AIMS *Mathematical Biosciences and Engineering*

MBE, 21(1): 96–115.
DOI: 10.3934/mbe.2024005
Received: 08 September 2023
Revived: 15 November 2023
Accepted: 29 November 2023
Published: 08 December 2023

http://www.aimspress.com/journal/MBE

Research article

An edge cloud and Fibonacci-Diffie-Hellman encryption scheme for secure printer data transmission

Yiqin Bao[1,4,*], Qiang Zhao[2], Jie Sun[1], Wenbin Xu[3] and Hongbing Lu[4]

[1] School of information engineering, Nanjing XiaoZhuang University, Nanjing 211171, China
[2] Department of Information Systems Schulich School of Business, Toronto 416647, Canada
[3] Jiangsu United Vocational and Technical College Suzhou Branch, Suzhou 215005, China
[4] College of software of Nanjing University, Nanjing 210093, China

* **Correspondence:** Email: baoyiqin@njxzc.edu.cn; Tel: + 8613851549080.

Abstract: Network printers face increasing security threats from network attacks that can lead to sensitive information leakage and data tampering. To address these risks, we propose a novel Fibonacci-Diffie-Hellman (FIB-DH) encryption scheme using edge cloud collaboration. Our approach utilizes properties of third-order Fibonacci matrices combined with the Diffie-Hellman key exchange to encrypt printer data transmissions. The encrypted data is transmitted via edge cloud servers and verified by the receiver using inverse Fibonacci transforms. Our experiments demonstrate that the FIB-DH scheme can effectively improve printer data transmission security against common attacks compared to conventional methods. The results show reduced vulnerabilities to leakage and tampering attacks in our approach. This work provides an innovative application of cryptographic techniques to strengthen security for network printer communications.

Keywords: Fibonacci; Diffie-Hellman; encryption technology; edge cloud collaboration; data transmission

1. Introduction

With the increasing demand for supporting mobile device printing, network printers that support mobile functions such as WiFi direct connection, NFC printing and cloud printing have gradually become indispensable electronic devices in people’s daily life and office. Schools, government departments, hospitals and other units and institutions all use printers. From a security perspective, as printing devices are deployed on internal networks, they can directly access various sensitive information, so their security is more important. However, due to its unique functionality, people often overlook its security, resulting in many printer security issues and a gradual increase in security incidents [1,2]. For example, a high school hacker from the UK, Stackoverflow, claimed to have used printer vulnerabilities to control over 150,000 printers. He attempted to directly transmit RAW protocol print jobs through port 9100 using printer process daemon (LPD) and Internet Printing Protocol (IPP), bypassing identity authentication. He also revealed that he had discovered an 0Day remote execution vulnerability (RCE) on Xerox's printer web management page. Columbia University researchers have found that a feature called "Remote Firmware Update" on some HP laser printers allows hackers to fully control the printer after installing malicious software on the machine, transmit printed files back to the hacker's computer, stop the printer from working and even cause the fixing device on the printer that heats and pressurizes the toner to continue heating until it catches fire. Now, someone has successfully invaded a printer connected to a public network. Andrew Auernheimer (codenamed "Weev" and previously a well-known hacker who was a member of the Goatse security team) admitted on his blog that he had invaded thousands of network printers and made them print content containing racist and anti-Semitic information. These are all very serious printer security incidents [3,4].

There have been many achievements in research on the security of data during network printing and the prevention of printing data leakage. First, Li [5] conducted research on network printer security risk analysis and prevention technologies. Li et al. [6] proposed suggestions for network printer security research and protection. Yan et al. [7] designed a security enhanced printer based on Trusted Computing 3.0, Feng et al. [8] evaluated and improved the network printing protocol based on the HCPN model detection method, Sulaiman et al. [9] developed a signature based Suricata network printer for theft prevention on PfSense, Huang et al. [10] designed a cloud based portable IoT inkjet printer, Nguyen et al. [11] designed a deep learning based micro print source printer recognition and Kakade et al. [12] designed an open IoT based real-time online monitoring system for FDM printers, The above achievements have achieved certain results in achieving network printing security.

This article is different from previous studies. In order to achieve security in data transmission of network printers, a FIB-DH data encryption technology scheme based on edge cloud collaboration is proposed. Network security is achieved through edge cloud collaboration and cryptographic methods. There have also been studies related to this. Cai et al. [13] designed an industrial internet intrusion detection method based on Res-CNN SRU, and Xiang et al. [14] proposed an APT attack detection event extraction method based on BERT BiGRU-CRF, Kimi et al. [15] conducted digital forensics for electronic IoT devices in smart cities, while Almuflih et al. [16] used efficient key exchange using identity-based encryption in a multipath TCP environment. Here, we combine the characteristics of the third-order Fibonacci matrix with Diffie-Hellman to ultimately achieve secure data transmission for network printers.

The major contributions of this paper include three aspects:

- By combining the third-order Fibonacci matrix with Diffie-Hellman through edge cloud collaboration, a FIB-DH data encryption technology architecture is designed.

- The process of implementing FIB-DH data encryption technology solution is provided.
- The feasibility of the FIB-DH scheme was verified through simulation attack experiments using the PRET tool and compared with normal network printing.

The paper is organized as follows: The second section of this article introduces the preliminary knowledge for implementing the technical solution of this paper, including the information flow of the printer, the risk of printing data transmission leakage, IPP protocol, the characteristics of the third-order Fibonacci matrix, Diffie-Hellman encryption technology and MQTT protocol; in Section 2, an architecture of FIB-DH encryption technology based on edge cloud collaboration was designed, providing the implementation process of the FIB-DH scheme; Section 3 conducted experiments and comparative analysis on the scheme through simulation; Finally, we summarize the entire article and propose future work.

2. Preliminary knowledge

2.1. The information flow of the printer

The printer mostly consists of three parts: the host part (including driver program and PC storage), the control card part (including the main control chip CPU) and the printer core (including LSU, toner cartridge and mechanical structure) [17]. The laser printer is composed of a mechanical part and an electronic control part, which is a typical mechatronics product. The electronic control part is usually highly integrated on the printer control card. Used to control the mechanical part to complete the entire printing work. The composition structure of the printer is shown in Figure 1.

