Advances in Technology Innovation, vol. 9, no. 4, 2024, pp. 301-318

A Secure and Robust Data Transmission for 2 × 2 MIMO-OFDM System Using Subcarrier Randomization with Elliptical Curve Cryptography

I Gede Puja Astawa*, Melki Mario Gulo, Amang Sudarsono

Department of Electrical Engineering Politeknik Elektronika Negeri Surabaya (PENS), Jawa Timur, Indonesia

Received 18 June 2024; received in revised form 13 August 2024; accepted 15 August 2024

DOI: https://doi.org/10.46604/aiti.2024.13864

Abstract

This research proposes a method that randomizes the subcarrier as a physical layer security (PLS) in the Multiple-Input Multiple-Output Orthogonal Frequency Division Multiplexing (MIMO-OFDM) communication system, aiming to secure information data. The research procedure incorporates the Elliptic Curve Cryptography (ECC) algorithm during subcarrier randomization, including processes such as public key generation, encryption, and decryption, and compares these with the Rivest Shamir-Adleman (RSA) method. The proposed method is validated through real-time laboratory experiments, yielding significant results. The RSA algorithm's average time is 6.73 and 53.21 seconds, while the ECC algorithm requires only 0.71 and 1.21 seconds for security bits of 80 and 112, respectively. The performance of bit error rate (BER) versus signal-to-noise ratio (SNR) is 0.123 times 10 to the power of negative 3, demonstrating that the subcarrier randomization and reconstruction system is successfully implemented and working correctly to ensure security based on the MIMO-OFDM system.

Keywords: Elliptic Curve Cryptography (ECC), Multiple-Input Multiple-Output Orthogonal Frequency Division Multiplexing (MIMO-OFDM), subcarrier randomization, encryption, decryption

1. Introduction

Nowadays, information and communication technology have become human necessities. The demand for information and communication technologies is increasing as technology improves. People now expect to utilize these technologies to communicate in various formats, including text, images, audio, and video. Orthogonal Frequency Division Multiplexing (OFDM) is one such technology that meets these diverse demands. OFDM is a popular wireless modulation technique employed in modern communication systems. It is used by several technologies, including Long Term Evolution (LTE) [1] and Digital Video Broadcasting-Second Generation Terrestrial (DVB-T2) [2]. Additionally, numerous studies of Fifth/Sixth Generation (5G/6G) technology have been proposed [3-4]. OFDM offers high data rates and handles problems like inter-symbol interference (ISI) and frequency selective fading, making it widely utilized in current wireless communication systems. Moreover, modern communication systems sometimes combine OFDM with Multiple-Input Multiple-Output (MIMO) [5-6].

MIMO is essential to support a wide range of services with 5G and 6G systems. It achieves higher spectral efficiency and broader network coverage. The tremendous growth in data rates is fueled by the increasing use of mobile devices and the emergence of new technologies and applications that demand high data rates and low latency. MIMO is a multiple-antenna technique used to improve the quality or data rate of the transmitted signal without expanding the bandwidth. There are two MIMO schemes: spatial multiplexing and spatial diversity. Spatial diversity is a MIMO technique that improves the link quality of the transmitter and receiver [7].

* Corresponding author. E-mail address: puja@pens.ac.id

English language proofreader: Yen-Chun Hsieh

Meanwhile, spatial multiplexing is a MIMO technique for improving data rates [8]. The combination of MIMO and OFDM enhances the resilience and suitability of communication systems, making them ideal for emerging communication systems that require greater channel capacity. However, the MIMO-OFDM system requires a robust security method to ensure its reliability, as the open-air nature of wireless communication systems makes them vulnerable to security risks. One of the security risks of the MIMO-OFDM communication system is eavesdropping, which is the unauthorized interception of information in a wireless communication channel. Eavesdropping in wireless services is one of the main threats to vehicle-to-vehicle (V2V) communications systems [9-10]. An in-network anti-eavesdropping scheme was developed using a cognitive risk control-based combined vehicle radar communication system [9]. In conventional wireless services, illegal eavesdropping is considered one of the critical security challenges in the network, and the research aims to increase the capacity of anti-eavesdropping communication and reduce jamming interference [10].

In wireless communication, data security is one of the most critical factors. Wireless communication is one of the most vulnerable communication media because the information data is widely transmitted, making it susceptible to several security threats. Several types of data security threats include (a) Eavesdropping, where an attacker can obtain information from the signal sent by the transmitter to the receiver; (b) Jamming, where the attacker sends noise that resembles a signal from the sender to the receiver, and (c) Spoofing, where the attacker becomes a Man-in-the-Middle (MITM). If a sender sends a signal to the receiver, the attacker creates a spoofed signal similar to the sender's but with different information.

To overcome the threat of eavesdropping security in wireless communication systems, the subcarrier randomizer technique is employed. A subcarrier randomizer is a subcarrier sequence randomization technique that changes the plaintext bit with ciphertext. The subcarrier randomizer technique uses a specific asymmetric cryptography method to encrypt plaintext into ciphertext. Asymmetric cryptography is a cryptography system that uses public and private keys to encrypt and decrypt certain information. A public key is available to anyone and is used for encrypting messages. Meanwhile, a private key is a key that is only shared with certain people that can be used to decrypt messages. The Rivest Shamir-Adleman (RSA) algorithm and the Elliptic Curve Cryptography (ECC) are two widely implemented asymmetric cryptography methods due to their high security. A comparison of the RSA and ECC within blockchain systems has been conducted [11-12], to evaluate the advantages of each method.

To ensure the security of the communication system, the MIMO-OFDM communication network must be protected. Extensive research has been conducted on encryption and security methods within MIMO-OFDM systems to improve user safety and convenience. However, the use of security systems in MIMO-OFDM is commonly limited to the top layer of the open systems interconnection (OSI) model, with a limited focus on physical layer security (PLS) [13-14]. PLS is a viable approach for wireless communication networks. Several studies have been undertaken on PLS in MIMO and OFDM systems [15-19].

Yusof et al. [20] employed a chaotic signal-scrambling system, such as the partial transmit sequence (PTS) and selected mapping (SLM), within the OFDM communication system. Additionally, Al-Ali and Hasan [21] investigated the security of image transmission over space-time block coding encoded through OFDM, enhanced by a sample scrambling algorithm using a one-dimensional chaotic map. Multiple researchers have combined cryptography with PLS to strengthen the security of MIMO-OFDM communication systems. For instance, turbo-based encryption has been used to improve reliability and security for wireless MIMO-OFDM affected by Doppler frequency offset. The secret key is generated from the parameter channel between legitimate users and serves as a seed to generate a pseudo-random bit sequence using an advanced encryption standard investigated [22-23].

Furthermore, Luo et al. [23] presented a channel frequency response-based secret key generation scheme for in-band full duplex MIMO systems, addressing intrinsic practical imperfections and their effects on probing errors. Among these cryptography and PLS combination methods, the ECC and PLS still need to be widely used in MIMO-OFDM communication

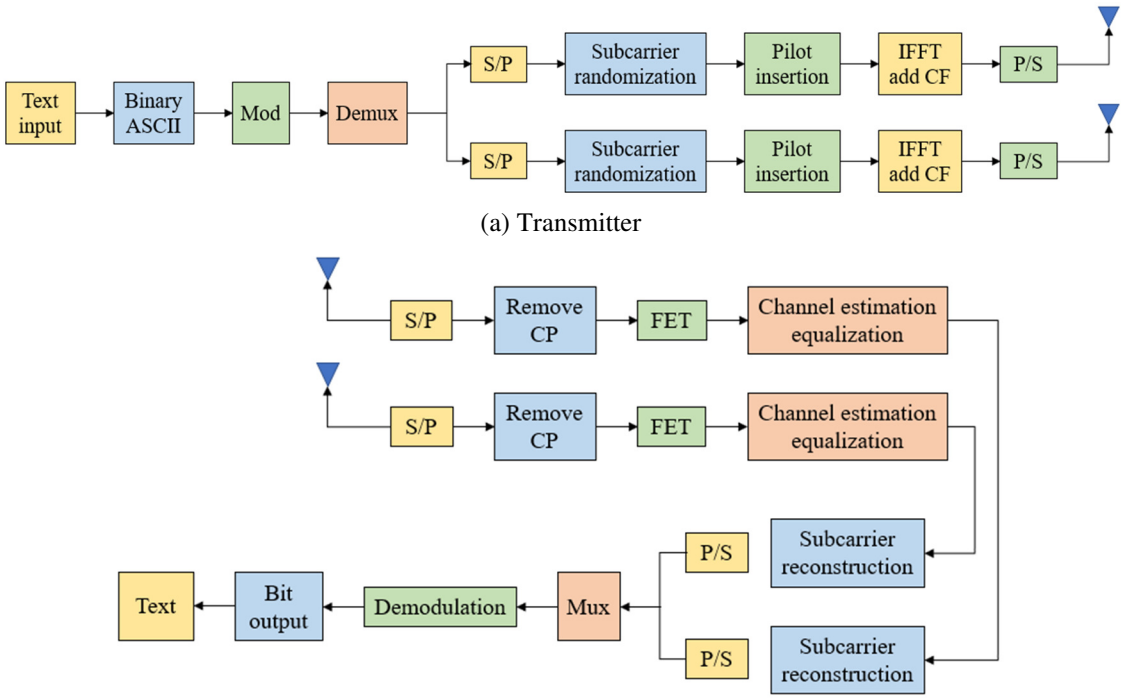
systems. ECC is a robust asymmetric cryptography algorithm known for its low computational cost. This efficiency makes the ECC algorithm widely used in devices with limited memory, such as Internet of Things (IoT) systems [24-25]. As previously mentioned, most of the existing research remains theoretical and has not been directly applied to hardware, so the environment is still ideal. To address this gap, this research proposes real-time applications with hardware carried out for security systems in MIMO-OFDM systems, and testing techniques are also shown.

