ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

Asymmetric Physical Layer Encryption Over Stationary Time Selective Wireless Communication Channel

Khalid Hamdnaalla[1]; AEbtihal Haider Gismalla Yousif[2,1]; Rashid Saeed[3,1]; Abdullah Khalil Mansour[4,2]

School of Electronic Engineering College [1], IT Department [2]
Sudan University of Science and Technology[1], EQLEED Group for IT Solution Company [2]
Khartoum, Sudan [1], Riyadh, Saudi Arabi[2]

Publication Date: 2025/01/30

Abstract: This paper proposes an asymmetric physical layer security scheme APLE based on Elliptic curve Diffie Helman (ECDH), channel state information (CSI), and stream cipher to achieve user authenticity, key agreement and confidentiality. Moreover, this work utilizes the most promising wireless communication model and multiple access combination. Multi-Input-Multi-Output (MIMO), and Orthogonal Frequency Division Multiplexing (OFDM) respectively. Unlike other relent schemes this paper considers stationary time selective Rayleigh fading channel. The proposed authentication protocol has been proven. PLE consists of stages; Modulation Encryptor and Crypto Filters based on minimal correlation coefficient have been proposed. The function of the Modulation Encryptor is to provide confusion. However, the function Crypto-Filter provides the diffusion. The proposed PLE scheme has been designed to work with modulation schemes with signal space greater than four. The proposed PLE is simulated based on QPSK and 16QAM, and some numerical results have been drowned. symbol error rate SER as function of signal to noise ration SNR with correlation coefficient have been used to measure security strength. Besides SER and peak signal to noise ratio PSNR used to evaluate the system reliability. The results show this scheme has strong security (SER at eavesdropper rich ninety five percent with correlation coefficient almost zero), and excellent reliability (same performance as no encryption).

Keywords*: ECDH; CSI; Stream Cipher; PLE; OFDM; MIMO.*

How to Cite: Khalid Hamdnaalla; AEbtihal Haider Gismalla Yousif; Rashid Saeed; Abdullah Khalil Mansour. (2025). Asymmetric Physical Layer Encryption Over Stationary Time Selective Wireless Communication Channel. *International Journal of Innovative Science and Research Technology*, 10(1), 1224-1237. https://doi.org/10.5281/zenodo.14769336.

I. INTRODUCTION

In recent years, data communication has become increasingly reliant on various wireless standards, such as 5G, LTE, WiMAX (IEEE802.16x family), and WLAN (IEEE802.11x family). Emerging technologies like the Internet of Things (IoT), Wireless Sensor Networks (WSN), Smart Homes, and Machine-to-Machine (M2M) communication are also heavily dependent on wireless standards, including IEEE802.15.x (e.g., Zigbee and Bluetooth) and the Z-wave wireless protocol [1]. While wireless communication serves as the primary channel for data transmission, its inherent broadcast nature exposes it to greater security risks. Consequently, security services have been integrated into wireless communication standards [2], covering aspects such as data confidentiality, integrity, and user authentication. Security services are defined as processes or devices that detect, prevent, or recover from attacks. These services depend on modern cryptographic techniques [3], which, although deemed computationally secure (e.g., AES, SNOW3, RSA, and elliptic curve schemes), face significant threats from emerging quantum cryptanalysis techniques [4]. This calls for physical layer security (PLS), a concept first introduced by “Shannon” [5], which aims to achieve unconditional security. While the term "physical layer" (PHY) may initially evoke an image of hardware components, it encompasses a broader definition that includes hardware specifications, encoding, signaling, data transmission/reception, network topology, and overall physical network design [6]. Unlike computational security, which is dependent on an adversary’s computational capabilities, unconditional security remains resilient regardless of the opponent's computational power. Security services are typically implemented in the upper layers of the OSI communication model, assuming a feasible PHY. While PLS, based on information theory, holds great theoretical potential for perfect secrecy, its implementation in wireless communication standards has yet to materialize [7]. Additionally, several approaches in the literature combine cryptography with PHY properties to enhance

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

communication security, such as PHY Encryption (PLE) and PHY Authentication and Key Agreement (PAKA) protocols. These methods leverage current schemes, including OFDM, MIMO, and modulation techniques, while also exploiting channel imperfections such as noise and fading (Channel State Information, CSI) alongside secure cryptographic mechanisms. These hybrid approaches are seen as more applicable in practice. Therefore, this paper is inspired by this category. The following section outlines some of these methods.

PLS confidentiality, often referred to as PLE, offers a more practical and effective security paradigm than traditional PLS secrecy. PLE makes use of secure cryptographic schemes, ensuring that the encryption process is unaffected by channel conditions. Unlike traditional cryptographic techniques, PLE can exploit channel impairments to enhance security. Numerous PLE schemes have been proposed for various systems, such as modulation-based PLE [8], [9], OFDM systems [2], [10], [11], [12], MIMO PLE systems [13], [14], [24], IEEE 802.15.4 protocols [15], and sparse code multiple access (SCMA) [16]. PLE is regarded as a hybrid security system, integrating PLS, cryptography, and signal processing. In the literature, PAKA is categorized into three types: key generation, key exchange, and PHY authentication. For key generation, legitimate communication parties either use CSI to derive shared keys [17] or extract information from the channel and exchange messages to agree on a common secret key [18], [19], [25]. Secret key exchange methods include cryptographic protocols [20], [21], jamming [22], and precoding [23]. Additionally, there are numerous studies proposing PHY authentication protocols, such as those in [26] and [27].

This paper proposes a PAKA protocol based on CSI, Diffie-Hellman Elliptic Curve (DHEC), and stream ciphers for MIMO/OFDM wireless communication systems over stationary, time-selective channels. The keys generated during the PAKA stage will be utilized by the proposed PLE. The proposed PLE consists of the Modulation Encryptor, and the OFDM Crypto Filters, which uses stream ciphers as pseudo random numbers generator. Therefore, the overall picture of this work is asymmetric PLE (APLE). The remainder of the paper is organized as follows: section (II) communication and cryptography primitives, section (III) PAKA based on ECDH, CSI and stream cipher, section (IV) PLE based on modulation encryptor and crypto filters, and section (V) performance analysis and numerical simulations.

II. COMMUNICATION AND CRYPTOGRAPHY PREMATIVES

This section introduces the notations, channel characteristics, communication schemes, and cryptographic primitives utilized by this work.

A. Notations

In this paper, italic lowercase/uppercase x/ X used to represent scalars, italic bold uppercase $\boldsymbol{X}_{N\times N}$, and $\boldsymbol{X}_{\mathbf{N}}$ denote square matrix with (N rows and N columns), and vector with (N columns) respectively, $CN\sim N(0,\sigma^2)$ stands for complex Gaussian random noise with a mean of zero "$\mu=0$", and variance equal to the noise power "$\sigma^2=N_0$". $\boldsymbol{X}_{\mathrm{N}\times\mathrm{N}}{}^{T}$, $\boldsymbol{X}_{\mathbf{N}\times\mathbf{N}}{}^{-1}$ and $\boldsymbol{X}_{\mathbf{N}\times\mathbf{N}}{}^{H}$ represent transpose, inverse and harmtion (transpose and conugate) of matrix repestively. $\boldsymbol{X}_{N}{}^{T}$ denotes N columns vector transpose. Notation E_k, D_k, Sig_k, and Ver_K represent encryption, decryption signature and verification using the key (k) respectively. Subscrpits "A" represents value, key or operation with respect to Alice, while the subscrpit "B" denotes Bob. The terms "channel state information CSI" and "channel matrix (e.g. $\boldsymbol{H}_A$)" are used interchangeably in this paper. The term $\widehat{X}$ is the crrupted received version of X. To make it easer $\boldsymbol{H}_A$ denotes Alice $N\times N$ complex channel matrix and $\boldsymbol{X}_A$ denotes N columns Alice transmitted vector.

B. System Model and Channel Characteristics

This paper considers Alice, Bob, and Ever as the legitimate transmitter, legitimate receiver, and passive attacker (eavesdropper), respectively. Additionally, it is assumed that the communication mode between the parties is fully duplex. The communication system is based on MIMO/OFDM architecture, with N antennas for both the transmitter and the receiver. The channel is a stationary time-selective channel, which remains constant throughout the transmission. However, the channel between Alice and Bob differs from the channel between Bob and Alice, the channel between Alice and Ever is not the same as the channel between Ever and Alice, and similarly, the channel between Bob and Ever differs from the channel between Ever and Bob. Besides, it assumes that the channel estimator is error free. See (Fig 1).

