial vector. In general, if G_l and H_l are highly correlated and $\tau_{\rm E} \approx \tau$, $K = M$ with a high probability. Note that if $\tau_{\rm E}$ is too small, there could also be random bits (of the indices in $\mathcal{I}^c$) within the selected K elements. In this case, the attack becomes unsuccessful. To avoid this, Eve can consider a large $\tau_{\rm E}$. In this case, however, K becomes small although the probability of successful attack is high. Consequently, $\tau_{\rm E}$ could play a crucial role in the known plain-text attack with the channel estimation attack.

Since K is a random variable and depends on $\tau_{\rm E}$, we now consider the average of K and derive a closed-form expression for it in terms of $\tau_{\rm E}$ and other parameters. Suppose that the lth element of $\mathbf{x}$, x_l, is chosen by Eve. Then, the conditional probability that this element is correctly determined becomes

$$\begin{aligned} \phi = (1 - \bar{\theta})\Pr(\alpha_l \geq \tau \,|\, \hat{\alpha}_l \geq \tau_{\rm E}) \\ + \frac{1}{2}\Pr(\alpha_l < \tau \,|\, \hat{\alpha}_l \geq \tau_{\rm E}), \end{aligned} \tag{19}$$

where $\bar{\theta}$ is the conditional error probability for given $\hat{\alpha}_l \geq \tau_{\rm E}$ or $|G_l|^2 = \beta_l \geq \bar{\tau}_{\rm E}$. That is, if $\alpha_l \geq \tau$, the conditional probability that x_l can be correctly decided becomes $1 - \bar{\theta}$. On the other hand, if $\alpha_l < \tau$, c_l is a randomized bit. Thus, the conditional probability that x_l can be correctly decided becomes $\frac{1}{2}$.

We can derive a closed-form expression for the expectation of K with ϕ as follows.

*Lemma 4: Under **A1** and **A2**, we have*

$$\begin{aligned} \bar{K}(\tau, \tau_E) &= \mathbb{E}[K] \\ &= LB(B + 1 - \varphi)^{L-1}. \end{aligned} \tag{20}$$

where

$$\varphi = \Pr(\hat{\alpha}_l \geq \tau_E) = e^{-\frac{\tau_E}{\sigma_{\hat{H}}^2}}$$
$$B = \frac{\varphi}{2} + \left(\frac{1}{2} - \bar{\theta}\right)P(\tau, \tau_E)e^{-\bar{\tau}}.$$

Proof: See Appendix D. ∎

The average of K in (20) is a function of τ and $\tau_{\rm E}$. Eve wants to choose $\tau_{\rm E}$ to maximize $\bar{K}(\tau, \tau_{\rm E})$.

In (20), we need to know $\bar{\theta}$. Unfortunately, it is not easy to find an exact closed-form expression for $\bar{\theta}$, but a lower-bound on $\bar{\theta}$ can be found as follows.

*Lemma 5: Under **A1**, the conditional error probability, $\bar{\theta}$ is lower-bounded as*

$$\bar{\theta} \geq \max_{\kappa \geq 1} \frac{C(\kappa)e^{-\frac{P\bar{\tau}_E\kappa}{N_0}}}{1 + \kappa\gamma_E}, \tag{21}$$

where $C(\kappa)$ is a function of κ, which is given by [33]

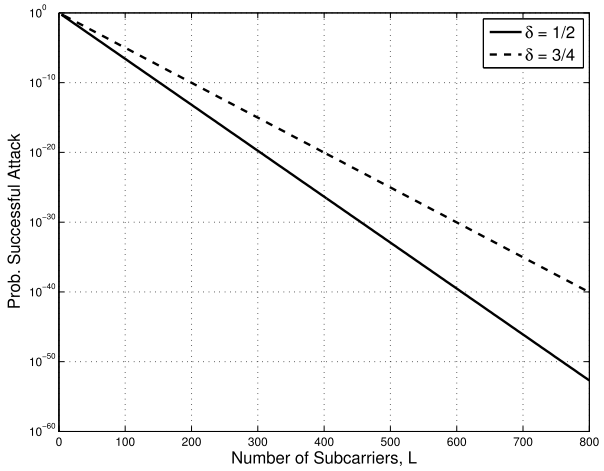
$$C(\kappa) = \frac{e^{(\pi(\kappa-1)+2)^{-1}}}{2\kappa}\sqrt{\frac{(\kappa-1)(\pi(\kappa-1)+2)}{\pi}}. \tag{22}$$

