electronics

MDPI

Article

Derogation of Physical Layer Security Breaches in Maturing Heterogeneous Optical Networks

Ammar Armghan

Department of Electrical Engineering, College of Engineering, Jouf University, Sakaka 72388, Saudi Arabia; aarmghan@ju.edu.sa

Abstract: The evolution journey of optical network (ON) towards heterogeneous and flexible frameworks with high order of applications is continued from the last decade. Furthermore, the prominence of optical security, amount of transmitted data, bandwidth, and dependable presentation are heightened. The performance of ON is degraded in view of various natures of attacks at the physical layer, such as service disrupting and access to carrier data. In order to deal with such security breaches, new and efficient ON must be identified. So, this paper elaborates a detailed structure on physical layer security for heterogeneous ON. Possible mechanisms, such as Elliptic-curve Diffie–Hellman (ECDH), are used to treat a physical layer attack, and an efficient framework is proposed in this paper for 64 quadrature amplitude modulation-based orthogonal frequency division multiplex (64QAM-OFDM) ONs. Finally, theoretical and simulation validations are presented, and the effective results of the proposed method and viewpoint are concluded.

Keywords: physical layer security breaches; heterogeneous optical networks; optical signal processing

Citation: Armghan, A. Derogation of Physical Layer Security Breaches in Maturing Heterogeneous Optical Networks. *Electronics* **2021**, *10*, 2021. https://doi.org/10.3390/electronics10162021

Academic Editors: Ivan Cvitić, Dragan Peraković, Anca Delia Jurcut and Goran Marković

Received: 22 June 2021
Accepted: 18 August 2021
Published: 21 August 2021

1. Introduction

The expanding request of client work for bigger transfer speed has introduced the development of heterogeneous optical networks (ONs) [1]. Such a framework adjusts to broaden high throughput, portability, and future information interconnects. To deliver such high limit connects to a client on move should require heterogeneous ONs. To satisfy the requests of group of future heterogeneous ON, different multiple access user technologies have been recommended [2]. This is comprised of wavelength division multiplex (WDM) [3] dependent ONs, code division various access (CDMA) [1] in light of ONs, and time division numerous entrance (TDMA) [3] in view of ONs. The essential element of using WDM licenses an enormous expansion in limit and segregation colligated with explicit wavelength to every customer. A solitary wavelength pair can be designated to each ON-unit (ONU) [4] for communicating with optical line terminals (OLT) [5]. However, the payoffs of ONs is degraded in view of various physical layer security breaches, such as service disrupting and access to carrier data. Seeing that presently data stream of the ONs surpass 100 Gbps, continuous executing, low-latency signal handling for data security has been progressively tested [6]. To treat such challenges, the parallelism and better speed of optical signal processing is considered a good option for continuously handling such signals in real time and the physical layer of the ONs. Adding to the previous discussion, the security of the encryption previously gave in the higher layer of protocol stack is enhanced in the optical layer [7]. In contrast to their digital parameters, the electromagnetic waves are not induced in optical domains; in results, less external interactions happen to the ONs.

1.1. Related Work

To minimize the impact of security breaches and increase the performance of heterogeneous ONs, many research studies have presented their models. The authors address a physical attack of ONs in Reference [8]. The technique including synchronized true

random sequences, and the photonic physical uncountable, is implemented in terms of one time paid and cryptographic key generated, respectively. In Reference [9], the authors propose optical-CDMA mechanism for improving physical layer security in ONs. The physical layer security is investigated for multimode ONs by authors in Reference [10]. Ref. [11] suggests physical layer security for WDM-based ONs using orthogonal frequency division multiplexer (OFDM) signals. Data encryption standard (DES) techniques are used in Reference [12] for enhancing the security in heterogeneous ONs. In Reference [13], the authors focus on optimal scheduling (OS) and cumulative distributive (CD) algorithms, overcoming security breaches in ONs. Physical layer security for mixed fading channels is determined in Reference [14]. The discussed state-of-the-art work concludes that encryption standards are not discussed for ONs including OLT at the end users. In this paper, the physical layer security is analyzed for 64 quadrature amplitude modulation-OFDM (64QAM-OFDM) utilizing the Elliptic-curve Diffie–Hellman (ECDH) algorithm.

1.2. Organization and Notation of Paper

The remaining sections of this paper are organized as follows. Section 2 explains the proposed layout, analytical modeling for secure communication is discussed in Section 3, Section 4 presents the results and discussion of the presented work, and the conclusion of the work is depicted in Section 5.

2. Proposed Layout

The essential objective of this research model is to design an ON, having ability to overcome security breaches with increased flexibility. For this purpose, the suggested model is presented in Figure 1. The transmitter, 'Tx', end includes secured 64QAM-OFDM-based modulation schemes, which double the system capacity. The encrypted OFDM symbols are induced by continuous wave (CW) laser source. The Lorentzian type of a CW laser is installed, aiming to generate efficient spectrum light rays. The OFDM encrypted waves are used for downstream transmission. Furthermore, the inter carrier interference (ICI) [15] and cross talk are ignored, for the purpose of maintaining the orthogonality of the signal. Total 64 subcarrier are used for transmission over WDM-based ON, and, as a result, the bandwidth spectrum is decreased. In order to upconvert baseband encrypted OFDM signals, the electrical amplifier with radio frequency (RF) is applied. As in the OFDM, encrypted symbols of 32QAM with 20 Gbps speed are produced easily from RF signals with 20 GHz frequency range. The OFDM-encrypted data are achieved by support of offline digital signal processing (DSP), which is performed by an ES-based public key cryptography algorithm, 16 to 32 bytes in size. For the computational complexity, the 64 QAM-OFDM partial information is taken for encryption, applying discrete cosine transform (DCT) compression method. The encrypted signals are then passed over a single model fiber (SMF) with the help of a WDM multiplexer. Keeping the signal amplification till 3 dBm range, the erbium-doped fiber amplifier (EDFA) is used beyond SMF. At the receiver, 'Rx' side, all received channels are divided for every ONU, where the signals are proceed over optical filter. After optical to electrical conversion using a photo-detector (PD), electrical amplification is applied on waves to suppress the amplified spontaneous emission (ASE) impairments. To avoid the use of private key for ES, ECDH algorithm is installed for maintained authentic transmission among channels.