The main objective of this study is to enhance data security by randomizing the subcarrier as a PLS method in the MIMO-OFDM system. To achieve this, an ECC algorithm is integrated during subcarrier randomization. The ECC procedures include public key generation, encryption, and decryption. This research will utilize Software Defined Radio (SDR) to simulate or analyze wireless communication systems. SDR devices are commonly used to emulate wireless communication systems due to their simple setup and programming. By using an SDR device, schema and system modifications can be implemented by modifying the program's logic without changing the SDR device's electronic design. In this research, an SDR-type National Instruments Universal Software Radio Peripheral (NI-USRP) device will be used to develop a MIMO-OFDM communication system, incorporating the ECC algorithm for subcarrier synchronization within the subcarrier randomization technique.

2. Proposed System

This section discusses the subcarrier randomization system using the ECC algorithm in MIMO-OFDM spatial multiplexing. It starts with a detailed explanation of the main parts of the MIMO-OFDM transceiver with a 2 × 2 antenna scheme that applies subcarrier randomization with elliptical curve cryptography to secure data transmission. Then, the working mechanism of elliptical curve cryptography, as well as the working mechanisms of subcarrier randomization and subcarrier reconstruction, are explained, which are an integral part of the research conducted.

2.1. MIMO-OFDM transmitter



(a) Transmitter

(b) Receiver

Fig. 1 Block diagram of MIMO-OFDM transceiver

In this research, the 2 × 2 MIMO-OFDM system is implemented to transmit and receive text messages, as shown in Fig. 1. The design of the MIMO-OFDM transmitter system is illustrated in Fig. 1(a). The system uses text data as input, which is then converted into a binary series based on its ASCII value. The bit sequence is then modulated using quadrature amplitude

modulation (QAM) to produce a complex signal symbol sequence. The QAM symbol is subsequently multiplexed to generate two signal streams for transmission. In MIMO-OFDM spatial multiplexing, the multiplexing process divides the signal stream in half, with the first transmitter transmitting the first half and the second transmitter transmitting the second half. In addition, the QAM symbol is transformed into a parallel form and fragmented into multiple smaller symbol streams on each OFDM subcarrier. The subcarrier randomization system processes each subcarrier on each transmitter to randomize the subcarriers.

The following section will discuss a more comprehensive design for the subcarrier randomization scheme. The randomized subcarrier is appended with the pilot and null symbols. After this, the signal is transformed into a time-domain signal using Inverse Fast Fourier Transform (IFFT). The IFFT procedure is represented as follows:

$$X(n) = \sum_{k=0}^{N-1} X[k] e^{j(2\pi nk/N)} \tag{1}$$

where $X[k]$ is the QAM symbol at the k-th where $k = 0,1,\cdots,(N-1)$, and N is the number of IFFT. The MIMO-OFDM signals processed by IFFT are combined with a Cyclic Prefix (CP) at the receiver to compensate for ISI. The signal is then processed by a Parallel to Serial (P/S) converter before being transmitted through the antenna.

2.2. MIMO-OFDM receiver

Fig. 1(b) shows the block diagram of the MIMO-OFDM receiver. After each receiver has received the signal, the CP removal procedure is executed. The Fast Fourier Transform (FFT) converts the signal removed from its CP into the frequency domain. The FFT process at the receiver is:

$$X(k) = \sum_{k=0}^{N-1} X[n] e^{j(2\pi nk/N)} \tag{2}$$

The signal at the receiver in the time domain is represented by $X[n]$ and N is the number of subcarriers. Channel estimation and equalization are processed at the receiver to eliminate the effects of fading channels on the OFDM system. This study uses the least squares method for channel estimation in the MIMO-OFDM system. The use of least squares for channel estimation in MIMO-OFDM has been successfully implemented in several previous studies [26-27]. The least squares method equation for channel estimation in the MIMO-OFDM system is:

$$H_{ls} = \arg\min_h \sum_{k=0}^{K-1} \left| y_k - \left(X_k^{(t)} \otimes I \right) h \right|^2 \tag{3}$$

where K is the channel's length, I is the channel matrix identity, and h is the channel impulse response. After a successful channel estimation, channel equalization is carried out. This research uses a zero-forcing (ZF) channel equalization method. ZF is a technique to equalize channels in MIMO-OFDM systems by dividing the received signal by the estimated channel [28]. The ZF formula is:

$$x = H_{ls}^{-1}.y \tag{4}$$

Then, the signal is processed by demodulation to produce an information signal in text messages.

2.3. Elliptical curve cryptography

In this research, ECC is used to encrypt messages, serving as a reference for subcarrier randomization. ECC is a widely implemented asymmetric cryptographic technique in modern communication systems due to its high-security level and low computational cost. Compared to other asymmetric cryptography methods, such as RSA, the ECC algorithm has advantages. Based on key management recommendations by the National Institute of Standards and Technology (NIST), a bit-level comparison table between RSA and ECC [29] is shown in Table 1.

Table 1 Comparison of security bit-level ECC vs. RSA by NIST

Security bit level	RSA bit parameter	ECC bit parameter
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Table 1 shows that to achieve the same security bit level, the RSA bit parameters are more significant than the ECC bit parameters. Messages are encrypted by the ECC algorithm based on an elliptic equation, which is expressed as follows:

$$y^2 = x^3 + ax + b \bmod p \tag{5}$$

where a, b, and p are defined by the number of bits used, y and x are variable. The ECC operation generates public and private keys using the following equation.

$$P_a = nA.G \tag{6}$$

where P_a is the public key, nA is the private key, and G is the initial coordinate, one of Eq. (6) results coordinates. Furthermore, the public key obtained from Eq. (6) generation encrypts the message. The message encryption equation using ECC is:

$$P_c = \{K.G, P_m + K.P_a\} \tag{7}$$

where P_c is message encryption, K is a random constant, and P_m is plain text, respectively.

2.4. Subcarrier randomization and subcarrier reconstruction

Subcarrier randomization is based on the different bits between plaintext and cipher messages, with the cipher message generated through the ECC algorithm encryption process. Meanwhile, subcarrier reconstruction is a process that returns the subcarrier sequence to its original state based on the difference bits between the cipher message and the plaintext message. The block diagram of the subcarrier randomization and subcarrier reconstruction is shown in Fig. 2.

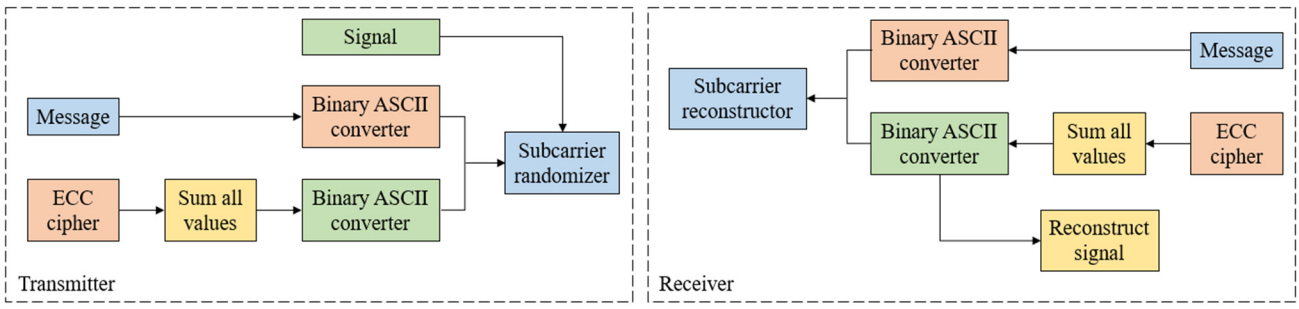
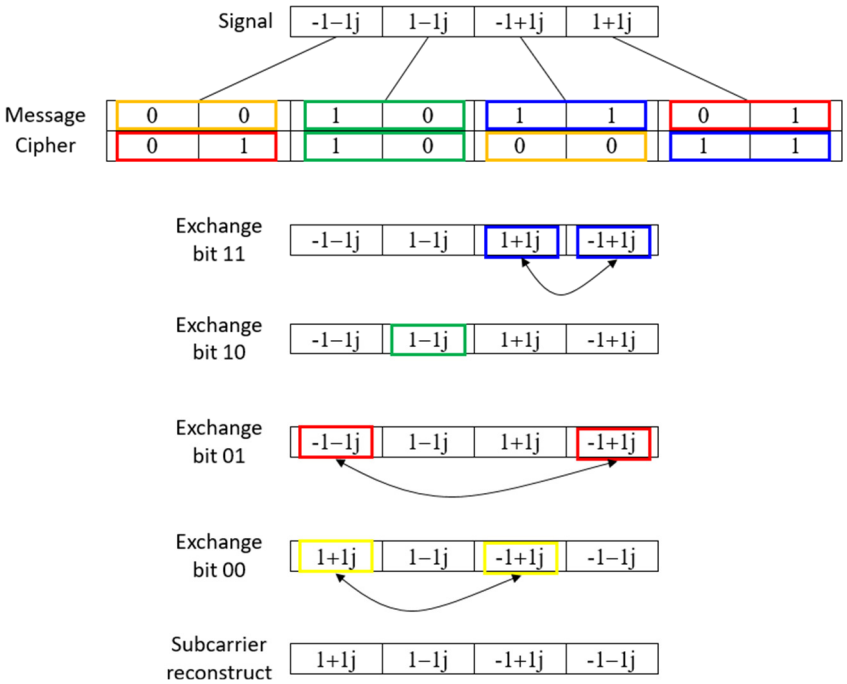
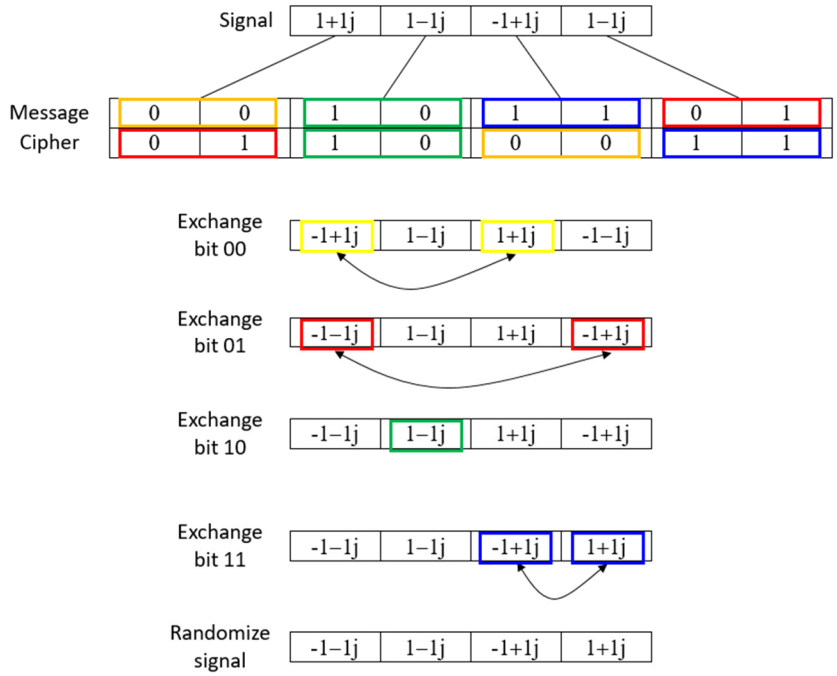