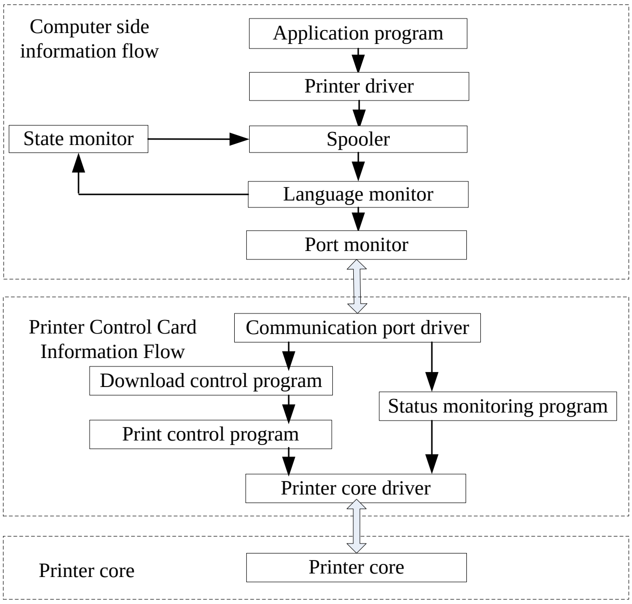

Figure 1. The information flow of the printer.

In response to the security risks of modules or components such as the printer’s main control unit, data transmission unit, external interface, driver, printing protocol, etc., attackers usually use the built-in backdoor program of the printer, control of the printer port, plaintext transmission of printing information, printing business authentication and processing of printing information cache data to attack printer security vulnerabilities.

2.2. Printing data transmission leakage risk

Although a printer is only one of the peripheral devices connected to a computer host, it has independent data processing capabilities and can interact with the host for data transmission, thus providing great security [18]. There are three main risks of printing data transmission leakage, as shown in Figure 2.

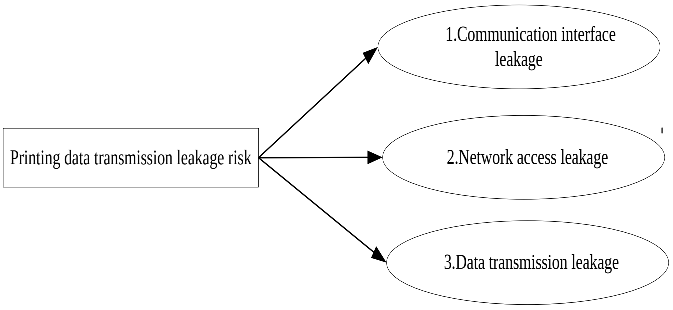
Printing data transmission leakage risk
1.Communication interface leakage
2.Network access leakage
3.Data transmission leakage

Figure 2. Types of risk of data transmission leakage during printing.

First, communication interface leaks. Modern printers are generally equipped with rich communication interfaces to meet diverse user needs. These interfaces can be divided into two categories: Wired communication interfaces such as USB, RJ45, RS232 and PCIExpress; the other type is wireless communication interfaces, such as Wi-Fi, GPRS, Bluetooth, infrared, etc. Although these interfaces extend the functionality of the printer, they also increase the avenues for unauthorized users to steal printing data.

Second, network access leaks. Currently, printers are developing towards comprehensive information management and output terminals, mostly integrating rich network functions. These functions not only improve work efficiency and enhance team collaboration capabilities, but also become a major channel for information leakage. When the printer is connected to an external network (such as the Internet), it will inevitably generate data exchange with the public network; in addition, some open ports can even be exploited by hackers, leading to illegal takeover of printers.

Third, data transmission leaks. During the process of sending print jobs to the printer, the computer needs to interact with the printer through data transmission media. During this process, if the printed data is not encrypted before transmission, once it is illegally hijacked by an intruder during transmission, the intruder can easily obtain the true printed data through protocol analysis tools.

2.3. IPP Protocol

IPP is the latest industry standard network printing protocol that can be used for client to server communication and server to printer communication. This protocol provides a basic model that includes printers and jobs, standard attributes of these printers and jobs and a set of standard operations that can be performed on these printers and jobs. Due to the standardization of objects, attributes and operations, IPP is a method used for communication between client and server systems, allowing users to perform remote printing and manage printing work through the internet [19].

The IPP protocol is based on the client/server mode. Network printers are connected to the internet or intranet through IPP, and users can directly observe the working and physical status of the printers. However, BinaryEdge normal scanning shows that on average, about 80000 printers are discovered through the IPP port every day, and these printers are exposed to the internet every day, which will cause many problems [20].

Therefore, the IPP protocol is not completely secure and is often exploited by attackers, Conduct an attack.

2.4. Characteristic analysis of third order Fibonacci matrix

People have been interested in studying Fibonacci sequences for hundreds of years. It was an interesting sequence, also known as the golden sequence, introduced by the Italian mathematician Fibonacci in the 13th century to solve the problem of rabbit reproduction, which is a second-order recursive sequence: $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$, n = 1, 2, 3…. Fibonacci has many unique properties and is widely used in computational mathematics, mathematical statistics, geometry and other fields [21,22]. Previous research has shown that Fibonacci sequences can be represented by Fibonacci matrices, and second-order Fibonacci sequences can be represented by second-order Fibonacci matrix T_2 [23], as shown in formula (1).

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = T_2^n \qquad n = 1,2,3\ldots \tag{1}$$

Third order Fibonacci sequence: $F_0 = 1$, $F_1 = 1$, $F_2 = 2$, $F_{n+1} = F_n + F_{n-1} + F_{n-2}$, n = 2, 3, 4…, can be represented by the third-order Fibonacci matrix T_3 [24] as shown in formula (2).

$$\begin{pmatrix} F_n & F_{n+1} - F_n & F_{n-1} \\ F_{n-1} & F_n - F_{n-1} & F_{n-2} \\ F_{n-2} & F_{n-1} - F_{n-2} & F_{n-3} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^n = T_3^n \quad n = 3,4,5\ldots \tag{2}$$

Due to the determinant $|T_3| = 1$, T_3 is reversible, so T_3^{-1} can be calculated, as shown in formula (3).

$$T_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad T_3^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & -1 \end{pmatrix} \tag{3}$$

Calculate T_3^n and $(T_3^n)^{-1}$ using formulas (4) and (5), as shown in formula (6).

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^{k1+k2} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^{k1} * \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^{k2} \tag{4}$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & -1 \end{pmatrix}^{k1+k2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & -1 \end{pmatrix}^{k1} * \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & -1 \end{pmatrix}^{k2} \tag{5}$$

$$T_3^n = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^n \quad (T_3^n)^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & -1 \end{pmatrix}^n \tag{6}$$

Using n as a parameter and formula (6), taking n = 4, calculate T_3^4 and $(T_3^4)^{-1}$, as shown in formula (7).

$$T_3^4 = \begin{pmatrix} 7 & 6 & 4 \\ 4 & 3 & 2 \\ 2 & 2 & 1 \end{pmatrix} \quad (T_3^4)^{-1} = \begin{pmatrix} -1 & 2 & 0 \\ 0 & -1 & 2 \\ 2 & -2 & -3 \end{pmatrix} \tag{7}$$

Using formula (6), take n = 5 and calculate $T_3^5$and $(T_3^5)^{-1}$, as shown in formula (8).

$$T_3^5 = \begin{pmatrix} 13 & 11 & 7 \\ 7 & 6 & 4 \\ 4 & 3 & 2 \end{pmatrix} \quad (T_3^5)^{-1} = \begin{pmatrix} 0 & -1 & 2 \\ 2 & -2 & -3 \\ -3 & 5 & 1 \end{pmatrix} \tag{8}$$

Similarly, we can easily calculate T_3^n and $(T_3^n)^{-1}$ by taking n = 6, 7, 8, 9, 10.

