Research

Internet of things encryption technology combining elliptic curve cryptosystem, hash function, and RFID-based authentication

Bin Zheng[1]

Received: 31 August 2024 / Accepted: 9 April 2025
Published online: 23 April 2025

Abstract

As an important means of connecting the physical world and the digital world, the reliability and security of the Internet of Things network are key issues. To raise the security of Internet of Things data, a research proposes an encryption technique that combines elliptic curve cryptosystem and hash functions. In this process, the radio frequency identification system is used as the central element for data encryption, with the elliptic curve cryptosystem employed to secure the transmitted data. Non-adjacent scalar representations are used to reduce the expected running time of scalar multiplication, and a bidirectional authentication protocol for Internet of Things encryption is designed using Hash functions. The experimental results showed that in the communication overhead test, the research method had a communication overhead of 242 bits when the Hash function output length was 40 bits in server communication. When analyzing the success rate of intercepting abnormal data access behavior, the research method achieved a success rate of 99.1% when the host file size was 100 Kb. In the analysis of scalar multiplication operation time, the research method only took 18 ms when the output length of the Hash function reached 340bits in a local area network environment. This illustrates that the raised method has a good encryption effect on the Internet of Things and can effectively ensure the security of Internet of Things communication. The research is expected to provide certain technical support for the development of the Internet of Things.

Highlights

(1) An encryption method combining elliptic curve encryption and hash function is proposed to improve the security of IOT.
(2) A two-way authentication protocol is designed to verify identity to effectively prevent man in the middle attack.
(3) Non adjacent scalar algorithm is introduced to optimize ECC operation and improve operation speed.

Keywords Elliptic curve cryptosystem · Internet of Things · Encryption · Hash function · Radio frequency identification

✉ Bin Zheng, zhengb8565@163.com; zhengb@bjou.edu.cn | [1]Affiliated College, Beijing Open University, Beijing 100000, China.

1 Introduction

Internet of Things (IoT) technology collects data through sensors and transmits it wirelessly to servers for processing and analysis. The application of IoT technology has greatly improved production efficiency and enhanced people's quality of life [1]. But with the popularization of the IoT, more and more security issues have arisen. Ensuring the security of IoT devices has become a critical issue in current technological development. The security issues of IoT devices mainly focus on the security of data transmission and storage. Currently, mainstream encryption technologies have certain limitations in the IoT environment [2, 3]. For example, although symmetric encryption algorithms have high computational efficiency, key management is complex and susceptible to man in the middle attacks. Although asymmetric encryption algorithms have high security, they have high compute requirements and are not suitable for resource-constrained IoT devices [4]. Some scholars have also designed specialized encryption techniques for the IoT, such as symmetric encryption, which has high computational efficiency and is suitable for quickly encrypting large amounts of data. However, key management is complex and susceptible to the risk of key leakage [5]. The elliptic curve cryptosystem (ECC) utilizes points on the elliptic curve for encryption and decryption operations, providing high security with smaller key lengths. However, ECC also faces the problem of complex scalar multiplication operations in practical applications. Hash functions can convert data of any length into fixed length hash values, and due to their unidirectionality, it is almost impossible for different input data to produce the same hash value, making Hash functions useful for verifying data uniqueness. In this context, research attempts to innovatively combine ECC and hash functions to optimize the encryption and authentication processes in the IoT encryption process, reduce computational complexity, and enhance confidentiality performance, to provide certain technical references for information security.

2 Related works

The IoT is widely used in people's daily lives, and its security issues have received great attention. Relevant scholars have proposed research on encryption technology for the IoT. Pu proposed a user-friendly Paeks scheme that completely avoided bilinear pairing operations when generating keyword ciphertexts and trapdoors. The results showed that compared with most existing classical public key encryption schemes with keyword search, this scheme significantly reduced computational overhead, and had better performance and security [2]. Zhu proposed a multi-class deep learning model called cost matrix spatiotemporal neural network for abnormal and encrypted IoT traffic, and built the model using multiple datasets. Compared with existing methods, this method had good performance in accuracy, precision, recall, and false positive rate [6]. Khayyat developed a new blockchain enabled shark odor optimization model to address security encryption issues in the IoT environment. This model employed composite chaotic mapping incorporated into staged logic and tent maps to pre-process the images and develop the variables required for Arnold mapping. This model stores encrypted pixel values in the image on the blockchain. This ensures the security and privacy of the image [7]. Gupta proposed an efficient method for encrypting images based on combining watermarking and cryptographic techniques. This method was based on two-level security, using a watermark scheme based on discrete wavelet transform in the first layer, and efficient image encryption techniques based on logistic chaotic mapping and crossover in the other layer. The outcomes indicated that the raised method improved security by enhancing encryption effectiveness [1]. Hedayati raised a data compression algorithm for image encryption to address the issue of low data rates in IoT devices. This algorithm encrypts image data in a single pass using scan-based block compression and selective pixel encryption methods. The outcomes showed that compared with existing algorithms, this algorithm reduced computational complexity and data volume, resulting in a decrease in device power consumption and packet rate [3].