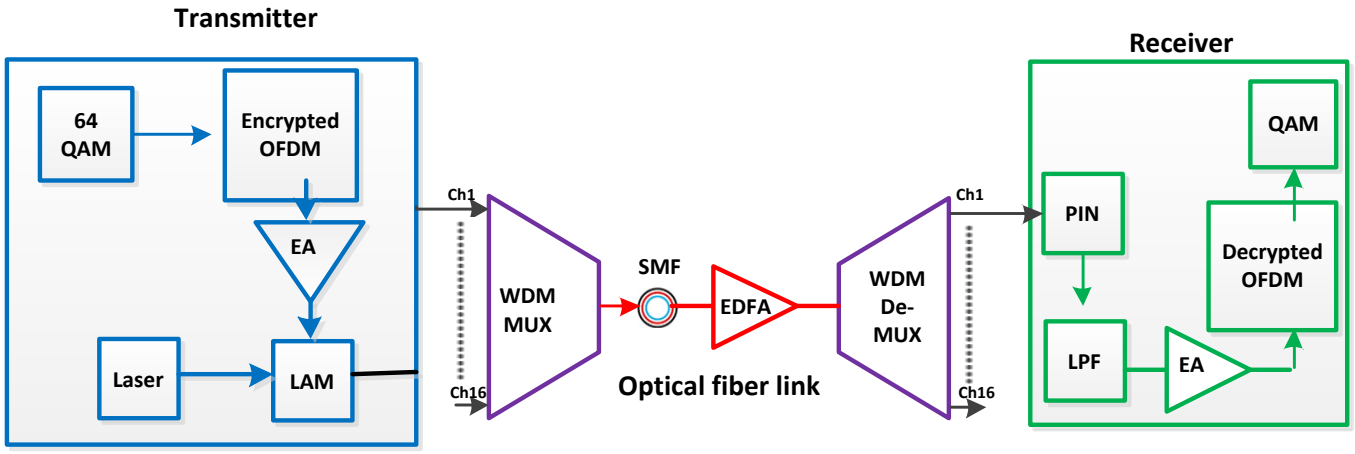


Figure 1. Enhanced physical layer security proposed ON against security breaches.

3. Analytical Modeling for Secure Communication

As discussed above, that physical layer security of flexible ONs can be enhanced utilizing an ES-based ECDH algorithm with decreased computational complexity. The architecture of ECDH-ES is depicted in Figure 2. The dogma of cryptography and interpretation are described by ECDH-ES algorithm for N numbers of channels in OLT, where the input in OLT is supported by cryptography, while decryption is applied at ONU of ON. The bit sequences are created by a pseudorandom bit sequence (PRBS) generator, which is formulated [16–18] as

$$B = W_T R_B, \tag{1}$$

$$B_G = B - L_z - L_t, \tag{2}$$

where B denotes number of bit sequence, W_T is time windows parameter bit rate is described by R_B, B_G is the number of generated bits, and the number of leading and trailing zeros are represented by L_z and L_t, respectively. Quadrature phase carrier and inphase quad bits are modulated to generate 64 QAM. The ES block is used to encrypt the real (I) and imaginary (Q) with key sequences [19]. After encryption of I and Q data, the DCT is applied in order to reduce the size of encrypted data. The time, energy, and computational complexity are rescued by encrypting only the important data of 64 QAM, instead of whole data. As a result, the main information is concealed. Moreover, the cryptography procedure of ES is symmetric; so, the ECDH is applied for inducing the session key. The parameter inside ES for 2^8 elements is calculated [20–22] as

$$E(A)c_7A^7 + \ldots + c_1A + c_0, c_k \in GF, \tag{3}$$

where GF is Galois field, and the ES module reduction is performed by irreducible polynomial and is estimated [23,24] as

$$E_p = E^8 + E^4 + E^3 + E + 1. \tag{4}$$

The EC group parameter over field Z_e should satisfy the all pair conditions $(a, b) \in Z_e$, which is written [24–27] as

$$b^2 = a^3 + x + a + y. \tag{5}$$

As for ECDH elements, the parameters of Equation (5) must be fulfilled. The power is measured as

$$P = (a_p, b_p), \tag{6}$$

and private and public keys are designed after establishing the OLT and ONU parameters, which include large integers and points on the curve. Owing to associative property, the OLT and ONU estimate the same outcomes, called joint secret key. Additionally, the joint

secret key works as a session key for encrypting and decrypting ES. The I and Q signals induce the encrypted data $N_E(k)$, defined as

$$N_E(k) = R(Q_E(k)) * C_E(k) + JI_k(Q_E) * d_E(k). \quad (7)$$

Here, $Q_E(k)$ is used for QAM output, and ES keys are denoted by $c_E(k)$ and $d_E(k)$. In the coming process, FFT is applied on $N_E(k)$ waves, aiming to attain frequency domain from time domain. The cryptography signal of OFDM is evaluated as

$$N_R(T) = \Sigma_{k=1}^{K-1} N_E(k) * exp(Js\pi(a(k) - 1)(T - 1)/K), \quad (8)$$

where $a(k)$ defines subcarrier index, time index is explained by T, and $N_R(T)$ is the encrypted OFDM signal. Last, the $N_R(T)$ waves are converted into RF waves; thus, the same procedure is continued for other channels. The outcomes of simulation model is evaluated using Equation (9), which is given as

$$Y_e = \Sigma_{\xi=1}^{\chi} Y_k[\chi] \left[\Sigma_{i=1, i\neq k}^{\chi} \frac{1}{2} erf(Q_{x1}/\sqrt{2}) \right], \quad (9)$$

where χ shows attained symbols, $Y_k[\chi]$ mentions the probability of occurrence of χ, and Q_{x1} is defined as

$$Q_{x1} = \frac{z_{x1}}{\delta_{xi} + \delta_{ix}}. \quad (10)$$

Here, z_{x1} is distance among regions x and i, and standard deviation is explained by $\delta_{xi} + \delta_{ix}$.