Finally, Fn is defined by formula (6), as shown in formula (9). By changing n, a third-order recursive sequence can be calculated.

$$F_n = T_3^n = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^n \quad F_n^{-1} = (T_3^n)^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & -1 \end{pmatrix}^n \tag{9}$$

In this study, we utilized the unique feature of third-order Fibonacci matrices being reversible and easy to calculate. Using n as a parameter and applying F_n and F_n^{-1} to the printing data transmission process, we achieved anti tampering and encryption effects. The sender sends data to the receiver, and the process is shown in Figure 3.

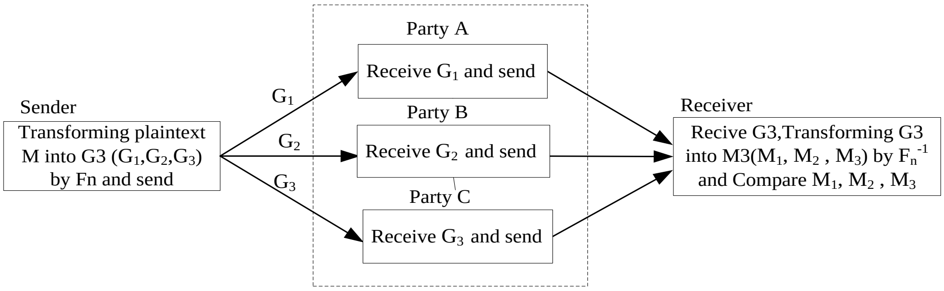
Middle-party
Party A
Receive G₁ and send
Party B
Receive G₂ and send
Party C
Receive G₃ and send
Sender
Transforming plaintext M into G3 (G₁,G₂,G₃) by Fn and send
G₁
G₂
G₃
Receiver
Recive G3,Transforming G3 into M3(M₁, M₂ , M₃) by Fₙ⁻¹ and Compare M₁, M₂ , M₃

Figure 3. Application process of third-order Fibonacci matrix.

The specific data communication process is as follows:

First, the sender and receiver have agreed on n, which is actually the agreement F_n and F_n^{-1}.

1) Sender: Transform the original text M through a third-order Fibonacci matrix. M is defined as a matrix with the same three columns, M3 = (M, M, M), Calculate G3 = M3 × F_n = (M, M, M) × F_n = (G_1, G_2, G_3) and send G3 to the intermediary.

2) Middle-party: There are three Middle-partys who receive G_1, G_2 and G_3 and forward them to the receiver.

3) Receiver: The receiver receives (G_1, G_2, G_3) and transforms G3 through the third-order Fibonacci inverse matrix to generate G3 × F_n^{-1} = (M_1, M_2, M_3).

If there is no tampering during the transmission process, it should be: G3 × F_n^{-1} = (G_1, G_2, G_3) × F_n^{-1} = (M, M, M) × F_n × F_n^{-1} = (M_1, M_2, M_3), M_1, M_2 and M_3 should all be equal. Therefore, the receiver can prevent data tampering by comparing whether M_1, M_2 and M_3 are equal, Moreover, due to the change in n, the intermediary receives three different data sets G_1, G_2 and G_3 from the original text, thus serving the purpose of encryption.

2.5. Diffie-Hellman encryption algorithm

Diffie-Hellman is a key consistency algorithm published by Whitfield Diffie and Martin Hellman in 1976. It is a method of establishing key exchange, aimed at enabling two users to securely exchange a secret key for future message encryption. Its effectiveness depends on the difficulty of calculating discrete logarithms. Diffie-Hellman is an asymmetric encryption algorithm commonly used in blockchain encryption schemes and also a public key algorithm [25,26]. Its working principle is that each communication party generates a private key and a public key, and the private key is not public. After the public key is publicly exchanged, the communication parties can calculate the shared key, which is shared. Therefore, both parties can encrypt and decrypt messages through the shared key, thus achieving encrypted transmission of messages [27–29]. Diffie-Hellman can negotiate a shared key through unreliable channels and is widely used in PKI key distribution in many industrial level security protocols.

Sender sends plaintext M to Receiver for encrypted transmission, as shown in Figure 4.

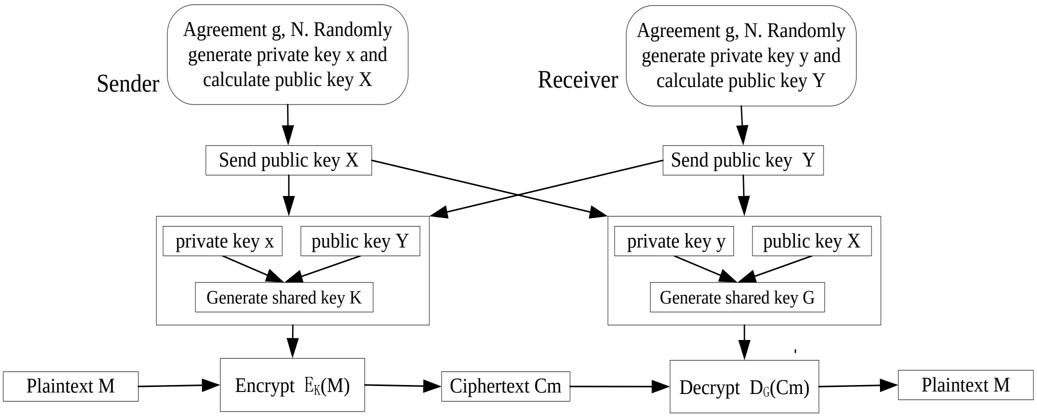

Figure 4. Diffie-Hellman encryption process flow diagram.

1) Sender and receiver first agree on two parameters g and N, and randomly generate their own private keys x and y, and calculate their respective public keys X and Y using formula (10).

$$X = g^x \bmod N,\ Y = g^y \bmod N \tag{10}$$

2) Sender and Receiver exchange X and Y

3) Sender calculates key K through x and Y, while Receiver calculates key G through y and X, as shown in formula (11).

$$K = Yx \bmod N = gxy \bmod N,\ G = XymodN = gxymod\ N \qquad (11)$$

From formula (11), it can be seen that K and G are equal, and therefore can be used as dual shared keys.

