Received 5 January 2023, accepted 16 January 2023, date of publication 20 January 2023, date of current version 25 January 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3238573

RESEARCH ARTICLE

Key Generation Technique Based on Channel Characteristics for MIMO-OFDM Wireless Communication Systems

DINH VAN LINH[1,2] **AND VU VAN YEM**[1]

[1]School of Electrical and Electronic Engineering, Hanoi University of Science and Technology, Hanoi 11615, Vietnam
[2]Academy of Cryptography Techniques, Hanoi 12511, Vietnam

Corresponding authors: Dinh Van Linh (vanlinh@actvn.edu.vn) and Vu Van Yem (yem.vuvan@hust.edu.vn)

ABSTRACT Dynamic secret key generation from wireless channel characteristics is a promising technique for physical layer security. One of the important issues in this field is extending the secret key's length while preserving its uniformity and randomness. This paper proposes a key generation method based on time-varying and the reciprocity of wireless channels for Multiple-Input Multiple-Output Orthogonal Frequency Division Multiplexing (MIMO-OFDM) wireless communication systems. In the proposed technique, the complex impulse response (CIR) of the estimated channel state information (CSI) is extracted, and a quantization algorithm is designed to convert the maximum peaks of the CIR into secret key bits. The effectiveness of the proposed key generation technique is assessed in terms of the randomness of the produced key bits with different key lengths by using a statistical test suite of the National Institute of Standards and Technology (NIST). The proposed technique is employed in the MIMO-OFDM systems with different modulation schemes through Additive White Gaussian Noise (AWGN) and Rayleigh channels. The simulation results show that the secret keys with various key lengths generated from the proposed technique for the MIMO-OFDM systems guarantee randomness. Moreover, the proposed CSI-based key generation technique provides better effectiveness in terms of security when compared to some existing techniques.

INDEX TERMS Secret key, reciprocity, channel state information, complex impulse response, NIST, randomness, MIMO-OFDM.

I. INTRODUCTION

Due to open-air communication, wireless communication is vulnerable to passive attacks, such as eavesdropping, supervising, etc, or active attacks including spoofing, jamming, etc [1]. The traditional cryptosystem can be used against the attacks above at higher layers, but it may not be effective in heterogeneous wireless communication systems due to the limited resources, key generation, management, and sharing of the secret keys between the different legitimate users. To address such problems, physical layer security techniques can be used to distribute secret keys between legitimate users for implementing the encryption and decryption processes.

In cryptography, the randomness of a key sequence is the most important aspect [2]. The cryptographic key must be generated from a random source and key lengths are easily extended according to the size of the encrypted data. The theoretical basis of the key generation techniques from the physical layer is based on a common source of randomness. In general, wireless channel characteristics are demonstrated to provide an unlimited source of the randomness required for secret key generation, which has recently attracted a lot of attention [2]. Especially, randomness and reciprocity are the two crucial features of the wireless channel that are necessary for the generation of secret keys [3]. Wireless channel has natural randomness due to the time-varying of the channel parameters. According to the reciprocity, the wireless channel is symmetrical, meaning that the channels used by legitimate parties will always be the same [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Feng.

Key generation methods can use a variety of wireless channel features, such as received signal strength (RSS), and channel state information (CSI) [5]. These key generation techniques are lightweight and don't need assistance from other users, so they provide a low complexity [2]. The authors in [6], [7], [8], and [9] applied the RSS for key extraction. In time division duplexing (TDD) mode, the variation of wireless channel amongst measurements has an impact on RSS-based key extraction, but it can be mitigated by using a fractional interpolation filter [4]. However, due to RSS is a parameter with a single dimension and each packet may only provide one RSS measurement, which causes a low key generation rate in RSS-based techniques. Moreover, because of the potential for predicted channel attacks, RSS-based methods can not always ensure complete security.

In recent years, CSI-based key generation methods have been investigated. Key generation techniques based on the channel phase have been proposed in [10] and [11], they can achieve a substantially faster speed compared to the RSS-based methods. However, synchronization and hardware fingerprint interference can seriously compromise the channel phase. Even though dynamic synchronization algorithms can be used to compensate for the synchronization error, the residual synchronization errors in the frequency and time domain have an impact on the channel phase changes. In [12], only the phase of the estimated CSI is used for secret key generation. This proposed technique combines with a special guard band scheme to achieve a better secret key disagreement ratio performance. In [13], the authors suggested extracting the secret key for Internet-of-Things (IoT) devices in a static environment. In this method, both the channel phase and amplitude are utilized in the key generation procedure. This study also suggests a mapping table-based key distribution strategy for IoT environments to improve the key agreement rate, the key generation rate, and the bit error rate. However, it will increase the complexity of IoT devices' deployment.

Multiple-Input Multiple-Output Orthogonal Frequency Division Multiplexing (MIMO-OFDM) technology provides a crucial role in the advancement of wireless communication systems. The MIMO-OFDM systems provide many benefits such as increased diversity, capacity, throughput, data rate, etc. However, the security of the MIMO-OFDM systems is a challenge, because the traditional security methods at the upper layers have high computational which is not suitable for real-time communication. Therefore, physical layer security has become more popular since it ensures reliable and secure communication for both present and future wireless systems. In recent years, key generation based on the MIMO channel characteristics is one of the physical layer security methods that is being focused on research. The authors in [14] proposed to generate secret keys for the MIMO systems from the received signal strength indicator (RSSI). This method indicates that Eve is impossible to obtain the secret keys from legitimate parties even increasing the number of receive antennas. In [15], the authors demonstrated that the secret key length is proportional to the number of antennas in the MIMO systems.

In this paper, we proposed a secret key generation technique based on the CSI for the MIMO-OFDM wireless communication systems. To do this purpose, the legitimate parties collect the highest peaks of the complex impulse response (CIR) during the channel probing. In the quantization stage, the average value of the maximum peaks is computed. Then, the secret key bits are generated by comparing the maximum peaks to the obtained average value. The secret keys are generated with different key lengths and checked by the National Institute of Standards and Technology (NIST) statistical test suite to evaluate the security.

The main contributions of this work are shown as follows:

- The CIR of the MIMO-OFDM wireless channels, which is an unlimited source of randomness, is proposed as a seed to generate the dynamic secret key.
- The quantization algorithm is suggested to convert the estimated CIR into the key bit sequence.
- The key length can be easily changed while ensuring the security of the key.
- The CIR-based key generation algorithm has low complexity and it is suitable for secure MIMO-OFDM wireless communication systems.