C. Maximum Ratio Combining MRC

In a MIMO system with N transmit antennas and N receive antennas, the MRC receiver combines the received signals with optimal weights based on the channel gains [28]. The output as in (1).

$$y_{mcr}=\sum_{i=1}^{N}\boldsymbol{X}_{N}{}^{T}\boldsymbol{W}_{mrc}+n_i \quad (1)$$

where:

$\boldsymbol{W}_{mrc}=H_{N\times N}{}^{H}\equiv$ MRC receiver beamformer

$\boldsymbol{H}\equiv$ channel matrix, consists of complex fading cofficients with amplitude follows Rayleigh random variable and phase follows uniform random varible

$X\equiv$ receive signals vector

$n_i\equiv i^{th}$ receiver CN noise

D. Zero Forcing Beamformer ZF

ZF Beamformer is a linear beamforming technique used in MIMO systems to eliminate inter-user interference by inverting the channel matrix. The ZF beamformer is designed at the transmitter to ensure that the transmitted signal is orthogonal to the interference, effectively "forcing"

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

the signal at the receiver to be interference-free, assuming perfect channel estimator [28]. ZF Beamformer formula as in (2).

$$W_{ZF} = \left(H_{N\times N}{}^{H} H_{N\times N}\right)^{-1} H_{N\times N}{}^{H} \quad (2)$$

where:

$W_{ZF} \equiv$ Beamformer

E. Elliptic Curve Diffie Hellman Key Exchange Protocol ECDH

ECDH protocol is a key establishment protocol which makes uses of DH key establishment protocol based on EC discrete logarithm problem ECDL. The EC is arithmetic of points on the curve with respect $Z_P = \{0,1,\ldots,p-1\}$, where P is prime number. The EC must satisfy conditions in (3).

$$y^2 = x^3 + ax + b \ mod \ P \quad (3)$$

with point o at infinity (The identity element)

condition:

$$P > 3$$

$$4a^3 + 27b^2 \ mod \ P \neq 0$$

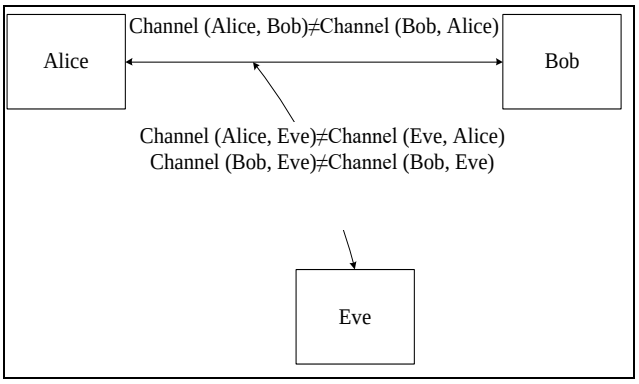


Fig 1: The Communication Model

EC discrete logarithm problem is that given point Q, and T defined on the EC, such that $T = d.Q$, where d is integer. Find d supposed to be hard problem [29]. The primitive element is an element in the group, such that all other elements can be generated from it using the group operation. In the case of EC, the primitive elements are some points on the curve. ECDH protocol steps as follows:

- E, P, and Q, where E is the EC, P is the prime number, and is a primitive element are public parameters available for all communication parties (Alice, Bob, and Eve).
- Alice (legitimate transmitter) chooses the private key a, compute: $A = a.Q = a.(x_Q, y_Q) = (x_A, y_A)$, then send A to Bob.
- Bob (legitimate receiver) chooses the private key b, compute: $B = b.Q = b.\left(x_Q, y_Q\right) = \left(x_B, y_B\right)$, then sends B to Alice.
- Alice and Bob computer $k_{AB} = a.B$, and $k_{AB} = b.A$ respectively. Therefore, Alice and Bob establish the same key (k_{AB}= a.b.Q).

There are several standard EC defined by National Institute of Standards and Technology (NIST) for primes number of lengths 192, 224, 256, 384, and 512 [30]. This work can be implemented using any one of them.

F. Stream Cipher

Stream ciphers are symmetric key cryptographic algorithms that encrypt data on a bit-by-bit or byte-by-byte basis, making them ideal for real-time applications. Additionally, they are commonly utilized as pseudo-random number generators. Several well-established stream ciphers are available for both software and hardware implementations. The schemes proposed in this paper can be applied to any cryptographically secure stream cipher. However, the numerical simulation results (section V) specifically employ the Trivium stream cipher algorithm. Trivium is a lightweight, secure stream cipher based on a nonlinear feedback shift register architecture, as depicted in (*Fig. 2*). It comprises three feedback shift registers—A (93 bits), B (84 bits), and C (111 bits)—with the output of A feeding into C, the output of B feeding into A, and the output of C feeding into B. The algorithm is initialized with an 80-bit key loaded into the leftmost locations of register B and an 80-bit initialization vector (IV) placed into the leftmost locations of register A. All

Other register bits are set to zero, except for the three rightmost bits of each register C, which are set to one. In addition to the feedback paths, feedforward paths, shown in (*Fig. 2*), are employed to introduce non-linearity through AND-gates. If the IV changes with each session, the primary known attack against Trivium remains exhaustive key search (brute force). The algorithm executes 1152 clock cycles before producing the first output [29]. EC points group consists of several points known as the primitive elements (generators).

G. Functions

- Hash function: is a cryptographic algorithm that transforms input data (of any size) into a fixed-size output, typically represented as a hash value or digest. It is designed to be fast, deterministic, and collision-resistant, ensuring that different inputs produce unique outputs. Commonly used in data integrity checks, password storage, and digital signatures, hash functions are vital in modern cryptography [31]. The schemes proposed in this paper can be applied to any cryptographically secure hash function such as Secure Hash Algorithm 256-bit (SHA-256).
- Shuffle function is used to rearrange elements in a data set randomly, ensuring that the order of elements is unpredictably altered. This is widely used in cryptographic applications like key generation and in protocols such as secure multi-party computations [31]. The schemes proposed in this paper can use any kind of shuffle such as right circular shift several times.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

III. PAKA BASED ON ECDH, CSI AND STREAM CIPHER

This paper proposes PAKA utilizing CSI, digital signature, and PLE based on stream cipher. The proposed PAKA protocol consists of a two-phase, setup phase (at the installation for fixed network or when a new device inters the network), and session phase.

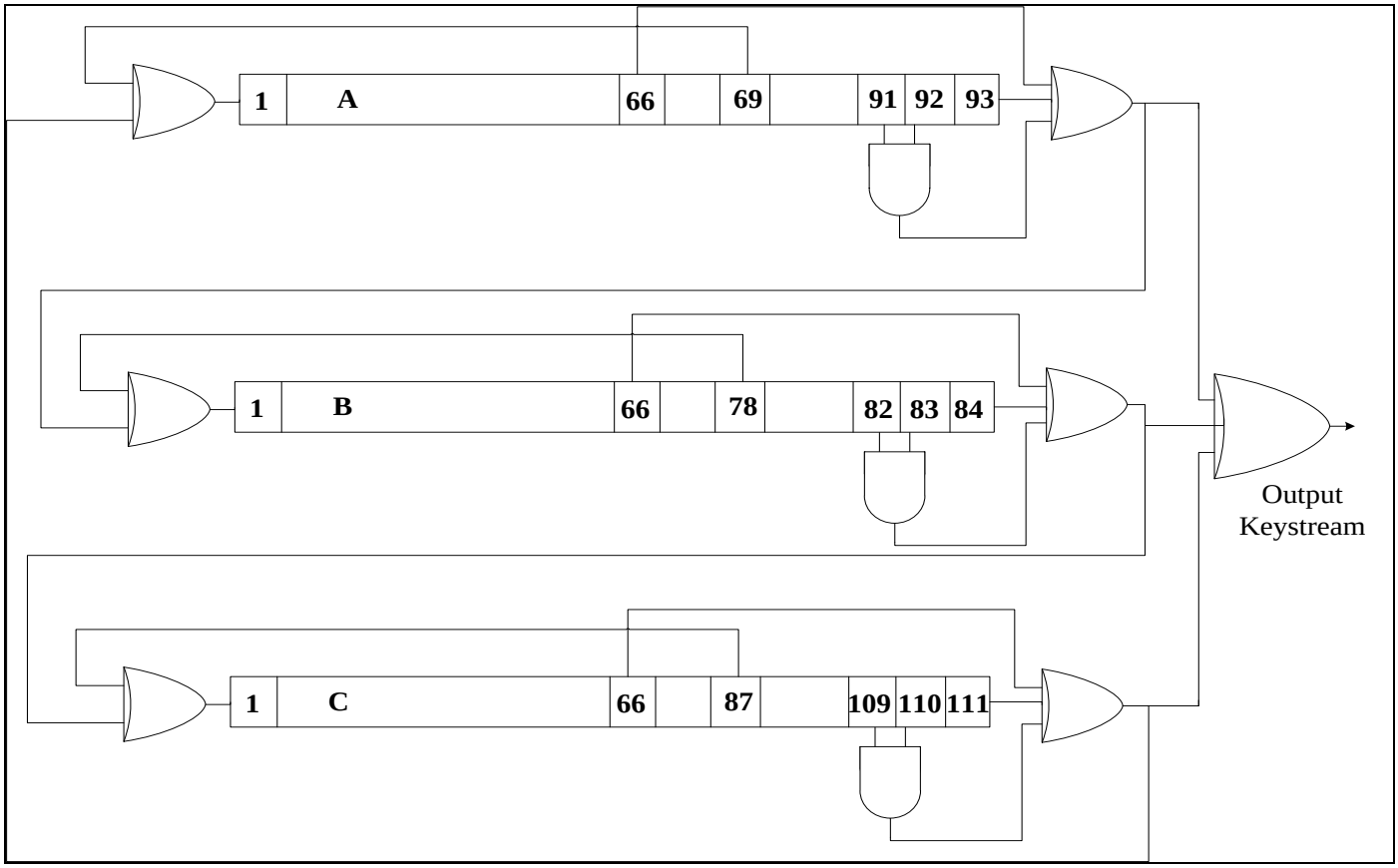


Fig 2: Trivium Stream Cipher

A. Setup Phase

➢ *The Setup Phase Consists of the Following Steps:*

- Alice transmits a request consisting of long training symbols, which are known to all parties. Bob receives these symbols and utilizes an error-free channel estimator to estimate the channel from Alice. Subsequently, he constructs a receiving beamformer MRC. Bob responds by transmitting long training symbols, which are also known to all parties. Alice receives these symbols and employs an error-free channel estimator to estimate Bob's channel. She then constructs a receiving beamformer based on MRC.
- Therefore, Alice and Bob agree on the same key using ECDH only once. They then authenticate each other and exchange their CSIs as demonstrated in protocol (1). The authentication, based on the proposed private key digital signature scheme, will be explained in the session phase.
- At this point, both Alice and Bob are aware of their CSIs. Consequently, they create ZF transmitting beamformers and establish the setup-phase key as outlined in protocol (1).

