IEEE 18th Wireless and Microwave Technology Conference (WAMICON), April 2017

Secure Key Management for 5G Physical Layer Security

Asim Mazin, Kemal Davaslioglu, and Richard D. Gitlin
Department of Electrical Engineering
University of South Florida
Tampa, Florida 33620, USA
Email: asimmazin@mail.usf.edu {kemald, richgitlin}@usf.edu

***Abstract*—Next generation 5G wireless networks pose several important security challenges. One fundamental challenge is key management between the two communicating parties. The goal is to establish a common secret key through an unsecured wireless medium. In this paper, we introduce a new physical layer paradigm for secure key exchange between the legitimate communication parties in the presence of a passive eavesdropper. The proposed method ensures secrecy via pre-equalization and guarantees reliable communications by the use of Low Density Parity Check (LDPC) codes. One of the main findings of this paper is to demonstrate through simulations that the diversity order of the eavesdropper will be zero unless the main and eavesdropping channels are almost correlated, while the probability of key mismatch between the legitimate transmitter and receiver will be low. Simulation results demonstrate that the proposed approach achieves very low secret key mismatch between the legitimate users, while ensuring very high error probability at the eavesdropper.**

Keywords—Key management, Physical layer security, LDPC, wiretap channel.

I. Introduction

The broadcast nature of wireless medium makes wireless transmissions vulnerable to eavesdropping. To ensure that the information is conveyed in a secure way, cryptographic encryption techniques are often employed in the upper layers of the communication protocol stack. For example, symmetric cryptography methods (e.g., Advanced Encryption Standard) employ a common private key that is pre-shared between the source and destination, referred to as Alice and Bob in this paper, to encrypt/decrypt data. In contrast to the symmetric cryptography, asymmetric cryptography methods such as Public key Cryptosystems (PKC) use public and private keys. In today's mobile communication systems, symmetric cryptography has been used due to its low computational cost compared to PKC. However, if the legitimate parties do not pre-share a common key, then the key needs to be established and conveyed to both parties through a private wireless channel, that may not always exist and is prone to be intercepted by an eavesdropper, referred to as Eve hereafter. For next generation wireless networks, such as 5G wireless, the process of key management (key generation and secure key exchange) will become even more important as the number of nodes increases to a massive scale and nodes become more heterogeneous in their computational capabilities. Also, physical layer security offers a good solution for interoperability between different systems where pre-shared keys may not exist. We envision that physical layer security methods will be used as an additional layer of security to complement traditional cryptographic methods.

Recently, physical layer security has gained a lot of attention since it offers enhanced wireless network security by exploiting wireless channel characteristics to generate a secret key between the communication nodes. Using training sequences (probing signals), both parties can measure the channel parameters such as the received signal strength indicator (RSSI) [1]-[4], the channel state information (CSI) [5]-[6], or the power spectral density (PSD) [7] of the probing signals to agree on a secret key. However, the randomness that can be extracted from the channel through the signal processing techniques proposed in [1]-[7] is limited by the randomness in the channel. For stationary or low-mobility users, the channel randomness is very low and the number of uncorrelated bits that can be generated from the channel is very few. Furthermore, the techniques proposed in [1]-[7] are prone to manipulation. An adversary may physically introduce blockage or digitally transmit/not transmit jamming signals to manipulate the distribution of bits. In [8]-[11], precoding matrix indicator (PMI) based key generation methods were proposed, which employ predefined codebooks to generate unique keys for devices with multiple antennas. To increase the key generation rate, a channel independent approach was proposed in [12] for fast secret key extraction. In [12], the receiver with a full-duplex transmission capability jams the one of the two copies of the secret key send by the transmitter. An Artificial Noise Injection (ANI) based physical layer approach was proposed in [13] to secure space-time block codes. ANI symbols are added to the information symbols such that they are aligned at the intended receiver and can be subtracted from the information symbols, while they degrade the unintended receiver performance. However, despite its good performance, it requires the legitimate transmitter to know the instantaneous channel of the eavesdropper that may not be possible in many practical applications. Another drawback of [12]-[13] is that jamming and ANI-based techniques increase the interference in the system and they are not energy efficient. Taking into account the green communication interests for the next generation wireless systems, we propose an energy efficient method that does not require the transmitter or any helper to inject noise into the system, which also prolongs its battery life. Furthermore, the key generation rate of the proposed method is high because it is not limited by the channel randomness.