The paper is organized as follows, Section II describes the system model. Then, the proposed CSI-based secret key generation for the MIMO-OFDM wireless communication systems is presented in Section III. Simulation results are shown in Section IV and finally, Section IV concludes this paper.

II. SYSTEM MODEL

We consider a wireless communication system in the TDD mode with three parties shown in Fig. 1. Alice and Bob are the legitimate entities that need to protect the transmission data, while Eve is a passive eavesdropper on Alice and Bob's channel. Assuming that the three parties have the same hardware structure of the MIMO-OFDM transceiver devices with M antennas. In addition, the complex impulse response (CIR) between Alice and Bob is denoted $h_a(t_1) \in \mathbb{C}^{M\times M}$, the Bob and Alice's CIR is denoted as $h_{a'}(t_2) \in \mathbb{C}^{M\times M}$.

Taking these assumptions, Alice sends Bob a signal $x_a(t_1) \in \mathbb{C}^{M\times 1}$ first for channel estimation. The received signal $y_b(t_1) \in \mathbb{C}^{M\times 1}$ at Bob's side is given by:

$$y_b(t_1) = h_a(t_1)\, x_a(t_1) + \eta_b(t_1) \tag{1}$$

Bob responds by sending Alice a signal $x_b(t_2)$. The received signal $y_a(t_2) \in \mathbb{C}^{M\times 1}$ at Alice's side is shown as follows:

$$y_a(t_2) = h_{a'}(t_2)\, x_b(t_2) + \eta_a(t_2) \tag{2}$$

In (1) and (2), $\eta_a(t_2)$ and $\eta_b(t_1)$ are the noise components in the received signals of Alice and Bob, respectively.

The process of transmitting signals to each other is done in two time slots of the TDD mode. When the difference

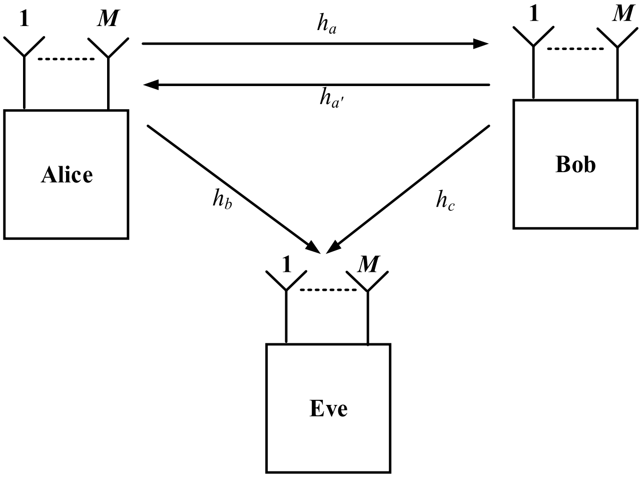

FIGURE 1. Wireless communication system model.

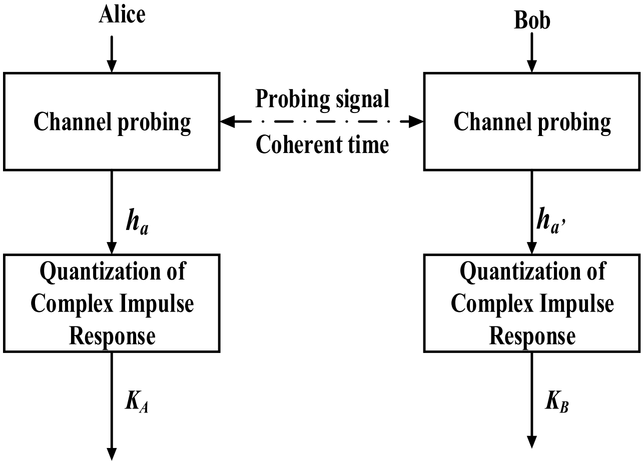

FIGURE 2. Flowchart of secret key generation.

time between t_1 and t_2 is smaller than the channel coherence time τ ($|t_1 - t_2| < \tau$), according to the short-time reciprocity of wireless channel characteristics, the wireless channels observed by both are the same between $h_a(t_1)$ and $h_{a'}(t_2)$, i.e., $h_a(t_1) = h_{a'}(t_2)$ [16].

Additionally, in our system model, Eve can listen in on every conversation between Alice and Bob and also has the same key generation algorithm. We also suppose that Eve stands far enough away from two legitimate users (more than half of wavelength) so that the propagation channel between Alice and Bob is independent of Eve's observation [16]. This indicates that no information about h_a and $h_{a'}$ is contained in the data Eve obtained.

III. PROPOSED CSI-BASED KEY GENERATION TECHNIQUE FOR THE MIMO-OFDM WIRELESS COMMUNICATION SYSTEMS

Fig. 2 depicts the CSI-based key generation procedure. The secret key is generated in two stages including channel probing, and quantization of the Complex Impulse Response (CIR).

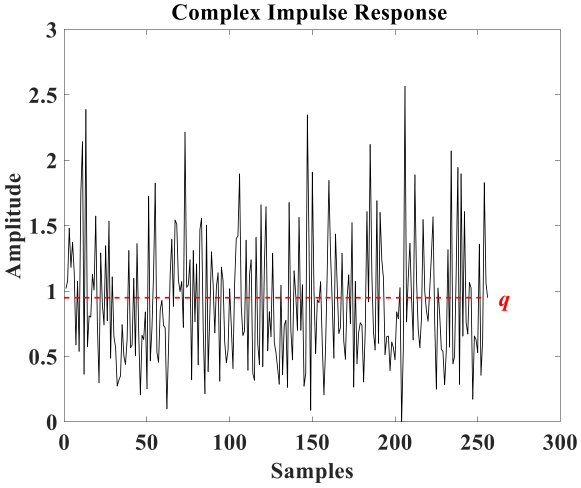

FIGURE 3. Example of the maximum amplitude of 256 CIR samples for the MIMO-OFDM 2 × 2 system.

A. STAGE 1: CHANNEL PROBING

In the channel probing stage, Alice and Bob use the pilot, which is known as a probing signal to estimate channels, and then obtain their channel vectors h_a and $h_{a'}$, respectively. Due to the reciprocity of the wireless channel, we have $h_a = h_{a'}$, which are known as forward and reverse channels for legal users [16]. On the other hand, Eve estimates Alice and Bob by h_b and h_c channels, respectively.