Fig. 2 Block diagram of subcarrier randomizer and subcarrier reconstructor

In Fig. 2, the subcarrier randomization process begins by converting the message into a bit sequence. Message conversion to bit series is done based on the ASCII value. Furthermore, the original message encrypted using the ECC algorithm produces a cipher in coordinates. These coordinates are added together to generate a series of ciphers, which are then converted into bits based on the ASCII value. The two resulting bit series of plaintext messages and cipher messages have different values, and this difference is used to randomize the subcarrier. An illustration of the subcarrier randomization process is shown in Fig. 3(a). Meanwhile, the subcarriers in the received signal are reconstructed to produce subcarriers that match the original arrangement during the subcarrier reconstruction process. The difference in bit series between the cipher message and the plaintext message is used in this operation. In contrast to the subcarrier randomization technique, this process differs in bit series. Fig. 3(b) shows an illustration of the subcarrier reconstruction procedure.



(a) Subcarrier randomization



(b) Subcarrier reconstruction

Fig. 3 Illustration of the process

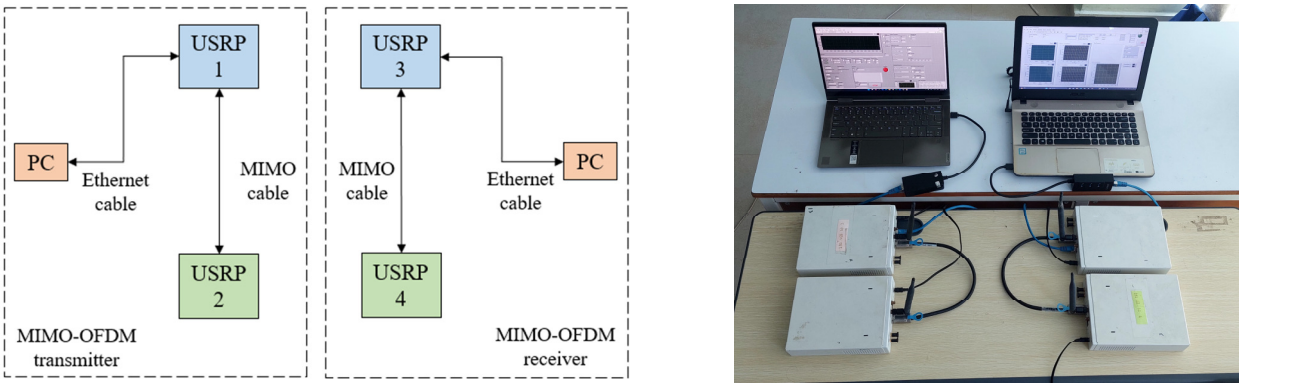
Fig. 3(a) illustrates the subcarrier randomization process using the difference in bit series between plaintext and cipher message bits. For example, this process has four subcarriers, eight message bits, and eight cipher bits. Each bit is then grouped into groups containing two bits. Furthermore, the group of bits in the message is exchanged with the group of bits in the cipher message. Exchange is done starting with bit 00 in the message being exchanged with bit 00 in the cipher, bit 01 in the message being exchanged with bit 01 in the cipher, then bit 10 in the message being exchanged with bit 10 in the cipher, and finally bit 11 in the message being exchanged with bit 11 in the cipher.

Fig. 3(b) is an illustration of the subcarrier reconstruction process. The reference used to perform the reconstruction is the difference in bit changes between the cipher and plaintext messages. As a result, the message bit must be owned first from the results of the message cipher decryption using the ECC algorithm. Furthermore, the subcarrier reconstruction process

exchanges each 2-bit message pair into a 2-bit cipher pair. In contrast to the subcarrier randomization process, in this process, the exchange starts from the 11 message bit pair to the 11 ciphers, then the ten message bit pair to the ten ciphers, then the 01-bit pair message to the 01 ciphers, and finally the 00-bit pair message to the 00 ciphers.

3. System Implementation

This section discusses the implementation of subcarrier randomization using the ECC algorithm on MIMO-OFDM based on NI-USRP devices. In implementing this system, the NI-USRP 2920 type device is used. The NI-USRP 2920 is an SDR device that can execute a Radio Frequency (RF) communication system. The block diagram of the system implementation on the USRP is shown in Fig. 4.



(a) Block diagram of MIMO-OFDM system (b) Realization of MIMO-OFDM transceiver on NI-USRP

Fig. 4 Block diagram of system implementation on the NI-USRP 2920

Fig. 4(a) shows the system implementation using four USRPs, with two for the transmitter, and two for the receiver. Each USRP is connected to a Personal Computer (PC) at both the transmitter and receiver. An ethernet cable is used to connect the USRP and PC because the USRP and PC connection is IP-based. Therefore, it is necessary to configure the PC's IP address so it can be connected to USRP. By default, USRP uses the IP address 192.168.10.x/24 as the IP address of the USRP. However, this IP address can be changed according to the scheme used.

In addition, the ethernet cable used to connect between the PC and USRP is a type of gigabit ethernet cable, so if the PC used is not a standardized gigabit ethernet, it is necessary to add a gigabit ethernet dongle to the PC. Additional devices, such as layer two switches, are required, but since the two USRP devices on the transmitter and receiver are interconnected with MIMO cables, only a PC connection to one of the USRP on the transmitter and receiver is required. A MIMO cable connecting two USRPs is used to synchronize clocks and frequencies. Implementing this system will create the program using the LabVIEW programming language and Python. LabVIEW is used because it has USRP driver support that can be used to run programs with USRP devices. The experimental setup for the MIMO-OFDM system is depicted in Fig. 4(b), and the device specifications are listed in Table 2.

Table 2 Devices specification

Device name	Specification
NI-USRP 2920	Frequency range: 50 MHz – 2.2 GHz. Antenna: VERT 900. Frequency range: 824 MHz – 960 MHz, 1710 MHz
Operating system	Windows 11 RAM: 8GB. Processor: Intel Core i5 2.4 GHz
	Windows 11 RAM: 8GB. Processor: AMD Ryzen 3 3200U 2.6 GHz

4. Result and Discussion

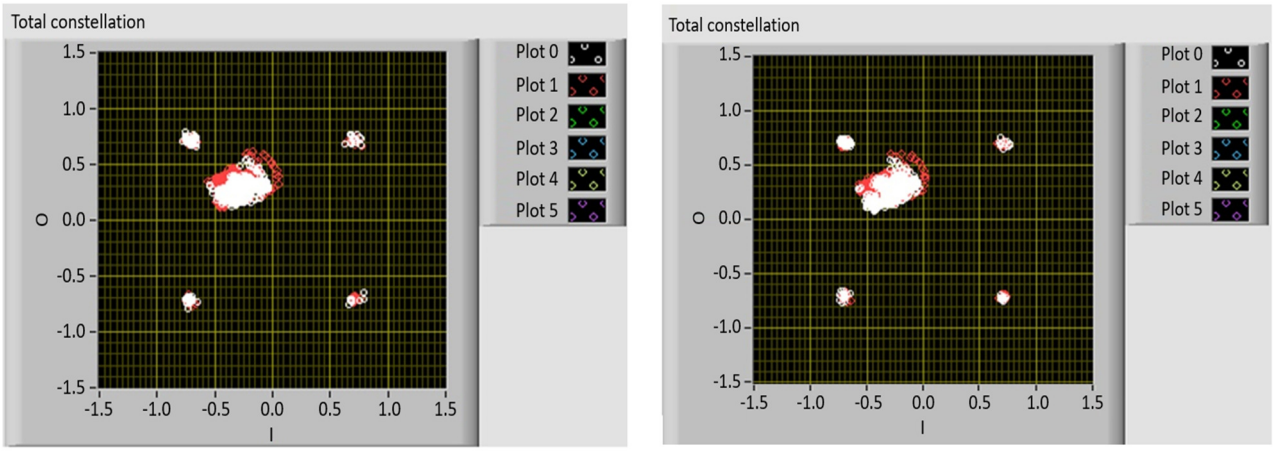
This section will analyze the results of implementing the subcarrier randomization system on MIMO-OFDM using NI-USRP 2920. Experimental results and comprehensive analyses include subcarrier randomization testing on the MIMO-OFDM system based on USRP, a comparative measurement of ECC parameters on system implementation, a performance comparison between RSA and ECC, and an analysis of the use of ECC in the MIMO-OFDM system. The simulation parameters used in this research include a 2 × 2 antenna scheme, QAM modulation, and an ECC parameter of 128 bits. Table 3 shows the details of the complete parameters used.