In this paper, we exploit the uniqueness of the main and eavesdropping channels to generate secret keys over wireless channels. A pre-equalization transmit filter that inverts the main channel is employed to decrease the probability of interception at Eve while permitting successful decoding at Bob. To achieve a low error rate between Alice and Bob, LDPC channel coding is used. Once the secret key is established between Alice and Bob, the key is input to the random number generators (RNGs) at both parties. The data to be transmitted is XORed with the output sequences of the RNG at Alice before the pre-equalization and LDPC blocks, while the inverse operations are carried out by Bob's receiver.

The remainder of this paper is organized as follows. Section II introduces the system model. In Section III, we describe the proposed approach. Section IV presents the performance results of the proposed procedure. In Section V, concluding remarks are made along with a brief summary of future research directions.

II. System model

Consider a generic wireless network system model as depicted in Fig. 1, where Alice and Bob are the legitimate communication nodes and Eve is the passive eavesdropper. Alice wants to share a secret sequence (private key) with Bob in the presence of Eve by pre-filtering the secret sequence using a filter that inverts the main channel. The notation in this paper is as follows. The symbol $\|\cdot\|$ stands for the Euclidean norm, $\boldsymbol{chol}(\cdot)$ is the Cholesky decomposition. The received signals at Bob and Eve can be respectively expressed as

$$y_B(k) = \sum_m h_{AB}(m)s(k-m) + n_B(k) \quad (1)$$
$$y_E(k) = \sum_m h_{AE}(m)s(k-m) + n_E(k)\,, \quad (2)$$

where $m = 0, 1, \cdots$ and k is the discrete time index and h_{AB}, h_{AE} are the main and the wiretap channels as depicted in Fig. 1. It is assumed that channels remain fixed during the transmission of a few symbols but may randomly change over time, s is the coded secret sequence (private key), which will be described in detail in section III and $n_B(k)$, $n_E(k)$ represent the i.i.d. additive Gaussian noise at Bob and Eve, respectively.

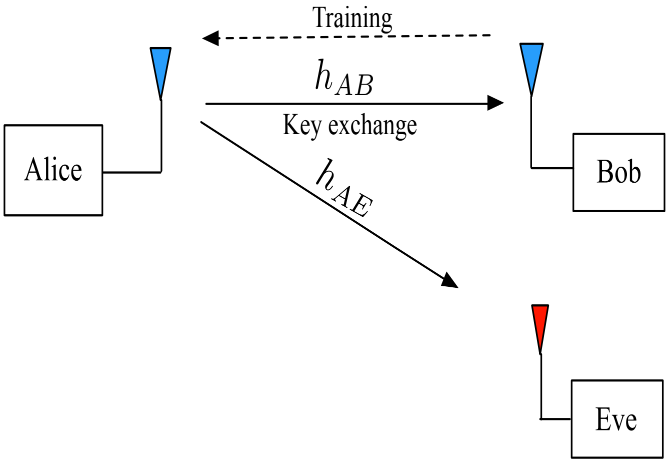

Fig. 1. System Model

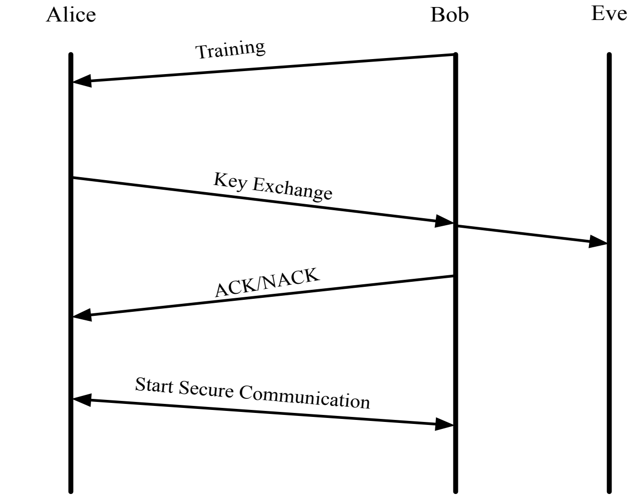

Fig. 2. Signaling Procedure

III. Proposed method

In this section, we describe the proposed physical layer security based key management. As mentioned in the previous sections, the objective is to securely share a private key between Alice and Bob. Before transmission, a secret key $\boldsymbol{x}$ with a length of N bits is processed by the transmitter (Alice) to ensure a low probability of interception at Eve. The proposed signaling procedure is shown in Fig. 2 and the steps are as follows:

1. Bob transmits a training sequence to Alice for channel estimation.
2. Alice estimates the channel and determines the transmit filter that inverts the channel. There is now a "perfect" channel between Alice and Bob.
3. Alice sends the secret key to Bob after passing it through an regular LDPC encoder with a rate $r = 1/2$ and a transmitter filter.
4. Bob receives the pre-equalized signal (containing the session key). The signal is then passed through an LDPC decoder.
5. Thus, the secure key sequence is conveyed from Alice to Bob.
6. Bob sends an ACK/NACK to Alice based on the code syndrome. If the syndrome has errors, a NACK is sent to Alice and Steps 1-5 are repeated. Otherwise, an ACK signal is sent indicating that the session key is established and the key exchange procedure is complete.
7. Key exchange for secure transmission has now been established between Alice and Bob. To convey the data in a secure way, the generated secret key is input to random number generators (RNGs) as a seed by Alice and Bob. The data bit sequence is XORed with the outputs of the RNGs to further confuse Eve, even if she perfectly estimates the received signal.

The proposed transmitter and receiver structures for key exchange are depicted in Fig. 3. In the following subsections, we describe the role of the blocks in Fig. 3.

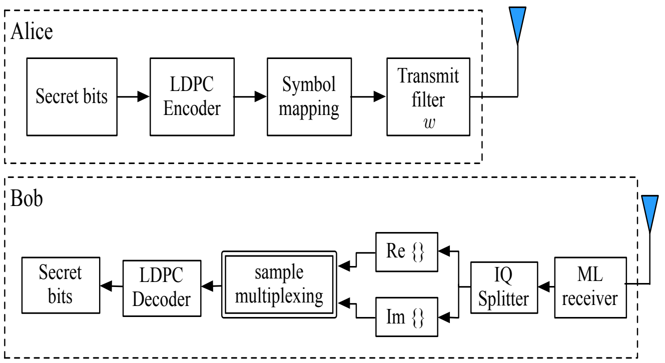

Fig. 3. Proposed Key Management Exchange

A. *Pre-Equalization Transmit Filter Design*

The encoded secret key bits $\boldsymbol{u}$ (LDPC encoder output) are mapped to b QPSK symbols. The modulated symbols b are passed through the transmit filter w to form

$$s(k) = \sum_m w(k-m)b(m), \tag{3}$$

where $s(k)$ is the transmitted signal in (1) and (2). The transmit filter w that inverts the main channel is designed to achieve high secrecy even if Eve knows her channel h_{AE} and the wiretap channel is less noisy than the main channel, i.e., Eve has a high signal-to-noise ratio (SNR) compared to Bob. Since Alice estimates the main channel h_{AB} using the training sequence sent by Bob, through a reciprocal main channel where $h_{AB} = h_{BA}$, the transmit filter w can be determined as

$$h_{BA}w = \|h_{BA}\|. \tag{4}$$

The normalized coefficients of the transmit filter w are determined by inverting h_{BA} in (4) directly, or by using Moore-Penrose Pseudoinverse if the channel h_{BA} contains nulls [14]. Therefore, the received signal at Bob can be rewritten as

$$y_B(k) = \|h_{BA}\|b(k) + n_B(k) \tag{5}$$

Then, Bob detects $\hat{b}$ by estimating the received signal power

$$\|h_{BA}\|^2 = \sum_{i=1}^{j} |y_B(k)|^2. \tag{6}$$

The security of the proposed scheme lies in the fact that Eve is unable to correctly decode the pre-filtered secret key in (3) due to the uncorrelated main and wiretap channels as we will discuss next.