Regarding the encryption technology of the IoT, scholars have proposed research on ECC. Kalaiarasi proposed a new parallel structure for elliptic curve scalar multiplication based on an improved Lopez-Dahab-Montgomery algorithm. It performed affine to projection transformation, and added and doubled points in the main loop during the process. Compared with existing technology, the reconstruction process reduced two multiplications [8]. Bashir proposed an improved ECC algorithm for asymmetric key problems. In this novel public key algorithm, the thought chaotic sequence was used to spread the image pixels, and the pixel values were used to arrange the image instead of the chaotic sequence. Simulation and security analysis showed that this algorithm is efficient, can resist various attacks, and has good prospects for practical use [9]. To address data security issues in wireless sensor networks, Ametepe AFX proposed a robust encryption scheme based on advanced encryption standards. The mapping technique involved the conversion of the plaintext into a sequence of points on an elliptic curve, before the arithmetic operations were performed to obtain the password. The outcomes indicated that the computation encryption process had a short running time, low memory usage, and low energy consumption [10]. Ye designed an advanced 3D continuous chaotic system based on password security problems. The system employed ImproBsys to implement compressive sensing and public key elliptic curve dual image encryption algorithm. The results indicated that this method could improve execution speed [11]. Prasad raised an asymmetric image encryption technique based on elliptic curves to address the issue of content security in digital images. The sender first put the pixel data together and converted it into a large amount of data. The sender used chaotic systems and ECC to encrypt large integers and created encrypted images using the encrypted large integers. Simulation data showed that the proposed algorithm exhibited excellent security and high efficiency [12].

Gao M and Lu YB proposed an ultra-lightweight authentication protocol based on Radio frequency identification (RFID) technology to solve the encryption problem in the Internet of Things. The protocol realizes the mutual authentication between devices by using only bit-by-bit operation, and solves the problems of high computational complexity and large storage requirements in traditional protocols. Performance evaluation shows that the protocol has superior performance in terms of computing costs, storage requirements and communication costs, and improves the security and efficiency of iot devices [13]. Lee et al. proposed a lightweight cloud computing authentication protocol based on RFID technology to solve the encryption and efficiency problems in the Internet of Things, and applied to electronic health systems. In order to solve the problem that RFID system has limited computing power and traditional encryption system is difficult to use, a physical non-cloning function is used to generate authentication keys, collect patients' physiological data through RFID and transmit it securely. This protocol improves efficiency through lightweight operation and improves the overall performance and security of the ehealth system [14]. Kumar et al. proposed an ultra-lightweight blockchain authentication protocol based on RFID technology to address encryption and supply chain security issues in the Internet of Things, and applied to supply chain management in the 5G mobile edge computing environment. The protocol combines blockchain technology to ensure data security, transparency and anti-counterfeiting, solving the problem of the safe transfer of goods in the supply chain. The results show that the proposed method is superior to other related protocols in calculation and communication costs, and improves the security and efficiency of the supply chain [15].

In summary, although there have been studies combining ECC and IoT encryption technology, there are still issues such as long running time, high memory usage, and high energy consumption. In view of this, research attempts to design an optimized IoT encryption technology based on ECC and combined with Hash functions, to provide certain technical support for the secure operation of the IoT. The innovation of the research lies in the proposed authentication protocol based on RFID and blockchain, which solves the security and efficiency problems of traditional RFID authentication in the supply chain. First of all, the combination of blockchain technology and RFID improves the transparency and tamper-proof ability of data transmission, avoiding the security risks of centralized databases. Secondly, a lightweight encryption algorithm is designed that uses rotation operations to ensure efficient operation on resource-constrained devices. Finally, security analysis verifies that the protocol can defend against a variety of attacks, and is superior to existing protocols in computing and communication costs, adapting to large-scale device access in the 5G environment.

3 Design of encryption technology combining elliptic curve cryptosystem and hash function

3.1 Optimization of IoT encryption technology based on elliptic curve cryptosystem

RFID as an important sensing layer data acquisition technology in the IoT, takes a decisive part in the security of the IoT. Moreover, the data transmission process of RFID systems mostly occurs in open wireless networks, which pose a high risk of interception. Therefore, high-quality encryption technology is needed to protect the data. The working process of the RFID system is denoted in Fig. 1.