Table 3 Simulation parameters

Part	Parameter	Value
Transmitter	Frequency	920 MHz
	N-IFFT	128
	Data symbol	96
	Pilot symbol	9
	Null symbol	23
	CP	32
	IQ rate	500 k
	Antenna	2
	ECC parameter	128-bit
	Modulation	QAM
Receiver	Channel equalization	Zero-forcing
	Channel estimation	Least square
	Frame sync	Zadoff-Chu
	Number of antennas	2

4.1. Subcarrier randomization testing on MIMO-OFDM system based on USRP

The results of the subcarrier randomization experiment on the MIMO-OFDM system will be discussed in this section. As analytical parameters in this experiment, a constellation graph and the message decoding results at the receiver will be used. The experiment was carried out by sending text messages from the transmitter to the receiver, with two scenarios: authorized and unauthorized recipients, as shown in Fig. 5.



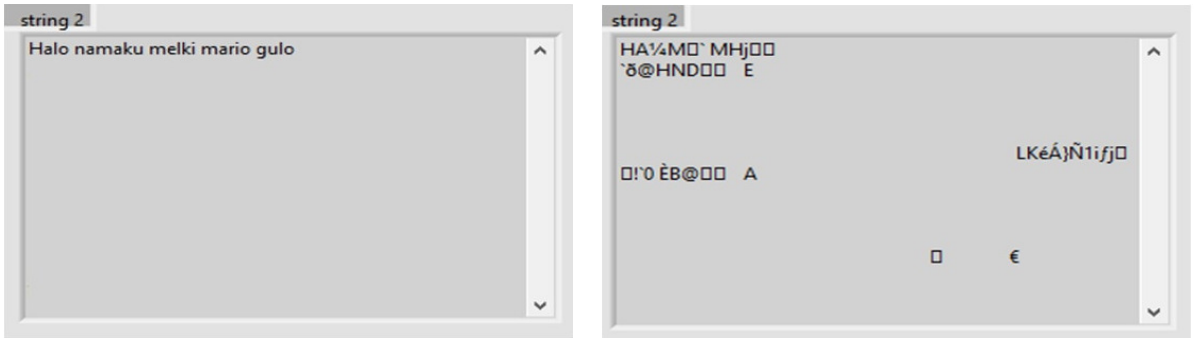
(a) Signal constellation on the authorized receiver (b) Signal constellation on the unauthorized receiver

Fig. 5 Signal constellation in receiver

In the authorized recipient scenario, as shown in Fig. 5(a), the signal constellation data is received by a recipient who has successfully decrypted the cipher sent to the receiver and used it in the subcarrier reconstruction process. The signal constellation on the receiver successfully forms a QAM constellation scheme, although there are still some residual signals in the constellation diagram. However, the residual signal is not used since the receiver uses the maximum likelihood algorithm.

The results of the text data from this scenario are shown in Fig. 6(a). This figure shows that the text for the receiver has the same result as the text for the sender. This happens because the receiver uses the same plaintext message reference and cipher message as the transmitter when performing the subcarrier reconstruction.

Obtain a constellation for the unauthorized recipient scenario, as shown in Fig. 5(b). The constellation in this scenario forms a QAM constellation similar to the results in Fig. 5(a). This happens because the subcarrier randomization process only randomizes 96 data subcarriers for the sender. Randomization was only done on the data subcarrier to keep the MIMO-OFDM signal from being messed up. Although it has the same signal constellation as the authorized receiver, the receiver fails to get the same message from the transmitter. This happens because the receiver uses a different plaintext message reference than the sender. So, even though the cipher message used is the same, the results are different. Because the process of changing bits is different between cipher and plaintext messages on the transmitter and the receiver, the results of the message to the receiver are shown in Fig. 6(b).

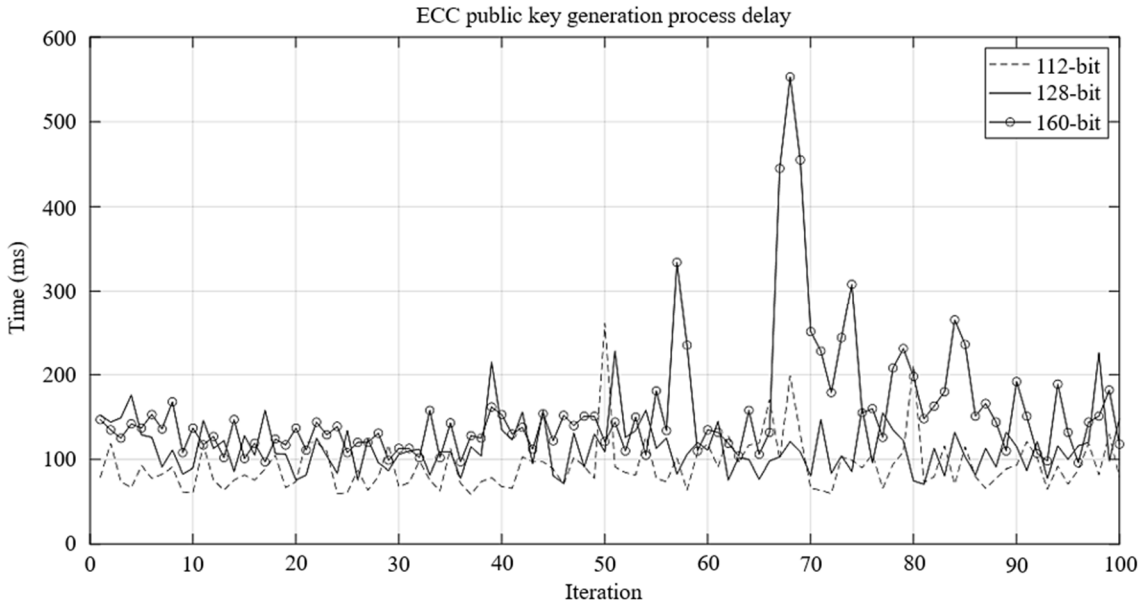


(a) Authorized receiver (b) Unauthorized receiver

Fig. 6 Received message on the receiver

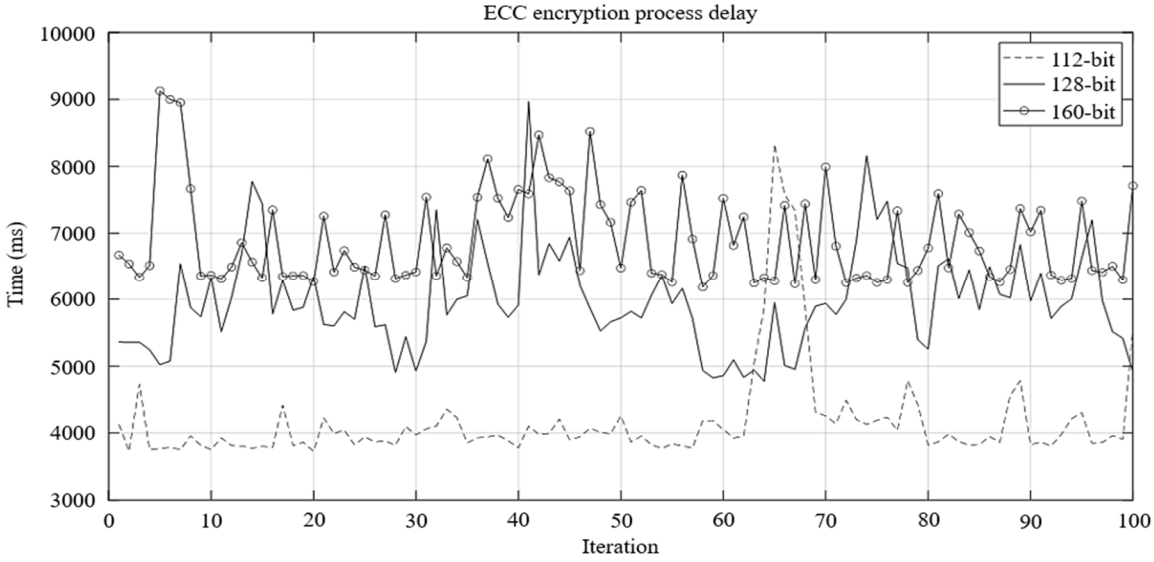
4.2. Comparative measurement of ECC parameters on system implementation

In this section, a comparative measurement of the ECC parameter was carried out in system implementation. Measurements were made to compare the computational delay of the 3 ECC parameters with values of 112-bit, 128-bit, and 160-bit. A comparison of the computational delay is performed for each ECC process. The first measurement process measures the delay in the public key generation of ECC. The results of this measurement are shown in Fig. 7.