Proof: See Appendix E. ∎

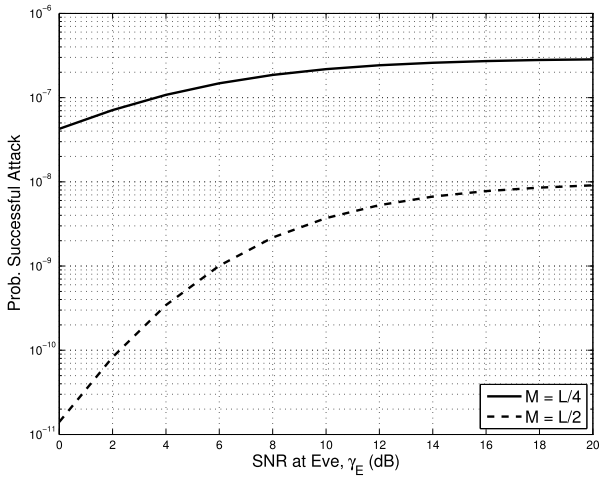
Note that we can find an upper-bound on $\mathbb{E}[K]$ using (21) in a closed-form.

IV. NUMERICAL RESULTS

In this section, we present numerical results for the probability of successful attack when the known plain-text attack is carried out by Eve under **A1** and **A2a** (i.e., $\sigma_H^2 = \sigma_G^2$ or $\gamma_{\rm B} = \gamma_{\rm E}$ in this case). In particular, we assume that $\sigma_H^2 = \sigma_G^2 = 1$.



(a)



(b)

FIGURE 2. Probability of successful attack: (a) P_{SA} versus L when $\gamma_E = 10$ dB; (b) P_{SA} versus γ_E when $M \in \{32, 64\}$ and $L = 128$.

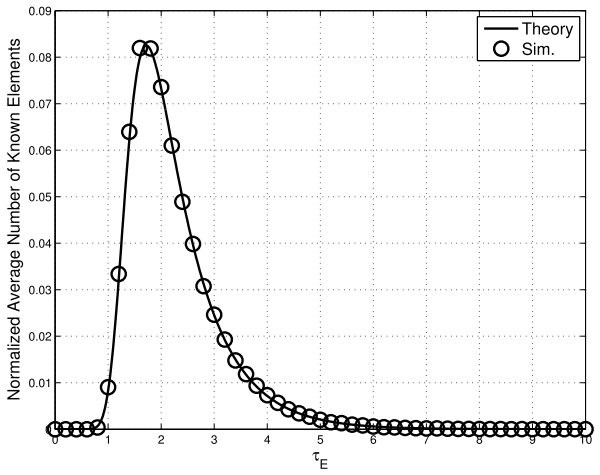


FIGURE 3. Normalized average number of known elements of x, $\frac{\mathbb{E}[K]}{L}$, for various values of τ_E when $L = 128$, $\gamma_B = \gamma_E = 10$ dB, $\tau = 1$, and $\rho = 0.9$.

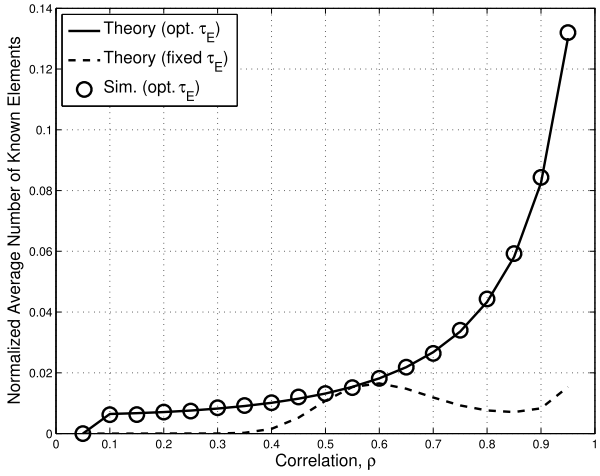


FIGURE 4. Normalized average number of known elements of x, $\frac{\mathbb{E}[K]}{L}$, for various values of ρ when $L = 128$, $\gamma_B = \gamma_E = 10$ dB, and $\tau = 1$. For fixed τ_E, we assume $\tau_E = \tau = 1$.