B. Session Phase

Alice and Bob use a shuffled version of the key established in the previous session, along with the proposed PLE based stream cipher, to sign, exchange, and then verify the channel matrices. This key, referred to as the ephemeral key, is denoted as k_E. Additionally, they authenticate each other using a private key digital signature scheme.

The signature scheme proposed in this paper is straightforward: Alice signs Bob's CSI with k_E. The signing function hashes Bob's CSI with k_E, producing a signature. Bob follows the same process.

After decrypting her CSI, Alice computes and verifies the signature. Bob performs the same verification. The validation of this scheme will be proved in section (V). Once authentication is complete, a session key can be established through the subsequent steps. Consequently, Alice and Bob construct the transmitting beamformers using Zero Forcing (ZF) as the initial layer of communication security. This approach ensures that Alice (the legitimate transmitter) directs the transmission exclusively towards Bob (the legitimate receiver). Then, the new session key established simply by hashing the new CSIs with k_E. The agreed key

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

will be used with the proposed symmetric key PLE to encrypt communication between legitimate parties.

IV. PLE BASED ON MODULATOR ENCRYPTOR AND CRYPTO-FILTERS

The proposed PLE involves two encryption operations: Modulation Encryptor, and OFDM-Crypto filters.

A. Modulation Encryptor

It consists of modulated symbols substitution table and constellation tilting.

- Modulated Symbols Substitution Table: for any symbols space M, there are (M!) modulation mapping tables, our proposed method exempts gray, and binary mapping tables. Therefore, the remaining tables are (M!-2). Thus, for block of M symbols only one table will be selected pseudo randomly based on the stream cipher. Algorithm (1) shows this scheme.
- Constellation Tilting: the output symbols from the modulated symbols substitution stage will be multiply by a constellation tilting factor. The complex constellation tilting factor T is pseudo randomly generated based on the stream cipher as in the algorithm (2).

The modulator encryptor is designed to work for $M \geq 4$ symbol space modulation schemes.

B. Crypto Filters

Let's start this session with correlation coefficient definition. The correlation coefficient is a statistical measure that describes the strength and direction of a linear relationship between two variables. It is typically denoted by *(r)*. The value of the coefficient correlation ranges from [-1,1], where:1 indicates a perfect positive linear relationship, −1 indicates a perfect negative linear relationship, and 0 indicates no linear relationship. This paper utilizes Pearson formula to calculate *r* as in (4), [32].

$$r = \frac{var(x)var(y)}{cov(x,y)} \quad (4)$$

where:

x, and $y \equiv$ variables

$var \equiv$ variance

$cov =$ covariance

OFDM Crypto-Filters involve two filters, named OFDM symbol encryption filter (Fig.3), and OFDM symbol decryption filter (Fig.4). Both filters utilize stream cipher pseudo random delays/ advances generator based on minimal correlation as shown in the Algorithm (3). The main idea behind OFDM symbol encryption filter is that the outputs of IFFT will be scrambled using delays (finite impulse response filters FIR) with impulse response of impulses shifted by the random indices. The function of the algorithm (3) is generating these random indices using the stream cipher. Expression in (6) represents the outputs of these filters utilizing the convolution as in (5) [33].

$$x[n] \circledast y[n] = \sum_{k=-\infty}^{\infty} x[k].y[n-k] \quad (5)$$

$$y[n] = x[n] \circledast \delta[n-k_i] = x[k_i] \quad (6)$$

where:

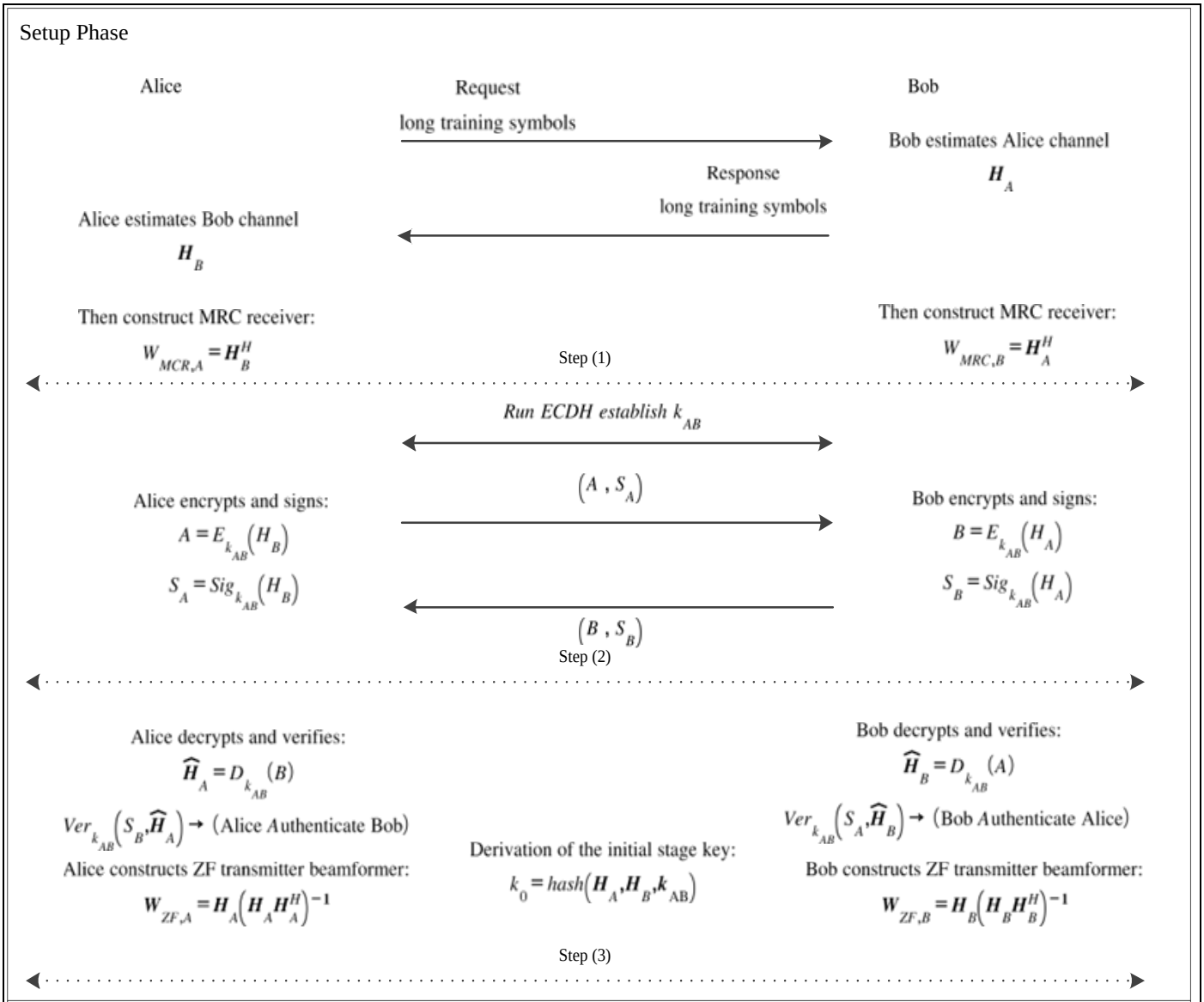
$\delta[n] \equiv$ impulse signal, $x[n] \equiv$ Input, and $y[n] \equiv$ Output

$i = 0,1,.....,N-1$, $k_i \equiv$ random index $\in Z_N$, such that

$k_i \neq k_j \; \forall (i,j)$ in one OFDM symbol

Then *r* between the encrypted OFDM symbol and plaintext OFDM symbol determined to strength of the encryption. Such that the OFDM symbol will be out if and only if, a weak correlation is deteteced (r<0.3) [34]. At receiver OFDM symbol decryption filter shown in Fig.4 will be used to recover the orignal OFDM symbol. The decryption process is same as the encryption process the only difference is delays become advances. The overall proposed MIMO-OFDM APLE scheme is shown in Fig.5.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.