As shown in Fig. 1, the IoT RFID system mainly contains three modules: the central data system, the reader, and the electronic tag. In both readers and electronic tags, there are power supply modules, antenna modules, and RF modules. During operation, clock data, energy, and electronic tag data are exchanged through each module. After the reader obtains the electronic tag data, it is transmitted to the central data system by the read–write module. To

Fig. 1 Working process of RFID system

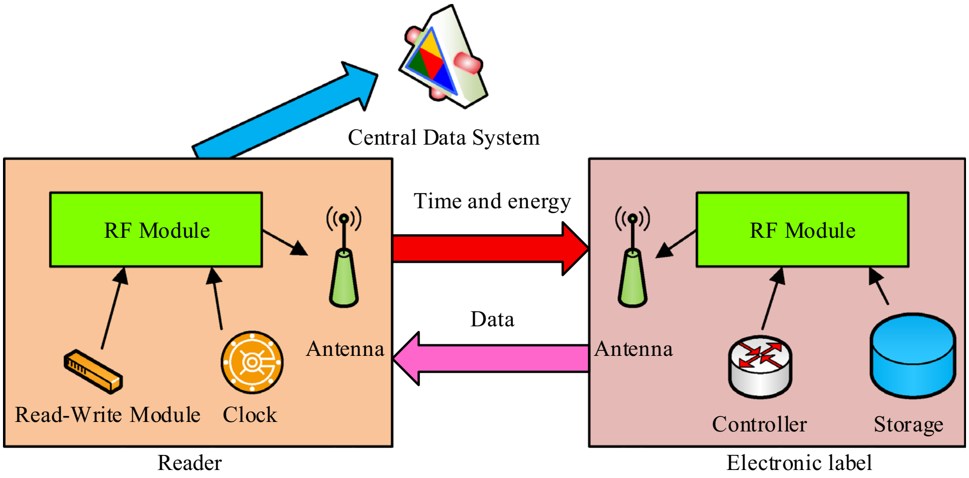
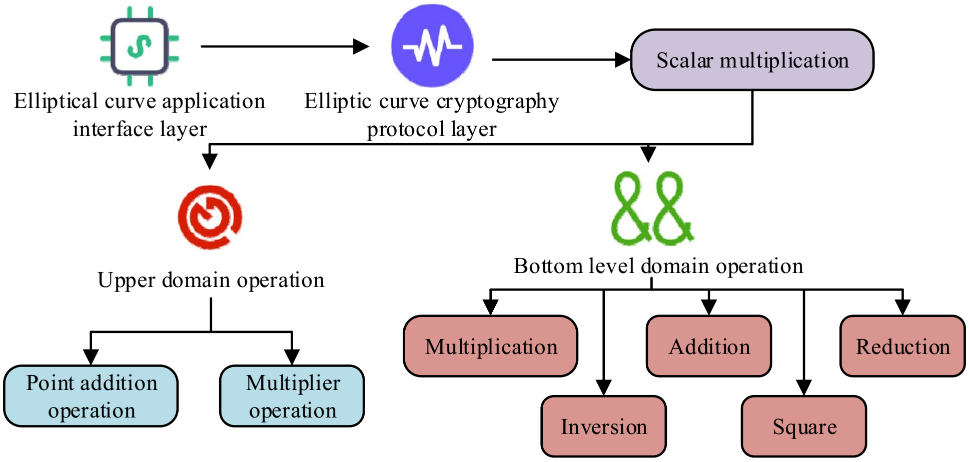


Fig. 2 The working structure of elliptic curve cryptosystem



adapt to the resource limited environment of most RFID systems, research is being conducted on using ECC for data encryption. The working structure of ECC is shown in Fig. 2.

In Fig. 2, during operation, the ECC system uses the application interface layer as the topmost structure, connects downwards to the cryptographic protocol layer, and then enters the scalar layer structure. The scalar multiplication structure can be broken into two parts: upper domain operations and stratigraphic domain operations. Upper domain operations include point addition and multiplication operations, while stratigraphic domain operations include more basic operations such as reduction, inversion, addition, sum of squares, and multiplication. As an efficient public key cryptosystem, elliptic curve encryption relies on the computational efficiency of elliptic curve scalar multiplication. The study introduces the Non-Adjacent Form scalar multiplication algorithm to optimize and improve elliptic curve scalar multiplication, using non-adjacent forms of scalar representation to reduce the expected running time of scalar multiplication [16]. Non-Adjacent forms are used to represent scalars in a non-adjacent Form and have a special property: it eliminates consecutive 1 s in the binary representation, allowing algorithms to skip the addition of certain points. This reduces the number of actual point operations required, especially compared to standard binary methods. In the binary calculation of scalar multiplication in ECC, the scalar multiplication calculation is shown in Eq. (1).

$$Q = [d]P = \sum_{i=0}^{l} d_i 2^i \times P \tag{1}$$

In Eq. (1), Q represents scalar multiplication. d stands for large integer scalar. l represents scalar binary length. P represents a point on a bounded elliptic curve. The scalar multiplication iteration is shown in Eq. (2).

$$\begin{cases} Q_1 = 2Q_0 + d_{l-1}P \\ Q_2 = 2Q_1 + d_{l-2}P \\ \vdots \\ Q_l = 2Q_{l-1} + d_0P \end{cases} \tag{2}$$

The Non-Adjacent Form scalar multiplication algorithm reduces Hamming weight and eliminates the precomputation step. The algorithm's computational complexity is denoted in Eq. (3).