B. *Correlation between the main channel and the wiretap channel*

The transmit filter w depends on the main channel which is expected to be uncorrelated with the eavesdropping channel for link distances larger than a half wavelength due to the spatial property of wireless transmission. However, in practice, there exists some correlation between the two channels as reported in [15]. To capture the correlation effects, without loss of generality, we consider the following correlation model [16]

$$[h_{AB}h_{AE}] = \boldsymbol{chol}\,(\Sigma)\, h_{iid}, \tag{7}$$

where $\Sigma = \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix}$ is the correlation matrix and $0 \leq \rho < 1$ is the correlation coefficient between the normalized channel impulse responses h_{AE} and h_{AB} as discussed in Section II. The term h_{iid} represents a i.i.d. Rayleigh fading channel symbols that have a zero correlation with h_{AB}. If $\rho = 0$, the main and wiretap channels are uncorrelated, whereas larger values of ρ indicate a higher correlation. When Eve is located very close to Bob (within a few wavelengths), a higher correlation between the main and wiretap channels may occur, which would help Eve detect the transmitted symbols by processing similar to Bob using (5) and (6). This would result in a higher probability of key intercept by Eve.

IV. Simulations Results

In this section, we present the simulation results of the proposed method. We have simulated the proposed secure key management algorithm in MATLAB and obtained the performance results in terms of Frame Error Probability (FEP) of the decoded signals (when the secret key is transmitted) at Bob and Eve during the secure key exchange phase. In the simulations, we used a 512-bit key length and assumed Rayleigh block fading channels at the main and wiretap channels using the correlation model in (7). All nodes are equipped with one antenna.

Fig. 4 illustrates the FEP for Bob and Eve for different channel correlations. The SNR of Bob and Eve are assumed to be the same and varied between 0 dB and 5 dB in 0.5 dB increments. We observe that due to the channel capacity achieving LDPC code, the probability of key mismatch between Alice and Bob essentially goes to zero when the SNR > 2.5 dB, whereas the FEP at Eve is very high for all SNR values for $\rho < 0.9$. This demonstrates that the proposed algorithm achieves a diversity order of zero for Eve when $\rho < 0.9$. In other words, the number of independent fading links between Alice and Eve is zero. However, when the main and eavesdropping channels are almost correlated, i.e., $\rho = 0.99$, then the probability of key intercept increases at Eve and the system security decreases. In fact, this is not a surprising result since the present physical layer security method relies on the uniqueness between the main and wiretap channels, which can be observed from Eve's FEP for different correlation values in Fig. 5. As the difference between the two channels disappears, so does the security. Note that for $\rho = 0.99$, the channels are not essentially the same and it is for this reason, there exists a slight difference in the FEP curves of Bob and Eve in Fig. 4.

Next, we fix the SNR of the wiretap channel at 10 dB and vary the SNR of Bob from 0 dB to 5 dB. This simulation scenario considers the case where Eve is closer to Alice than Bob. Even though the previous scenario cannot physically exist when the channels are almost correlated, yet it is an interesting point to simulate. The key-mismatch FEP results for Bob and Eve are shown in Fig. 6 for different correlation coefficients ρ between the wiretap channel and the main channel. Although Eve has better SNR than Bob, her FEP remains high for all $\rho < 0.9$ values. For clarity in Figs. 4 and 5, we have only shown the correlation of $\rho = 0.9,$ but the results are true for all $\rho < 0.9$. Note that when the channels are almost correlated $\rho = 0.99$, Bob makes an error until the SNR exceeds 2.5 dB, whereas Eve does not make an error since her SNR is fixed to 10 dB. This is again due to the same reason as above where the security that can be achieved with physical layer methods degrades as the main and wiretap channels become highly correlated.