Session Phase

For a new session (i):

1. Alice and Bob exchange long training symbols and estimate channels
2. Alice and Bob construct receiving beamformers based on MRC
3. Alice and Bob derive ephemeral key $k_E = shuffle(k_{i-1})$
4. Alice send out: $A = E_{k_E}(H_B), S_A = Sig_{k_E}(H_B)$
5. Bob send out: $B = E_{k_E}(H_A), S_B = Sig_{k_E}(H_A)$
6. Alice: $\widehat{H}_A = D_{k_E}(B)$, $Ver_{k_E}(S_B, \widehat{H}_A) \rightarrow$ Alice authenticate Bob
7. Alice: construct $W_{ZF,A}$, and compute the session key $k_i = hash(H_A, H_B, k_E)$
8. Bob: $\widehat{H}_B = D_{k_E}(A)$, $Ver_{k_E}(S_A, \widehat{H}_B) \rightarrow$ Bob authenticate Alice
9. *Bob*: construct $W_{ZF,B}$, and compute the session key $k_i = hash(H_A, H_B, k_E)$

Protocol 1: PAKAP Based on ECDH, CSI and Stream Cipher

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

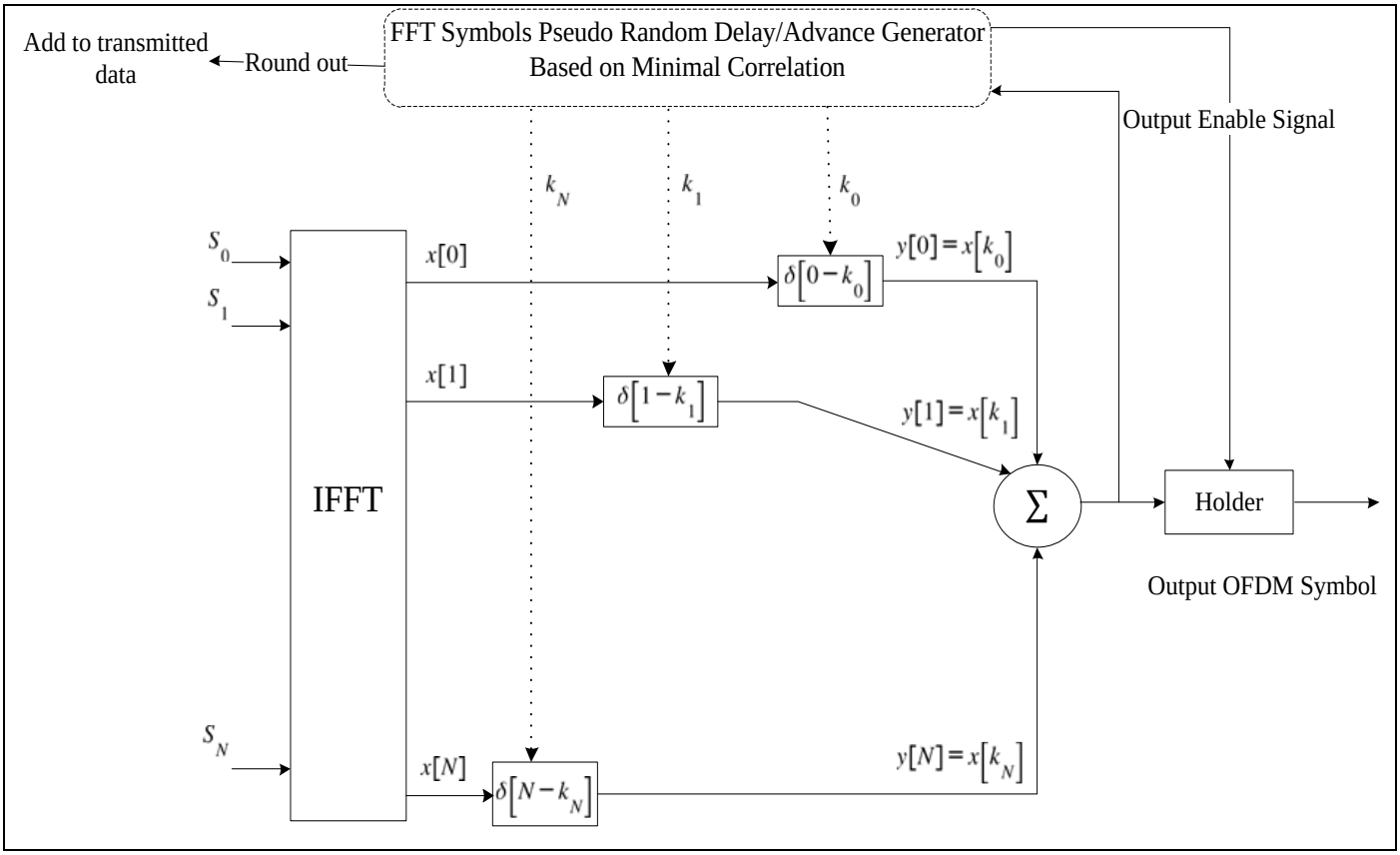


Fig 3: OFDM Encryption Filter

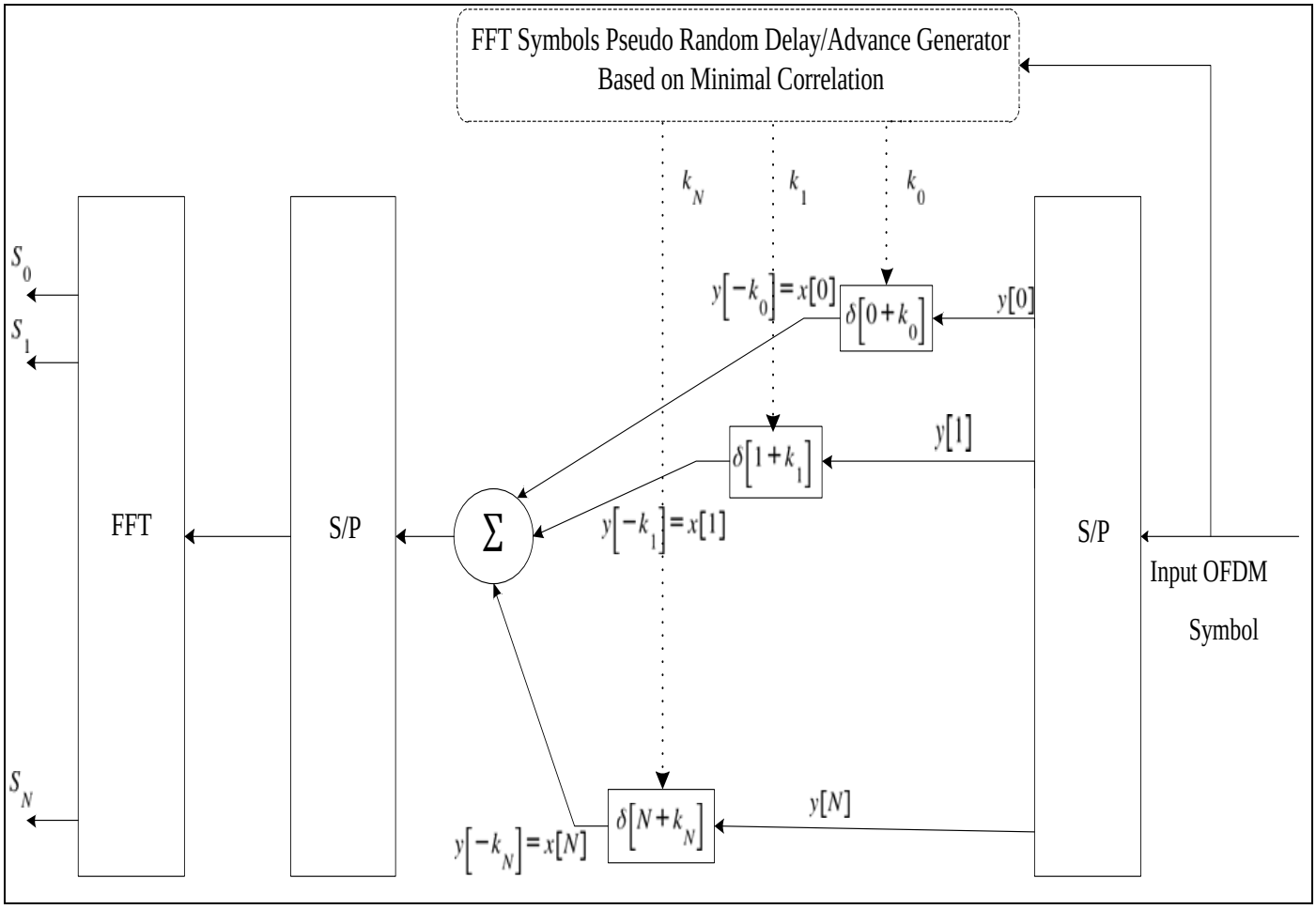


Fig 4: OFDM Decryption Filter

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

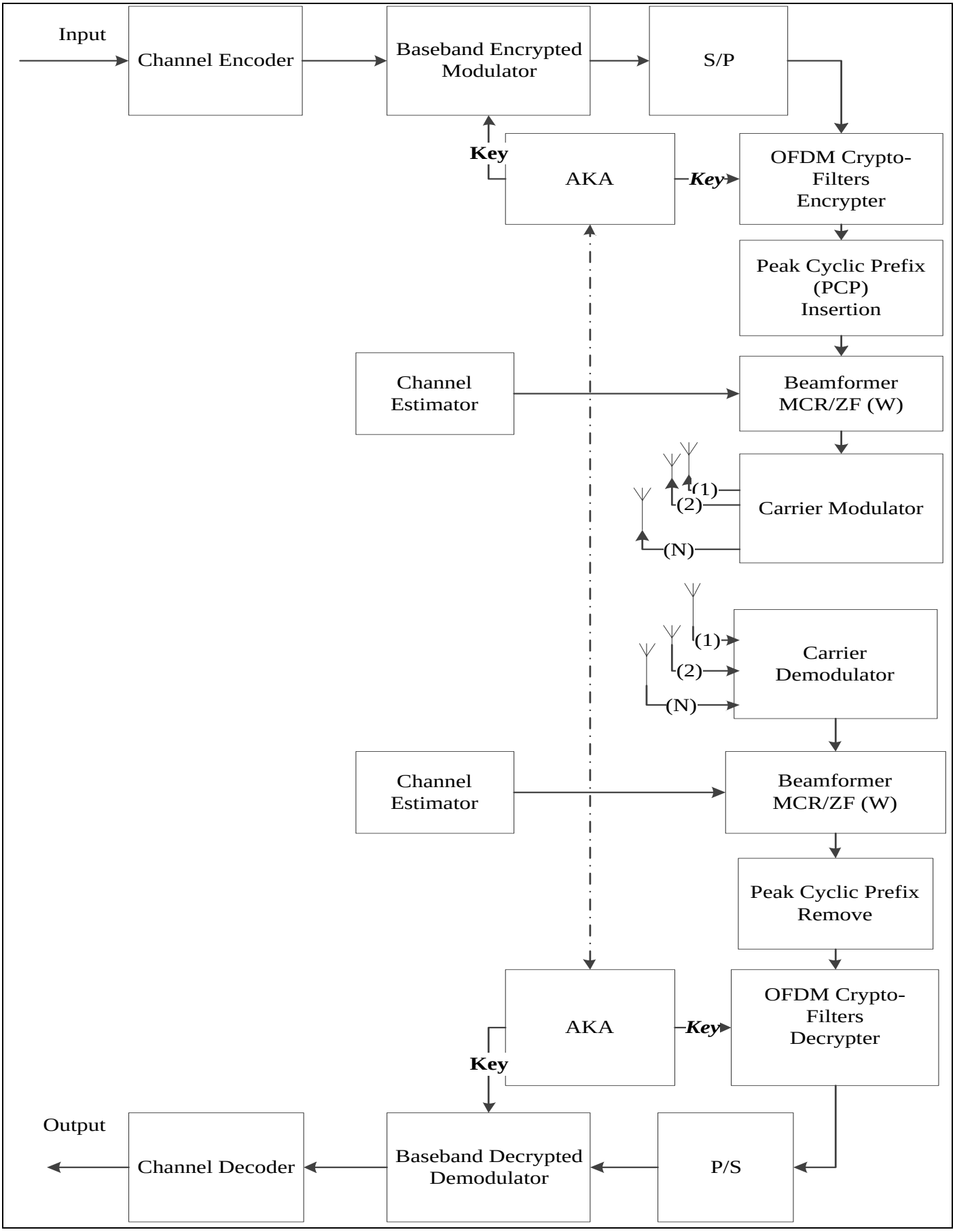


Fig 5: APLE Overall System

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

Algorithm 1: Modulator Encryptor Substitution Tables

1. ***Start***
2. ***inputs*** $\leftarrow (key, type, M)$

   where:

   $key \equiv$ *Encryption Key*

   $type \equiv$ *Modulation Type*

   $binary2decimal \equiv$ *convert binary to decimal number*
3. $depth = \log_2(M)$
4. $Tables[\ ] \leftarrow construct(type, M, depth)$

   where:

   $Tables \equiv$ *Modulation Tables, each with dimesnsion* M *by* 2, *each ceil signs a block of bits equal to the depth to unique signal*.

   Note: *gray and binary code are exempt*.
5. $index \leftarrow binary2decimal(\textbf{\textit{StreamCpher}}(key, depth))$
6. $randindex = mod(index, M! - 2)$
7. ***set*** $i \leftarrow 0$
8. ***for*** $i = 0: M - 1:$
9. ***output*** $\leftarrow Tables[randindex]$
10. $i = i + 1$
11. ***clear*** *randindex*
12. ***End***

V. PERFORMANCE ANALYSIS AND NUMERICAL SIMULATIONS

in section the proposed PHY digital signature scheme is validated. Additionally, the simulation of the proposed PLE is conducted using Python version 3.12, a high-level interpreted programming language known for its extensive libraries that facilitate the simulation and evaluation of such systems. The Python libraries employed in this simulation include **NUMPY, SCIPY, MODULATIONPY, and PYLAB.**

A. Proposed PHY Digital Signature Validation

As demonstrated in Protocol (1), the authentication proposed in this paper is both mutual and symmetric based on digital signature. Consequently, proving the correctness for one party is sufficient. To illustrate, let us consider Bob authenticating Alice. The following steps outline the proof of correctness.

1) *Alice signs* $S_A = Sig_{k_E}(H_B) \xrightarrow{def} hash(H_B, k_E)$

2) *Alice encrypt* $A = E_{k_E}(H_B, S_A) \xrightarrow{def} PLE_{k_E}(H_B, S_A)$

3) *Alice transmits* $x_A = A \rightarrow X_A$

4) *Bob receives* $y_B \leftarrow Y_B = W_{B,r} H_A X_A + N$

5) $y_B = |H_A|^2 X_A + N,\ y_B = \sum_{i=1}^{N} |H_A|^2 X_A + n = \widehat{A}$

6) *Bob decrypts* $(\widehat{H}_B, \widehat{S}_A) = D_{k_E}(\widehat{A}) \xrightarrow{def} PLD_{k_E}(\widehat{A})$

7) *Bob Compute* $S = hash(\widehat{H}_B, k_E)$

Algorithm 2: Constellation Tilting Algorithm

1. **Start**
2. $Input \leftarrow (M, key, status)$

   where $M \equiv$ Number of Constellation Symbols
3. $Bitdepth \leftarrow \log_2(M)$
4. $ref \leftarrow array(Store\ past\ 255\ of\ n)$
5. ***while*** *True*:
6. $n \leftarrow binary2decimal(\textbf{\textit{StreamCipher}}(key, Bitdepth))$
7. ***if*** $n \notin ref$:
8. ***break***
9. $T = Exp(jn\pi/255)$, where $T \equiv$ Tilting Coefficient
10. $ref \leftarrow Circular\_Shift_{left}(ref, 1)$
11. $ref[254] \leftarrow n$
12. ***set*** $j \leftarrow 0$
13. ***for*** $j = 0{:}1{:}M - 1{:}$
14. ***if*** $(status == Encryption)$
15. ***Output*** $\rightarrow (T)$
16. ***else***:
17. ***Output*** $\rightarrow (T^{-1})$
18. ***End***

8) *Bob verfies whether or not*