$$\beta = \frac{l * A}{3} + l * D \tag{3}$$

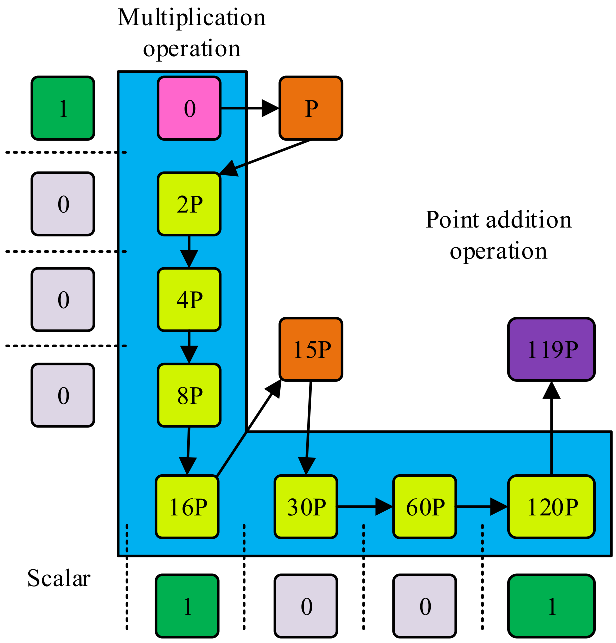
In Eq. (3), β refers to the computational complexity of the algorithm. A represents point addition operation. D stands for multiple point operation. Taking the setting scalar as 119 as an example, the calculation of Non-Adjacent Form scalar multiplication algorithm is shown in Fig. 3.

In Fig. 3, the Non-Adjacent Form scalar multiplication algorithm performs a dot addition operation at runtime, corresponding to a scalar of 1. Four consecutive multiplication operations are performed, with all scalars being 0 during the process. Then it completes a dot addition operation, and the scalar will change to 1 and the dot multiple will change to 15. 3 multiplication operations are performed again to increase the dot multiple to 120 times, and finally one dot addition operation is used to make the dot multiple reach 119 of the set scalar, resulting in a final scalar of 1. In the process of scalar conversion, the Non-Adjacent Form of the scalar is generated bit by bit. To accelerate the speed of scalar generation, a calculation process is studied to establish a single simultaneous generation of two bit scalars. In ECC, scalar multiplication algorithm replaces modular operation with bit operation and division operation with shift operation to improve computational efficiency. The multi-bit generation algorithm avoids modular operations, subtraction, and division in traditional algorithms, and only implements the operation process through bit operations and shift operations, reducing the amount of operations by about half. Moreover, the amount of addition operations has also been reduced to one-fifth of the original. Furthermore, it achieves a theoretical increase in computational efficiency of nearly 50%.

3.2 Design of IoT encryption authentication protocol combining Hash function

While using ECC to encrypt data transmitted in the IoT ensures that the content of the transmitted data is protected, it does not fully address the integrity of the data during transmission. Specifically, ECC focuses on securing the data itself

Fig. 3 Non-Adjacent Form scalar multiplication algorithm calculation



but overlooks the operational process involved in transmitting this data, which could expose the system to potential risks. Therefore, encryption authentication protocols are essential to safeguard against unauthorized users accessing or tampering with the system. These protocols are critical in reducing the risk of data manipulation and ensuring that only designated users can authenticate and access the system [17]. To enhance the security of IoT communication, this research proposes a bidirectional authentication protocol combining ECC and Hash functions. This protocol ensures mutual authentication, meaning both the client and the server must verify each other's identity. By implementing mutual authentication, it effectively mitigates the risk of man-in-the-middle attacks, where an unauthorized third party could masquerade as either the client or the server. The protocol not only ensures the security of data transmission but also protects the integrity of the authentication process itself, making it a vital component in securing IoT networks. The study specifically considers the central data system and the reader as a cohesive unit, and the authentication process is illustrated in Fig. 4.

In Fig. 4, during protocol authentication, the authentication process is initialized first. After assigning an identifier and saving the reader base point, the reader selects a random number as its private key and generates the corresponding public key. In the authentication phase, the reader initially generates a random number and calculates a point. Subsequently, a request message, along with the aforementioned point, is transmitted to the target tag. Following the reception of said request, the tag generates an additional random number and computes two points. Using the calculation results, the tag generates a temporary key and an encrypted message, and sends these two points and the encrypted message back to the reader. The temporary key calculation is shown in Eq. (4).

$$K_T = r_T M_1 + r_T R_P \tag{4}$$

In Eq. (4), K_T represents the temporary key. r_T represents the first random number generated. m_1 represents the scalar multiplication result of a random number generated by the reader first. R_p stands for reader public key. The calculation of encrypted information is shown in Eq. (5).

$$C = tid_i + H\left(m_2, K_T\right) \tag{5}$$

In Eq. (5), C represents encrypted information. tid_i stands for tag identity identifier. H stands for Hash function. m_2 represents the scalar multiplication result of a random number generated by the reader for the second time. After receiving the information, the reader calculates a temporary key and attempts to decrypt the encrypted information to obtain the identity identifier of the tag. If decryption is successful, the reader verifies the identity identifier of the tag, returns tag related information, and calculates and sends an encrypted message to the tag. The scalar multiplication result of a random number generated by the reader for the third time is calculated as shown in Eq. (6).

