Optical communication security transmission based on blockchain*

YAN Jianghong[1], **ZHANG Yu**[1], **LU Ye**[1]**, **and LI Chuanqi**[2]**

1. Optoelectronics and Optical Communication Laboratory, School of Electronic Engineering, Guangxi Normal University, Guilin 541004, China

2. School of Physics and Electronics, Nanning Normal University, Nanning 530001, China

(Received 16 July 2021; Revised 8 October 2021)

Information leakage, which damages the transmission medium in optical communication systems, is becoming increasingly serious. The existing optical communication systems can easily expose data to unauthorized users, specifically when malicious users control the target demodulator. Therefore, based on the alliance chain, the data are encrypted first based on the elliptic curve encryption algorithm and the signature algorithm, and then they are transmitted through the optical network system. Thus, a blockchain-based optical communication security transmission system scheme is proposed. The scheme has a high modulation and demodulation efficiency, fast operation speed, and verifiability. The theoretical analysis and experimental results indicate that the scheme has better security and high performance, and it generates the security requirements of optical communication systems during data transmission.

Document code: A **Article ID:** 1673-1905(2022)04-0227-6

DOI https://doi.org/10.1007/s11801-022-1119-5

An optical fiber communication network is a transmission system that carries most of the world's data. With the development of optical communication systems, information security has attracted significant attention[1,2]. The current optical transmission network transmits information directly in the form of optical bit codes on optical fiber links, without any security measures on the optical physical layer for optical signals. Stealing optical signals will lead to information leakage[3]. The widely used optical code division multiple access (OCDMA) transmission system adopts the principle of spread spectrum communication, that is, the bandwidth of signal transmission is larger than that of the original information signal transmitted. It has strong anti-interference ability, good concealment, and confidentiality, but after spreading spectrum technology, the bandwidth occupied by its transmission signal increases, making it unsuitable for high-speed transmission systems. Therefore, it is imperative to find a solution that guarantees the security of the optical network and increases the utilization rate of the frequency band.

In 2018, TAN et al[4] conducted a security study on the physical layer of a coherent spreading time code division multiple access system. The scheme revealed the relationship between the system security capacity and the change in different system parameters, proving that selecting appropriate system parameter values could improve the security level of the coherent time-extending OCDMA system. However, it cannot guarantee the safety of the original parameter data from the root cause. In 2020, they proposed an anti-interception communication system based on optical encoding/decoding technology[5], constructed a large-capacity two-dimensional frequency-hopping spread-time address code, designed a new anti-interception communication system, and established the channel model to verify the transmission and security performance of the anti-interception communication system. However, the channel bandwidth occupied by the large-capacity address code increases, and invalid symbols reduce the frequency band utilization rate of the communication system.

Blockchain is a secure distributed ledger technology that involves multiple nodes[6]. The high system reliability is ensured by the characteristics of anonymity, credibility, traceability, and anti-tampering owing to the existence of time stamps[7-9]. Therefore, it is effective to apply blockchain technology to optical network communication to ensure its security.

YANG et al successively proposed a blockchain-based optical fiber network trusted cloud radio solution for 5G fronthaul[10], a blockchain-based securely distributed control solution for software-defined optical networks[11], and a distributed blockchain-based trusted control scheme which is suitable for software in 5G[12]. LIANG et al[13] proposed that efficient recovery based on the blockchain can realize secure distributed control in a

* This work has been supported by the Guangxi Science and Technology Program (Nos.AB17292082 and AB18126025).

** E-mails: luye@mailbox.gxnu.edu.cn; lcq@mailbox.gxnu.edu.cn

software-defined optical network program. All these schemes prove the security of optical network source data after applying blockchain technology, but they do not consider the deteriorated demodulation of optical network data during transmission.

Therefore, we propose a blockchain-based optical communication security transmission to ensure the security of the optical communication transmission system and improve the frequency band utilization. During transmission, if a malicious demodulator obtains data, data leakage can be solved using the one-way function principle of blockchain cryptography.

Because the signature constructed by bilinear mapping is safe, short, and efficient, it is often used to construct digital signatures[14]. Suppose (G_1, +), (G_2, +), and (G_T, ·) are three cyclic groups, where G_1, G_2, and G_T are the additive and multiplicative groups in order of large prime number N, respectively. P is the generator of G_1 and Q is the generator of G_2. When the mapping e: $G_1 \times G_2 \rightarrow G_T$ is a bilinear mapping, it satisfies the following properties.