a) If $(S == S_A)$:

Bob authenicate Alice

b) Else:

Invalild authenication start over

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

B. The Proposed PLE Performance Evaluation

The proposed PLE is simulated based on two widely used modulation schemes: QPSK and 16QAM. The simulation involves a 4x4-OFDM system with a symbol length of 1024 modulated symbols. The channel model used is a Rayleigh fading channel, represented along with complex noise (CN). A 24KB image in JPEG format is used as the data source.

To measure the security strength the symbol error rate (SER) as a function of signal to noise ratio (SNR), along with the correlation coefficient (r) are used. SER is a ratio of the number of symbols received with error to the total number of transmitted symbols as in (7). SER is measured at Bob, Eve and plaintext receiver. The plaintext refers to transmission and reception without encryption. The correlation coefficient calculated between the original signal and decrypted signal at both Bob (intended receiver) and Eve (unintended receiver).

To evaluate the communication reliability peak to signal to noise ratio (PSNR) is measured between the transmitted signal (at Alice) and the received signals at Bob and plaintext receivers, with respect to the SNR. The PSNR is calculated as in (8), [35]. Besides, SER also used to evaluate communication fidelity.

Table (1) and Table (2) represent the evaluation results of the proposed PLE with respect to QPSK, and 16QAM respectively. Besides, Fig.5 and Fig.6 show SER as function of SNR for all receivers. Moreover, Fig.7 and Fig.8 show constellations analysis at tilting coefficient of ($T = 54/255$) with respect to QPSK and 16QAM respectively. Furthermore, Fig.9, and Fig.10 show the received images at Bob and Eve at SNR of 10dB and 20dB with respect to QPSK and 16QAM respectively.

$$SER = \frac{N_e}{N} \quad (7)$$

$$where:$$

$$N_e \equiv Number\ of\ symbols\ received\ with\ error$$

$$N = The\ total\ number\ of\ transmitted\ symbols$$

$$PSNR = 10\log\left(\frac{max(x)^2}{mean\left([x - x']^2\right)}\right) \quad (8)$$

$$where:$$

$$x \equiv original\ signal$$

$$x' \equiv noisy\ signal$$

$$max \equiv maximum\ value$$

$$mean \equiv arithmetic\ mean$$

VI. CONCLUSION

- This work is APLE which utilizes the ECHD to establish the initial phase key. Thus, the session key will be established. Therefore, there is no need to key management and distribution center as other private key schemes need.
- This work provided mutual proven mutual authentication, which is necessary in today's security.
- This work utilizes stream cipher, which is lightweight. Therefore, such schemes will be suitable for applications with power and resources constraints such as WSN.
- For the PLE simulation with respect to QPSK, the results show that the security strength of this scheme is strong. Because, if you look at SER at the Eve receiver is independent of SNR and is about 76% erroneous. Besides, the correlation coefficient between the transmitted signal and received signal at Bob is very close to zero, which gives indication of no correlation. That implies the confusion introduced by the Modulation encryptor and the diffusion introduced by the crypto filters are very strong. Besides, SER and PSNR at the Bob receiver and the plaintext receiver are almost the same. Therefore, the performance of QPSK-PLE is reliable.
- Also, from the PLE simulation with respect to 16QAM, the results show that the security strength of this scheme is very strong. Because, if you look at SER at the Eve receiver is independent of SNR and is about 95% erroneous. Besides, the correlation coefficient between the transmitted signal and received signal at Bob is almost zero, which gives indication of no correlation. That implies the confusion introduced by the Modulation encryptor and the diffusion introduced by the crypto filters are very strong. Although, SER and PSNR at the Bob receiver and the plaintext receiver are slightly different. However, this difference is in an acceptable range (approximately 0.2% for SER).