Due to the channel noise, the parties obtain inaccurate estimations of the channels, which are shown in the following equations:

$$\overline{h}_{a'} = h_{a'} + \boldsymbol{\varepsilon}_1 \tag{3}$$

$$\overline{h}_a = h_a + \varepsilon_2 \tag{4}$$

$$\overline{h}_b = h_b + \varepsilon_3 \tag{5}$$

$$\overline{h}_c = h_c + \varepsilon_4 \tag{6}$$

In (3)-(6), Alice, Bob, and Eve obtain estimation errors $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$ during estimating their channels.

The CIRs $\overline{h}_a$ and $\overline{h}_{a'}$ estimated at each node of the transmission link should ideally stay the same and symmetric. As a result, we can achieve:

$$\overline{h} = \overline{h}_a = \overline{h}_{a'} \tag{7}$$

However, some real cases are non-reciprocity due to the asynchronous errors and different noises at both parties. To address this issue, the authors in [17], [18], and [19] proposed techniques to mitigate the noise and asynchronous error effects.

B. STAGE 2: QUANTIZATION

In the quantization stage, we propose a quantization algorithm to convert the obtained CIRs into binary values. Fig. 3 shows an example of the CIR with the maximum peaks. The quantization algorithm can be expressed as follows:

- Based on the obtained CIR $\overline{h}$, Alice and Bob find the highest peaks of CIR Q.

- Then, they calculate the average value q of the highest peaks of CIR Q.
- Alice and Bob compare each excursion of CIR's peak Q with q. If the excursion's value is greater than the average value q, we obtain bit 1. Otherwise, bit 0 is achieved if the excursion's value is lower than q.

$$Q(i) = \begin{cases} 1 & if\ Q(i) \geq q \\ 0 & if\ Q(i) < q \end{cases} \tag{8}$$

By applying this quantization algorithm, Alice and Bob will receive two bit sequences, K_A and K_B.

By applying our proposed method, the number of maximum CIR peaks can be easily expanded, thus the key generation system can generate keys of different lengths.

The key generation technique aims to generate secret keys for data encryption and authentication. The randomness and refresh rate of the key must fulfill specific specifications for the applications. As a result, the key generation algorithms may be assessed by using three metrics: randomness, key generation rate, and key disagreement rate, in which randomness is the most essential feature [2].

IV. SIMULATION RESULTS

This section illustrates the simulation results obtained from MATLAB and investigates the performance of the proposed CSI-based key generation technique for the MIMO-OFDM wireless communication systems. The key bits are generated from the highest peaks of the CIR by applying our proposed key generation technique. The performance of the proposed technique is evaluated by the randomness of the generated key with different key lengths. The randomness of the generated key is examined by the National Institute of Standards and Technology (NIST) statistical test suite. There are a total of 15 tests, each of which can be used in a sequence. For instance, the monobit test concentrates on the ratio of ones to zeros; the frequency test within a block is utilized to assess whether the percentage of 1 in one block is approximately half a block; the run test is employed to check whether a key sequence's oscillations of 1 and 0 are quick or slow in comparison to a random sequence; the length of the 1 from the test key is matched to the anticipated length of 1 from the random sequence using the longest run of ones in a block test; the discrete Fourier transform (DFT) test finds the periodic pattern of the sequence; the approximate entropy test is applied to estimate the frequency of all potential overlapping data bits in a key sequence; the cumulative sums test is performed to assess whether the cumulative amount of elements of the sequence is large or small for the desired cumulative amount of a random sequence; etc. Each test is dependent on a determined test statistic value that is a function of the data and it produces a p-value. The p-value is related to the size of the tested sequence, the quantity and the arrangement of the 0s and 1s in the block of the tested sequence, thus it will vary in the range from 0 to 1 [20]. To assess randomness in each test, the p-value is compared to a significant level α, which typically has a value between [0.001, 0.01]. If p-value $> \alpha$, the sequence is considered random. As in other research, we decide on α being 0.01. Therefore, the key sequence passes the test when the p-value test result is greater than 0.01.

TABLE 1. Parameters of MIMO-OFDM wireless communication systems.

Parameters	Specifications
Channel model	AWGN
	Rayleigh
Modulation schemes	BPSK
	QPSK
Guard interval percentage	1/4
Number of subcarriers	64
Number of data subcarriers	48
FFT/IFFT size	64 points
Number of pilot subcarriers	4
Bandwidth	20 MHz
Bit rate	12 Mbps for BPSK
	36 Mbps for QPSK
Coding rate	1/2
Number of antennas	$N_t = N_r$ =2
	$N_t = N_r$ =4
	$N_t = N_r$ =16

TABLE 2. The parameters of the NIST test.

NIST tests	Block length
Block Frequency Test	128
Non-overlapping Template Matching Test	9
Overlapping Template Matching Test	9
Approximate Entropy Test	10
Serial Test	4
Linear Complexity Test	500

The proposed technique is applied in both Additive White Gaussian Noise (AWGN) and Rayleigh channels for the MIMO-OFDM systems. Assuming that Alice is a transmitter, and Bob is a receiver. Two legitimate parties use the MIMO-OFDM systems with the same number of antennas. In this work, we simulate the MIMO-OFDM systems configured with 2Tx-2Rx, 4Tx-4Rx, and 16Tx-16Rx for the BPSK and QPSK modulation schemes. Some parameters of the MIMO-OFDM systems are referenced from [14] and [15] and shown in Table 1. Meanwhile, the parameters of the NIST tests are listed in Table 2 and referenced from [21].

Case study 1: We consider that the channel is impacted by AWGN. Firstly, we simulate the MIMO-OFDM 2 × 2, 4 × 4, and 16 × 16 systems for the BPSK modulation scheme. The secret keys are generated with different key lengths of 256 bits, 1024 bits, 102400 bits, and 1024000. Table 3 shows the NIST test results for the generated secret keys.