Property 1 (bilinearity) $\forall P \in G_1, \forall Q \in G_2$, satisfying

$$e(aP,bQ)=e(P,Q)^{ab}, \quad a,b \in Z_q^* . \tag{1}$$

Property 2 (non-degenerate) $\forall P \in G_1, \forall Q \in G_2$, satisfying

$$e(P,Q) \neq 1 . \tag{2}$$

Property 3 (computability) $\forall P \in G_1, \forall Q \in G_2$, there is an effective calculation method to calculate $e(P, Q)$. (3)

Blockchain mainly uses digital signatures to achieve permission control, identify the legal identity of the transaction initiator, and prevent the identity of malicious nodes from being impersonated. The digital signature algorithm includes two operations, signature and signature verification. After the data are signed, it is very easy to verify the integrity and cannot be denied[15,16]. Digital signatures use asymmetric encryption algorithms, that is, each node requires a private and a public key pair. The private key means that only one person can own it, and a public key means that everyone can obtain it. Digital signatures are generally attached to the original message as additional information to identify the message sender. Different private keys signify the same piece of data completely differently. All nodes can obtain the public keys of the other nodes to verify the legitimacy of their identities.

Hash algorithm generates a fixed-length string of any length through a certain calculation, and the output string is called the input hash value. Its features, such as fast forward speed, sensitive input, difficult reverse direction, and strong anti-collision, ensure that the blockchain cannot be tampered with.

Homomorphic encryption is a special method that directly processes the ciphertext and then encrypts the processing result after processing the plaintext, and the obtained result is the same. The commonly used types are as follows.

Additive homomorphism:

$$f(A)+f(B)=f(A+B). \tag{4}$$

Multiplication homomorphism:

$$f(A)\times f(B)=f(A\times B). \tag{5}$$

Various digital baseband signals are converted into digital modulated signals (modulated or frequency band signals) suitable for channel transmission, and then the received digital frequency band signals are restored to digital baseband signals at the receiving end[17].

The blockchain network must send to the user both the original data and the digest value signed by the user's public key. Thereafter, the users decrypt it with their private keys to obtain the digest value, calculate the digest value from the original data, and then perform a comparison. The user's private key can decrypt the digital signature to ensure that the original data is indeed from the blockchain network, and the decrypted digest value is the same as the digest value obtained by recalculating the original data, ensuring that the original data has not been tempered during transmission.

The overall architecture of the proposed solution is shown in Fig.1. The solution proposed in this article mainly includes five parts as follows. The data sender (DS) is the carrier that generates data. The access network (AN) receives data and sends it to the core network. The block chain network (BCN) provides services such as storing data, generating secret keys for all users, and encrypting data. The optical communication system (OCS) transmits modulated and demodulated signals via optical fiber links. At the requesting data terminal, only authorized users can decrypt the data.

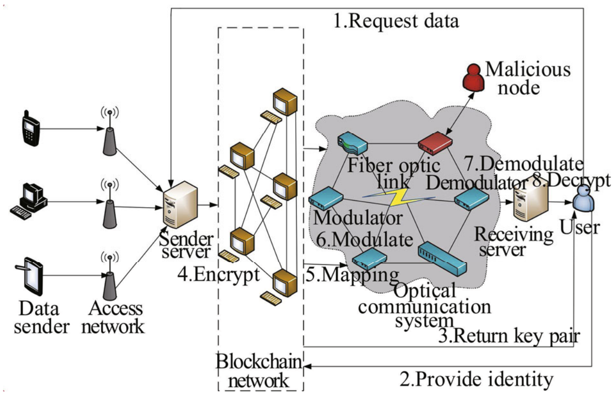

Fig.1 Architecture model of the proposed scheme

As shown in Fig.2, the coherent optical receiver receives the packaged data from the blockchain. The data is first processed by digital signals, and then is converted to an optical fiber by the electro-optic modulator. To ensure a certain transmission quality of the optical signal in the channel, transmission loss of the optical signal in the single-mode fiber is reduced by optical devices such as the erbium doped fiber amplifier (EDFA) polarization controller during transmission. At the receiving end, through coherent detection, photoelectric conversion, and sampling, the optical signal is converted into discrete electrical signals and sent to the digital signal processor (DSP) for processing. Clock synchronization, dispersion compensation, polarization tracking, frequency offset, and phase recovery algorithms are used in the DSP. The original data is restored after processing the signal.