$$m_3 = tid_i{\prime} \oplus H\left(\left[R_S\right]m_2\right) \tag{6}$$

In Eq. (6), m_3 represents the scalar multiplication result of a random number generated by the reader for the third time. R_S represents the reader private key. After receiving the encrypted message, the tag decrypts and verifies its

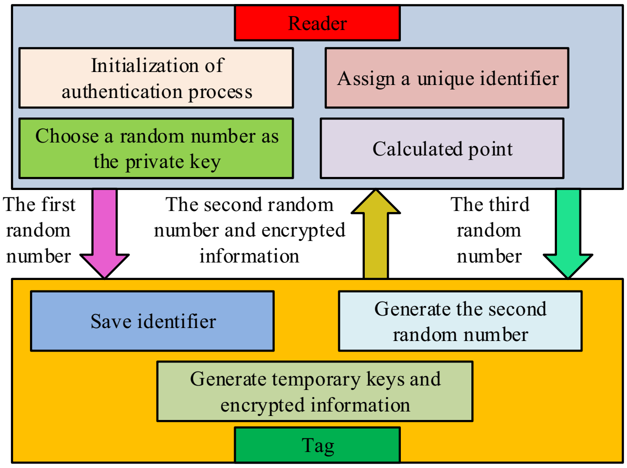

Reader
Initialization of authentication process
Assign a unique identifier
Choose a random number as the private key
Calculated point
The first random number
The second random number and encrypted information
The third random number
Save identifier
Generate the second random number
Generate temporary keys and encrypted information
Tag

Fig. 4 Protocol authentication process

content. If the verification is successful, the tag confirms that the reader is a legitimate server and completes the authentication process. To further ensure the security of the protocol, Burrows, Abadi, and Needham logic are introduced for formal analysis of the protocol, as shown in Fig. 5.

In Fig. 5, when conducting logical formal analysis, the first step is to describe the message exchange process in the protocol, including the messages sent and received by all parties in the protocol. The nest is to abstract the message exchange in the actual protocol and simplify it into logical expressions for logical reasoning. The facts or assumptions known at the beginning of the protocol are listed, such as the key knowledge and initial state of each party. The inference rules in Burrows, Abadi, and Needham logic are utilized to derive the security of message meaning rules, temporary value verification rules, belief rules, and freshness rules protocols. When conducting protocol proof, starting from the initialization assumption, it gradually derives the security objectives of the protocol, and each step of derivation is based on the outcomes and logical rules of the previous step. The protocol description is shown in Eq. (7).

$$\begin{cases} R \rightarrow T : \{Query, m_1\} \\ T \rightarrow R : \{m_2, C\} \\ R \rightarrow T : \{m_3\} \end{cases} \tag{7}$$

In Eq. (7), R represents the reader. T stands for label. *Query* represents the query request sent by the reader to the tag. The process of protocol idealization is shown in Eq. (8).

$$\begin{cases} R \triangleleft \left\{ m_2, \{tid_i, r_T, r_R, R_P\}_{tid_i} \right\} \\ T \triangleleft \left\{ m_1, \{r_T, tid_i\prime\}_{R_S} \right\} \end{cases} \tag{8}$$

In Eq. (8), r_R represents the generated second random number. The protocol objective is established as shown in Eq. (9).

$$\begin{cases} T| \equiv tid_i\prime \\ R| \equiv tid_i \end{cases} \tag{9}$$

The temporary verification rule during the reasoning process is indicated in Eq. (10).

$$\frac{P| \equiv \#(X), P| \equiv Q| \sim X}{P| \equiv Q| \equiv X} \tag{10}$$

In Eq. (10), X represents the entity content of a specific data item. The jurisdictional rules are shown in Eq. (11).

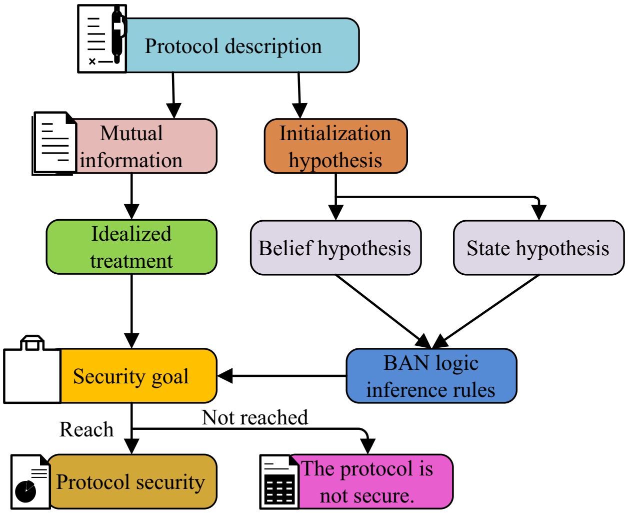


Fig. 5 Burrows, Abadi, and Needham's formal analysis of logic

$$\frac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X} \tag{11}$$

The freshness rule is shown in Eq. (12).