4) Sender encrypts plaintext M through K, with Cm = E_k(M); The receiver decrypts D_G(Cm) through G, and since K and G are equal, the receiver can obtain plaintext M = D_G(E_K(M)).

Diffie-Hellman is the foundation of authentication key exchange (AKE) schemes in the post quantum computing era [30]. It combines the third-order Fibonacci matrix with Diffie-Hellman encryption algorithm to form a new FIB-DH encryption technology scheme, which is a specific application of Diffie-Hellman in network printer encryption schemes.

2.6. MQTT protocol

The full name of the MQTT protocol is Message Queuing Telemetry Transport, which means Message Queuing Transport Detection. It is a client server-based message publish/subscribe transport protocol under the ISO standard, based on the TCP/IP protocol cluster, published by IBM in 1999. The biggest advantage of MQTT is that it is lightweight, simple, open and easy to implement. It can provide real-time and reliable messaging services for remote connected devices with minimal code and limited bandwidth. As a low-cost, low bandwidth instant messaging protocol, it has a wide range of applications in the Internet of Things, small devices, mobile applications and other fields [31,32].

Implementing the MQTT protocol requires communication between the client and server. During the communication process, there are three identities in the MOTT protocol: Publisher, Broker (server) and Subscriber. Both the publisher and subscriber of the message are the client, while the message broker is the server. The message publisher can simultaneously send messages to the subscriber [33,34], as shown in Figure 5.

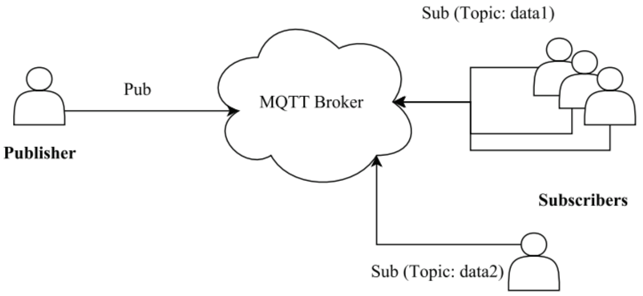

Figure 5. Schematic diagram of MQTT message publish/subscribe.

From Figure 5, it can be seen that the subscriber has subscribed to topic data1 or data2. As long as the publisher publishes topic data1 or data2, the subscriber can receive it. Therefore, broadcasting transmission and reception can be achieved, which can be one-to-many or many-to-one.

The messages transmitted by MQTT are mostly divided into two parts: Topic and payload:

1) Topic: It can be understood as the type of message (the type of data command transmitted). After subscribing to (Subscribe), the subscriber will receive the message content (payload) of the topic.

2) Payload: Can be understood as the content of the message (transmitted data body content), referring to the specific content that the subscriber needs to use. Payload can contain printed data content.

3. FIB-DH encryption technology scheme based on edge cloud collaboration

3.1. System scheme architecture

The FIB-DH encryption technology scheme based on edge cloud collaboration mostly includes five parts: Client computer (CC), MQTT cloud server (MCS), edge computer (EC), printing computer (PC) and printer (PT). 1) Customer computer is a customer computer that allows users to operate network printing, which can be printed locally on a local area network or remotely on the internet; 2) MQTT cloud server, remote communication management between customers and printing computers, and FIB-DH edge cloud collaboration; 3) Edge computer, at the edge of local area network, mainly realizes FIB-DH edge cloud collaboration; 4) The printing computer is connected to the printer USB in the local LAN to achieve FIB-DH edge cloud collaboration and transmit the verified printing data to the printer; 5) Printer, responsible for printing document data. The scheme architecture is shown in Figure 6.

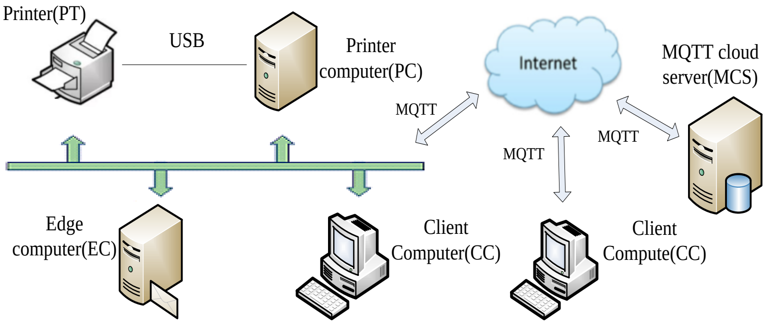

Figure 6. FIB-DH scheme architecture.

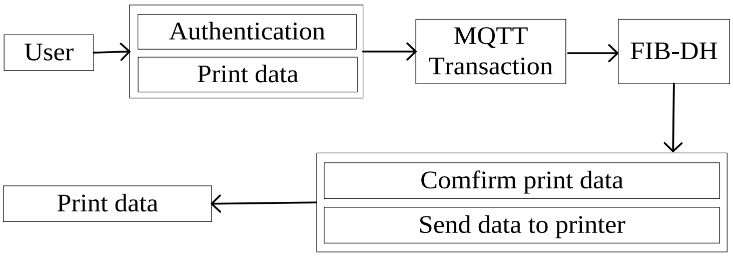

Figure 7. Task implementation flowchart.

In the FIB-DH encryption technology scheme, users send printed data through the client's computer. When the system is implemented, the major tasks include two types: 1) User connection authentication, and 2) printing document data, as shown in Figure 7.

In the connection authentication stage, users use FIB-DH data encryption technology scheme to perform connection authentication. During the document printing phase, users encrypt, transmit and verify printed data through edge cloud collaboration and FIB-DH scheme to avoid man in the middle attacks and prevent leaked printed documents

3.2. FIB-DH encryption scheme

By utilizing the characteristics of the third-order Fibonacci matrix and combining it with the Diffie-Hellman encryption algorithm, a new FIB-DH encryption algorithm is formed. In the FIB-DH encryption algorithm, first, due to the fact that each encryption key is random and undergoes Fibonacci transformation, the generated ciphertext is different each time. If the intermediary obtains the ciphertext, it is ambiguous to analyze. Second, due to the use of key vectors, it is necessary to compare and vote on the results to achieve verification purposes. The FIB-DH encryption process in which the user sends plaintext M to the terminal is shown in Figure 8.

1) Sender and Receiver first agree on three parameters g, N, n (n is the n in F_n in formula 9) and randomly generate their own private key vectors x = (x1, x2, x3) and y = (y1, y2, y3), and calculate their respective public key vectors X and Y through formula (12).

$$X = (g^{x1} \bmod N, g^{x2} \bmod N, g^{x3} \bmod N)$$

$$Y = (g^{y1} \bmod N, g^{y2} \bmod N, g^{y3} \bmod N) \tag{12}$$

2) Sender and Receiver exchange X and Y.