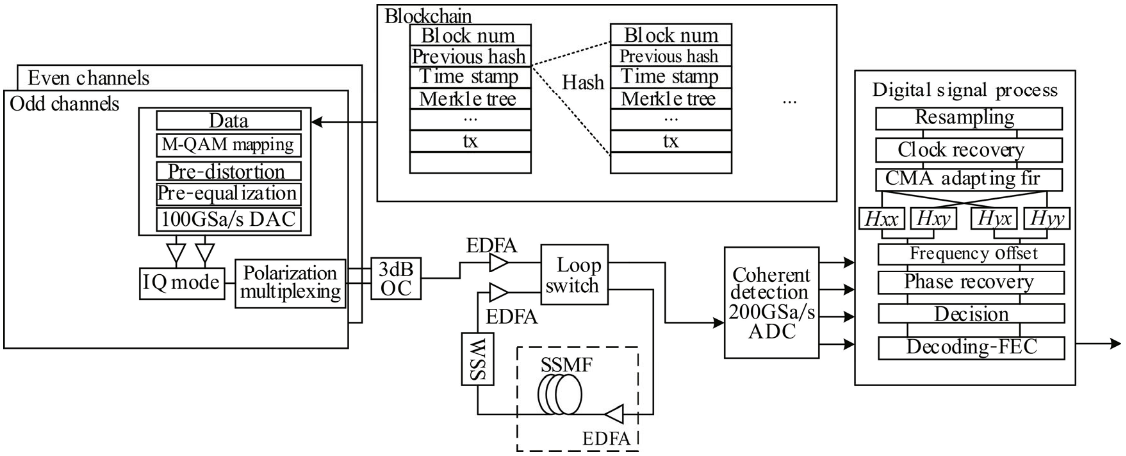

Fig.2 Schematic diagram of the proposed blockchain-based optical communication security transmission system

Assuming that A is a BCN, B is a user, and M is the message to be signed, the specific operation steps are shown in Fig.3. After the receiving end user B initiates a data request to the sending end server, a pair of keys is generated. The random number $ke \in [1, N-1]$ is generated by the key generation center (KGC) in A which is used as the encryption master private key, and the encryption master public key is calculated as

$$P_{\text{pub-s}}=[ke]P_2. \tag{6}$$

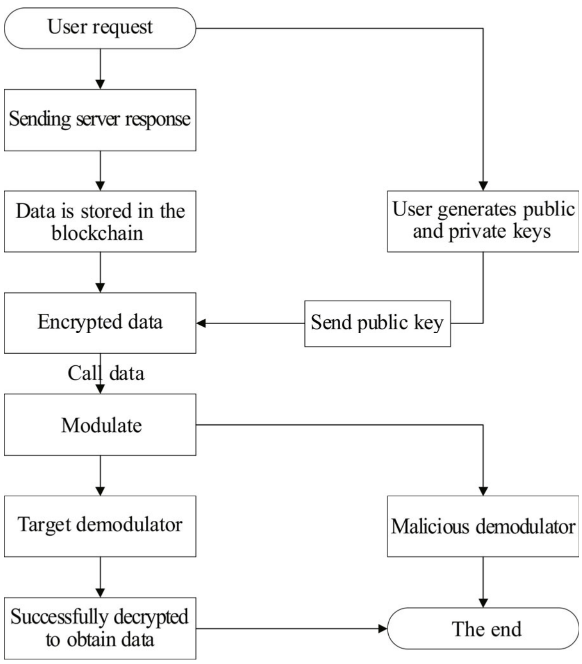

Fig.3 Procedure of blockchain-based optical communication secure transmission

Thereafter, the encryption master key pair is (ke, $P_{\text{pub-s}}$). The identification of data d is DT_A. To generate the encrypted private key ds_A of data d, KGC calculates Eqs.(7) and (8) on the finite field F_N as

$$t_1 = H_1(DT_A, N) + ke, t_2 = ke \times t_1^{-1}, \tag{7}$$

$$ds_A = [t_2]P_1. \tag{8}$$

Thereafter, B saves the private key, and the public key is broadcast to all nodes on the blockchain.