Algorithm 3: FFT Symbols Pseudo Random Delay/Advance Generator Based on Minimal Correlation.

1. **Start**
2. ***Input*** ← (*N*, *key*)
   where N ≡ OFDM symbol length (FFT block size)
3. *L* ← *decmail2binary*(*N*)
4. *Bitdepth* ← *Length*(*L*)
5. *ref* ← *array*([0:1:*N* − 1])
6. *randomIndex* = *array*[ ]
7. ***Set*** *j* ← 0
8. ***While*** *j* ≤ *N* − 1:
9. *RandBits* = ***StreamCipher***(*key*,*Bitdepth*)
10. *Index* = *binary2decmail*(*RandBits*)
11. ***if*** *index* ≤ *N* − 1:
12. ***elseif*** *Index* ∉ *randomIndex*:
13. *randomIndex*[*j*] = *Index*
14. *j* = *j* + 1
15. ***else***:
16. *j* = *j*
17. ***else***:
18. *j* = *j*
19. ***End elsif***
20. ***End if***
21. ***End while***
22. $r = corrcoef\left(symbol_{OFDM}[ref], symbol_{OFDM}[randomIndex]\right)$
23. where *r* ≡ Correlation Coefficient
24. *set round* ← 0
25. ***while*** *Ture*:
26. ***if*** *r* (*randomIndex*, *ref*) < 0.3:
27. *break*
28. ***else***:
29. *randomIndex* = *shuffle*(*randomIndex*)
30. $symbol_{OFDM}[randomIndex]$
31. *Calculate r as in line 22*
32. *round* = *round* + 1
33. ***End if***
34. ***End while***
35. *Outputs* ← (*Round*,*randomIndex*)
36. ***End***

Fig 6: PLE-QPSK, SER with Respect to SNR at Bob, Eve and No-Encryption Receivers

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to my supervisor Prof. Rashid Saeed and co-supervisor Dr. AEbtihal Haider for their invaluable guidance and support throughout this work. I also extend my appreciation to the school of electronic engineering at Sudan university of science and technology for providing a conducive research environment. Additionally, I am grateful to my friend Mr. Abdullah Khalil, from the EQLEED Group for their insightful discussions and assistance.

REFERENCES

[1]. Al Mtawa, Yaser, et al. "Smart home networks: Security perspective and ml-based ddos detection." 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). IEEE, 2020.
[2]. Li, Wei, et al. "Asymmetric physical layer encryption for wireless communications." IEEE Access 7 (2019): 46959-46967.
[3]. Stallings, William. Network security essentials: applications and standards. Pearson, 2016.
[4]. Pecorella, Tommaso, Luca Brilli, and Lorenzo Mucchi. "The role of physical layer security in IoT: A novel perspective." Information 7.3 (2016): 49.
[5]. Shannon, Claude E. "Communication theory of secrecy systems." The Bell system technical journal 28.4 (1949): 656-715.
[6]. Zhou, Xiangyun, Lingyang Song, and Yan Zhang, eds. Physical layer security in wireless communications. Crc Press, 2013.
[7]. Mucchi, Lorenzo, et al. "Physical-layer security in 6G networks." IEEE Open Journal of the Communications Society 2 (2021): 1901-1914.
[8]. Li, Wei, et al. "Mathematical model and framework of physical layer encryption for wireless communications." 2018 IEEE Globecom Workshops (GC Wkshps). IEEE, 2018.
[9]. Huo, Fei, and Guang Gong. "XOR encryption versus phase encryption, an in-depth analysis." IEEE Transactions on Electromagnetic Compatibility 57.4 (2015): 903-911.
[10]. J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an ofdm physical layer encryption scheme," IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2114–2127, 2017.
[11]. J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an ofdm physical layer encryption scheme," IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2114–2127, 2017.
[12]. M. Sakai, H. Lin, and K. Yamashita, "Intrinsic interference based physical layer encryption for ofdm/oqam," IEEE Communications Letters, vol. 21, no. 5, pp. 1059–1062, 2017.
[13]. T. R. Dean and A. J. Goldsmith, "Physical-layer cryptography through massive mimo," IEEE Transactions on Information Theory, vol. 63, no. 8, pp. 5419–5436, 2017.
[14]. B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive mimo eavesdropper," IEEE Access, vol. 4, pp.3016–3025, 2016.
[15]. K. Nain, J. Bandaru, M. A. Zubair, and R. Pachamuthu, "A secure phase-encrypted ieee 802.15.4 transceiver design," IEEE Transactions on Computers, vol. 66, no. 8, pp. 1421–1427, 2017.
[16]. K. Lai, J. Lei, L. Wen, G. Chen, W. Li, and P. Xiao, ``Secure transmission with randomized constellation rotation for downlink sparse code multiple access system," IEEE Access, vol. 6, pp. 5049_5063, 2018.
[17]. Melki, Reem, et al. "An efficient OFDM-based encryption scheme using a dynamic key approach." IEEE Internet of Things Journal 6.1 (2018): 361-378.
[18]. Sahin, B. Katz, and K. Dandekar, "Secure and robust symmetric key generation using physical layer techniques under various wireless environments," in Proc. IEEE Radio and Wireless Sympos. (RWS). Austin, TX, USA: IEEE, Jan. 2016, pp. 211–214.
[19]. H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in Proc. IEEE Int. Conf. Computer Commun. (INFOCOM), Turin, Italy, Apr. 2013, pp. 3048–3056.
[20]. Y. Al-Moliki, M. Alresheedi, and Y. Al-Harthi, "Robust key generation from optical OFDM signal in indoor VLC networks," IEEE Photon. Technol. Lett., vol. 28, no. 22, pp. 2629–2632, Nov. 2016.
[21]. R. Horstmeyer, B. Judkewitz, I. Vellekoop, S. Assawaworrarit, and C. Yang, "Physical key-protected one time pad," Jun. 2015, US Patent 9,054,871.
[22]. S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in Proc. IEEE Int. Conf. Computer Commun. (INFOCOM), Shanghai, China, Apr. 2011, pp. 1125–1133.
[23]. Mazin, K. Davaslioglu, and R. Gitlin, "Secure key management for 5G physical layer security," in Proc. IEEE Wireless and Microw. Technol.
[24]. Yu, Daizhong, et al. "Physical Layer Security in Spherical-Wave Channel Using Massive MIMO." 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). IEEE, 2022.
[25]. Zhao, Hong, et al. "A physical-layer key generation approach based on received signal strength in smart homes." IEEE Internet of Things Journal 9.7 (2021): 4917-4927.
[26]. Melki, Reem, Hassan N. Noura, and Ali Chehab. "Lightweight and secure D2D authentication & key management based on PLS." 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall). IEEE, 2019.
[27]. Pirayesh, Jamshid, et al. "A PLS-HECC-based device authentication and key agreement scheme for smart home networks." Computer Networks 216 (2022): 109077.

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

[28]. Ngo, Hoang Anh, and Lajos Hanzo. "Hybrid automatic-repeat-request systems for cooperative wireless communications." IEEE Communications Surveys & Tutorials 16.1 (2013): 25-45.
[29]. Paar, Christof, and Jan Pelzl. Understanding cryptography. Vol. 1. Springer-Verlag Berlin Heidelberg, 2010.
[30]. Fips Pub 186-4 Federal Information Processing Standards Publication Digital Signature Standard (DSS), Standard FIPS PUB 186-4, National Institute of Standards and Technology Standard, Jul. 2013. [Online]. Available:https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.
[31]. Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 2018.
[32]. Pearson, Karl. "VII. Mathematical contributions to the theory of evolution. —III. Regression, heredity, and panmixia." Philosophical Transactions of the Royal Society of London. Series A, containing papers of a mathematical or physical character 187 (1896): 253-318.
[33]. Ludeman, Lonnie C. Random processes: filtering, estimation, and detection. John Wiley & Sons, Inc., 2003.
[34]. Cohen, Jacob. Statistical power analysis for the behavioral sciences. routledge, 2013.
[35]. Bovik, Alan C. Handbook of image and video processing. Academic press, 2010.