We first consider the case that Eve does not consider the channel estimation attack. In Fig. 2 (a), when $\gamma_E = 10$ dB, the probability of successful attack for various values of L is shown with fixed δ, which is shown in (12). We can confirm that it is beneficial to have a large L as the probability of successful attack decreases exponentially with L for a fixed δ. In Fig. 2 (b), the probability of successful attack is shown for various values of γ_E. Clearly, a better known plain-text attack can be carried out as γ_E is high.

We now consider the case that Eve performs the channel estimation attack to improve the performance of the known plain-text attack. To see the performance, we consider the normalized average number of known elements of $\mathbf{x}$, i.e., $\frac{\mathbb{E}[K]}{L}$.

Fig. 3 shows the normalized average number of known elements of $\mathbf{x}$, $\frac{\mathbb{E}[K]}{L}$, for various values of τ_E when $L = 128$, $\tau = 2$, and $\rho = 0.9$. As expected, it is possible for Eve to choose the optimal value of τ_E that maximizes $\mathbb{E}[K]$. Note that the theoretical results in Fig. 3 are obtained with the lower-bound on $\bar{\theta}$ in (21).

In Fig. 4, $\frac{\mathbb{E}[K]}{L}$ is shown for various values of ρ when $L = 128$, $\gamma_B = \gamma_E = 10$ dB, and $\tau = 1$. For fixed τ_E, we assume $\tau_E = \tau = 1$. We can see that as ρ increases, $\frac{\mathbb{E}[K]}{L}$ becomes larger. Thus, for a better channel estimation attack to improve the performance of the known plain-text attack, Eve's antenna should physically approach Bob's antenna to increase the correlation. This also implies that Bob has to prevent Eve from approaching him for secure communications with Alice. For example, in Fig. 4, if $\rho < 0.6$, Eve can only know up to 2% of the key subsequence by the known-plain text attack.

V. CONCLUDING REMARKS

In this paper, we studied a simple physical-layer encryption scheme based on CA randomization. To see the performance gain of CA randomization, the known plain-text attack was considered and the probability of successful attack was derived as a closed-form expression. Since CA randomization

is vulnerable to the channel estimation attack, its impact on the average number of known elements of a key subsequence was analyzed when the known plain-text attack is carried out. From the analysis, we observed that it is important to keep a low correlation between Bob's and Eve' channels for secure transmissions.

APPENDIX A
PROOF OF LEMMA 1

If Eve can have t correctly selected t subcarriers out of M randomly chosen subcarriers, the probability of successful attack is $(1-\theta)^t \left(\frac{1}{2}\right)^{M-t}$. Thus, the average probability of successful attack is given by

$$P_{\mathrm{SA}} = \sum_{t=0}^{M} \binom{M}{t} (1-\theta)^t \left(\frac{1}{2}\right)^{M-t} \eta(t), \tag{23}$$

where $\eta(t)$ is the probability that Eve can choose t correct indices among M selected received signals out of $\mathbf{z}$. Since Eve performs a random selection as $\mathbf{H}$ is not available, $\eta(t)$ becomes

$$\eta(t) = \left(\frac{M}{L}\right)^t \left(1-\frac{M}{L}\right)^{M-t}. \tag{24}$$

Substituting (24) into (23), we have (12).

APPENDIX B
PROOF OF LEMMA 2

Consider the logarithm of $P_{\mathrm{SA}}(M)$, which is given by

$$\begin{aligned} A(M) &= \ln P_{\mathrm{SA}}(M) \\ &= M \ln\,(c_1 + c_2\, M), \end{aligned}$$

where $c_1 = \frac{1}{2}$ and $c_2 = \frac{1-2\theta}{2L}$. We can show that

$$\begin{aligned} A'(M) &= \frac{dA(M)}{dM} \\ &= \ln(c_1 + c_2 M) + \frac{c_2 M}{c_1 + c_2 M}, \end{aligned} \tag{25}$$

which is an increasing function of $M \in [0, L]$. Thus, the second derivative of $A(M)$ is positive, which means that $A(M)$ is convex and $P_{\mathrm{SA}}(M)$ has log-convex.