To hide the identity of the sender, all data are collected to the sender server through various display devices and antennas, decentralized unit (DU), as well as centralized unit (CU). The sender server sends the data to the blockchain transaction pool and performs a digital signature described as

$$g = e(P_{\text{pub-s}}, P_1), \tag{9}$$

$$r \in [1, N-1], \tag{10}$$

$$w = g^r, h = H(M \| w, N), l = (r-h) \bmod N, \tag{11}$$

$$S = [l]ds_A. \tag{12}$$

Thereafter, the signature of M means calculating (h, S). After all nodes reach a consensus through the byzantine consensus algorithm, the data are packaged into the blockchain.

The first responding node on the blockchain encrypts the corresponding data with the public key of the receiving end user, generates a fixed-length hash value, and maps it to the "01" sequence required by the optical communication system through the ASCII code. Thereafter, the original and encrypted data are sent to the modulator of the shortest path required for modulation, and the modulated signal reaches the demodulator through the optical fiber link.

When the signal reaches the target demodulator smoothly, the receiving end user decrypts the signal using the private key to obtain the hash value, calculates the hash value of the original data for comparison, and obtains the required data if they are consistent after obtaining the signal. Finally, a success signal is returned. The decryption principle is as follows.

To verify the signature (h', S'') of message M', B performs the following calculation.

$$g_1 = e(P_{\text{pub-s}}, P_1)\,, \tag{13}$$

$$t = g_1^{h'}, h_1 = H(DT_A, N)\,, \tag{14}$$

$$P = [h_1]P_1 + P_{\text{pub-s}}, u = e(P, S'), w' = u \times t\,, \tag{15}$$

$$h_2 = H_2(M' \| w', N). \tag{16}$$

When h_2=h', the signature verification passes, otherwise it fails.

By verifying whether the results are correct, we can decide whether h_2 and h' are equal because

$$h_2 = H_2(M' \| w', N), h' = H_2(M \| w, N)\,, \tag{17}$$

and by verifying whether the two are equal, we can decide whether w and w' are equal.

From the bilinear pair property, we can evaluate Eqs.(18)—(20)

$$u = e(S', P) = e(P_1, P_2)^{(r-h)[\sum_{j=1}^{k} t_j] \times (h_1 + ks)}\,, \tag{18}$$

$$t = g^{h'} = e(P_1, P_2)^{h \times [\sum_{j=1}^{k} ke_j]}\,, \tag{19}$$

$$w' = u \times t = w. \tag{20}$$

Thus, the verification is passed, and the correctness of the signature algorithm is proved.

When the signal is demodulated by a malicious demodulator, there are two situations.

The attacker obtains the demodulated signal and does not have the private key to decrypt it. Even if the original data are obtained, the authenticity of the data cannot be determined, and the receiving end user will send a failed signal feedback when the response time is exceeded. All servers and the blockchain nodes respond, trace back to the original data to re-transact and block the attacker's server data.

The signal demodulated by the malicious demodulator is sent to the receiving end user, and the hash value of the original data after decryption is inconsistent with the original data, and the failed signal is fed back. When the blockchain node calculates the shortest path, it is excluded as a malicious demodulator of feedback.

First, we perform

$$S_1 = (r_2^{-1}) \times (r_1 - h) \times ds_A\,, \tag{21}$$

$$ds_A = [H_1(DT_A \| hid, N) + ks]^{-1} [\sum_{j=1}^{k} ke_j] P_1. \tag{22}$$

This algorithm is a one-way algorithm that includes a hash function. Moreover, there is a problem in solving the discrete logarithm on the elliptic curve, which makes it extremely difficult for malicious nodes to obtain the original data. Therefore, this solution can ensure the safety of the optical communication systems.

Second, we use additive homomorphic encryption technology to guarantee the security of information as

$$f(M') = f(M_1) + f(M_2) = f(M_1 + M_2) = f(M). \tag{23}$$

This algorithm processes the ciphertext directly, and then encrypts the processed result after processing the plaintext, and the result obtained is the same. Therefore, this solution can ensure the safety of the optical communication system.

The main test plan in this study was based on the Python language, MATLAB language, and OptiSystem platform to build the system shown in Fig.2. Windows10 system was used, and the processor was an Intel(R) Core (TM) i5-9500 CPU at 3.00 GHz, and 8 GB of memory. A 28 Gbaud dual-polarization non-return-to-zero quadrature phase-shift keying (NRZ-QPSK) coherent optical transmission system was built on the OptiSystem based optical simulation platform, with a total transmission rate of 112 Gbit/s. The new block in the blockchain platform was generated by one node and it was verified by 10 nodes.