Table 1: PLE-QPSK Simulation Results

SNR (dB)	Bob			Eve		plaintext	
	PSNR (dB)	BER	r	BER	r	BER	PSNR
0	14.34	0.459	0.521	0.755	0.002	0.460	14.34
2	15.59	0.300	0.734	0.740	0.0002	0.299	15.62
4	19.72	0.109	0.923	0.758	0.009	0.117	19.75
6	31.25	0.0145	0.995	0.764	0.007	0.0137	31.4
8	∞	0	1	0.768	0.003	0	∞
10	∞	0	1	0.769	0.026	0	∞

Table 2: PLE-16QAM Simulation Results

SNR (dB)	Bob			Eve		plaintext	
	PSNR (dB)	BER	r	BER	r	BER	PSNR (dB)
8	14.41	0.648	0.176	0.931	0.0024	0.670	14.62
10	15.25	0.432	0.304	0.9423	0.0053	0.427	15.86
12	17.05	0.239	0.530	0.940	0.0001	0.143	19.48
14	20.33	0.096	0.774	0.944	0.0009	0.022	28.66
16	26.72	0.028	0.946	0.945	0.0030	0	∞
18	40.94	0.002	0.998	0.940	0.0087	0	∞
20	∞	0	1	0.940	0.0007	0	∞