According to the NIST standard [20], an input length of at least 100 bits, 38912 bits, and 1000000 bits need to be evaluated through 8 NIST tests, 9 NIST tests, and 15 NIST tests, respectively. Therefore, we choose 8 NIST tests for the generated key length of 256 bits and 1024 bits, including monobit, block frequency, runs, longest run of ones, DFT, serial (this test generates two p-values including serial-1 and serial-2), approximate entropy, cumulative sums test. For 102400 bits, we also need to conduct 8 NIST tests like 256 bits and 1024 bits scenarios, and one additional binary matrix rank test. We do all 15 NIST tests for the key length of 1024000 bits. It can be observed from Table 3 that the p-values of all the situations range from 0.01 to 1. When we modify the number of MIMO-OFDM antennas and the key lengths, the p-values of the available NIST tests are greater than 0.01. Moreover, the greater p-value of each NIST test provides the higher the unpredictability of the resulting bit, thus the resulting key sequence is more random. The detailed results of some NIST tests are as follows:

– For the monobit test, all p-values obtained from the MIMO-OFDM systems with different key lengths are 1. It is indicated that the number of 1s and 0s in the generated keys are the same as would be required for perfectly random sequences.
– In the frequency test within a block (block frequency) test, the highest p-value is achieved on the 1024000-bit key generated by the CIR of the MIMO-OFDM 16 × 16 system (p-value = 0.96). This result illustrates that the generated keys have a ratio of 1, which is close to the half block.
– In the runs test, the result of a key length of 102400 bits generated by the CIR of the MIMO-OFDM 16 × 16 system shows a greater p-value compared to the other keys (p-value = 0.85). Based on this finding, it can be indicated that this key oscillates more quickly than other keys.
– For the longest run of ones in a block test, the secret key with a key length of 256 bits of the MIMO-OFDM 4 × 4 system has a length of 1 more stable than the expected length of 1 from the other keys.
– The binary matrix rank test is only used to evaluate the 102400-bit and 1024000-bit keys. It can be seen that the 1024000-bit key offers a better linear dependence than the 102400-bit key.
– In the discrete Fourier transform, the value of the 1024-bit key of the MIMO-OFDM 16 × 16 system is superior to other key lengths.
– For the 1024000-bit key, the highest p-values are 0.05, 0.75, 0.96, and 0.49 for the non-overlapping template matching test, overlapping template matching test, universal statistical test, and linear complexity test, respectively.
– In the serial test, the greatest p-value is achieved on the 102400-bit key of the MIMO-OFDM 4 × 4 system which is equal to 0.99.
– The approximate entropy test reveals that all p-values of the 256-bit and 1024-bit keys of the MIMO-OFDM systems are equal to 1. These p-values are greater than that of 102400-bit and 1024000-bit keys. The higher p-value of the approximate entropy test indicates the higher unpredictability of the generated bits.
– The results of the cumulative sums test show that the p-value of the 1024000-bit key of the MIMO-OFDM 2 × 2 system is smaller than the other keys, so this key contains a large number of 1s or 0s at the start and the end of the key sequence.
– There are 8 evaluated states and 18 evaluated states for the random excursions test and random excursions variant test, respectively. It can be observed that the p-values of both these NIST tests range from 0.01 to 0.99.

Secondly, we simulate the MIMO-OFDM systems for the QPSK modulation scheme and the simulation results are shown in Table 4. It can be observed that the p-values of the QPSK modulation scheme are different from the BPSK modulation scheme in all required tests, but there are still greater than 0.01. As a result, the generated secret keys satisfy the requirements for randomness. Specific details are described below:

– For the monobit test, all p-values are 1, so the secret keys of the MIMO-OFDM systems provide the same proportion of 1 and 0.
– In the block frequency test, the 1024-bit key of the MIMO-OFDM 16 × 16 system obtains the highest p-value.
– The runs test indicates that the 256-bit key of the MIMO-OFDM 4 × 4 system oscillates more quickly than other keys.
– The test overcome of the longest run of ones test reveals that the 256-bit key generated by the CIR of the MIMO-OFDM 16 × 16 system has a length of 1, which is more consistent with the desired length of 1 from the random key sequence.
– The binary matrix rank test displays that most p-values of the 102400-bit key are higher than those of the 1024000-bit key.
– In the discrete Fourier transform test, the p-value of the 256-bit key of the MIMO-OFDM 16 × 16 system (p-value = 0.82) shows a greater p-value compared to the other situations.
– In 4 NIST tests, including the non-overlapping template matching test, overlapping template matching test, universal statistical test, and linear complexity test, the p-value range is from 0.02 to 0.85.
– In the serial test, two generated p-values fluctuate between 0.19 and 0.88.
– The approximate entropy test indicates that the 256-bit and 1024-bit keys outperform the 102400-bit and 1024000-bit keys in the randomness feature.
– The cumulative sums test results illustrate that the total number of generated keys matches the intended total number of a random sequence. All p-values of this test are greater than 0.57, thus the key sequences do not contain too many 1 or 0 at the beginning and the end.

TABLE 3. Results of NIST statistical test suite for the MIMO-OFDM systems with the BPSK modulation scheme over AWGN channel.