Fig.4 shows that the input information {amount: 5 transactions, recipient: (someone-other-address) receiver address, sender: (d4ee26eee15148ee92...) sender address} is encrypted to generate 'b"\Xbb\xfd\x89......"'. It can be observed that the encrypted data is extremely complicated, and its association with the original data cannot be observed.

Fig.4 Input and encrypted information

Fig.5 and Fig.6 show that when the node confirms that the information is correct for generating transaction information, the transaction information sent to all nodes is successfully uploaded to the chain. Therefore, blockchain platforms have been successfully developed.

Fig.5 Transaction successfully packaged into the block

Fig.7 shows that after the encrypted data enters the optical communication system module, it is modulated and demodulated. Although there is some noise interference, the output result is consistent with the input and does not affect the critical of the result. Thus, the optical communication system module can meet the expectations of the actual operation of the system.

Fig.6 Review of the blockchain

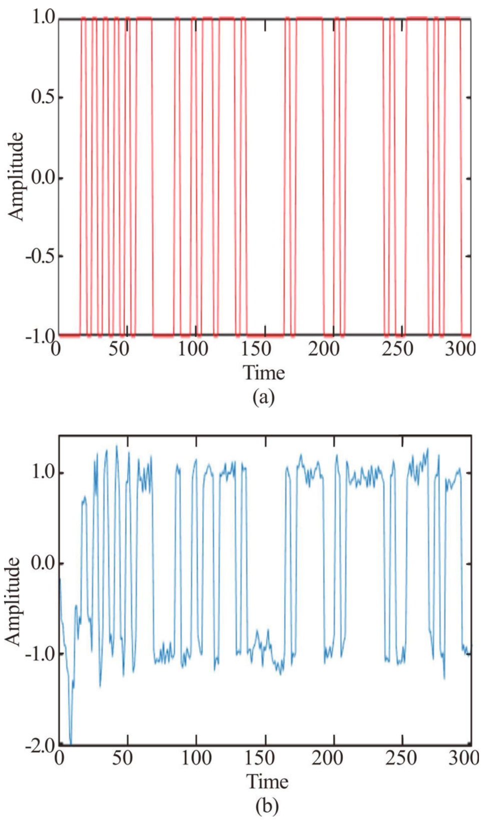

Fig.7 (a) Modulation and (b) demodulation output diagrams

Fig.8 shows that the signature verification is passed, that is, the only receiving end user who has the decryption private key has successfully decrypted it. The time required to generate the signature and complete the verification was 1.994 6 ms and 5.985 3 ms, which is significantly short, thus, the entire system can meet the expectations of the system actual operation.

As summarized in Tab.1, the solution in this study has the highest security features compared to the five security features of public verification, accountability traceability, privacy protection, anti-interception, and fault tolerance.

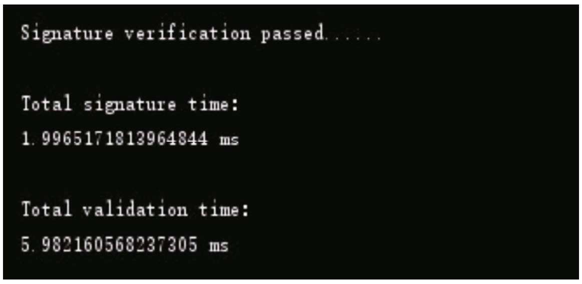

Fig.8 Result of successful verification

Tab.1 Comparison of security features

Program	Anti-interception communication system based on optical encoding/decoding technology[5]	System performance analysis of double-length modified quality codes[18]	Two-dimensional encryption system[19] solution	This article
Publicly verifiable	N	N	Y	Y
Responsibility can be traced	Y	N	N	Y
Privacy protection	N	Y	Y	Y
Anti-interception	Y	N	Y	Y
Fault tolerance	N	Y	Y	Y

Data insecurity is a problem that cannot be avoided by any system, specifically communication that is closely related to modern life. Therefore, we apply the security advantages of blockchain technology to the traditional optical communication system to solve the security problem in the optical communication transmission process. The hash algorithm in the blockchain ensures a constant data size, and only a fixed bandwidth value is required with no additional bandwidth. Through feasibility, correctness, and security analysis, it is proved that after applying the cryptographic signature algorithm, elliptic encryption algorithm, hash algorithm, and additive homomorphic encryption algorithm in the blockchain, the scheme of this article outperforms the traditional optical communication encrypted transmission scheme, which is more secure and does not cause wastage of frequency band resources.