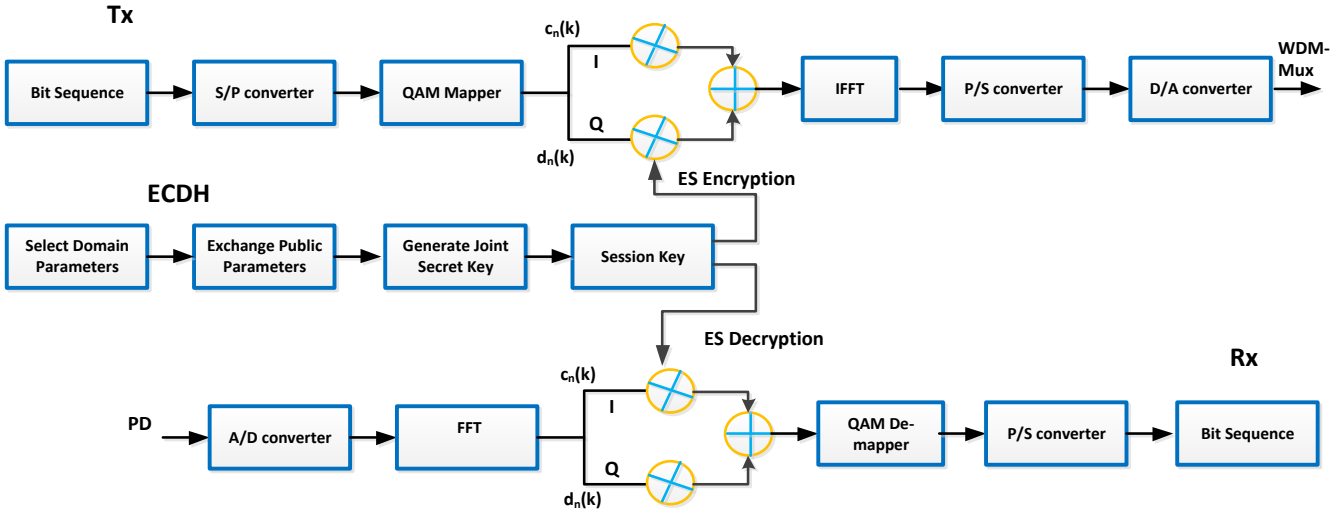


Figure 2. Architecture of ECDH-based ES algorithm used for proposed model.

4. Results and Discussion

To validate the proposed analytical and architecture models, the simulation analysis is performed in this section. The explanation of exercised elements is depicted in Table 1 for computing the efficiency of the proposed model in terms of security breaches in ONs. Table 1 explains that some parameters are kept constant for evaluating the system outcomes, such as line width, gain, symbol rate, and noise figure.

Table 1. Description of parameters utilized for evaluating proposed system performance.

Name	Description
Lorentzian laser	1540.4 nm, 256 samples
Subcarrier	1200
Length	200 km
Launch power	−10 to 4 dBm
Data rate	100 Gbps
No FFT point	1200
Line width	0.15 MHz
Symbol rate	2.5×10^9
Noise figure	4 dB
Gain	30 dB

The elements, such as length, input power, laser wavelength, and data rate, are varied to analyze the impact of security breaches. WDM-based ON is designed in this work, employing encrypted 64QAM-OFDM modulation scheme. The light source is provided by Lorentzian CW laser with 1540.40 nm wavelength and 256 samples per bit. Each OFDM needs 12 symbols for cycle prefix, where, then, ES-based ECDH algorithm is applied to secure the OFDM transmitted waves, for which the procedure is declared in Algorithm 1. Figure 3 shows the link among analytical model and simulation model. The data flow is generated using Equations (1) and (2), and then ECDH technique is applied over each channel for starting the encryption the I and Q data. The data is transmitted after fulfilling all the encrypted conditions using Equations (5)–(10) to increase physical layer security against security breaches. The relation among encrypted ON and unencrypted ON is provided in Figure 4. The results are measured for 50 and 100 km transmission ranges, using input power as a function of bit error rate (BER). The input power is employed with magnitude −10 to 4 dBm over 50 and 100 km fiber length ONs. Figure 4 depicts a clear variance within encrypted and unencrypted setups of ONs. It shows that, with increase length of fiber, BER decreases from 10^{-7} to 10^{-5}. For the same range of fiber length, Figure 4 declares that, in view of unencrypted model, unwanted waves are added with real transmitted signals. As a result, the signal quality is degraded. So, it is recorded that, at −2 dBm, input power and 50 km transmitted encrypted ONs give 10^{-7} BER, while, when using even ONs with the unencrypted model, the BER is degraded to 10^{-6}. With improving the input power, the BER decreases for both encrypted and unencrypted signals. The reduction in BER is fast among −10 to −5 dBm; on the other side, after −5 dBm, minimum changes are shown to have occurred in BER, in view of increase in impairments, as it can be seen from the curve portion in Figure 4. The result analysis for fiber length against BER is expressed in Figure 5, where the comparison among several mechanisms is explored, such as Ronald Shamir Adleman (RSA), elliptic curve cryptography (ECC), and ECDH-based ES. It can be seen from Figure 5 that the unencrypted model presents a worse response because of the addition of undesired signals in the system. Secondly, Figure 5 explains that the performance of ECDH-ES against security breaches is more efficient than the ECC and RSA algorithm. In other words, the computational complexity of RSA and ECC are more than the ECDH-ES algorithm. Investigating the consequences of the proposed ONs at 100 km, 10^{-8} achieves for installing ECDH-ES. On the other side, RSA and ECC-based ON give 10^{-7} and 10^{-6} BER, respectively. Thus, the physical layer security of ONs enhances, using ECDH-based ES methodology.