Test		*p*-value											
		256 bits			1024 bits			102400 bits			1024000 bits		
		MIMO 2x2	MIMO 4x4	MIMO 16x16	MIMO 2x2	MIMO 4x4	MIMO 16x16	MIMO 2x2	MIMO 4x4	MIMO 16x16	MIMO 2x2	MIMO 4x4	MIMO 16x16
Monobit		1	1	1	1	1	1	1	1	1	1	1	1
Block frequency		0.88	0.75	0.88	0.69	0.72	0.95	0.83	0.08	0.89	0.52	0.92	0.96
Runs		0.38	0.53	0.26	0.66	0.61	0.31	0.22	0.01	0.85	0.48	0.82	0.66
Longest Run of Ones		0.52	0.93	0.42	0.76	0.39	0.18	0.09	0.11	0.42	0.67	0.58	0.31
Binary Matrix Rank		-	-	-	-	-	-	0.78	0.31	0.42	0.95	0.99	0.21
Discrete Fourier Transform		0.82	0.42	0.42	0.07	0.06	0.86	0.77	0.36	0.22	0.70	0.51	0.39
Non-overlapping Template Matching		-	-	-	-	-	-	-	-	-	0.02	0.04	0.05
Overlapping Template Matching		-	-	-	-	-	-	-	-	-	0.75	0.12	0.46
Universal Statistical		-	-	-	-	-	-	-	-	-	0.96	0.31	0.41
Linear Complexity		-	-	-	-	-	-	-	-	-	0.49	0.10	0.27
Serial		0.32	0.07	0.23	0.41	0.11	0.14	0.71	0.16	0.99	0.39	0.75	0.89
		0.44	0.10	0.09	0.43	0.14	0.05	0.77	0.42	0.86	0.22	0.31	0.57
Approximate Entropy		1	1	1	1	1	1	0.99	0.82	0.89	0.78	0.33	0.52
Cumulative Sums		0.99	0.95	0.80	0.80	0.91	0.99	0.72	0.71	0.77	0.60	0.97	0.77
Random Excursions	x=-4	-	-	-	-	-	-	-	-	-	0.28	0.58	0.73
	x=-3	-	-	-	-	-	-	-	-	-	0.91	0.53	0.49
	x=-2	-	-	-	-	-	-	-	-	-	0.90	0.10	0.96
	x=-1	-	-	-	-	-	-	-	-	-	0.28	0.15	0.51
	x=1	-	-	-	-	-	-	-	-	-	0.40	0.15	0.30
	x=2	-	-	-	-	-	-	-	-	-	0.55	0.39	0.82
	x=3	-	-	-	-	-	-	-	-	-	0.89	0.58	0.79
	x=4	-	-	-	-	-	-	-	-	-	0.82	0.38	0.21
Random Excursions Variant	x=-9	-	-	-	-	-	-	-	-	-	0.27	0.44	0.47
	x=-8	-	-	-	-	-	-	-	-	-	0.18	0.24	0.44
	x=-7	-	-	-	-	-	-	-	-	-	0.16	0.14	0.70
	x=-6	-	-	-	-	-	-	-	-	-	0.20	0.09	0.95
	x=-5	-	-	-	-	-	-	-	-	-	0.13	0.07	0.98
	x=-4	-	-	-	-	-	-	-	-	-	0.18	0.07	0.99
	x=-3	-	-	-	-	-	-	-	-	-	0.65	0.03	0.96
	x=-2	-	-	-	-	-	-	-	-	-	0.65	0.01	0.81
	x=-1	-	-	-	-	-	-	-	-	-	0.19	0.04	0.96
	x=1	-	-	-	-	-	-	-	-	-	0.28	0.11	0.61
	x=2	-	-	-	-	-	-	-	-	-	0.50	0.29	0.20
	x=3	-	-	-	-	-	-	-	-	-	0.25	0.20	0.06
	x=4	-	-	-	-	-	-	-	-	-	0.36	0.25	0.02
	x=5	-	-	-	-	-	-	-	-	-	0.73	0.19	0.03
	x=6	-	-	-	-	-	-	-	-	-	0.70	0.03	0.04
	x=7	-	-	-	-	-	-	-	-	-	0.65	0.02	0.08
	x=8	-	-	-	-	-	-	-	-	-	0.64	0.07	0.21
	x=9	-	-	-	-	-	-	-	-	-	0.59	0.23	0.36

7

TABLE 4. Results of NIST statistical test suite for the MIMO-OFDM systems with the QPSK modulation scheme over AWGN channel.

Test		*p*-value											
		256 bits			1024 bits			102400 bits			1024000 bits		
		MIMO 2x2	MIMO 4x4	MIMO 16x16	MIMO 2x2	MIMO 4x4	MIMO 16x16	MIMO 2x2	MIMO 4x4	MIMO 16x16	MIMO 2x2	MIMO 4x4	MIMO 16x16
Monobit		1	1	1	1	1	1	1	1	1	1	1	1
Block frequency		0.61	0.88	0.75	0.93	0.72	0.99	0.53	0.62	0.36	0.16	0.56	0.90
Runs		0.21	0.81	0.80	0.66	0.24	0.05	0.57	0.59	0.05	0.24	0.68	0.40
Longest Run of Ones		0.51	0.23	0.81	0.77	0.47	0.30	0.48	0.46	0.22	0.17	0.75	0.68
Binary Matrix Rank		-	-	-	-	-	-	0.74	0.73	0.38	0.25	0.19	0.65
Discrete Fourier Transform		0.73	0.17	0.82	0.46	0.49	0.69	0.25	0.22	0.15	0.71	0.54	0.54
Non-overlapping Template Matching		-	-	-	-	-	-	-	-	-	0.14	0.06	0.02
Overlapping Template Matching		-	-	-	-	-	-	-	-	-	0.41	0.85	0.18
Universal Statistical		-	-	-	-	-	-	-	-	-	0.44	0.58	0.35
Linear Complexity		-	-	-	-	-	-	-	-	-	0.51	0.76	0.34
Serial		0.63	0.50	0.23	0.88	0.54	0.19	0.86	0.52	0.41	0.60	0.55	0.65
		0.57	0.15	0.53	0.83	0.38	0.25	0.61	0.72	0.57	0.37	0.87	0.64
Approximate Entropy		1	1	1	1	1	1	0.97	0.45	0.17	0.28	0.53	0.11
Cumulative Sums		0.57	1	0.91	0.77	0.91	0.98	0.69	0.67	1	0.68	0.76	0.90
Random Excursions	x=-4	-	-	-	-	-	-	-	-	-	0.69	0.56	0.65
	x=-3	-	-	-	-	-	-	-	-	-	0.87	0.87	0.95
	x=-2	-	-	-	-	-	-	-	-	-	0.79	0.65	0.56
	x=-1	-	-	-	-	-	-	-	-	-	0.48	0.64	0.74
	x=1	-	-	-	-	-	-	-	-	-	0.93	0.17	0.58
	x=2	-	-	-	-	-	-	-	-	-	0.41	0.10	0.79
	x=3	-	-	-	-	-	-	-	-	-	0.29	0.67	0.84
	x=4	-	-	-	-	-	-	-	-	-	0.42	0.05	0.84
Random Excursions Variant	x=-9	-	-	-	-	-	-	-	-	-	0.67	0.46	0.57
	x=-8	-	-	-	-	-	-	-	-	-	0.77	0.70	0.41
	x=-7	-	-	-	-	-	-	-	-	-	0.91	0.91	0.34
	x=-6	-	-	-	-	-	-	-	-	-	0.58	0.91	0.72
	x=-5	-	-	-	-	-	-	-	-	-	0.43	0.80	0.75
	x=-4	-	-	-	-	-	-	-	-	-	0.43	0.77	0.53
	x=-3	-	-	-	-	-	-	-	-	-	0.48	0.57	0.35
	x=-2	-	-	-	-	-	-	-	-	-	0.55	0.47	0.35
	x=-1	-	-	-	-	-	-	-	-	-	0.70	0.62	0.56
	x=1	-	-	-	-	-	-	-	-	-	0.45	0.53	0.73
	x=2	-	-	-	-	-	-	-	-	-	0.44	0.78	0.52
	x=3	-	-	-	-	-	-	-	-	-	0.43	0.90	0.38
	x=4	-	-	-	-	-	-	-	-	-	0.61	0.94	0.19
	x=5	-	-	-	-	-	-	-	-	-	0.77	0.83	0.12
	x=6	-	-	-	-	-	-	-	-	-	0.49	0.91	0.19
	x=7	-	-	-	-	-	-	-	-	-	0.40	0.74	0.40
	x=8	-	-	-	-	-	-	-	-	-	0.47	0.67	0.78
	x=9	-	-	-	-	-	-	-	-	-	0.33	0.64	0.96