3) Sender calculates the key vector K through x and Y, while Receiver calculates the key vector G through y and X, as shown in formula (13).

$$K = Yx = (g^{x1 \times y1} \bmod N, g^{x2 \times y2} \bmod N, g^{x3 \times y3} \bmod N)$$

$$G = Xy = (g^{x1 \times y1} \bmod N, g^{x2 \times y2} \bmod N, g^{x3 \times y3} \bmod N） \tag{13}$$

From formula (13), it can be seen that K and G are equal and can therefore serve as shared keys for both parties.

4) Sender encrypts plaintext M through K, with Cm = E_k(M), as shown in formulas (14) and (15); Calculate Em through F_n transformation, as shown in formulas (16) and (17); Then the sender sends {E1, E2, E3} to the intermediate party (Party A, Party B, Party C).

After receiving the data from the intermediary, the receiver calculates Cm through F_n^{-1} transformation, as shown in formula (18). Due to formula (19), formula (20) can be derived, and then D_G(Cm) can be decrypted through G, as shown in formula (21). Due to the equality of K and G, the three data {M1, M2, M3} in formula (22) should be equal. Therefore, the original M can be obtained through a voting algorithm.

For example, if the original file M has 5 bytes (if the multi byte principle is the same), M = (m1, m2, m3, m4, m5), (if n bytes, the principle is the same).

$$Cm = E_k(M) \tag{14}$$

$$\mathrm{Cm} = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \\ C_{41} & C_{42} & C_{43} \\ C_{51} & C_{52} & C_{53} \end{pmatrix} \qquad (15)$$

$$\mathrm{Em} = \mathrm{Cm} \times F_n = \begin{pmatrix} E_{11} & E_{12} & E_{13} \\ E_{21} & E_{22} & E_{23} \\ E_{31} & E_{32} & E_{33} \\ E_{41} & E_{42} & E_{43} \\ E_{51} & E_{52} & E_{53} \end{pmatrix} \qquad (16)$$

$$\mathrm{Em} = \{E1, E2, E3\} \qquad (17)$$

$$\mathrm{Cm} = E \times F_n^{-1} \qquad (18)$$

$$F_n \times F_n^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad (19)$$

$$\mathrm{Cm} = \begin{pmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \\ C_{41} & C_{42} & C_{43} \\ C_{51} & C_{52} & C_{53} \end{pmatrix} \qquad (20)$$

$$\mathrm{Mn} = D_G(\mathrm{Cm}) = \begin{pmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \\ M_{31} & M_{32} & M_{33} \\ M_{41} & M_{42} & M_{43} \\ M_{51} & M_{52} & M_{53} \end{pmatrix} \qquad (21)$$

$$\mathrm{Mn} = \{M1, M2, M3\} \qquad (22)$$

Finally, perform a time complexity analysis of the algorithm:

In the FIB-DH encryption scheme, due to $\mathrm{Em} = \mathrm{Cm} \times F_n$ and $\mathrm{Cm} = E \times F_n^{-1}$, based on the characteristics of the Fibonacci matrix, F_n and F_n^{-1} can be calculated in advance. Therefore, its time complexity is O(n). The Elliptic Encryption Algorithm (ECC) is a public key encryption system based on Diffie-Hellman and is commonly used on mobile devices to ensure data security. ECC defines (x, y) at a point on G using the elliptic curve [35] equation G: $y^2 + gxy + hy = x^3 + ix^2 + jx + k$, using key $X \times G$ and $Y \times G$ transformations for encryption and decryption. Based on this feature, its time complexity is O(n3). Therefore, the FIB-DH encryption method has lower time and complexity compared to the Elliptic Encryption Algorithm (ECC).

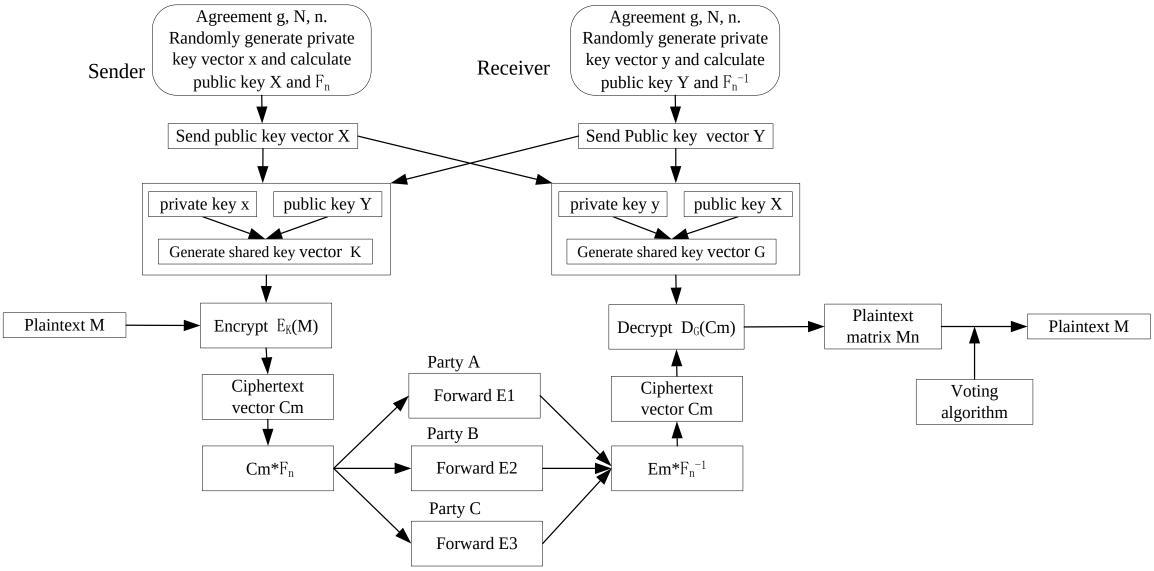

Figure 8. FIB-DH encryption process flow diagram.