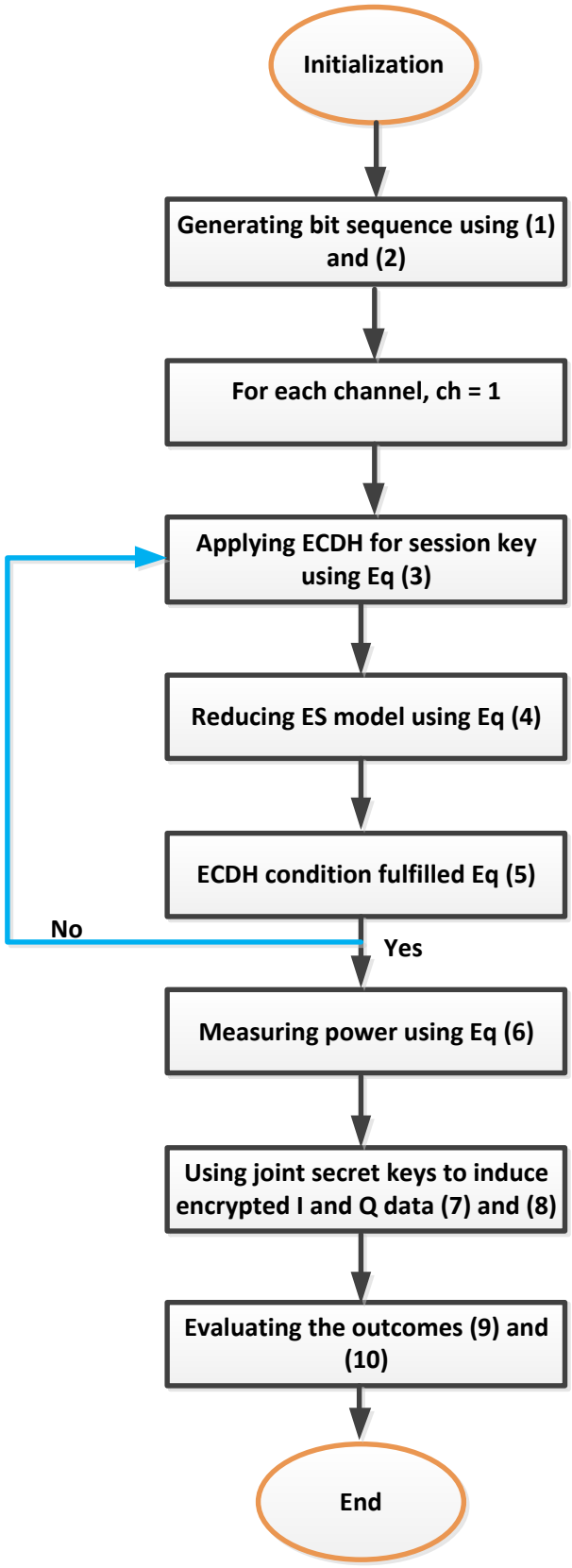


Figure 3. The description of flowchart for evaluating the physics behind the mathematical model and simulation model.

Algorithm 1: Proposed ES-based ECDH algorithm for enhancing physical layer security in ONs

ine x and y private keys are selected, including primitive parameters using Equations (5) and (6):
$M_{XY} = (a_{XY}, b_{XY})$, ECDH session key is computed for OLT, and ONU in ON.
: **For** key extension
: H = $[H_0, H_1 \ldots H_n]$, where $H \in N_{xy}$
: Initialize b_r
for k = n + 1 to 59.
temp = nbox($H_t - 1$)
v = temp$\oplus$ recon(b_r + 1)
$H_k = H_{k-n-1} \oplus$v
$H_{k+1} = H_{k-n} \oplus H_k$
$H_{k+2} = H_{k-n+1} \oplus H_{k+1}$
if key size = 256 bits
H_{k+n} = nbox(H_{k+3})
For 128, 192, and 256 bit key, estimate 3,5 and 7 sub-keys
k = k + n + 1
b_r is incremented
Modify H and go to (initialize b_r)
While encryption
generate I and Q data in 128, 192, and 256 blocks
initial phase = block(1 − input) $\oplus$ block(first − sub-key)
for round 9, 11, and 13 down to 1
bytesubs = nbox (first phase)
for shift row
circular shift row 1, 2, 3, and 4 left
for each row and column, mcol = constant $\times$ shift row, addrv = mcol $\oplus$ block(round-subkey)
for final step, out = repeat (bytesub to circular shift)
ciphertext = out
go to (generated I and Q step)

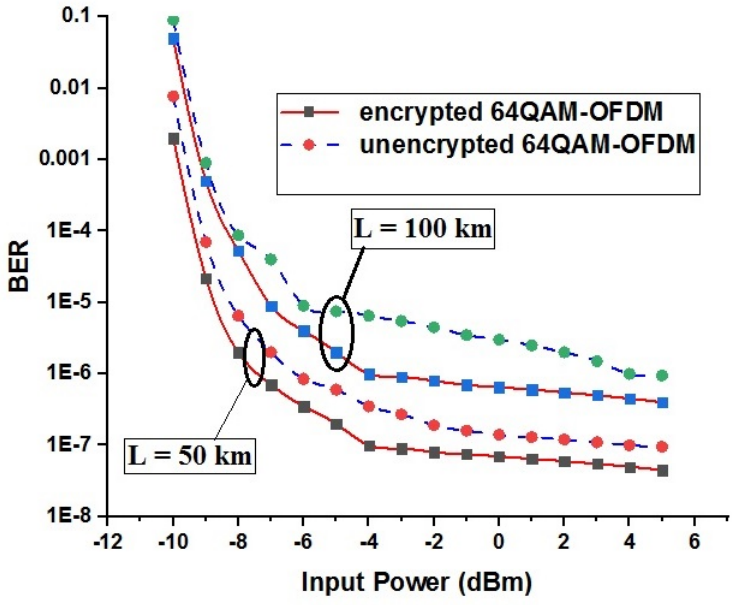


Figure 4. Encrypted 64QAM-OFDM and unencrypted 64QAM-OFDM model comparison in terms of input power and BER at 50 and 100 km distance.

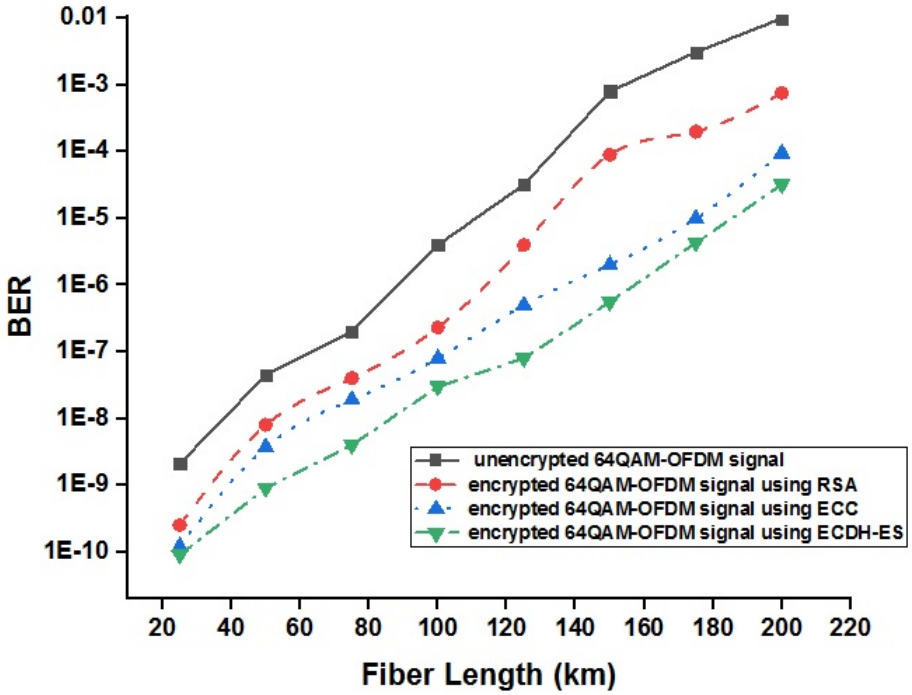


Figure 5. Comparison of ECC, RSA, and ECDH-ES algorithms used for enlarging quality of physical layer security of matured ON.