$$\frac{P|\equiv \#(X)}{P|\equiv \#(X, Y)} \tag{12}$$

In Eq. (12), Y represents the entity attribute. In the RFID system studied, the authentication process ensures the secure communication between the tag and the reader. First, when the reader sends a request, the tag generates a response through an encryption algorithm, usually based on a shared key or a physically unclonable function. The response of the tag is received and verified by the reader to ensure that the data is not tampered with or forged. If the tag authentication is successful, a secure communication channel may be established between the reader and the tag for data exchange. In the two-way authentication protocol, the reader will also generate a challenge and verify the response of the tag to ensure the legitimacy of the tag. Through lightweight encryption technology, the authentication process not only ensures security, but also adapts to the characteristics of limited computing resources of RFID devices. The complete protocol proof process is shown in Fig. 6.

In Fig. 6, when performing protocol proof, it is necessary to first provide a protocol description that includes a description of the information exchange process. Then is to abstract the message exchange in the protocol and convert actual messages into logical expressions. It lists the assumptions at the beginning of the protocol, especially the public and private keys of the reader and tag. Message meaning rules are utilized to analyze message meanings and freshness rules are utilized to verify message freshness, ensuring that messages are not intercepted before the current protocol runs. Belief rules are used to derive readers' and tags' beliefs or knowledge about certain facts. Starting from the initialization assumption using inference rules, it gradually deduces the protocol effect, and determines whether the protocol can achieve the security goal to determine security. During the operation of the IoT, research methods are used to encrypt data and real-time determine the integrity and effectiveness of encryption operations, achieving protection of the IoT system.

The proposed encryption authentication protocol combines ECC and hash function, which can effectively provide multiple security features. First, the two-way authentication mechanism ensures that the identities of both parties are verified, thereby effectively preventing man-in-the-middle attacks and preventing unauthorized third parties from masquerading as legitimate communication parties. Secondly, the protocol prevents replay attacks by introducing random numbers and hash values, ensuring that each communication is unique and timely. Data encryption and hash verification effectively prevent data tampering and forgery, ensuring that data is not tampered with or forged during transmission.

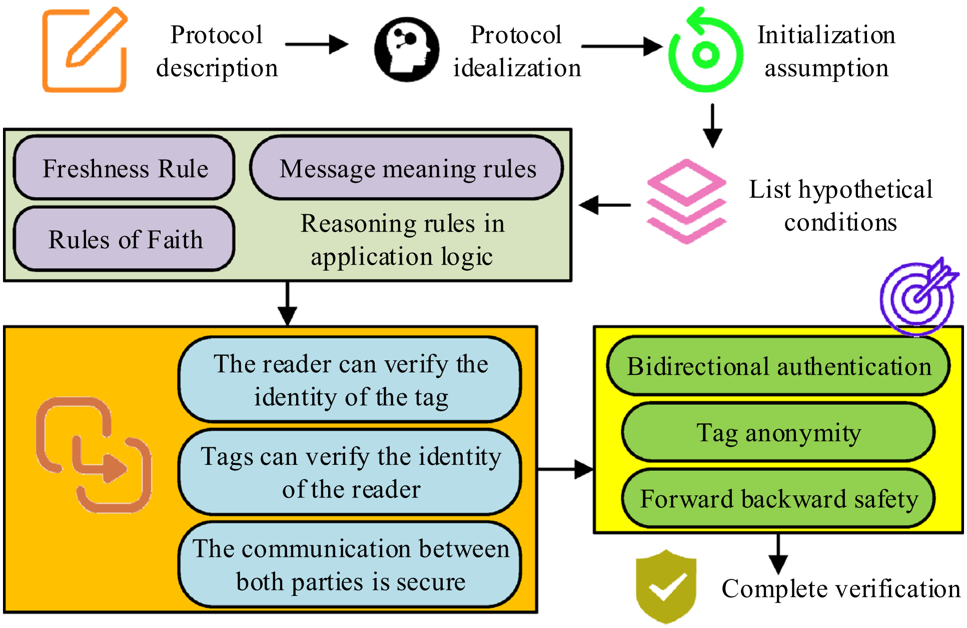

Protocol description
Protocol idealization
Initialization assumption
List hypothetical conditions
Freshness Rule
Message meaning rules
Rules of Faith
Reasoning rules in application logic
The reader can verify the identity of the tag
Tags can verify the identity of the reader
The communication between both parties is secure
Bidirectional authentication
Tag anonymity
Forward backward safety
Complete verification

Fig. 6 Protocol proof process

Table 1 Simulation of the experimental environment setting

Hardware configuration		Software configuration	
CPU	Intel(R) Core(TM) i5-13,490	Operating system	Windows 10 Professional
GPU	Nvidia GTX 4080	Elliptic curve standard	Secp256k1
RAM	32 GB DDR4 3200	Programming tools	IDEA
Storage device	Hard disk space 1 TB	Programming Language	JAVA