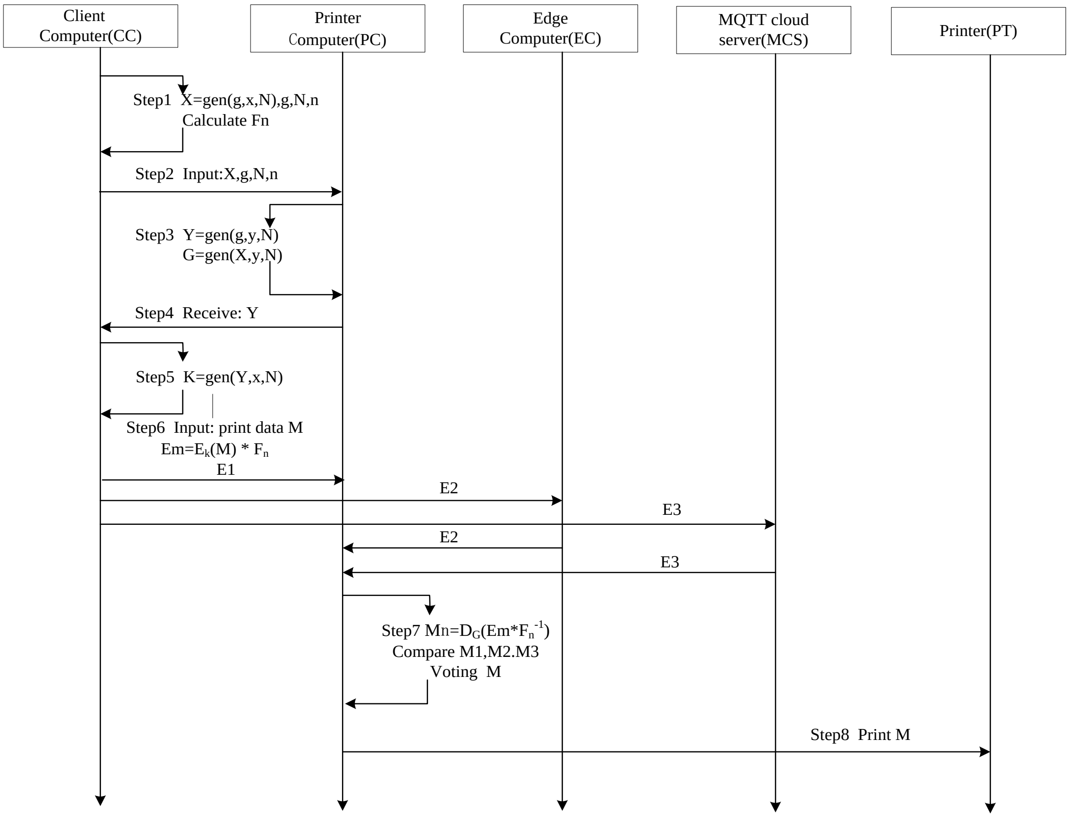

Figure 9. Flow chart for network printing through FIB-DH scheme.

3.3. Implementation process of FIB-DH scheme

Corresponding to Figure 8 of the FIB-DH scheme, the sender is Client Computer (CC), the receiver is Printer Computer (PC) and the intermediaries (Party A, Party B and Party C) are Edge

Computer (EC), MQTT cloud server (MCS) and Printer Computer (PC). According to the FIB-DH encryption scheme in Section 3.1, the specific flowchart for implementing network printing is shown in Figure 9.

The implementation process is as follows:

Step1. CC set three parameters g, N and n, to randomly generate the private key x, and calculate

$X = g^x \bmod N, F_n$.

Step2. CC send three parameters g, N and n, and public key X to PC through the MQTT protocol.

CC = >PC:{ X, g， N， n}

Step3. PC randomly generates its own private key y and calculates Y = gen (g,y,N) based on the g, N transmitted by CC, Y serves as the public key of the PC; Simultaneously calculating encryption key G.

Step4. PC passes the public key Y to CC through the MQTT protocol.

PC = >CC:{Y}

Step5. CC calculates the encryption key based on the Y transmitted from the PC.

$K = Y^x \bmod N = g^{xy} \bmod N$

Step6. CC input printing data, calculate $Em = E_k(M) \times F_n$ through key K and F_n, then send {E1, E2,E3} to PC, EC and MCS respectively.

CC- > PC:{E1}, CC- > EC:{E2}, CC- > MCS:{E3}

Step7. PC receives E2 and E3, merges them into Em and calculates $Mn = D_G\ (Em \times F_n^{-1})$ through keys G and F_n, as shown in formula (22) , compare M1, M2, M3 and vote for M.

Step8. Finally, the PC outputs to the PT via USB for printing.

4. Experimental analysis

4.1. Experimental tool

In order to simulate attacks on network printers, during the testing process, we used the printer intrusion tool kit PRET. PRET is an automated program based on Python language that can simulate various attack tests on the target printer. In actual use, it is necessary to install the PRET third-party components as follows:

```
# pip install colorama pysnmp
# pip install win_unicode_console
# apt-get install imagemagick ghostscript
```

The format of the PRET command is as follows:

```
usage: pret.py [-h] [-s] [-q] [-d] [-i file] [-o file] target {ps,pjl,pcl}
```

Among them, the PRET command position arguments are shown in Table 1.

Table 1. PRET positional arguments.

Arguments	Describe
Target	Printer device or hostname
{ps,pjl,pcl}	Printing language

The PRET command optional arguments are shown in Table 2.

Table 2. PRET optional arguments.

Arguments	Describe
-h, --help	show this help message and exit
-s, --safe	verify if language is supported
-q, --quiet	suppress warnings and chit-chat
-d, --debug	enter debug mode (show traffic)
-i file, --load file	load and run commands from file
-o file, --log file	log raw data sent to the target

The PRET command can be used to conduct various attacks on network printers, including DoS attacks, authorization, print task control, remote code operation, information leakage, information tampering, etc. These attacks can be used to test the anti-attack ability of remote network printing on network printers.

4.2. Experiment and comparative analysis

Experimental comparison subjects: 1) Group 1: Local Network Printing (LN-PT), 2) Group 2: Remote Network Printing (RN-PT) and Group 3: FIB-DH Scheme Network Printing (FD-PT). Experimental address: In the IoT laboratory of the School of Artificial Intelligence. The system sets two parameters: 1) Set the number of network printing attacks using the PRET tool to simulate six network types of attacks: DoS attacks, authorization, print task control, remote code operation, information leakage and information tampering. The number of attacks for each type is shown in Table 3, with a total of 100 attacks. 2) Number of printing tasks, each task requires printing 10 2-page documents. In the experimental comparison, the number of printing tasks varies, and the accuracy of printing tasks is evaluated as the task burden increases.

Table 3. PRET simulation attacks on printers.

Attack type	Number of attacks
DoS attacks	15
Authorization	15
Print task control	15
Remote code operation	15
Information leakage	20
Information tampering	20

The first group (Group1): Local Network Printing (LN-PT), under the same experimental conditions, achieves document printing through user computers on a local area network. The number of printing tasks is constantly changing, and it also simulates attacks on printers through PRET, ultimately comparing the accuracy of printing.

The second group (Group2): Remote Network System (RN-PT), under the same experimental conditions, remotely prints documents through user computers on the Internet. The number of printing tasks is constantly changing, and while printing, PRET is also used to simulate attacks on printers, ultimately comparing the accuracy of printing.

The third group (Group3): FIB-DH scheme network printing (FD-PT), under the same experimental conditions, remotely printing documents through user computers on the Internet. The number of printing tasks is constantly changing, and while printing, PRET simulation is also used to attack the printer, ultimately comparing the accuracy of printing.