It can be shown that $A'(0) = \ln(c_1) = -\ln 2 < 0$ and $A'(L) = \frac{\frac{1}{2}-\theta}{1-\theta} + \ln(1-\theta)$. Since $\frac{x}{1+x} \le \ln(1+x) \le x$, $x > -1$, we can show that $A'(L) > 0$ if $\frac{\frac{1}{2}-\theta}{1-\theta} - \frac{\theta}{1-\theta} = \frac{\frac{1}{2}-2\theta}{1-\theta} > 0$. Thus, if $\theta < \frac{1}{4}$, $A'(L) > 0$, which implies that the minimum point of $A(M)$ lies between 0 and L, because $A'(0) < 0$ and $A'(L) > 0$.

APPENDIX C
PROOF OF LEMMA 3

For convenience, we omit the index l. From (13) and (16), we have

$$\hat{H} = \psi |\rho|^2 H + \psi \rho^* U,$$

which shows that $\hat{H}$ becomes a scaled noncentral chi-squared random variable with 2 degrees of freedom (for given H), In particular,

$$\frac{2}{\sigma_U^2 \psi^2 |\rho|^2} |\hat{H}|^2 = \frac{2\beta}{\sigma_U^2 \psi^2 |\rho|^2} = \zeta \sim f(\zeta; 2, \lambda), \tag{26}$$

where $f(x; n, \lambda)$ denotes the pdf of the noncentral chi-squared random variable with n degrees of freedom and parameter λ. Here, λ becomes

$$\lambda = \frac{2}{\sigma_U^2 \psi^2 |\rho|^2} \psi^2 |\rho|^4 |H|^2 = \frac{2|\rho|^2 |H|^2}{\sigma_U^2}.$$

Thus, we can show that

$$\begin{aligned} \Pr(|\hat{H}|^2 \ge \tau_{\mathrm{E}} \,|\, |H|) &= \Pr\left(\zeta \ge \nu \,|\, |H|\right) \\ &= \mathcal{Q}_1(\sqrt{\lambda}, \sqrt{\nu}). \end{aligned} \tag{27}$$

Letting $t = |H|$, from (27), we can show that

$$\begin{aligned} P(\tau, \tau_{\mathrm{E}}) &= \frac{\int_{\sqrt{\tau}}^{\infty} \Pr(\zeta \ge \nu, t)\, dt}{\int_{\sqrt{\tau}}^{\infty} f_{|H|}(t) dt} \\ &= \frac{\int_{\sqrt{\tau}}^{\infty} \Pr\left(\zeta \ge \nu \,|\, t\right) f_{|H|}(t) dt}{\int_{\sqrt{\tau}}^{\infty} f_{|H|}(t) dt} \\ &= \frac{\int_{\sqrt{\tau}}^{\infty} \mathcal{Q}_1(\sqrt{\lambda(t)}, \sqrt{\nu}) f_{|H|}(t) dt}{\int_{\sqrt{\tau}}^{\infty} f_{|H|}(t) dt}, \end{aligned} \tag{28}$$

where $f_{|H|}(x)$ denotes the pdf of $|H_l|$, which is the Rayleigh pdf as $f_{|H|}(x) = \frac{2x}{\sigma_H^2} e^{-\frac{x^2}{\sigma_H^2}}$, $x \ge 0$, and $\lambda(t) = \frac{2|\rho|^2 t^2}{\sigma_U^2} = a^2 t^2$. Since $\sqrt{\lambda(t)} = at$, we have