Similarly, the payoff of mature ONs is investigated in terms of peak to average power (PAPR) and complementary cumulative distributed function (CCDF), as assessed in Figure 6, which elaborates the outcomes of encrypted 64QAM-OFDM and unencrypted 64QAM-OFDM flexible ON, employing ECDH-ES, RSA, and ECC techniques. Figure 6 shows that fruitful PAPR is recorded for ECDH-ES-based secured 64QAM-OFDM signal as compared to RSA and ECC algorithm. It is also depicted in Figure 6 that physical layer security is improved in the proposed ON; hence, secure communication can be possible up to long range with huge capacity. Figure 7 compares the secured transmitted OFDM signals and unsecured transmitted signals of ON at 100 Gbps data rate speed and 200 length of fiber. That clarifies that the data is disrupted badly using unencrypted ON. The frequency domain of the OFDM signal in ONs is measured, implementing optical spectrum analyzer, which is assessed in Figure 8. The spectrum of unencrypted transmitted signal diverges and generates noisy waves, as presented in Figure 8. As for the eye diagram presentation of the proposed secured structure, Figure 9 describes the eye diagrams of noisy signals attacked ON and the encrypted model. The framework of this proposed model is compared with current existence models, as mentioned in Table 2, which explains the efficient performance of the proposed work as compared to currently presented models. The comparison of the proposed model in terms of security is illustrated in Table 3, which includes the authenticated-ECDH (A-ECDH) and Biswas security set up. Table 3 also shows that the Biswas scheme and proposed model have similar security features. Moreover, the proposed authentication scheme has better performance than the Biswas scheme. Consequently, the proposed scheme provides all the features of security by offering better performance than the other two schemes.

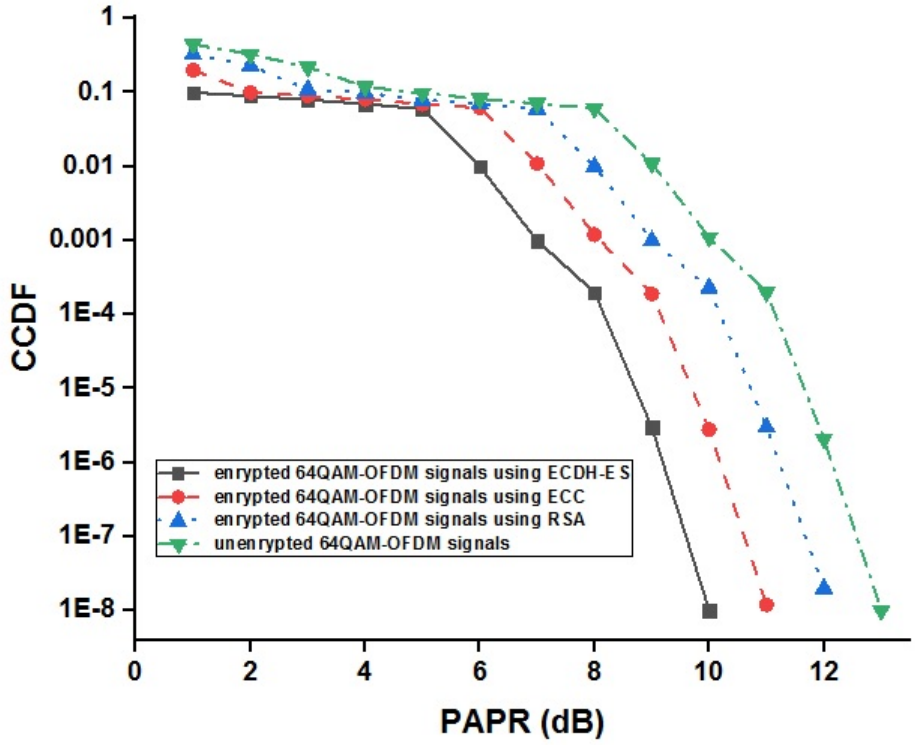


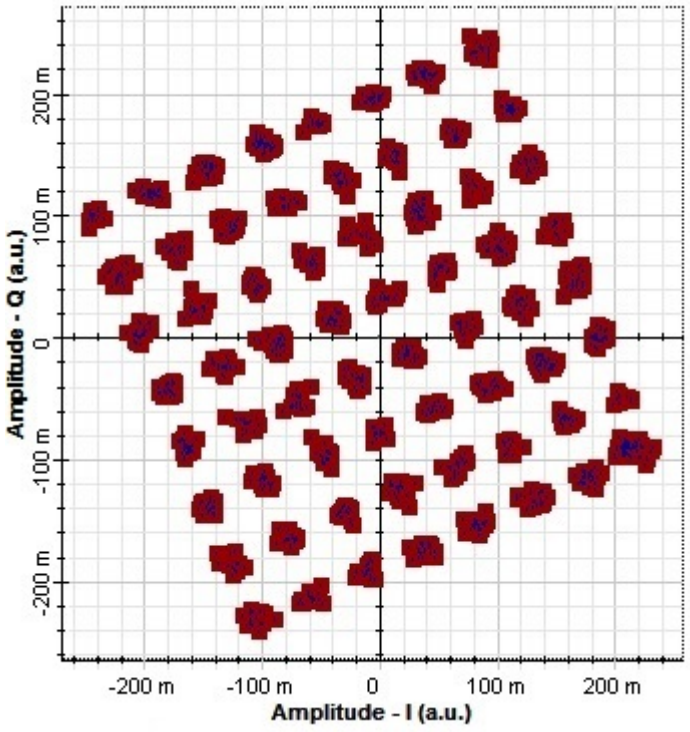
Figure 6. Investing PAPR as a function of CCDF for different RSA, ECC, and ECDH-ES algorithms.

Table 2. Comparison of the proposed model with existing approaches.