V. Conclusion

In this paper, a novel method is proposed to exchange a secret key between two legitimate users using physical layer security methods. The uniqueness of the wireless channel between the legitimate users and an eavesdropper is exploited to create a low probability of interception and magnify the FEP at the unintended receiver, while the intended receiver successfully receives the transmitted signal with a very low FEP. The proposed method builds upon a pre-equalization filter and LDPC encoding at the transmitter. The simulation results demonstrate that secure communication can be established unless the main and eavesdropping channels are almost correlated. Future research directions are to implement the proposed algorithm in a real experimental testbed using a Software Defined Radio (SDR) platforms such as the Ettus Research's Universal Software Radio Peripheral (USRP). This would demonstrate further results on the correlation between the main and wiretap channels for different spatial and temporal scenarios, and verify the theoretical and simulation results presented in this paper. Furthermore, extensions to multiple legitimate users and multiple eavesdroppers are of interest.

ACKNOWLEGMENT

Asim Mazin is supported by Libyan Ministry of Higher Education and Scientific Research, Libya, Tripoli. The statements made herein are solely the responsibility of the authors.

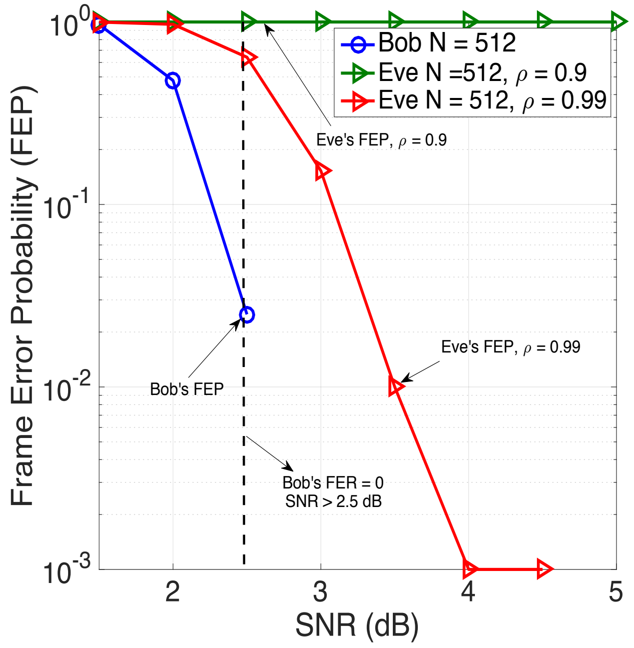

Fig. 4 Bob FER results and Eve 's FER results for key exchange mismatch for different correlation values ρ between the main and wiretap channels.

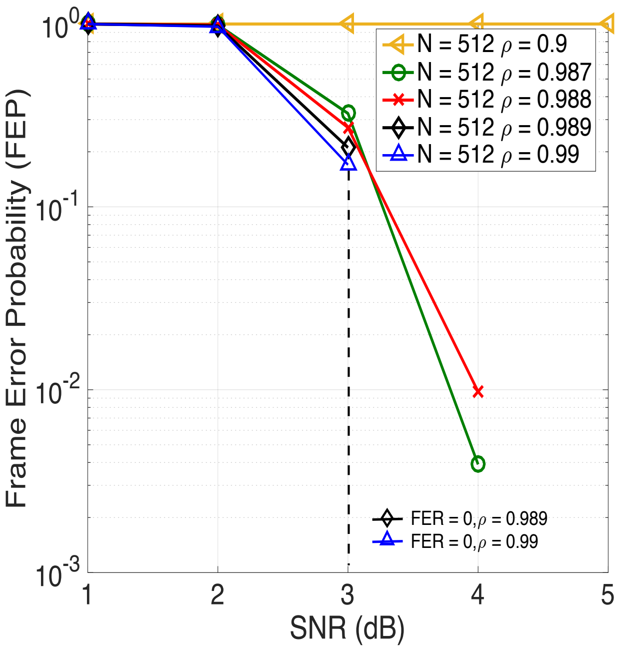

Fig. 5 Eve FER results for different correlation values.