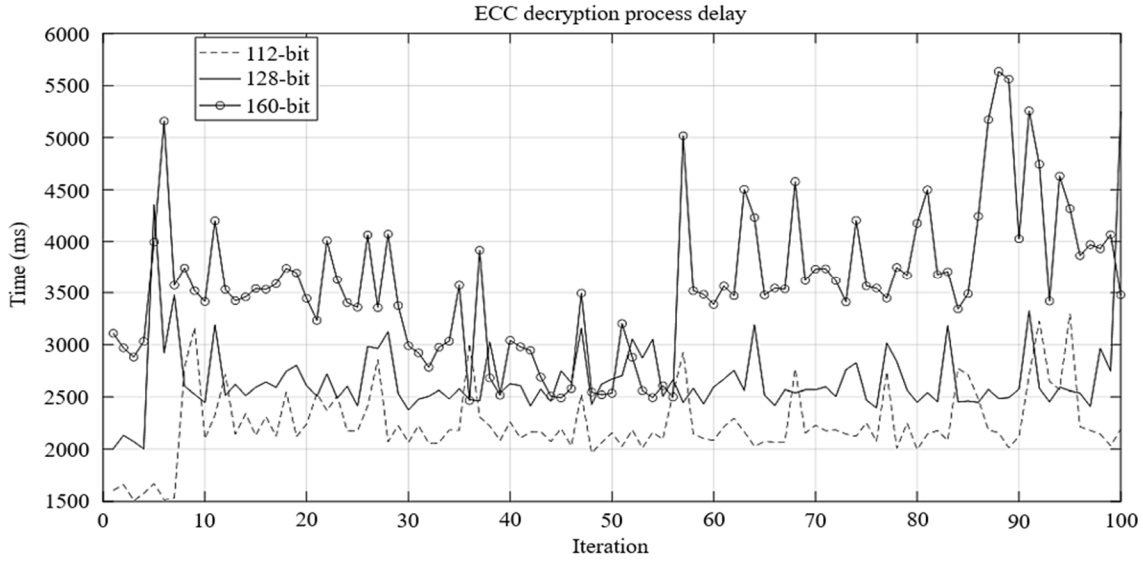


(a) Public key generation

Fig. 7 Delay measurement ECC



(b) Encryption



(c) Decryption

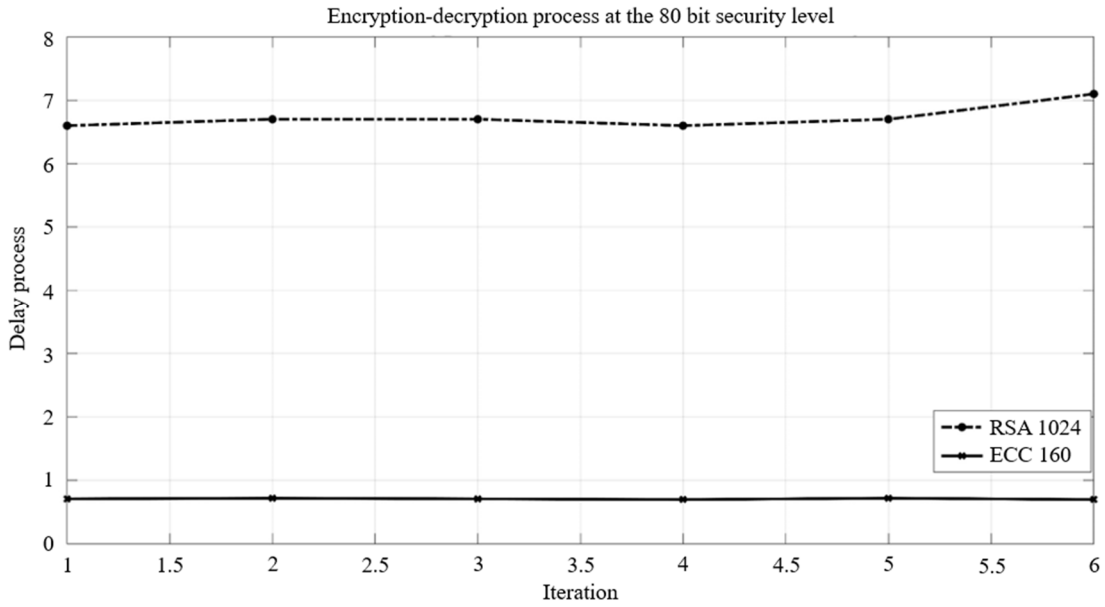
Fig. 7 Delay measurement ECC (continued)

Fig. 7(a) shows that the 112-bit ECC is faster at generating the public key, and the 160-bit ECC requires a longer process to generate the public key. This can also be observed from the average calculation of the delay data. The average process delay on 112-bit ECC is 93.11 ms, 128-bit ECC is 114.5 ms, and 160-bit ECC is 156.97 ms. Furthermore, the encryption process delay is compared across the three ECC parameters. The results of this comparison are shown in Fig. 7(b). From this figure, it is evident that the 112-bit ECC encryption process has a lower time than the others. This can also be seen from the average value of 4181.2 ms, while for 128-bit ECC, the average encryption time is 5986.73 ms, and for 160-bit ECC, the average encryption time is 6897.89 ms. This encryption time is calculated using a message length of 24 characters. The time difference is quite significant between ECC 112-bit and ECC 160-bit, 305, which is 2716.69 ms.

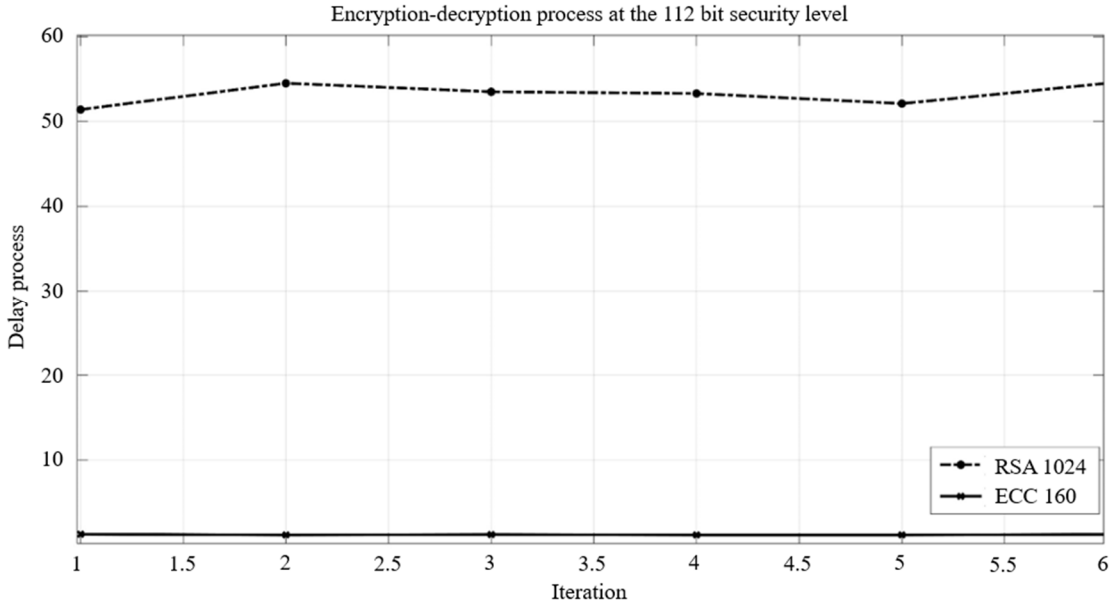
The following comparison process is carried out to compare the data 306 delay of the ECC decryption process with the previous three parameters. The results of the 307 comparison of the decryption delay are shown in Fig. 7(c), which shows that the delay in the 112-bit ECC decryption process has a lower time than the 160-bit ECC. The average delay value for the 112-bit ECC decryption process is 2238.5 ms, while that for the 128-bit ECC is 2668.95 ms, and that for the 160-bit ECC is 3563.08 ms. In Fig. 7(c), it is evident that the decryption process takes a shorter time when compared to the encryption process. This is due to the decryption process creating fewer jobs than encryption. In the decryption process, only the subtraction process occurs between the cipher coordinates and the multiplication between the public key and the scrambler constant.

4.3. Performance comparison between RSA and ECC

This section will analyze the performance comparison between the ECC and RSA algorithms. A comparison is made between the computational delays of ECC and RSA on several security bit levels, which refers to Table 1. Fig. 8 shows data comparing the encryption and decryption processes for security bit levels (80 and 112) between RSA 1024-bit and ECC 160-bit.



(a) The 80-bit security level



(b) The 112-bit security level

Fig. 8 Comparison graph of the delay in the encryption-decryption process

Fig. 8(a) graph shows that ECC has a computational delay much smaller than RSA for security bit level 80. The average ECC computational delay in this scenario is 0.71 seconds. The average time running an RSA algorithm is 6.73 seconds, it takes about 947.88% of the average time to run an ECC algorithm. Compared to previous research conducted by Khan et al. [12], the ECC method takes about 318% of the average time to run an ECC algorithm for a security bit level of 80, compared to the RSA method. It can be seen from the results obtained from this experiment that the use of the ECC method compared to RSA results is almost three times faster for average time running applied to security systems in MIMO OFDM systems compared to the results obtained from previous research [12].

Meanwhile, Fig. 8(b) compares the computational delay for the encryption-decryption process at the 112-bit security level between the RSA 2048-bit and ECC 224-bit algorithms. From the graph, it is observed that ECC has a minor computational delay compared to RSA. The average computational delay for ECC to obtain security bit level 112 is 1.21 seconds. In comparison, the RSA algorithm has an average time of 53.21 seconds, which is the average time value of the ECC algorithm. This means that the RSA algorithm takes about 4297% of the average time to run an ECC algorithm. Compared to previous research [12], the ECC method requires only about 14.7% of the average time running an ECC algorithm for a security bit level of 112, compared to the RSA method. The experiment results show that the ECC method results are almost two hundred times faster than RSA when applied to security systems in MIMO OFDM systems, compared to the previous research [12]. From the graphs in Fig. 8(a) and Fig. 8(b), it can be concluded that ECC has a lower computational cost than RSA to achieve the same bit security level.

4.4. Analysis of the use of ECC in MIMO-OFDM system

This section measures the performance of the subcarrier randomizer and subcarrier reconstructor algorithms. First, the randomization percentage of 96 subcarriers was calculated based on the number of characters of the encrypted plaintext message. This measurement is carried out because the randomization process refers to changing the plaintext message and cipher text. The measurement data of this scenario is shown in Table 4.