Statements and Declarations

The authors declare that there are no conflicts of interest related to this article.

References

[1] LIU Z. Status and key technologies of optical network security[J]. Communication world, 2019, 26(11)：48-49. (in Chinese)

[2] ZIAUR R, IBRAHIM K, XUN Y, et al. Blockchain-based security framework for a critical industry 4.0 cyber-physical system[J]. IEEE communications magazine, 2021, 59(5)：128-134.

[3] WANG H, LI W F, LI Z Y. Overview of the development of foreign security optical communication technology[J]. Optical communication technology, 2013, 37(08)：40-43. (in Chinese)

[4] TAN Y T, PU T, XIANG P, et al. Research on the physical layer security of coherent spreading time code division multiple access systems[J]. Journal of quantum electronics, 2018, 35(01)：115- 121. (in Chinese)

[5] TAN Y T, PU T, ZHENG J L, et al. Research on anti-interception communication system based on optical encoding/decoding technology[J]. Acta optics, 2020, 40(09)：32-39. (in Chinese)

[6] YUAN Y, WANG F Y. Current status and prospects of blockchain technology development[J]. Acta automatica sinica, 2016, 42(04)：481-494. (in Chinese)

[7] ZHOU Y S, CHEN L J. Blockchain-based secure storage and deletion of fine-grained cloud data[J]. Journal of electronics and information, 2021, 43(7)：1856-1863. (in Chinese)

[8] KOU S Q. Research on consensus of trusted optical network resources based on blockchain technology[D]. Beijing：Beijing University of Posts and Telecommunications, 2019. (in Chinese)

[9] TAN H B, ZHOU T, ZHAO H, et al. Blockchain-based archival data protection and sharing method[J]. Journal of software, 2019, 30(09)：2620-2635. (in Chinese)

[10] YANG H, WU Y, ZHANG J, et al. BlockONet：blockchain-based trusted cloud radio over optical fiber network for 5G fronthaul[C]//2018 Optical Fiber Communications Conference and Exposition (OFC), March 11-15, 2018, San Diego, CA, USA. New York：IEEE, 2018：17843214.

[11] YANG H, LIANG Y S, YAO Q Y, et al. Blockchain-based secure distributed control for software defined optical networking[J]. China communications, 2019, 16(06)：42-54.

[12] YANG H, LI Y, GUO S, et al. Distributed blockchain-based trusted control with multi-controller collaboration for software defined data center optical networks in 5G and beyond[C]//2019 Optical Fiber Communications Conference and Exhibition (OFC), March 3-7, 2019, San Diego, CA, USA. New York：IEEE, 2019.

[13] LIANG Y, YANG H, YAO Q, et al. Blockchain-based efficient recovery for secure distributed control in software defined optical networks[C]//2019 Optical Fiber Communications Conference and Exhibition (OFC), March 3-7, 2019, San Diego, CA, USA. New York：IEEE, 2019.

[14] CHEN S J, ZHAI S P, WANG Y J. A blockchain privacy protection algorithm based on ring signature[J]. Journal of Xidian University, 2020, 47(05)：86-93. (in Chinese)

[15] LI P L, XU H X. Blockchain user anonymity and traceability technology[J]. Journal of electronics and information technology, 2020, 42(05)：1061-1067. (in Chinese)

[16] SAVVA G, MANOUSAKIS K, ELLINAS G, et al. Confidentiality meets protection in elastic optical networks[J]. Optical switching and networking, 2021, 42：100620.

[17] ZHANG H X. Security technology of large-capacity optical access network in the 5G era[J]. ZTE technology, 2019, 25(04)：36-42. (in Chinese)

[18] MORSY A M, ABDULAZIZ S A. Performance analysis of OCDMA wireless communication system based on double length modified prime code for security improvement[J]. IET communications, 2020, 14(7)：1139-1146.

[19] IKEDA K, SATO Y, KOYAMA O, et al. Two-dimensional encryption system for secure free-space optical communication of time-series data streams[J]. Electronics letters, 2019, 55(13)：752-754.