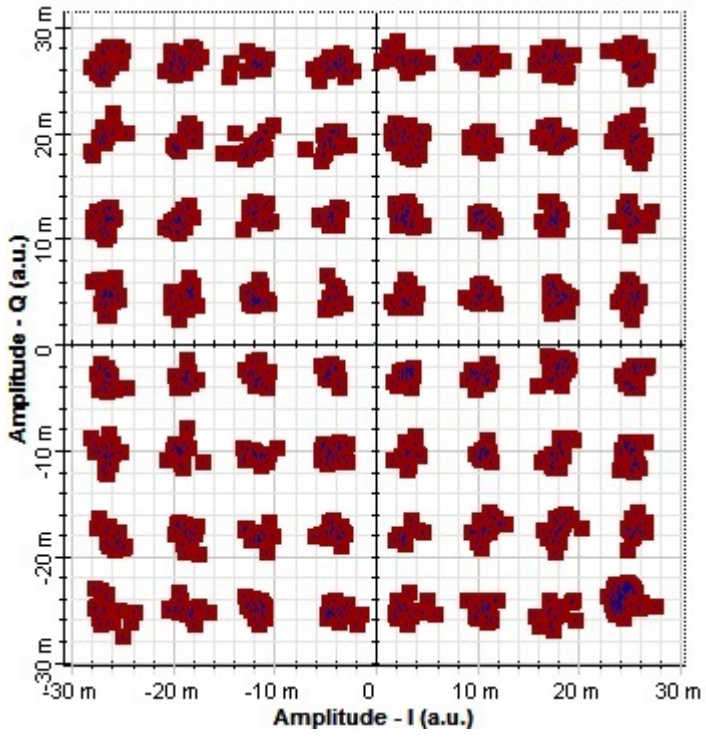
Used Methodology	[28]	[29]	Presented Model
Modulation Format	16QAM-OFDM	16QAM-OFDM	64QAM-OFDM
Encryption Technique	3- level chaotic encryption	Quantum Key Distribution (QKD)	ECDH-ES
Data Rate	10 Gbps	40 Gbps	100 Gbps
Sumbol Rate	10^5	10^7	2.5×10^9
Fiber length	20 km	100 km	200 km

Table 3. Comparison of the proposed model with existing approaches in terms of security.

Parameter	ECDH [30]	Biswas approach [31]	Presented ECDH-ES
Session Key	-	yes	yes
Mutual Encryption	Exist	Exist	Exist
Joint Secret Key	-	-	yes
Impersonation security breach	Not Secure	Not Secure	Secure
No of I and Q Generated Blocks	128	128	128, 192, and 256

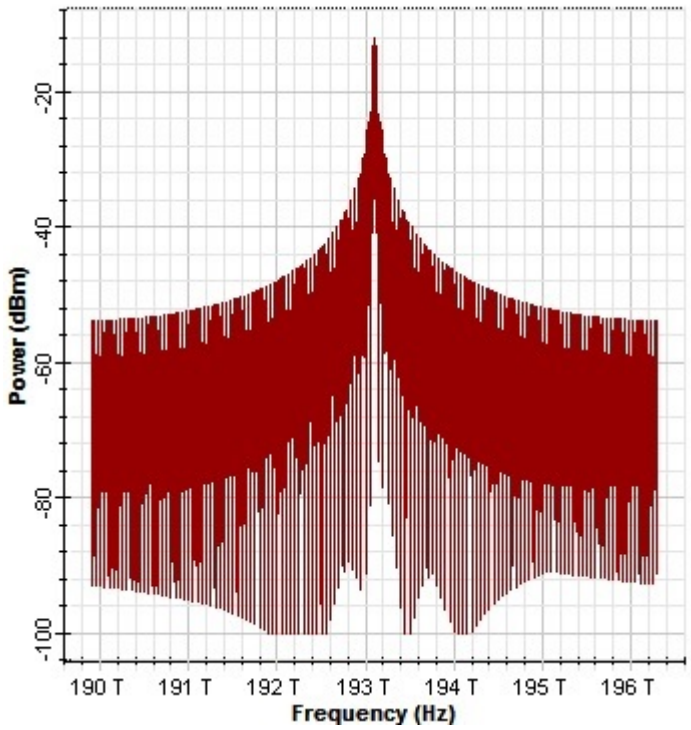


(**a**)

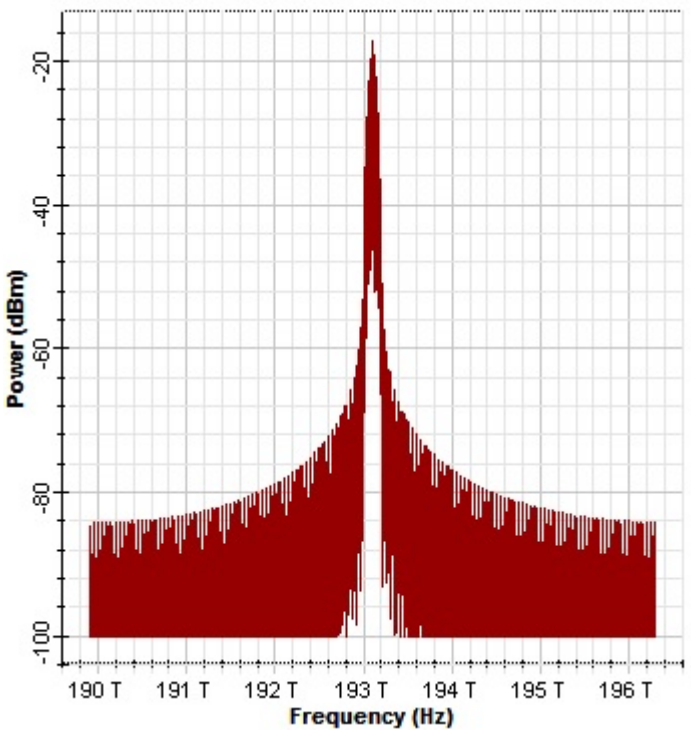


(**b**)

Figure 7. (**a**) Distort constellation analyzer diagram of unencrypted ON. (**b**) Constellation diagram of protected model.