Table 2 Comparison of protocol security performance indicators

Safety performance indicators	Baptista Chaos [18]	Homomorphic encryption [19]	Attribute encryption [20]	Key management [21]	Elliptic hash
Bidirectional authentication	No	Yes	Yes	Yes	Yes
Anonymity	Yes	No	Yes	Yes	Yes
Forward backward safety	Yes	Yes	No	Yes	Yes
Anti counterfeiting attacks	Yes	Yes	Yes	No	Yes
Anti tracking attack	Yes	No	Yes	No	Yes

In addition, the high computational complexity of ECC enhances the system's resilience to denial-of-service attacks, reducing the risk of malicious attackers crippling the system with a large number of requests. By combining ECC and hash functions, the protocol ensures data privacy, integrity, and reliability, while resisting many common cyber attacks such as identity forgery, data tampering, and denial of service, providing a strong security guarantee for iot systems.

4 Analysis of the effectiveness of IoT encryption technology

4.1 Performance testing and security comparison of IoT encryption technology operation

To test the performance and analyze the security of the IoT encryption technology designed for research, a Windows 10 Professional experimental environment was built for testing. In the simulation environment studied, the specifications of RFID tags and readers are respectively: RFID tags are passive RFID tags, storage capacity is 256 bytes, support 13.56 MHz communication frequency (in accordance with ISO 15693 standard), and support ECC and hashing algorithm hardware acceleration; The RFID reader is a fixed type, supports a communication frequency of 13.56 MHz, is equipped with an ARM Cortex-M4 processor for encryption and authentication, and has a storage capacity of 1 MB, which is responsible for two-way authentication and encrypted communication with the tag. In the simulation process, the communication between the tag and the reader is based on the ISO 15693 standard. First, the reader issues an initialization request, including the random number and the unique identifier of the tag. After the tag is received, a random number is generated, and the temporary key is calculated and returned using ECC algorithm based on the UID and the random number. After authentication, the reader calculates the authentication information of the tag through the ECC algorithm and hash function, encrypts it, and sends it to the tag for verification. After successful authentication, both parties can begin a secure data exchange, with all data encrypted by ECC and integrity verified by a hash function. Each communication uses different random numbers and encryption keys to ensure the security of data transmission. The simulation environment is modeled using MATLAB/Simulink. The hardware configuration includes ARM Cortex-M4 processor with hardware-accelerated ECC, 256-byte label storage and 1 MB reader storage. The simulation tool simulates the authentication process between the label and the reader. The encryption speed, communication latency and attack resistance are analyzed to verify the validity and security of the proposed protocol. The experimental environment settings are indicated in Table 1.

During testing, the research method was be abbreviated as the Elliptic Hash method and compared with commonly used techniques such as Baptist Chaos, Homomorphic encryption, Attribute encryption, and Key Management. The protocol security performance involved in different methods was compared, as indicated in Table 2.

In Table 2, different methods had certain differences in the coverage of key security performance indicators. Baptista Chaos could balance anti-impersonation attacks and anti-tracking attacks, but lacked a certain degree of comprehensiveness in identity authentication. The lack of performance in anonymity and resistance to tracking attacks in Homomorphic encryption limited its application scenarios and made it difficult to be effectively used in public networks. Attribute encryption could resist attacks and complete bidirectional authentication, but it did not have sufficient forward backward security, which limits its application in complex data interaction scenarios. Key Management lacked sufficient coverage in terms of anti-counterfeiting and anti-tracking attack performance, resulting in the need to rely on other technologies for assistance in ensuring data security. Elliptic Hash had good coverage in terms of bidirectional authentication, anonymity, forward backward security, anti-counterfeiting attacks, and anti-tracking attacks, indicating that the research method has sufficient comprehensiveness. Communication overhead is the sum of encrypted data size, authentication information size, hash output size, random number/temporary key size. The communication overhead of different methods was tested, as shown in Fig. 7.

In Fig. 7, during communication overhead testing, the communication overhead of servers and tags using different methods increased with the length of the Hash function output. The increase in communication overhead is mainly caused by the change in the output length of the hash function, and a longer hash output requires more bits to be transmitted, resulting in an increase in overhead. In addition, the size of ECC encrypted data and temporary key generation during authentication also have an impact on the total overhead. Figure 7a shows that, in the server communication overhead test, Baptista Chaos' communication overhead increased to 727 bits when the hash function output length reached 120 bits. The server communication overhead of Homomorphic encryption increased relatively faster, with the communication overhead rising to 832 bits when the output length of the Hash function reached 120 bits. The communication overhead of Elliptic Hash was 242 bits when the output length of the Hash function was 40 bits, and it increased to 409 bits when the output length of the Hash function reached 120 bits. In Fig. 7b, in the tag communication overhead test, the increase rates of communication overhead for the four methods were relatively close. The communication overhead of Homomorphic encryption increased to 748 bits when the output length of the Hash function reached 120 bits. The communication overhead of Attribute encryption increased to 686 bits when the output length of the Hash function reached 120 bits. The communication overhead of Elliptic Hash increased to 443 bits when the output length of the Hash function reached 120 bits. This indicates that the research method has better communication resource conservation performance during runtime.