Table 4 The percentage average of 96 subcarrier randomization for the number of message characters

No	Number of message characters	Messages	Percentage average of subcarrier randomization
1	4	gulo	8.979167%
2	8	aku gulo	22.58333%
3	12	hai aku gulo	33.8125%
4	16	halo namaku gulo	50.8125%
5	20	halo namaku mario!!!	62.6875%
6	24	halo namaku mario gulo!!	76.25%

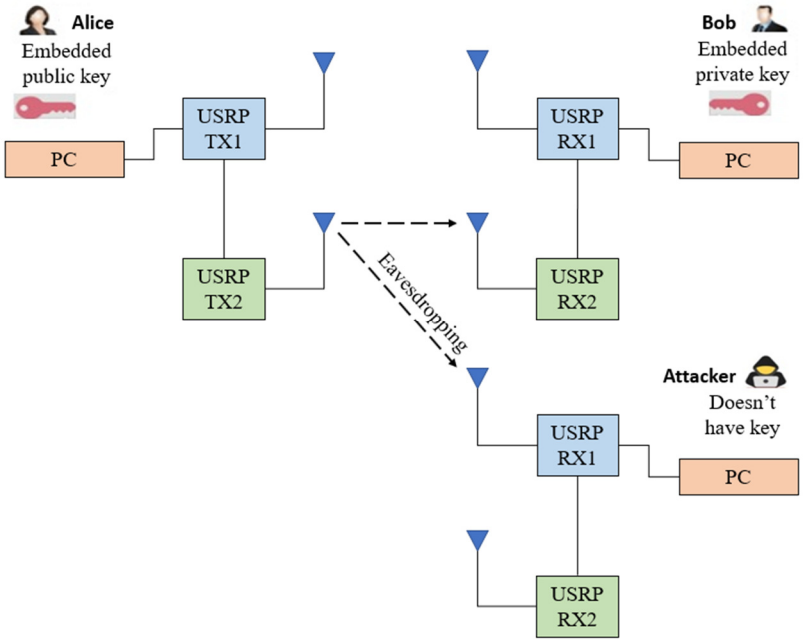


Fig. 9 Experiment scenario of subcarrier randomizer and subcarrier reconstructor

From Table 4, it can observed that as the number of message characters increases, the subcarrier will be more scrambled. For example, a 24-character message has an average subcarrier scrambling of 76.25%, whereas a message with only four characters has an average subcarrier scrambling of 8.97%. This indicates that to achieve higher security, more message

characters are required. In the following measurement scenario, the performance of the subcarrier randomizer and subcarrier reconstruction algorithms were tested to secure the communication from attacker interference. The diagram of the testing scenario is shown in Fig. 9.

In this scenario, Alice is a MIMO-OFDM system transmitter who wants to send an image to the receiver, Bob. However, an attacker is eavesdropping on the ongoing communication between Alice and Bob during the communication process. Before starting the image transmission communication session, Alice performs encryption using the ECC public key embedded in the PC transmitter. The public key on Alice is obtained through the generation of the private key embedded in Bob. The public key used by Alice is shown in Fig. 10. Furthermore, this public key will be used to encrypt the message, as shown in Fig. 11.

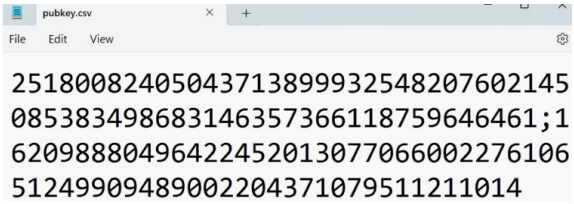


Fig. 10 Public key Alice

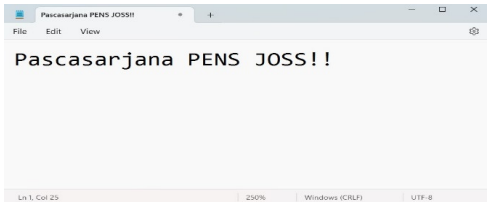


Fig. 11 Plaintext messages

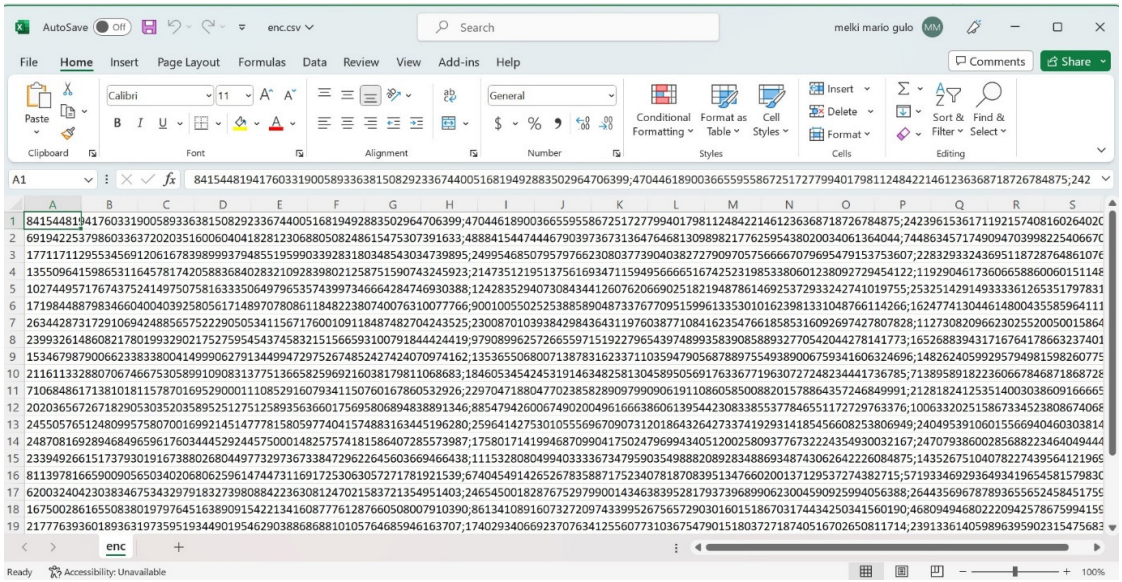


Fig. 12 Ciphertext

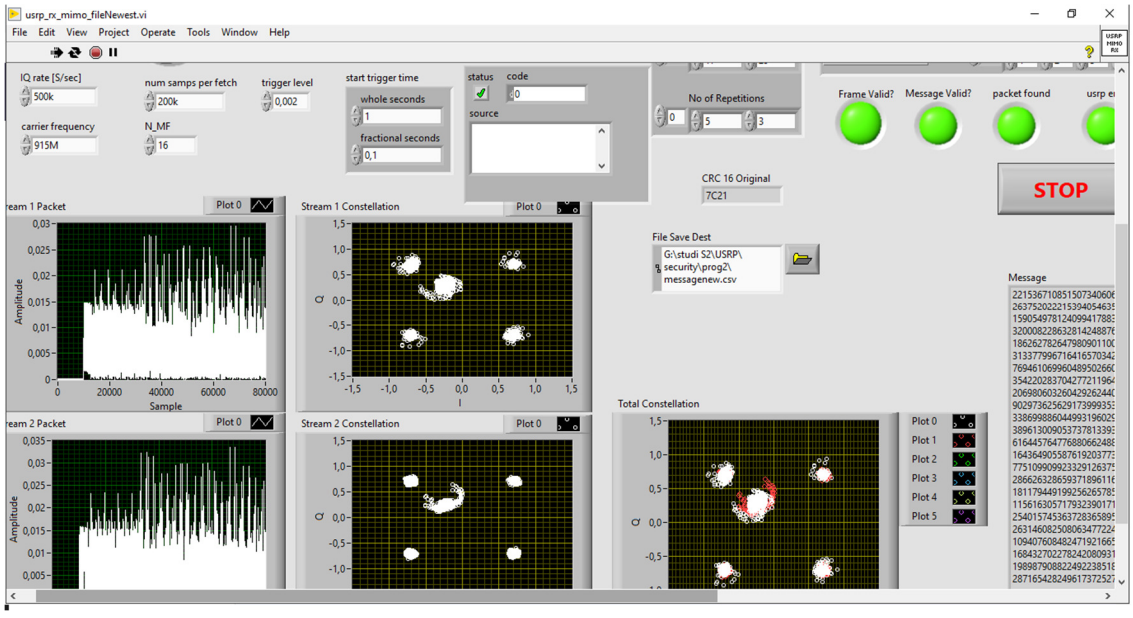


Fig. 13 The receiver (Bob, Attacker) receives the complete ciphertext

The encryption process is carried out with an ECC parameter of 224-bit. The cipher message is obtained from this encryption process, as shown in Fig. 12. The ciphertext obtained by Alice is then sent through the MIMO-OFDM communication system so that Bob gets this ciphertext message. However, in the middle of the communication session, an attacker also gets the ciphertext sent by the MIMO-OFDM system. In sending ciphertext, each receiver will check the ciphertext file sent. Checking is done to determine the completeness of the file sent. The CRC-16 algorithm is used to perform this check. Recipients who receive a complete ciphertext will have a display like Fig. 13.

After the ciphertext received is complete, Bob decrypts it using the private key embedded in the receiving computer of the MIMO-OFDM system. The private key owned by Bob is presented in Fig. 14. Then Bob performs the decryption process with the private key image 92 and the same ECC parameters as Alice. Because the private key owned by Bob is valid, the plaintext result of the decryption process is obtained following Alice's, as shown in Fig. 15.

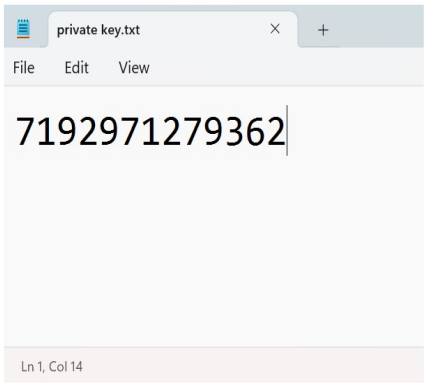


Fig. 14 Private key owned by Bob

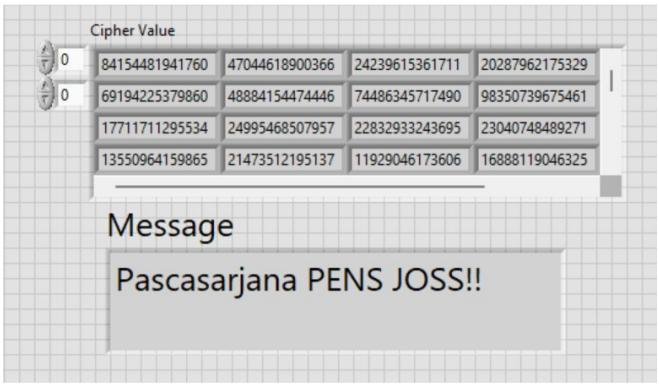


Fig. 15 Plaintext decryption result by Bob

At the same time, the attacker tries to decrypt the sent ciphertext. Assuming that the attacker knows the ECC parameters but does not have a valid private key. Then, the attacker will try to guess the private key used by the valid recipient. The attacker guesses the private key, and the resulting private key is invalid, as shown in Fig. 16. Because the guessed private key is invalid when performing the ciphertext decryption process, the decryption result is obtained, as shown in Fig. 17.