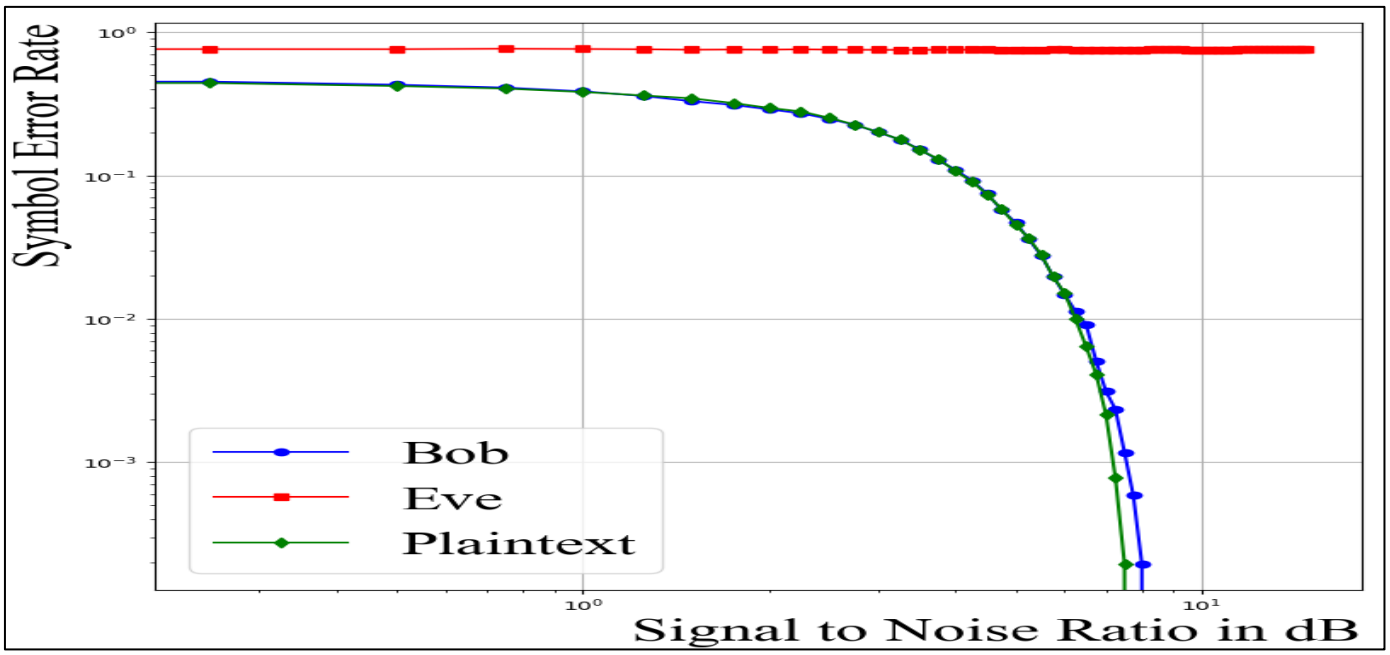


Fig 7: PLE-QPSK, SER with Respect to all Receivers

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

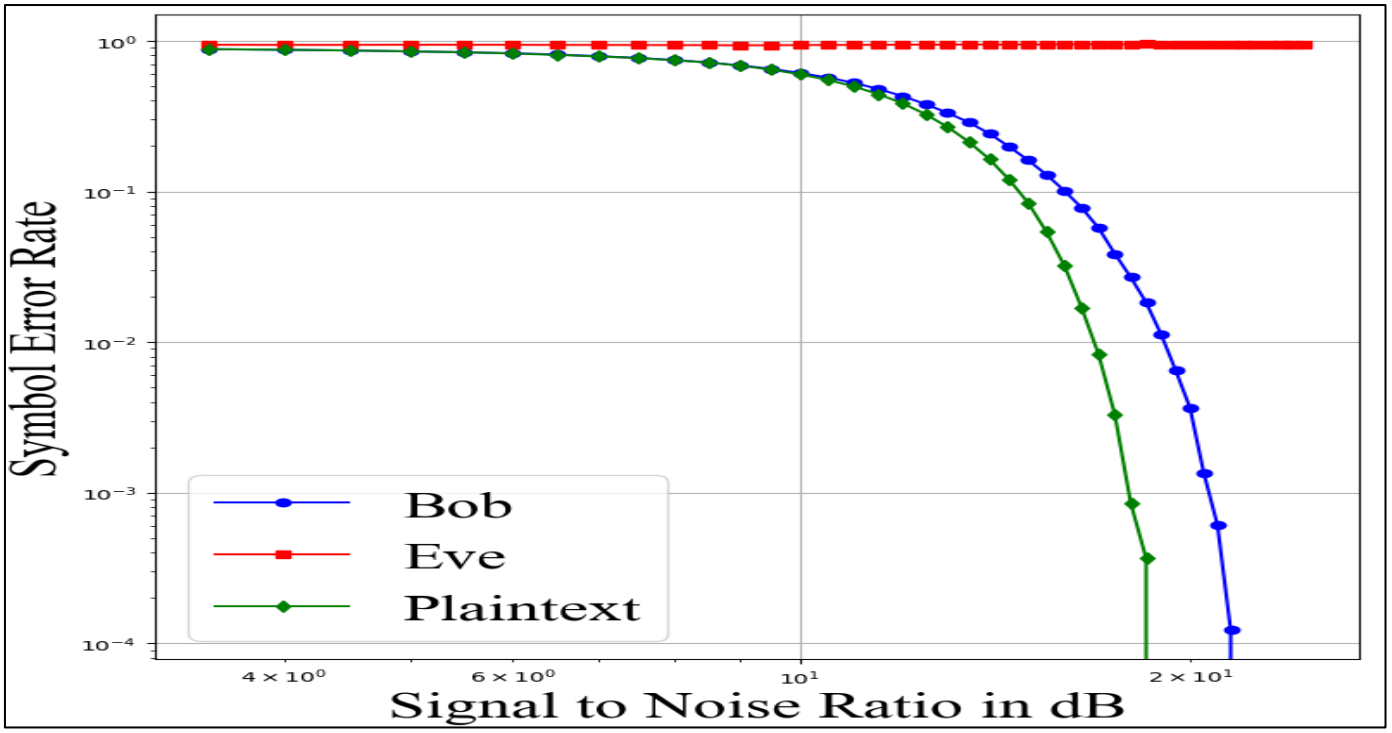


Fig 8: PLE-16QAM SER as Function of SNR at all Receivers

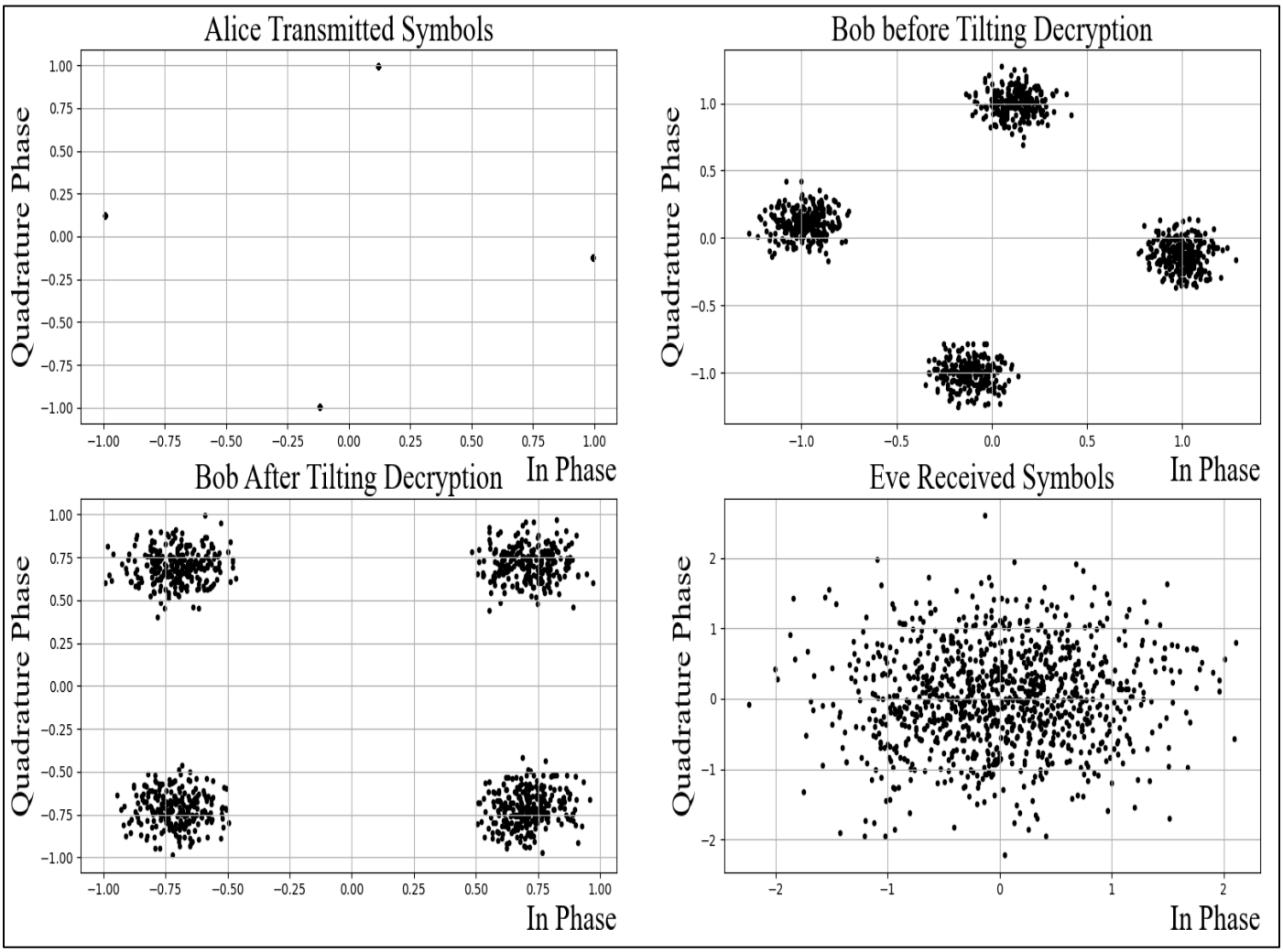


Fig 9: PLE-QPSK Constellation at Alice, Bob and Eve

ISSN No:-2456-2165 https://doi.org/10.5281/zenodo.14769336.

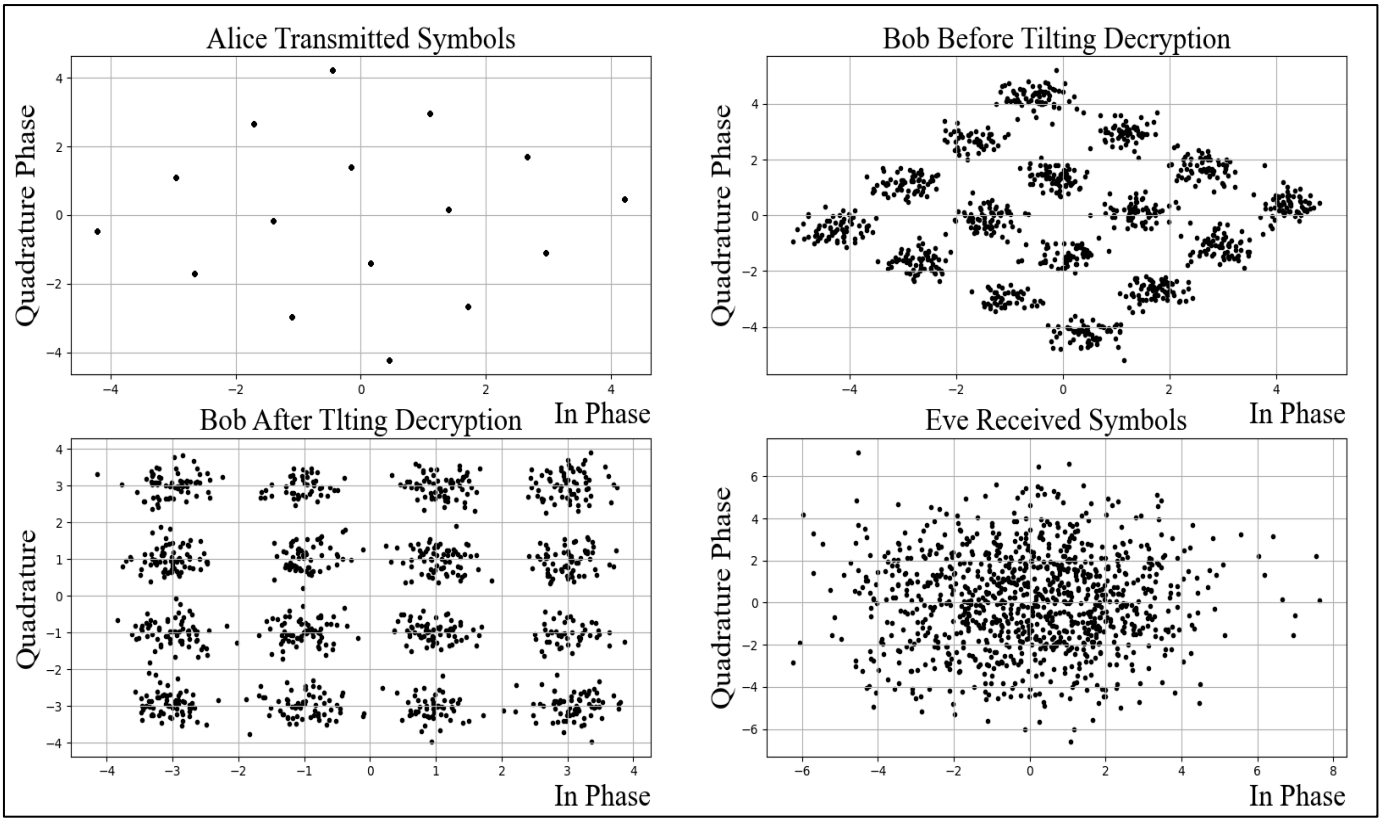


Fig 10: PLE-16QAM Constellation at Alice, Bob and Eve

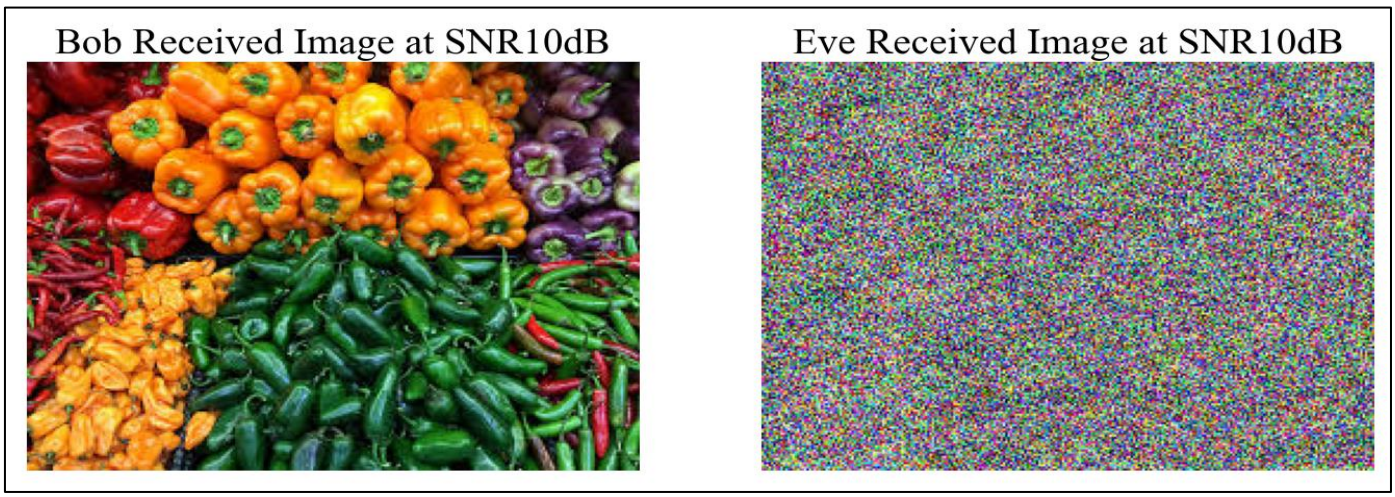


Fig 11: PLE-QPSK Received Images

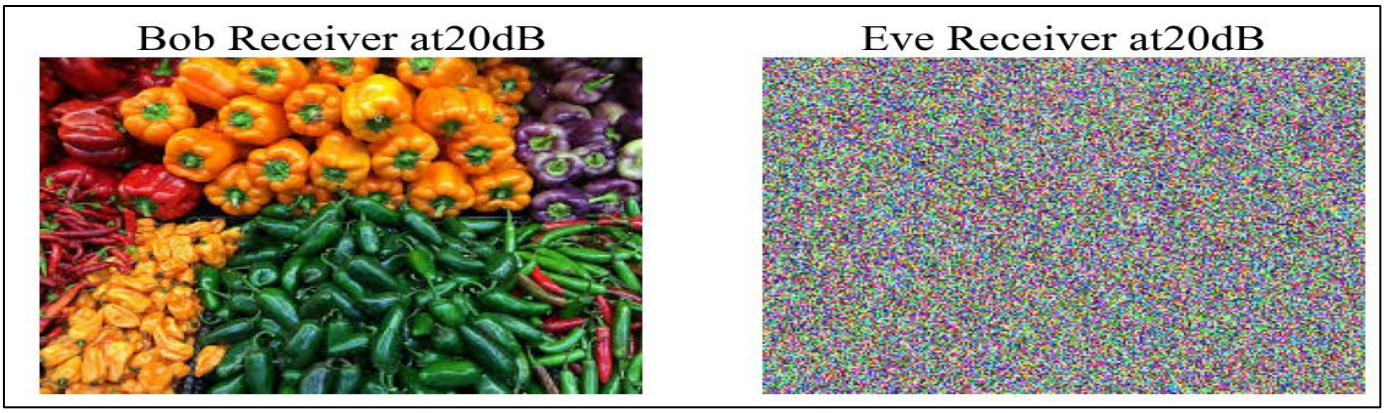


Fig 12: PLE-16QAM Received Images