TABLE 5. Results of NIST statistical test suite for the MIMO-OFDM systems with the BPSK modulation scheme over rayleigh fading.

Test		*p*-value											
		256 bits			1024 bits			102400 bits			1024000 bits		
		MIMO 2x2	MIMO 4x4	MIMO 16x16	MIMO 2x2	MIMO 4x4	MIMO 16x16	MIMO 2x2	MIMO 4x4	MIMO 16x16	MIMO 2x2	MIMO 4x4	MIMO 16x16
Monobit		1	1	1	1	1	1	1	1	1	1	1	1
Block frequency		0.32	0.97	1	0.22	0.15	0.99	0.75	0.81	0.50	0.85	0.09	0.63
Runs		0.62	0.80	0.17	0.06	1	0.03	0.42	0.22	0.22	0.52	0.63	0.99
Longest Run of Ones		0.75	0.07	0.64	0.83	0.22	0.02	0.77	0.48	0.94	0.48	0.82	0.92
Binary Matrix Rank		-	-	-	-	-	-	0.83	0.85	0.65	0.50	0.60	0.57
Discrete Fourier Transform		0.14	0.14	0.42	0.46	0.33	0.07	0.13	0.66	0.60	0.95	0.47	0.82
Non-overlapping Template Matching		-	-	-	-	-	-	-	-	-	0.01	0.18	0.03
Overlapping Template Matching		-	-	-	-	-	-	-	-	-	0.57	0.66	0.05
Universal Statistical		-	-	-	-	-	-	-	-	-	0.33	0.69	0.85
Linear Complexity		-	-	-	-	-	-	-	-	-	0.56	0.89	0.1
Serial		0.86	0.29	0.70	0.31	0.26	0.45	0.53	0.65	0.66	0.1	0.82	0.07
		0.62	0.13	0.87	0.44	0.49	0.64	0.26	0.90	0.89	0.03	0.47	0.52
Approximate Entropy		1	1	1	1	0.98	1	0.63	0.06	0.06	0.92	0.07	0.64
Cumulative Sums		0.68	0.75	1	0.18	0.86	0.91	0.97	0.45	0.45	0.67	0.86	0.62
Random Excursions	x=-4	-	-	-	-	-	-	-	-	-	0.46	0.95	0.80
	x=-3	-	-	-	-	-	-	-	-	-	0.32	0.93	0.23
	x=-2	-	-	-	-	-	-	-	-	-	0.56	0.99	0.04
	x=-1	-	-	-	-	-	-	-	-	-	0.17	0.92	0.05
	x=1	-	-	-	-	-	-	-	-	-	0.43	0.61	0.06
	x=2	-	-	-	-	-	-	-	-	-	0.74	0.90	0.57
	x=3	-	-	-	-	-	-	-	-	-	0.77	0.87	0.21
	x=4	-	-	-	-	-	-	-	-	-	0.95	0.99	0.68
Random Excursions Variant	x=-9	-	-	-	-	-	-	-	-	-	0.14	0.21	0.49
	x=-8	-	-	-	-	-	-	-	-	-	0.10	0.17	0.39
	x=-7	-	-	-	-	-	-	-	-	-	0.22	0.15	0.31
	x=-6	-	-	-	-	-	-	-	-	-	0.47	0.16	0.47
	x=-5	-	-	-	-	-	-	-	-	-	0.85	0.28	0.83
	x=-4	-	-	-	-	-	-	-	-	-	0.62	0.56	0.69
	x=-3	-	-	-	-	-	-	-	-	-	0.26	0.89	0.45
	x=-2	-	-	-	-	-	-	-	-	-	0.07	0.79	0.63
	x=-1	-	-	-	-	-	-	-	-	-	0.07	0.46	0.55
	x=1	-	-	-	-	-	-	-	-	-	0.99	0.94	0.54
	x=2	-	-	-	-	-	-	-	-	-	0.98	0.67	0.75
	x=3	-	-	-	-	-	-	-	-	-	0.50	0.98	0.79
	x=4	-	-	-	-	-	-	-	-	-	0.23	0.97	0.70
	x=5	-	-	-	-	-	-	-	-	-	0.27	0.67	0.63
	x=6	-	-	-	-	-	-	-	-	-	0.39	0.69	0.69
	x=7	-	-	-	-	-	-	-	-	-	0.29	0.82	0.71
	x=8	-	-	-	-	-	-	-	-	-	0.19	0.73	0.70
	x=9	-	-	-	-	-	-	-	-	-	0.23	0.54	0.80

TABLE 6. Results of NIST statistical test suite for the MIMO-OFDM systems with the QPSK modulation scheme over rayleigh fading.