1) Comparison of printing accuracy

By conducting network printing comparative experiments on three groups of systems, the task size varied from 100 to 300 with an increment level of 20. Finally, the comparative results were obtained as shown in Table 4. From the table, it can be seen that the FIB-DH network printing has the best printing accuracy under the same task.

Table 4. Comparison of network printing accuracy with task changes.

Number of printing tasks	Local network printing accuracy (LN-RT)(%)	Remote network printing accuracy (RN-PT)(%)	FIB-DH network printing accuracy (FD-PT)(%)
100	92.0	90.1	98.2
120	92.2	90.3	98.3
140	92.3	90.4	98.4
160	92.4	90.6	98.6
180	92.6	90.7	98.7
200	92.8	90.9	98.9
220	92.9	91.1	99.0
240	93.0	91.3	99.1
260	93.2	91.6	99.3
280	93.3	91.8	99.4
300	93.5	92.1	99.6

When we set the number of printing tasks to 100, 200 and 300, we compared the three groups of network printing. The bar chart is shown in Figure 10, which shows that FIB-DH network printing has more advantages.

The comparison of the printing accuracy of three sets of networks under different tasks is shown in Figure 11. From this line breaking chart, it can be clearly seen that the FIB-DH scheme has the best network printing accuracy under different tasks, with an improvement of about 6%.

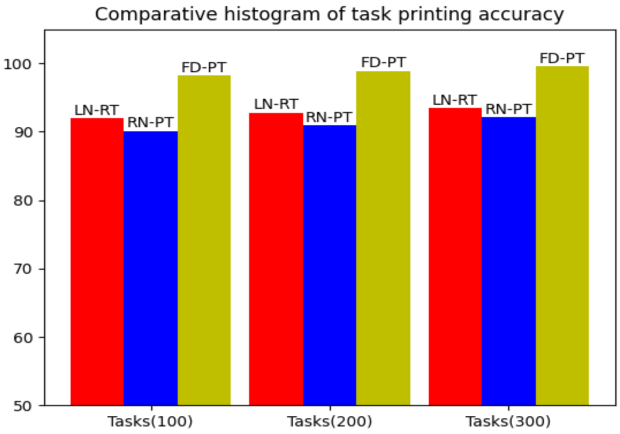

Figure 10. Comparative histograms of three groups of network printing accuracy.

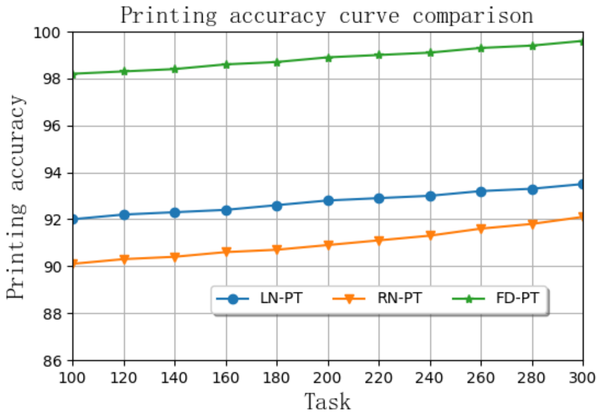

Figure 11. Network printing accuracy curve comparison with task change.

2) Comparison of printing time cost

Similarly, we set the number of printing tasks to 100, 200 and 300, and compare the time cost of three sets of network printing, the comparison results are shown in Table 5. Due to the fact that LN-RT is printed on a local network, the printing time cost is obviously lower than RN-PT and FD-PT. Therefore, we focus on comparing FD-PT and RN-PT. From the table, it can be seen that the printing time cost of FD-PT is slightly higher than that of FD-PT, and the difference is not significant, about 3%.

Table 5. Comparison of network printing time cost with task changes.

Number of printing tasks	Local network printing accuracy (LN-RT)(Min)	Remote network printing accuracy (RN-PT)(Min)	FIB-DH network printing accuracy (FD-PT)(Min)
100	8.4	10.5	11.2
200	16.6	20.9	21.8
300	25.8	30.8	31.7

Summary of the experiment: 1) Compared the important indicator of network printing accuracy under three schemes, the FIB-DH scheme improved the network printing accuracy by about 6% under network attacks, making it more secure. 2) The FIB-DH scheme also has certain shortcomings in network printing. From the perspective of printing time cost, the FIB-DH scheme does not have an advantage in network printing, increasing by about 3% compared to others, but improving the printing accuracy by about 6%. In order to improve the security of network printing, it is inevitable to increase system complexity, and adding some printing time cost is not considered.

5. Conclusions and future works

Network printers are a combination of traditional printers and internet applications, which perfectly solves the interconnection and sharing problems in office work and meets the office needs of government agencies. However, network printing poses security risks, and information leakage and network attacks may occur through network printing. In this article, we propose a FIB-DH data encryption technology scheme based on edge cloud collaboration to address the security of network printing, especially the risk of leakage during data transmission. By mining the characteristics of third-order Fibonacci matrices and combining Diffie-Hellman encryption technology, edge cloud collaboration is used to achieve the security of printed data. Through PRET tool simulation experiments, compared with conventional network printing, the accuracy of network printing data has been improved, effectively improving the security of network printing and preventing the leakage and tampering of printing information.

However, its technical scheme also has certain limitations. While improving network printing security, the complexity of its implementation has also increased. In future work, we will continue to compare and analyze privacy-protecting algorithms to improve their security while reducing the complexity of system implementation. This article can provide some reference for future research on network printing security models.

Use of AI tools declaration

The authors declare that they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This study was supported by the Natural Science Foundation Project of China (61976118), the Natural Science Foundation Project of Jiangsu Province (BK20180142), and the key topics of the “13th five-year plan” for Education Science in Jiangsu Province (B-b /2020/01/18).

Conflict of Interest

All authors declare no conflicts of interest in this paper.