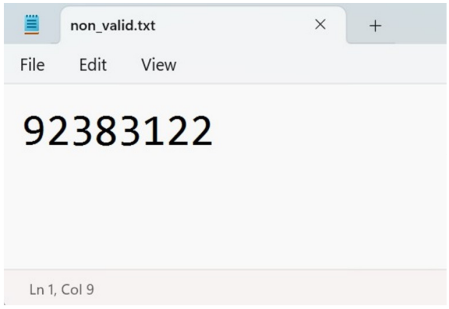


Fig. 16 Private key invalid by Attacker

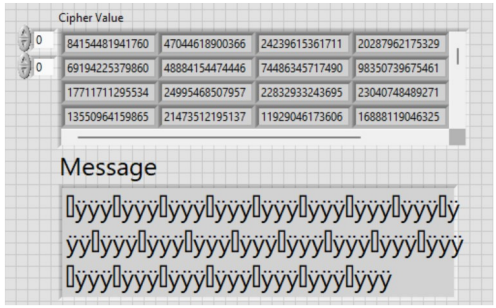


Fig. 17 Invalid plaintext

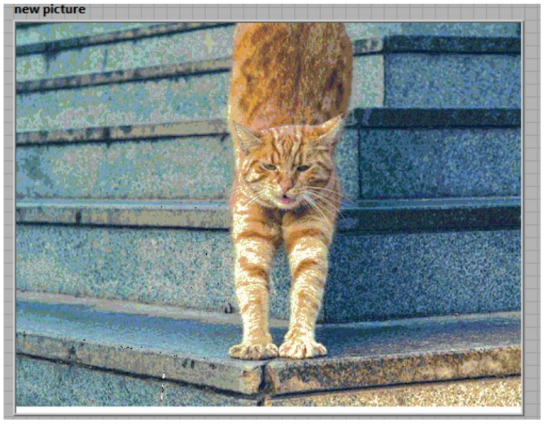


Fig. 18 Image transmission by Alice

After Alice sends the ciphertext, Bob and the attacker decrypt it. Alice starts transmitting the image with the subcarrier randomizer algorithm. The image data sent by Alice in this section is presented in Fig. 18. Fig. 18 is then sent by Alice to Bob by first performing a subcarrier randomizer using the plaintext reference and also the additional text of the entire ciphertext, as shown in Fig. 19. After decrypting the ciphertext data, Bob uses the plaintext data and the addition text of the entire ciphertext, as demonstrated in Fig. 20, to perform subcarrier reconstruction on the MIMO-OFDM signal received from Alice.

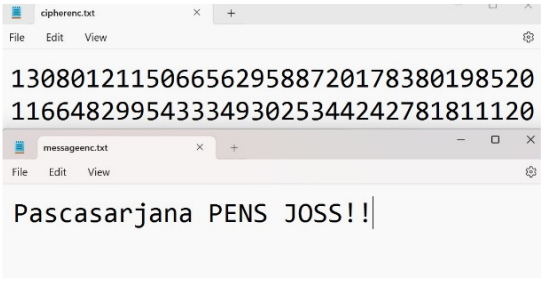


Fig. 19 Subcarrier randomizer reference on Alice

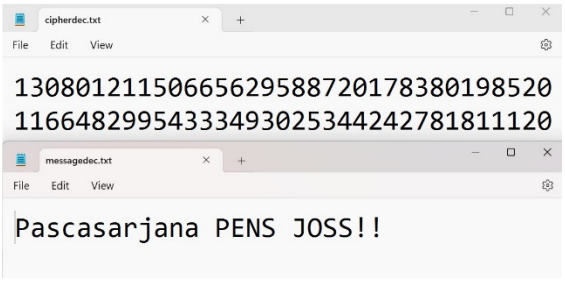


Fig. 20 Subcarrier reconstruction on Bob

Meanwhile, the attacker also tries to use invalid plaintext data resulting from incorrect ciphertext decryption and text addition of the entire ciphertext, as shown in Fig. 21, to perform the subcarrier reconstruction process. Since the bob uses a valid subcarrier reconstruction reference, the image received by the bob is presented in Fig. 22.

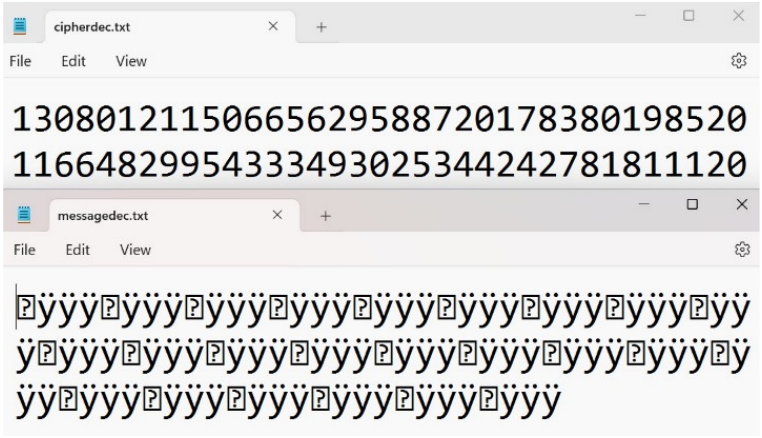


Fig. 21 Subcarrier reconstruction reference on Attacker

Fig. 22 The image received by Bob

From Fig. 22, Bob obtained an image similar to the image sent by Alice. This happens because Bob can perform subcarrier reconstruction on the MIMO-OFDM signal sent by Alice. In contrast, the attacker fails to perform subcarrier reconstruction because there is no valid reference. Fig. 23 illustrates that the image is scrambled, making it difficult to recognize the original data in the image. Thus, a failed subcarrier reconstruction process will scramble the transmitted data. The image obtained by the attacker in this process is shown in Fig. 23.

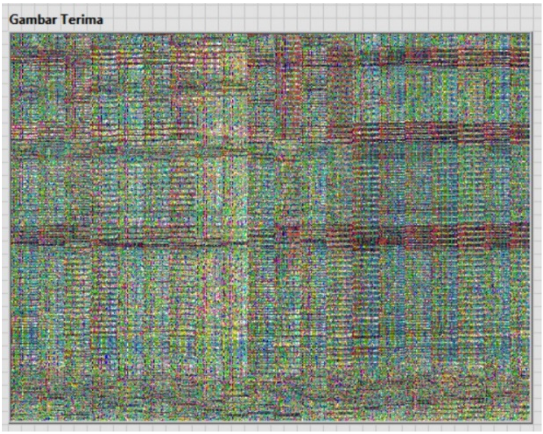


Fig. 23 Image received by the Attacker

Through several times of experiments and data measurements, a graph of the bit error rate (BER) function compared to the signal-to-noise ratio (SNR) in the subcarrier randomizer and subcarrier reconstruction system in MIMO-OFDM was obtained. The resulting graph, comparing authorized and unauthorized receivers, is shown in Fig. 24. The BER graph in Fig. 24 indicates that the BER graph for unauthorized receivers is greater than the BER graph for authorized receivers. This is due to the data received by the unauthorized receiver having many errors, as the receiver cannot reconstruct the data sent by the transmitter.

From Fig. 24, the lowest value of BER on the authorized receiver is 0.123×10^{-3} at 9.67 dB of SNR. While on the unauthorized receiver, the lowest BER value is 0.459×10^{-1} at 8.47 dB of SNR. The BER value at the unauthorized receiver is very high, even for the lowest BER value. Thus, it can concluded that the performance of the subcarrier randomization and subcarrier reconstruction system effectively secures based MIMO-OFDM communication system.

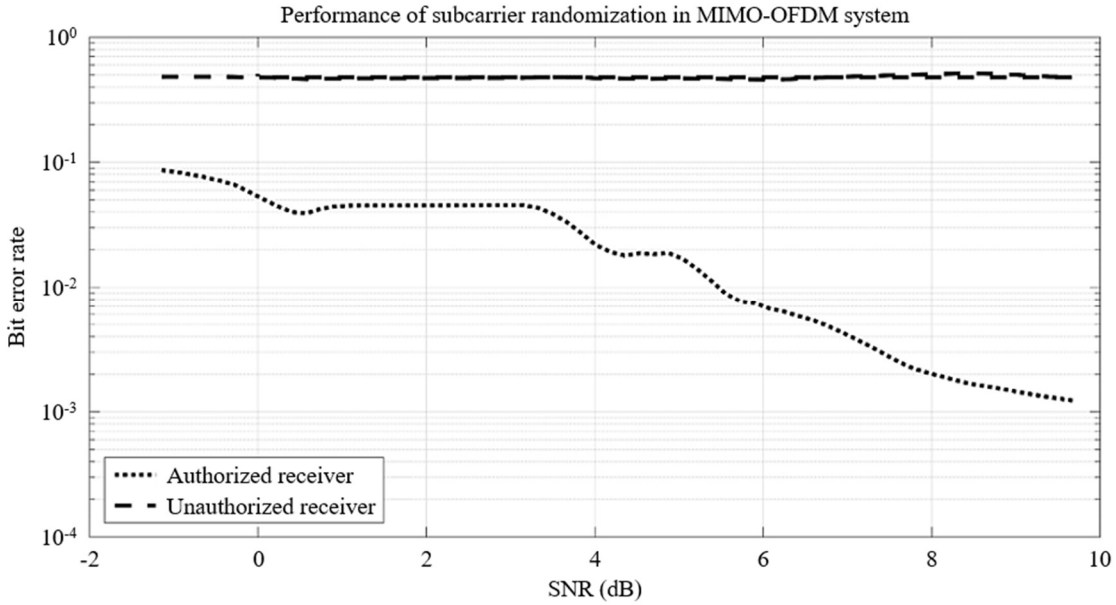


Fig. 24 BER vs SNR for the authorized and the unauthorized receiver by subcarrier randomizer in MIMO-OFDM

5. Conclusions

In this study, the subcarrier randomization system has been successfully implemented in MIMO-OFDM using USRP. Subcarrier randomization is a PLS method that randomizes the subcarrier based on message synchronization and the ECC algorithm cipher. In implementing this system, due to the receiver's inability to rearrange the subcarrier and decode the message, the unauthorized receiver will get a signal with a randomized subcarrier, which causes a random message at the receiver. Notably, the unauthorized receiver scenario exhibits a constellation almost identical to that of the authorized receiver. This is because the subcarrier randomization process only randomizes the transmitter's data subcarrier, while the receiver uses a different plaintext message reference than the transmitter. Consequently, even though the same cipher message is used, the results are different.