$$\begin{aligned} &\int_{\sqrt{\tau}}^{\infty} \mathcal{Q}_1(\sqrt{\lambda(t)}, \sqrt{\nu}) f_{|H|}(t) dt \\ &= \frac{2}{\sigma_H^2} \int_{\sqrt{\tau}}^{\infty} t \exp\left(-\frac{t^2}{\sigma_H^2}\right) \mathcal{Q}_1(at, \sqrt{\nu}) dt \\ &= e^{-\frac{\tau}{\sigma_H^2}} \mathcal{Q}_1\left(a\sqrt{\tau}, \sqrt{\nu}\right) + e^{-\frac{\nu}{2+a^2\sigma_H^2}} \\ &\quad \times \left(1 - \mathcal{Q}_1\left(\sqrt{\tau\left(\frac{2}{\sigma_H^2} + a^2\right)}, \frac{a\sqrt{\nu}}{\sqrt{\frac{2}{\sigma_H^2} + a^2}}\right)\right), \end{aligned} \tag{29}$$

where the last equality is due to [34, Eq. (14)].

APPENDIX D
PROOF OF LEMMA 4

For a given τ_{E}, suppose that there are N elements of $\{\hat{\alpha}_l\}$ that are greater than or equal to τ_{E}, i.e., $N = |\{l \,|\, \hat{\alpha}_l \ge \tau_{\mathrm{E}}\}|$. Then, $K = N$ if all N elements are correctly decided. Otherwise, $K = 0$. Thus, $\mathbb{E}[K \,|\, N] \ge N\phi^N$. Since N is a binomial random variable, we have

$$\mathbb{E}[K] = \mathbb{E}[N\phi^N] = \sum_{n=0}^{L} n \binom{L}{n} \phi^n \varphi^n (1-\varphi)^{L-n}$$

$$= \phi \frac{d}{d\phi} \sum_{n=0}^{L} \binom{L}{n} \phi^n \varphi^n (1-\varphi)^{L-n}$$
$$= LB(B+1-\varphi)^{L-1}, \tag{30}$$

where $B = \phi\varphi$.

Furthermore, from (19), we can show that

$$\phi = (1-\bar{\theta}) \Pr(\alpha_l \geq \tau \mid \hat{\alpha}_l \geq \tau_{\mathrm{E}}) + \frac{1}{2}\left(1 - \Pr(\alpha_l \geq \tau \mid \hat{\alpha}_l \geq \tau_{\mathrm{E}})\right)$$
$$= \frac{1}{2} + \left(\frac{1}{2} - \bar{\theta}\right) \Pr(\alpha_l \geq \tau \mid \hat{\alpha}_l \geq \tau_{\mathrm{E}}).$$

Thus, it can be shown that

$$B = \phi\varphi = \frac{\varphi}{2} + \left(\frac{1}{2} - \bar{\theta}\right) \Pr(\alpha_l \geq \tau, \hat{\alpha}_l \geq \tau_{\mathrm{E}})$$
$$= \frac{\varphi}{2} + \left(\frac{1}{2} - \bar{\theta}\right) P(\tau, \tau_{\mathrm{E}}) \Pr(\alpha_l \geq \tau). \tag{31}$$

APPENDIX E
PROOF OF LEMMA 5

From (11), using the memoryless property of the exponential random variable [35], we have

$$\bar{\theta} = \mathbb{E}\left[\mathcal{Q}\left(\sqrt{\frac{2P\beta_l}{N_0}} \right) \middle| \beta_l \geq \bar{\tau}_{\mathrm{E}} \right]$$
$$= \mathbb{E}\left[\mathcal{Q}\left(\sqrt{\frac{2P(\beta_l + \bar{\tau}_{\mathrm{E}})}{N_0}} \right) \right]$$
$$\geq \mathbb{E}\left[C(\kappa) \exp\left(-\kappa \frac{P(\beta_l + \bar{\tau}_{\mathrm{E}})}{N_0} \right) \right]$$
$$= C(\kappa) e^{-\frac{P\bar{\tau}_{\mathrm{E}}\kappa}{N_0}} \mathbb{E}\left[e^{-\frac{P\beta_l\kappa}{N_0}} \right] = \frac{C(\kappa) e^{-\frac{P\bar{\tau}_{\mathrm{E}}\kappa}{N_0}}}{1+\kappa\gamma_{\mathrm{E}}}, \tag{32}$$

where the inequality is due to the following lower-bound:

$$\mathcal{Q}(x) \geq C(\kappa) e^{-\frac{\kappa x^2}{2}}, \quad \kappa \geq 1,$$

which is derived in [33]. The maximization in (21) is used to find a tight bound.