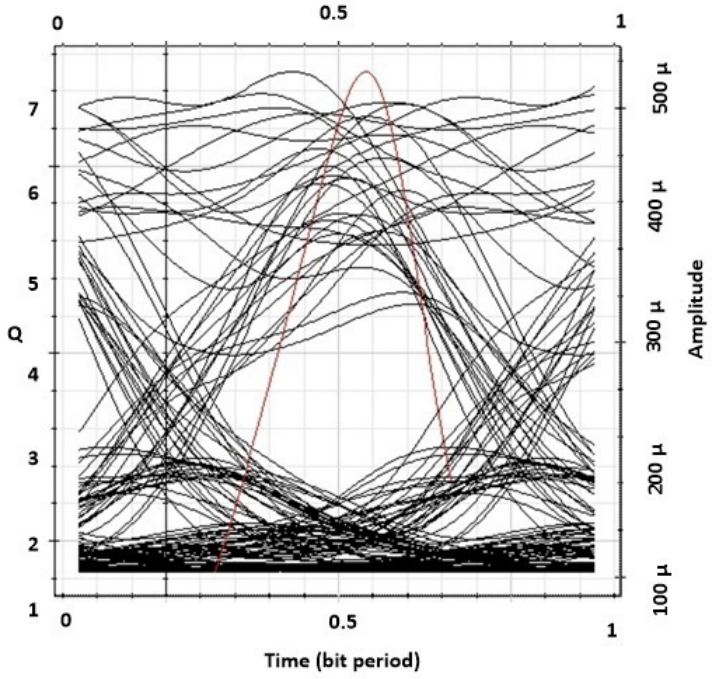


(**a**)

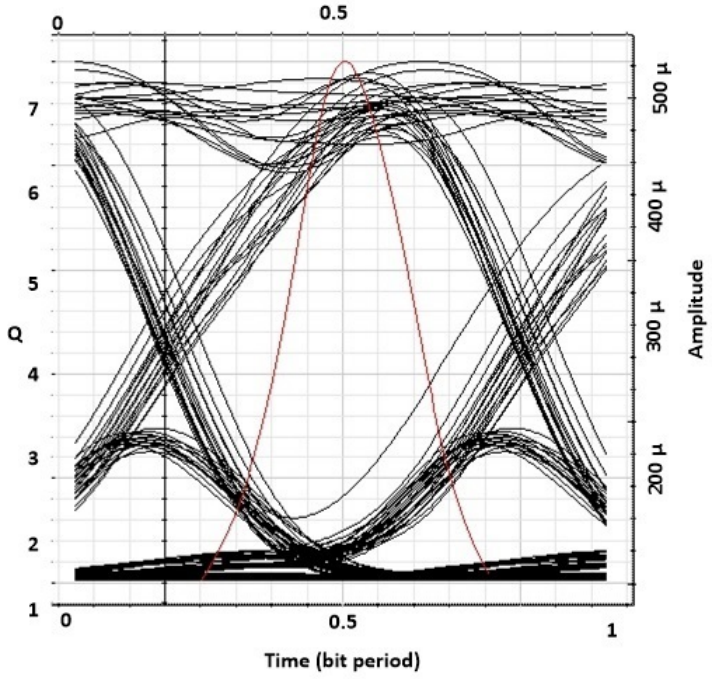


(**b**)

Figure 8. (**a**) Optical spectrum analyzer diagram for interrupted signals due to addition of unwanted data. (**b**) Secured optical spectrum analyzer diagram.



(**a**)



(**b**)

Figure 9. (**a**) Worse representation of eye diagram due to unsecure model. (**b**) Eye diagram of encrypted proposed model.

5. Conclusions

Secure and long range consistent communication framework is set to become a crucial demand in the near future. Thus, in this paper, the breaches on physical layer of ONs are discussed. Several models, such as RSA and ECC, are compared with proposed ECDH-ES-based encrypted OFDM signals. The proposed ON is designed using private and session keys in order to increase fidelity of system against the attacks of authorized signals. For this purpose, the mathematical model is studied to present how the security

breach distorts the transmitted signals and how to treat such distortions. The proposed framework provides mutual authentication, session key security, general joint key security, and known key security simultaneously. It protects the communication from the attacks, such as key compromise impersonation attack, service disrupting, and access to carrier data. Compared to Biswas and A-ECDH schemes, the proposed ECDH-ES setup consumes less computation time with latest authenticated secret session key scheme. The simulation model is declared based on the proposed and mathematical models, which is analyzed using different parameters, such as wavelength of laser, length of fiber, data rate, line width, noise figure, gain, and no FFT points. The measuring elements, such as BER, PAPR, CCDF, and eye diagram, are used to test the outcomes of the proposed model against encrypted 64QAM-OFDM using ECDH-ES, ECC, and RSA and unencrypted 64QAM-OFDM signals. The proposed framework is beneficial for improving the physical layer security of future generation optical heterogeneous network. It is founded from the simulation analysis that encrypted-based 64QAM-OFDM ON gives good results. It is also concluded that the system PAPR is improved using ECDH-ES algorithm for securing transmitting data.

Funding: The author extend his appreciation to the Deanship of Scientific Research at Jouf University for funding this work through research grant No (DSR-2021-02-0204).

Conflicts of Interest: The author declares no conflict of interest.