The comparison measurement of ECC parameters is conducted by comparing the computational delay of the three ECC parameters, specifically during the public key generation, encryption, and decryption process. The results indicate that the decryption process requires less time than the encryption process due to generating less work. The performance comparison between ECC and RSA algorithms underscores the importance of selecting ECC parameters to reduce the computational cost of both transmitter and receiver systems. ECC demonstrates a lower computational cost compared to the RSA method at the same bit security level. Experiment results reveal that the lowest value of BER for the authorized receiver is 0.123×10^{-3} at 9.67 dB of SNR, whereas for the unauthorized receiver, the lowest BER value is 0.459×10^{-1} at 8.47 dB of SNR.

Acknowledgments

This research was supported by the Directorate General of Vocational Education of the Indonesian Ministry of Education, Culture, Research and Technology and Politeknik Elektronika Negeri Surabaya (PENS).

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] M. Nikhita, and R. Mohan, "Analysis of LTE and IEEE 802.11n Channel Models for Wireless Communication Networks," 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), pp. 940-946, October 2023.

[2] T. D. A. Costa, A. S. Macedo, E. M. C. Matos, B. S. L. Castro, F. D. S. Farias, C. M. M. Cardoso, et al., "A Temporal Methodology for Assessing the Performance of Concatenated Codes in OFDM Systems for 4K-UHD Video Transmission," Applied Sciences, vol. 14, no. 9, article no. 3581, May 2024.

[3] A. Iqbal, M. Drieberg, V. Jeoti, A. A. Aziz, G. M. Stojanovic, M. Simic, et al., "Advancing Multiband OFDM Channel Sounding: An Iterative Time Domain Estimation for Spectrally Constrained Systems," IEEE Access, vol. 11, pp. 103333-103349, 2023.

[4] N. H. Trung and N. T. Anh, "Beamforming-as-a-Service for Multicast and Broadcast Services in 5G Systems and Beyond," IEEE Access, vol. 11, pp. 142794-142815, 2023.

[5] L. Ge, C. Shi, S. Niu, G. Chen, and Y. Guo, "Mixed RNN-DNN Based Channel Prediction for Massive MIMO-OFDM Systems," IET Communications, vol. 17, no. 19, pp. 2152-2161, December 2023.

[6] N. U. Saqib, M. S. Haroon, H. Y. Lee, K. Park, H. G. Song, and S. W. Jeon, "THz Communications: A Key Enabler for Future Cellular Networks," IEEE Access, vol. 11, pp. 117474-117493, 2023.

[7] H. Xu, N. Pillay, and F. Yang, "N-Ary Alamouti Space-Time Block Coding With and Without Golden Codewords," IEEE Access, vol. 11, pp. 129954-129962, 2023.

[8] G. Interdonato, S. Buzzi, C. D'Andrea, L. Venturino, C. D'Elia, and P. Vendittelli, "On the Coexistence of eMBB and URLLC in Multi-Cell Massive MIMO," IEEE Open Journal of the Communications Society, vol. 4, pp.1040-1059, 2023.

[9] Y. Yao, F. Shu, Z. Li, X. Cheng, and L. Wu, "Secure Transmission Scheme Based on Joint Radar and Communication in Mobile Vehicular Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 9, pp. 10027-10037, September 2023.

[10] Y. Yao, J. Zhao, Z. Li, X. Cheng, and L. Wu, "Jamming and Eavesdropping Defense Scheme Based on Deep Reinforcement Learning in Autonomous Vehicle Networks," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1211-1224, 2023.

[11] S. Chandel, W. Cao, Z. Sun, J. Yang, B. Zhang, and T. Y. Ni, "A Multi-Dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption," Future of Information and Communication Conference, pp. 988-1003, March 2019.

[12] M. R. Khan, K. Upreti, M. I. Alam, H. Khan, S. T. Siddiqui, M. Haque, et al., "Analysis of Elliptic Curve Cryptography & RSA," Journal of ICT Standardization, vol. 11, no. 4, pp. 355-378, November 2023.

[13] D. V. Linh and V. V. Yem, "Key Generation Technique Based on Channel Characteristics for MIMO-OFDM Wireless Communication Systems," IEEE Access, vol. 11, pp. 7309-7319, 2023.

[14] M. M. Hasan, M. Cheffena, and S. Petrovic, "Physical-Layer Security Improvement in MIMO OFDM Systems Using Multilevel Chaotic Encryption," IEEE Access, vol. 11, pp. 64468-64475, 2023.

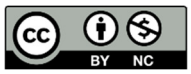
[15] Y. Katsuki, G. T. F. de Abreu, K. Ishibashi, and N. Ishikawa, "Noncoherent Massive MIMO With Embedded One-Way Function Physical Layer Security," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 3158-3170, 2023.

[16] J. Martins, M. Gomes, V. Silva, and R. Dinis, "Physical Layer Spoofing Detection in MIMO SVD Communications," IEEE International Mediterranean Conference on Communications and Networking, pp. 364-368, September 2023.

[17] X. Liu, L. Zhang, W. Xie, Y. Cao, and C. Fan, "Physical Layer Security of the MIMO-NOMA Systems Under Near-Field Scenario," Electronics, vol. 13, no. 4, article no. 670, February 2024.

[18] W. Abdallah, "A Physical Layer Security Scheme for 6G Wireless Networks Using Post-Quantum Cryptography," Computer Communications, vol. 218, pp. 176-187, March 2024.

[19] Y. M. Al-Moliki, M. T. Alresheedi, Y. Al-Harthi, and A. H. Alqahtani, "Channel-Independent Quantum Mapping-Substitution OFDM-Based Spatial Modulation for Physical-Layer Encryption in VLC Networks," Vehicular Communications, vol. 45, article no. 100706, February 2024.
[20] A. Yusof, E. Abdullah, A. Idris, and W. A. Mustafa, "PAPR Reduction in Cyclic Prefix OFDM (5G) System Using Group Codeword Shifting Technique," Journal of Advanced Research in Applied Mechanics, vol. 107, no. 1, pp. 30-40, July 2023.
[21] A. K. H. Al-Ali and F. S. Hasan, "High Level Security of Image Transmission Through STBC-COFDM System," International Journal of Intelligent Engineering and Systems, vol. 16, no. 1, pp. 154-162, 2023.
[22] D. V. Linh and V. V. Yem, "A Turbo-Based Encryption and Coding Scheme for Multiple-Input Multiple-Output Orthogonal Frequency Division Multiplexing Wireless Communication Systems Affected by Doppler Frequency Offset," IET Communications, vol. 17, no. 5, pp. 632-640, March 2023.
[23] H. Luo, N. Garg, and T. Ratnarajah, "A Channel Frequency Response-Based Secret Key Generation Scheme in In-Band Full-Duplex MIMO-OFDM Systems," IEEE Journal on Selected Areas in Communications, vol. 41, no. 9, pp. 2951-2965, September 2023.
[24] M. Kaur, A. A. Alzubi, T. S. Walia, V. Yadav, N. Kumar, D. Singh, et al., "EGCrypto: A Low-Complexity Elliptic Galois Cryptography Model for Secure Data Transmission in IoT," IEEE Access, vol. 11, pp. 90739-90748, 2023.
[25] C. Silva, V. A. Cunha, J. P. Barraca, and R. L. Aguiar, "Analysis of the Cryptographic Algorithms in IoT Communications," Information Systems Frontiers, vol. 26, no. 4, pp. 1243-1260, August 2024.
[26] W. Hussein, K. Audah, N. K. Noordin, H. Kraiem, A. Flah, M. Fadlee, et al., "Least Square Estimation-Based Different Fast Fading Channel Models in MIMO-OFDM Systems," International Transactions on Electrical Energy Systems, vol. 2023, article no. 5547634, 2023.
[27] H. Yang, X. Geng, H. Xu, and Y. Shi, "An Improved Least Squares (LS) Channel Estimation Method Based on CNN for OFDM Systems," Electronic Research Archive, vol. 31, no. 9, pp. 5780-5792, 2023.
[28] R. Zayani, J. B. Dore, B. Miscopein, and D. Demmer, "Local PAPR-Aware Precoding for Energy-Efficient Cell-Free Massive MIMO-OFDM Systems," IEEE Transactions on Green Communications and Networking, vol. 7, no. 3, pp. 1267-1284, September 2023.
[29] Z. Cao and L. Liu, "The Practical Advantage of RSA Over ECC and Pairings," unpublished.



Copyright© by the authors. Licensee TAETI, Taiwan. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) license (https://creativecommons.org/licenses/by-nc/4.0/).