Test		*p*-value											
		256 bits			1024 bits			102400 bits			1024000 bits		
		MIMO 2x2	MIMO 4x4	MIMO 16x16	MIMO 2x2	MIMO 4x4	MIMO 16x16	MIMO 2x2	MIMO 4x4	MIMO 16x16	MIMO 2x2	MIMO 4x4	MIMO 16x16
Monobit		1	1	1	1	1	1	1	1	1	1	1	1
Block frequency		0.88	0.61	1	0.14	0.76	0.85	0.81	0.38	0.65	0.58	0.75	0.14
Runs		0.08	0.90	0.80	0.95	0.04	0.15	0.22	0.76	0.36	0.45	0.19	0.78
Longest Run of Ones		0.75	0.47	0.29	0.58	0.74	0.20	0.48	0.53	0.96	0.24	0.57	0.05
Binary Matrix Rank		-	-	-	-	-	-	0.85	0.97	0.97	0.70	0.40	0.26
Discrete Fourier Transform		0.05	0.42	0.42	0.86	0.69	0.46	0.67	0.77	0.46	0.97	0.82	0.28
Non-overlapping Template Matching		-	-	-	-	-	-	-	-	-	0.02	0.10	0.08
Overlapping Template Matching		-	-	-	-	-	-	-	-	-	0.99	0.79	0.93
Universal Statistical		-	-	-	-	-	-	-	-	-	0.07	0.58	0.52
Linear Complexity		-	-	-	-	-	-	-	-	-	0.46	0.89	0.59
Serial		0.47	0.81	0.99	0.32	0.29	0.28	0.65	0.88	0.12	0.18	0.70	0.27
		0.83	0.42	0.93	0.49	0.68	0.49	0.90	0.50	0.67	0.08	0.49	0.07
Approximate Entropy		1	1	1	0.97	1	0.99	0.06	0.66	0.62	0.12	0.52	0.67
Cumulative Sums		0.91	0.69	0.97	0.83	0.94	0.65	0.45	0.73	0.89	0.55	0.58	0.75
Random Excursions	x=-4	-	-	-	-	-	-	-	-	-	0.57	0.64	0.77
	x=-3	-	-	-	-	-	-	-	-	-	0.03	0.31	0.90
	x=-2	-	-	-	-	-	-	-	-	-	0.76	0.67	0.65
	x=-1	-	-	-	-	-	-	-	-	-	0.33	0.64	0.96
	x=1	-	-	-	-	-	-	-	-	-	0.39	0.09	0.73
	x=2	-	-	-	-	-	-	-	-	-	0.75	0.53	0.33
	x=3	-	-	-	-	-	-	-	-	-	0.86	0.38	0.77
	x=4	-	-	-	-	-	-	-	-	-	0.70	0.42	0.12
Random Excursions Variant	x=-9	-	-	-	-	-	-	-	-	-	0.63	0.71	0.72
	x=-8	-	-	-	-	-	-	-	-	-	0.43	0.66	0.58
	x=-7	-	-	-	-	-	-	-	-	-	0.50	0.32	0.72
	x=-6	-	-	-	-	-	-	-	-	-	0.69	0.37	0.86
	x=-5	-	-	-	-	-	-	-	-	-	0.86	0.48	0.92
	x=-4	-	-	-	-	-	-	-	-	-	0.92	0.73	0.82
	x=-3	-	-	-	-	-	-	-	-	-	0.98	0.59	0.83
	x=-2	-	-	-	-	-	-	-	-	-	0.85	0.45	0.94
	x=-1	-	-	-	-	-	-	-	-	-	0.65	0.71	0.88
	x=1	-	-	-	-	-	-	-	-	-	0.11	0.23	0.51
	x=2	-	-	-	-	-	-	-	-	-	0.13	0.32	0.57
	x=3	-	-	-	-	-	-	-	-	-	0.51	0.24	0.97
	x=4	-	-	-	-	-	-	-	-	-	0.60	0.13	0.24
	x=5	-	-	-	-	-	-	-	-	-	0.73	0.12	0.15
	x=6	-	-	-	-	-	-	-	-	-	0.99	0.19	0.20
	x=7	-	-	-	-	-	-	-	-	-	0.72	0.51	0.15
	x=8	-	-	-	-	-	-	-	-	-	0.59	0.83	0.13
	x=9	-	-	-	-	-	-	-	-	-	0.74	0.84	0.14

TABLE 7. Comparing our method to previous methods with input key length of at least 100 bits.

Test	Our method	Method in [4]				Method in [5]
		$D =$ 32	$D =$ 64	$D =$ 128	$D =$ 256	
Monobit	Pass	Pass	Pass	Pass	Pass	Pass
Block frequency	Pass	Pass	Pass	Pass	Pass	Pass
Runs	Pass	No pass	Pass	Pass	Pass	Pass
Longest Run of Ones	Pass	No pass	No pass	Pass	Pass	No pass
Discrete Fourier Transform	Pass	Pass	Pass	Pass	Pass	Pass
Serial	Pass	No pass	Pass	Pass	Pass	No pass
Approx. Entropy	Pass	No pass	Pass	Pass	Pass	Pass

- In the random excursions and random excursions variant tests, all p-values of the states exceed 0.01.

Case study 2: We simulate the MIMO-OFDM 2 × 2, 4 × 4, and 16 × 16 systems affected by the Rayleigh channel. There is a similarity to the first case study, we pick 8 different NIST tests for 256 bits and 1024 bits, 9 NIST tests for 102400 bits, and 15 NIST tests for 1024000 bits, respectively. The simulation results of the BPSK and QPSK modulation schemes are illustrated in Table 5 and Table 6, respectively. It can be easily observed from both tables that all p-values range from 0.01 to 1. The values of both tables can be analyzed as follows:

- The monobit test indicates that the number of 1s is the same as the number of 0s in any generated keys.
- For the block frequency test, the 256-bit key of the MIMO-OFDM 16 × 16 system for the BPSK and QPSK modulation schemes would be achieved perfect randomness since the p-value is equal to 1.
- In the runs test, the highest p-values are 1 for the 1024-bit key of the MIMO-OFDM 4 × 4 system with the BPSK and 0.95 for the 1024-bit key of the MIMO-OFDM 2×2 system with the QPSK, respectively.
- The longest run of ones test of both modulation schemes shows that the 1024000-bit key of the MIMO-OFDM 16 × 16 system with the QPSK has a length of 1 that is more consistent with the normal length of 1 from a random key set.
- For the binary matrix rank test, it can be seen that the keys with shorter key lengths give better linear correlation.
- In the discrete Fourier transform, the p-values range from 0.07 to 0.95 for the BPSK and 0.05 to 0.97 for the QPSK, respectively.
- In three NIST tests including the non-overlapping template matching test, overlapping template matching test, universal statistical test, and linear complexity test, all results are higher than 0.01.
- The p-values obtained in Table 5 and Table 6 demonstrate that the generated keys pass the serial test.
- In the approximate entropy test, the 256-bit key and 1024-bit key of the MIMO-OFDM systems are more random than other generated keys.
- For the cumulative sums test, the p-values of the BPSK can reach 1, while the greatest p-values of QPSK is 0.97.
- For various states of both the random excursions test and random excursions variant, every p-value is greater than 0.01.