References

1. Y. Zhou, Z. R. Lu, Analysis of security hazards and protection strategies for network printers, *Network Secur. Technol. Appl.*, **11** (2020), 2–8. https://doi.org/10.3969/j.issn.1009-6833.2020.11.099
2. L. M. Fan, Network security protection of network printers, *Dig. Technol. Appl.*, **7** (2016), 1–7.
3. S. B. Li, Q. B. Pan, Y. Zhao, Research on security analysis and situation awareness technology of networked printers, *Network Secur. Technol. Appl.*, **10** (2021), 2–8. https://doi.org/10.3969/j.issn.1009-6833.2021.10.016
4. S. X. Chen, Research on network printer information security, *Manage. Inf.*, **21** (2018), 3–11.
5. S. L. Li, Research on network printer security risk analysis and prevention technology, *Police Technol.*, **5** (2022), 65–68. https://doi.org/10.3969/j.issn.1009-9875.2022.05.016
6. L. Li, S. Y. Chen, Z. Y. Yang, Research on network printer security and protection suggestions, *Electron. Prod. World*, **3** (2019), 58–61.
7. Z. X. Yan, H. B. Hou, Design of a security enhanced printer based on Trusted Computing 3.0, *J. Inf. Secur. Res.*, **5** (2023), 1–8.
8. T. Feng, H. R. Bei, Evaluation and improvement of Internet printing protocol based on HCPN model detection method, *Appl. Sci.*, **13** (2023), 10–25. https://doi.org/10.3390/app13063467
9. F. S. Sulaiman, H. B. Seta, N. Falih, Exploitation prevention on network printer with signature-based Suricata on PfSense, in *2021 Internation*al Conferenc*e on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*, (2021), 35–39. https://doi.org/10.1109/ICIMCIS53775.2021.9699133
10. M. Huang, N. Zhao, Cloud-based portable IoT Inkjet printer, in *2019 4th International Conference on Communication and Information Systems (ICCIS)*, (2019), 70–74. https://doi.org/10.1109/ICCIS49662.2019.00018
11. Q. T. Nguyen, A. Mai, L. Chagas, N. Reverdy-Bruas, Microscopic printing analysis and application for classification of source printer, *Comput. Secur.*, **108** (2021), 102320. https://doi.org/10.1016/j.cose.2021.102320
12. S. Kakade, A. Mulay, S. Patil, IoT-based real-time online monitoring system for open ware FDM printers, *Mater. Today Proc.*, **2** (2022), 363–367. https://doi.org/10.1016/j.matpr.2022.07.210
13. Z. Cai, Y. Si, J. Zhang, L. Zhu, P. Li, Y. Feng, Industrial Internet intrusion detection based on Res-CNN-SRU, *Electronics*, **12** (2023), 3267. https://doi.org/10.3390/electronics12153267
14. G. Xiang, C. Shi, Y. Zhang, An APT event extraction method based on BERT-BiGRU-CRF for APT attack detection, *Electronics*, **12** (2023), 3349. https://doi.org/10.3390/electronics12153349
15. M. Kim, T. Shon, Digital Forensics for e-IoT devices in smart cities, *Electronics*, **12** (2023), 3233. https://doi.org/10.3390/electronics12153233
16. A. S. Almuflih, K. Popat, V. V. Kapdia, M. R. Qureshi, N. Almakayeel, R. E. Mamlook, Efficient key exchange using identity-based encryption in multipath TCP environment, *Appl. Sci.*, **12** (2022), 7575. https://doi.org/10.3390/app12157575
17. L. D. Wang, H. Tu, W. R. Hou, Research on printer security risk analysis and information protection framework, *Network Secur. Technol. Appl.*, **6** (2023), 140–142. https://doi.org/10.3969/j.issn.1009-6833.2023.06.063

18. G. Shi, S. Li, Analysis of printer security risks and prevention, *Confident. Sci. Technol.*, **76** (2017), 26.
19. W. L. Wang, Research and implementation of network printing monitoring based on IPP protocol, *J. Bohai Univ. Natl. Sci. Edition*, **25** (2004), 4–10.
20. H. Y. Xu, Application of TCP/IP protocol stack in embedded systems-Research and implementation of IPP network printing protocol, *J. Jiangnan Univ.*, **8** (2023), 27. https://doi.org/10.7666/d.y968159
21. G. Y. Lee, S. H. Cho, The generalized pascal matrix via the generalized Fibonacci matrix and generalized pell matrix, *Korean Math. Soc.*, **45** (2008), 479–491. https://doi.org/10.4134/JKMS.2008.45.2.479
22. S. Chen, Z. Wang, The general term and property of the five order Fibonacci series, *J. Hainan Norm. Univ. China*, **12** (2014), 241–245. https://doi.org/10.1002/cjoc.201400011
23. X. G. Xie, Discussion and application of Fibonacci matrix, *Sci. Technol. Inf.*, **24** (2008), 2. https://doi.org/10.3969/j.issn.1001-9960.2008.24.204
24. L. X. Peng, Properties and applications of third-order Fibonacci sequence, *J. Putian Univ.*, **5** (2006), 5. https://doi.org/10.3969/j.issn.1672-4143.2006.05.002
25. Z. H. Chen, Q. Li, Improved PBFT consensus mechanism based on K-medoids, *Comput. Sci.*, **46** (2019), 101–107. https://Doi.org/10.11896/jsjkx.181002014
26. C. Feng, Q. Zhang, C. J. Tang, A reliable Diffie-Hellman key exchange protocol automatic proof, *J. Commun. China*, **12** (2011), 119–123. https://doi.org/10.3969/j.issn.1000-436X.2011.10.015
27. E. Järpe, An alternative Diffie-Hellman protocol, *Cryptography*, **4** (2020), 5. https://doi.org/10.3390/cryptography4010005
28. R. Flores-Carapia, V. M. Silva-García, M. A. Cardona-López, A dynamic hybrid cryptosystem using chaos and diffie–hellman protocol: An image encryption application, *Appl. Sci.*, **13** (2023), 7168. https://doi.org/10.3390/app13127168
29. Z. X. Yang, Y. Q. Bao, Y. Liu, Q. Zhao, H. Zheng, W. B. Xu, Lightweight blockchain fuzzy decision scheme through MQTT and Fibonacci for sustainable transport, *Math. Biosci. Eng.*, **19** (2022), 11935–11956. https://doi.org/10.3934/mbe.2022556
30. M. Chen, A composable authentication key exchange scheme with post-quantum forward secrecy, *J. Comput. Res. Develop.*, **57** (2020), 2158–2176. https://doi.org/10.7544/issn1000-1239.2020.20200472
31. J. Samandari, C. Gritti, Post-quantum authentication in the MQTT protocol, *J. Cybersecur. Priv.*, **3** (2023), 416–434. https://doi.org/10.3390/jcp3030021
32. Y. Q. Bao, H. Zheng, Q. Zhao, Development and practice of mobile Internet experimental platform system, *J. Int. Technol.*, **23** (2022), 207–214. https://jit.ndhu.edu.tw/article/view/2678
33. S. Choi, J. Cho, Novel feature extraction method for detecting malicious MQTT traffic using Seq2Seq, *Appl. Sci.*, **12** (2022), 12306. https://doi.org/10.3390/app122312306

34. A. Alzahrani,T. H. Aldhyani, Artificial intelligence algorithms for detecting and classifying MQTT protocol Internet of Things attacks, *Electronics*, **11** (2022), 3837. https://doi.org/10.3390/electronics11223837
35. P. Kocher, Timing attacks on implementations of Diffie-Hellman, RSA DSS and other systems, *Adv. Cryptol.*, **1109** (1996), 104–113. https://doi.org/10.1007/3-540-68697-5_9