References

1. Ali, F.; Muhammad, F.; Habib, U.; Khan, Y.; Usman, M. Modeling and minimization of FWM effects in DWDM-based long-haul optical communication systems. *Photon Netw. Commun.* **2020**, *41*, 36–46. [CrossRef]
2. Kani, J.; Bourgart, F.; Cui, A.; Rafel, A.; Rodrigues, S. Next generation PON-part I: Technology roadmap and general requirements. *IEEE Commun. Mag.* **2009**, *47*, 43–49 [CrossRef]
3. Ali, F.; Khan, Y.; Muhammad, F.; Habib, U.; Abbas, Z.H.; Khan, M.A.; Ali, A. Extenuation of phase shift influenced nonlinear impairments in fiber optics network. *Trans. Emerg. Telecommun. Technol.* **2020**, 31, e3930. [CrossRef]
4. Mesaritakis, C.; Akriotou, M.; Kapsalis, A.; Grivas, E.; Chaintoutis, C.; Nikas, T.; Syvridis, D. Physical unclonable function based on a multi-mode optical waveguide. *Sci. Rep.* **2018**, *8*, 1–12. [CrossRef] [PubMed]
5. Uppu, R.; Wolterink, T.A.; Goorden, S.A.; Chen, B.; Škorić, B.; Mosk, A.P.; Pinkse, P.W. Asymmetric cryptography with physical unclonable keys. *Quantum Sci. Technol.* **2019**, *4*, 045011. [CrossRef]
6. Ji, J.; Zhang, G.; Wang, K.; Xu, M. Improvement of physical-layer security and reliability in coherent time-spreading OCDMA wiretap channel. *Opt. Quant. Electron.* **2018**, *50*, 215. [CrossRef]
7. Skorin-Kapov, N.; Furdek, M.; Zsigmond, S.; Wosinska, L. Physical-layer security in evolving optical networks. *IEEE Commun. Mag.* **2016**, *54*, 110–117. [CrossRef]
8. Wang, Z; Xiao, Y; Wang, S; Yan, Y; Wang, B; Chen, Y; Zhou, Z; He, J; Yang, L. Probabilistic shaping based constellation encryption for physical layer security in OFDM RoF system. *Opt. Express* **2021**, *29*, 17890–17901. [CrossRef]
9. Ji, J.; Zhang, G.; Li, W.; Sun, L.; Wang, K.; Xu, M. Performance analysis of physical-layer security in OCDMA-based wiretap channel. *J. Opt. Commun. Netw.* **2017**, *9*, 813–818. [CrossRef]
10. Javidi, B.; Carnicer, A.; Yamaguchi, M.; Nomura, T.; Pérez-Cabré, E.; Millán, M.S.; Nishchal, N.K.; Torroba, R.; Barrera, J.F.; He, W.; et al. Roadmap on optical security. *J. Opt.* **2016**, *18*, 083001. [CrossRef]
11. Situ, G.; Gopinathan, U.; Monaghan, D.S.; Sheridan, J.T. Cryptanalysis of optical security systems with significant output images. *Appl. Opt.* **2017**, *46*, 5257–5262. [CrossRef]
12. Guan, K.; Tulino, A.M.; Winzer, P.J.; Soljanin, E. Secrecy capacities in space-division multiplexed fiber optic communication systems. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1325–1335. [CrossRef]
13. Furdek, M.; Skorin-Kapov, N.; Wosinska, L. Attack-Aware Dedicated Path Protection in Optical Networks. *J. Light. Technol.* **2016**, *34*, 1050–1061. [CrossRef]
14. Furdek, M.; Natalino, C.; Giglio, A.D.; Schiano, M. Optical network security management: Requirements, architecture, and efficient machine learning models for detection of evolving threats. *IEEE/Osa J. Opt. Commun. Netw.* **2021**, *13*, A144–A155. [CrossRef]
15. Bai, W.; Yang, H.; Zhao, Y.; Zhang, J.; Tan, Y.; Zhu, X.; Ding, H. Security strategy against multipoint eavesdropping in Elastic Optical Networks. In Proceedings of the 2016 21st OptoElectronics and Communications Conference (OECC) Held Jointly with 2016 International Conference on Photonics in Switching (PS), Niigata, Japan, 3–7 July 2016; pp. 1–3.
16. Yang, X.; Shen, Z.; Hu, X.; Hu, W. Physical layer encryption algorithm for chaotic optical OFDM transmission against chosen-plaintext attacks. In Proceedings of the 2016 18th International Conference on Transparent Optical Networks (ICTON), Trento, Italy, 10–14 July 2016; pp. 1–5. [CrossRef]

17. Abbade, M.L.F.; Lessa, L.S.; Santos, M.d.O.; Prado, A.J.d.; Aldaya, I. A New DSP-Based Physical Layer Encryption Technique Applied to Passive Optical Networks. In Proceedings of the 2018 20th International Conference on Transparent Optical Networks (ICTON), Bucharest, Romania, 1–5 July 2018; pp. 1–4. [CrossRef]
18. Dahan, D.; Mahlab, U. Security threats and protection procedures for optical networks. *IET Optoelectron.* **2017**, *11*, 186–200. [CrossRef]
19. Abbade, M.L.; Cvijetic, M.; Messani, C.A.; Alves, C.J.; Tenenbaum, S. All-optical cryptography of M-QAM formats by using two-dimensional spectrally sliced keys. *Appl. Opt.* **2015**, *54*, 4359–4365. [CrossRef]
20. Savva, G.; Manousakis, K.; Rak, J.; Tomkos, I.; Ellinas, G. High-Power Jamming Attack Mitigation Techniques in Spectrally-Spatially Flexible Optical Networks. *Access IEEE* **2021**, *9*, 28558–28572. [CrossRef]
21. Xiao, Y.; Wang, Z.; Cao, J.; Deng, R.; Liu, Y.; He, J.; Chen, L. Time-frequency domain encryption with SLM scheme for physical-layer security in an OFDM-PON system. *IEEE/OSA J. Opt. Commun. Netw.* **2018**, *10*, 46–51. [CrossRef]
22. Wu, Y.; Yu, Y.; Hu, Y.; Sun, Y.; Wang, T.; Zhang, Q. Channel-Based Dynamic Key Generation for Physical Layer Security in OFDM-PON Systems. *IEEE Photonics J.* **2021**, *13*, 1–9. [CrossRef]
23. Liu, B.; Zhang, L.; Xin, X.; Liu, N. Piecewise Chaotic Permutation Method for Physical Layer Security in OFDM-PON. *IEEE Photonics Technol. Lett.* **2016**, *28*, 2359–2362. [CrossRef]
24. Zhang, W.; Zhang, C.; Chen, C.; Zhang, H.; Jin, W.; Qiu, K. Hybrid Chaotic Confusion and Diffusion for Physical Layer Security in OFDM-PON. *IEEE Photonics J.* **2017**, *9*, 1–10. [CrossRef]
25. Cvijetic, N. OFDM for next-generation optical access networks. *J. Lightw. Technol.* **2012**, *30*, 384–398. [CrossRef]
26. Zhang, W.; Zhang, C.; Jin, W.; Chen, C.; Jiang, N.; Qiu, K. Chaos coding-based QAM IQ-encryption for improved security in OFDMA-PON. *IEEE Photon. Technol. Lett.* **2014**, *26*, 1964–1967. [CrossRef]
27. Chang, J.; Cvijetic, N.; Wang, T.; Prucnal, P. Adaptive Photonic Beamforming for Physical Layer Security of Mobile Signals in Optical Fronthaul Networks. In *Frontiers in Optics*; OSA Technical Digest (Online); Paper FTh1B.5; Optical Society of America: Tucson, Arizona United States, 2014.
28. Hu, X.; Yang, X.; Shen, Z.; He, H.; Hu, W.; Bai, C. Chaos-Based Partial Transmit Sequence Technique for Physical Layer Security in OFDM-PON. *IEEE Photonics Technol. Lett.* **2015**, *27*, 2429–2432. [CrossRef]
29. Rothe, S.; Koukourakis, N.; Radner, H.; Lonnstrom, A.; Jorswieck, E.; Czarske, J.W. Physical Layer Security in Multimode Fiber Optical Networks. *Sci. Rep.* **2020**, *10*, 2740. [CrossRef] [PubMed]
30. Mehibel, N.; Hamadouche, M. Authenticated secret session key using elliptic curve digital signature algorithm. *Secur. Priv.* **2021**, *4*, e148.
31. Biswas, G.P. Establishment of authenticated secret session keys using digital signature standard. *Inform Secur J.* **2011**, *20*, 9–16. [CrossRef]