Overall, the results of the NIST tests in both case studies give p-values that surpass 0.01. It can be concluded that the keys generated by our proposed technique satisfy the randomness requirements and can be utilized to encrypt information in wireless communications.

Table 7 compares our proposed approach to the previous techniques reported in [4] and [5] with an input key length of at least 100 bits. This table illustrates that our proposed method passes all 8 required NIST tests. The method in [5] only passes 5 NIST tests. In [4], the authors evaluated the NIST test for different downsample factors (D) for simulation data. The method in [4] passes 4 NIST tests for D = 32 and 7 NIST tests for D = 64, respectively. When D is greater than 128, the key generated from the method reported in [4] will pass all required NIST tests. However, the number of generated key bits will be directly decreased by a large downsample factor since fewer subcarriers are preserved for the key distillation. Therefore, the method in [4] could not generate a long key length. Meanwhile, our method can generate any key sequences ensured by the NIST statistical test suite. Consequently, the secret key generated by our proposed method outperforms the methods shown in [4] and [5] in terms of randomness.

V. CONCLUSION

This research proposes a physical layer key generation method based on the CSI for the MIMO-OFDM wireless communication systems to enhance the key randomness. According to the time-varying and reciprocity of the wireless channel, two legitimate communicators use the same CIR to distill the key in coherence time. Our proposed key generation is applied for the MIMO-OFDM systems configured 2Tx-2Rx, 4Tx-4Rx, and 16Tx-16Rx with the BPSK and QPSK modulation schemes through AWGN channel and Rayleigh fading. The generated keys are checked by the NIST statistical test suite. The achieved results show that the generated keys from the proposed technique pass 8 obligate NIST tests for at least 100 key bits, 9 obligate NIST tests for at least 38912 bits, and 15 obligate NIST tests for 1000000 bits, respectively. Therefore, the proposed method ensures the randomness of the extracted keys. In addition, our method performs better effectiveness when compared to previous works in the field of key generation. Our proposed technique could be widely used in secure MIMO-OFDM wireless communication systems. Especially, it is appropriate for military wireless communication systems. In future work, we will focus on evaluating other performance metrics of the proposed key generation method, such as key generation rate and key disagreement rate.

REFERENCES

[1] H. M. Furqan, M. S. J. Solaija, H. Turkmen, and H. Arslan, "Wireless communication, sensing, and REM: A security perspective," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 287–321, 2021.

[2] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[3] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2692–2705, 2020.

[4] L. Peng, G. Li, J. Zhang, R. Woods, M. Liu, and A. Hu, "An investigation of using loop-back mechanism for channel reciprocity enhancement in secret key generation," *IEEE Trans. Mobile Comput.*, vol. 18, no. 3, pp. 507–519, Mar. 2019.

[5] R. Lin, L. Xu, H. Fang, and C. Huang, "Efficient physical layer key generation technique in wireless communications," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–15, Dec. 2020.

[6] T. Castel, P. Van Torre, and H. Rogier, "RSS-based secret key generation for indoor and outdoor WBANs using on-body sensor nodes," in *Proc. Int. Conf. Mil. Commun. Inf. Syst. (ICMCIS)*, May 2016, pp. 9–13.

[7] T. Nguyen and J. Dricot, "CSI-based versus RSS-based secret-key generation under correlated eavesdropping," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1868–1881, Mar. 2021.

[8] M. F. Awan, K. Kansanen, S. Perez-Simbor, C. Garcia-Pardo, S. Castello-Palacios, and N. Cardona, "RSS-based secret key generation in wireless in-body networks," in *Proc. 13th Int. Symp. Med. Inf. Commun. Technol. (ISMICT)*, May 2019, p. 5.

[9] X. Shang, A. Liu, H. Yin, Y. Wang, and Y. Wang, "RSS-AoA-based physical layer secret key generation for mobile wireless nodes," *J. Phys., Conf.*, vol. 1169, Feb. 2019, Art. no. 012067.

[10] X. Lu, J. Lei, Y. Shi, and W. Li, "Applying intelligent reflective surface to channel phase probing in wireless secret key generation," *Springer Nat.*, p. 16, 2022.

[11] L. Cheng, L. Zhou, B.-C. Seet, W. Li, D. Ma, and J. Wei, "Efficient physical-layer secret key generation and authentication schemes based on wireless channel-phase," *Mobile Inf. Syst.*, vol. 2017, pp. 1–13, Jul. 2017.

[12] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5176–5186, Aug. 2017.

[13] M. Usman, S. Althunibat, and M. Qaraqe, "A channel state information-based key generation scheme for Internet of Things," *Secur. Commun. Netw.*, vol. 2022, pp. 1–15, May 2022.

[14] K. Zeng, D. Wu, A. J. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. IEEE INFOCOM*, 2010, pp. 1837–1845.

[15] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," in *Proc. Int. Symp. Wireless Commun. Syst.*, Oct. 2016, pp. 597–602.

[16] X. Lu, J. Lei, W. Li, K. Lai, and Z. Pan, "Physical layer encryption algorithm based on polar codes and chaotic sequences," *IEEE Access*, vol. 7, pp. 4380–4390, 2019.

[17] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2763–2776, Dec. 2013.

[18] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 927–935.

[19] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1422–1430.

[20] A. Rukhin, J. Soto, and J. Nechvatal, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, vol. 22. Gaithersburg, MD, USA: NIST, Apr. 2010.

[21] A. Yamaguchi, T. Seo, and K. Yoshikawa, "On the pass rate of NIST statistical test suite for randomness," *JSIAM Lett.*, vol. 2, pp. 123–126, Sep. 2010.

DINH VAN LINH was born in Vietnam, in 1991. He received the bachelor's degree from the Politehnica University of Bucharest, Romania, in 2015, and the master's degree from the Hanoi University of Science and Technology, in 2020, where he is currently pursuing the Ph.D. degree. His research interests include physical layer security, information security, and wireless communication technology.

VU VAN YEM was born in Vietnam, in 1975. He received the bachelor's and master's degrees from the Hanoi University of Science and Technology, Vietnam, and the Doctor of Philosophy degree in electronics and telecommunication engineering from the Télécom ParisTech, in 2005. He is currently working as a Full Professor with the School of Electrical and Electronic Engineering, Hanoi University of Science and Technology. His research interests include multi-antenna wireless communication systems, antennas, and ultra-high frequency techniques.