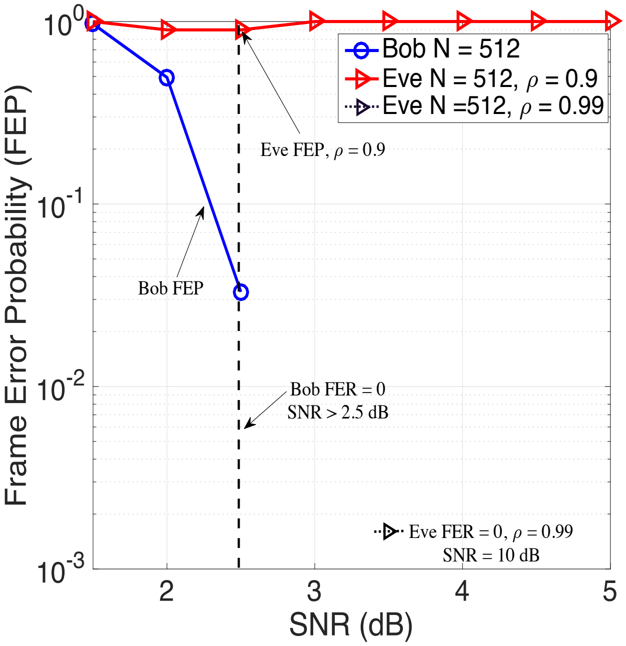

Fig. 6. Key exchange mismatch FER at Bob and Eve for different ρ between the main and the wiretap channel and the SNR of Eve is fixed to 10 dB.

REFERENCES

[1] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in Proc. *of the 14th ACM International Conference on Mobile Computing and Networking* (MobiCom '08). New York, NY, USA, Septemper 2008, pp. 128–139.

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

[3] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, “Exploiting multiple-antenna diversity for shared secret key generation in wireless networks,” in Proc. *IEEE INFOCOM*, San Diego, CA, USA March 2010, pp. 1–9.

[4] M. Wilhelm, I. Martinovic, and J. B. Schmitt, “Secure key generation in sensor networks based on frequency-selective channels,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1779–1790, September 2013.

[5] Y. Liu, S. C. Draper, and A. M. Sayeed, “Exploiting channel diversity in secret key generation from multipath fading randomness,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, July 2012.

[6] H. Liu, Y. Wang, J. Yang, and Y. Chen, “Fast and practical secret key extraction by exploiting channel response,” in Proc. *of the 32nd IEEE International Conference on Computer Communications (INFOCOM),* Turin, Italy, April 2013, pp. 3048–3056.

[7] Y. Qiao, K. Srinivasan, and A. Arora, “Shape matters, not the size: A new approach to extract secrets from channel,” in Proc. *of the 1st ACM Workshop on Hot Topics in Wireless (HotWireless’14)*. New York, NY, USA, Septemper 2014, pp. 37–42.

[8] C.Y. Wu, P.C. Lan, P.C. Yeh, C.H. Lee, and C.M. Cheng, “Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1687–1700, September 2013.

[9] H. Taha and E. Alsusa, “Physical layer secret key exchange using phase randomization in MIMO-OFDM,” in Proc. *IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, USA December 2015, pp. 1–6.

[10] H. Taha and E. Alsusa, “A MIMO precoding based physical layer security technique for key exchange encryption,” in Proc. *IEEE Vehicular Technology Conference (VTC Spring)*, Glasgow, Scotland, May 2015, pp. 1–5.

[11] H. Taha and E. Alsusa, “Secret key exchange under physical layer security using MIMO private random precoding in FDD systems,” in Proc. *IEEE International Conference on Communications (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[12] S. Gollakota and D. Katabi, “Physical layer wireless security made fast and channel independent,” in Proc. *30th IEEE Conf. Comput. Commun., (INFOCOM 2011),* Shanghi, China, April 2011, pp. 1125–1133.

[13] S. A. A. Fakoorian, H. Jafarkhani, and A. L. Swindlehurst, “Secure space-time block coding via artificial noise alignment,” in Proc. *Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Pacific Grove, CA, USA, November 2011, pp. 651–655.

[14] G. Strang, *Introduction to linear algebra*. Wellesly, MA: Wellesley-Cambridge Press, 2003.

[15] H. Taha and E. Alsusa, “Physical layer secret key exchange using phase randomization in MIMO-OFDM,” in Proc. *IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, USA, December 2015, pp. 1–6

[16] M. Edman, A. Kiayias, and B. Yener, “On passive inference attacks against physical-layer key extraction?” in Proc. *Fourth European Workshop on System Security (EUROSEC ’11)*, Salzburg, Austria, April 2011, pp. 1–6.