REFERENCES

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

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

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

[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[6] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[7] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct. 2015.

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

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

[10] W. K. Harrison and S. W. McLaughlin, "Physical-layer security: Combining error control coding and cryptography," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2009, pp. 1–5.

[11] H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 619–625, Apr. 2013.

[12] J. Choi and E. Hwang, "Secure multiple access based on multicarrier CDMA with induced random flipping," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5099–5108, Jun. 2017.

[13] R. L. Rivest and A. T. Sherman, "Randomized encryption techniques," in *Advances in Cryptology*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Boston, MA, USA: Springer, 1983, pp. 145–163.

[14] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, Apr. 1984.

[15] J. Katz and Y. Lindell, *Introduction to Modern Cryptography: Principles and Protocols* (Cryptography and Network Security Series). London, U.K.: Chapman & Hall, 2007.

[16] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[17] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[18] E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.

[19] J. Choi, "Secure transmissions via compressive sensing in multicarrier systems," *IEEE Signal Process. Lett.*, vol. 23, no. 10, pp. 1315–1319, Oct. 2016.

[20] N. Y. Yu, "Indistinguishability of compressed encryption with circulant matrices for wireless security," *IEEE Signal Process. Lett.*, vol. 24, no. 2, pp. 181–185, Feb. 2017.

[21] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 813–817.

[22] S. Agrawal and S. Vishwanath, "Secrecy using compressive sensing," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Oct. 2011, pp. 563–567.

[23] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[24] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[25] A. El Shafie, Z. Ding, and N. Al-Dhahir, "Hybrid spatio-temporal artificial noise design for secure MIMOME-OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3871–3886, May 2017.

[26] H. Li, X. Wang, and J. Y. Chouinard, "Eavesdropping-resilient OFDM system using sorted subcarrier interleaving," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1155–1165, Feb. 2015.

[27] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[28] J. L. Massey, "Some applications of source coding in cryptography," *Eur. Trans. Telecommun.*, vol. 5, no. 4, pp. 421–430, 1994.

[29] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," *J. Cryptol.*, vol. 1, no. 3, pp. 159–176, 1989.

[30] W. Meier, "Fast correlation attacks: Methods and countermeasures," in *Fast Software Encryption* (Lecture Notes in Computer Science), A. Joux, Ed. Berlin, Germany: Springer, 2011, pp. 55–67.

[31] J. Proakis, *Digital Communications*, 4th ed. New York, NY, USA: McGraw-Hill, 2000.

[32] B. D. O. Anderson and J. B. Moore, *Optimal Filtering*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1979.

[33] F. D. Côté, I. N. Psaromiligkos, and W. J. Gross. (Feb. 2012). "A chernoff-type lower bound for the Gaussian Q-function." [Online]. Available: https://arxiv.org/abs/1202.6483

[34] A. H. Nuttall, "Some integrals involving the Q_M function (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 21, no. 1, pp. 95–96, Jan. 1975.

[35] S. M. Ross, *Stochastic Processes*. New York, NY, USA: Wiley, 1983.

JINHO CHOI (SM'02) was born in Seoul, South Korea. He received B.E. degree (*magna cum laude*) in electronics engineering from Sogang University, Seoul, in 1989 and the M.S.E. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology in 1991 and 1994, respectively. He was a Professor/Chair in wireless with the College of Engineering, Swansea University, U.K. He has been with the Gwangju Institute of Science and Technology as a Professor, since 2013. He authored two books published by Cambridge University Press in 2006 and 2010. His research interests include wireless communications and array/statistical signal processing. He received the 1999 Best Paper Award for Signal Processing from EURASIP, 2009 Best Paper Award from WPMC (Conference). He is currently an Editor of the IEEE TRANSACTIONS on COMMUNICATIONS and the IEEE WIRELESS COMMUNICATIONS LETTERS and had served as an Associate Editor or Editor of other journals including IEEE COMMUNICATIONS LETTERS, *Journal of Communications and Networks*, the IEEE TRANSACTIONS on VEHICULAR TECHNOLOGY, and *ETRI journal.*