4.2 Analysis of the actual application effect of IoT encryption technology

To further determine the performance of the research method, the study applied the research method in practical IoT application scenarios and collected different data performances during application for analysis. Specifically, the study selected a typical smart city environment that contains multiple sensor devices, RFID tags, and data transmission modules. In this scenario, RFID tags are used for item tracking and authentication, while readers communicate with a central data system. Abnormal data access behavior may occur in the system, such as unauthorized devices trying to obtain or tamper with sensor data, or malicious third parties conducting man-in-the-middle attacks on communications. In this application scenario, the research method ensures the security of data transmission by implementing two-way authentication and ECC encryption between the RFID tag and the reader. During application analysis, the data collected includes the success

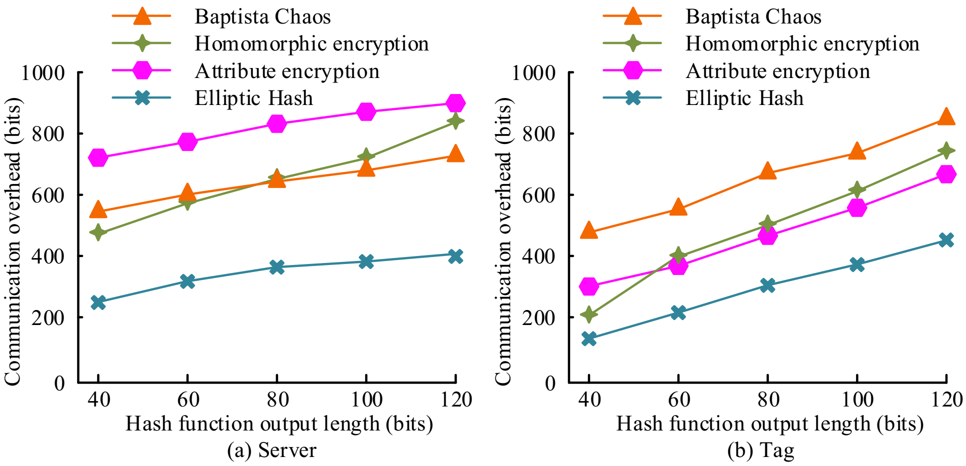


Fig. 7 Communication overhead testing

rate of successfully intercepting abnormal data access behavior, communication overhead, hardware operating load, and scalar multiplication operation time. In the study, the files were generated by iot devices and contained environmental monitoring data as well as encrypted information about the devices. The sender is an iot device and the receiver is a central data system or server. Whether a file contains abnormal data is determined by the preset security protocol and anomaly detection mechanism, such as whether the comparison data matches the normal range, or whether there is an encryption verification error. Abnormal data is intercepted by the monitoring system or intrusion detection system during file transmission, and the data is not tampered with through encryption authentication and identity authentication. The success rate of intercepting abnormal data access behavior was analyzed using different methods, as shown in Fig. 8.

In Fig. 8, the success rate of intercepting abnormal data access behavior using different methods decreased as the file size increased. The success rate of intercepting abnormal data access behavior refers to the ability of a system to effectively identify and block unauthorized access to or tampering with data in an iot environment. Specifically, interception refers to the system monitoring and blocking operations during communication that do not conform to the expected security behavior. Typically, these anomalies may include unauthorized devices attempting to access or modify data, or malicious actors tampering with data through man-in-the-middle attacks, for example. In the study, abnormal data refers to data that is not transmitted according to a legitimate protocol, such as data sent through an uncertified device or data that has been tampered with during transmission. This data can be inserted, modified or forged by attackers, threatening the security of iot systems. Figure 8a shows that the interception success rate of Homomorphic encryption on mobile devices was 99.2% when the file size was 100 Kb. The interception success rate dropped to 96.6% when the file size was 500 Kb. The interception success rate of Elliptic Hash was 99.6% when the file size was 100 Kb. The interception success rate dropped to 98.8% when the file size was 500 Kb. In Fig. 8b, on the host side, the interception success rate of Baptista Chaos was 98.5% when the file size was 100 Kb. The interception success rate dropped to 96.3% when the file size was 500 Kb. The interception success rate of Homomorphic encryption was 98.1% when the file size was 100 Kb. The interception success rate dropped to 96.5% when the file size was 500 Kb. The interception success rate of Elliptic Hash was 99.1% when the file size was 100 Kb. The interception success rate dropped to 98.3% when the file size was 500 Kb. This indicated that the research method had a stronger ability to intercept abnormal data access behavior, providing stronger security for the IoT. The burden on hardware caused by different methods when running was analyzed, as shown in Fig. 9.

In Fig. 9, different methods had different pressures on the processor during runtime. Figure 9a showed that Baptista Chaos achieved a maximum processor occupancy rate of 89% during a 1000 s run. During this period, 5% of computing processors had a usage rate of over 70%, 40% of computing processors had a usage rate of over 30%, and 90% of computing processors had a usage rate of over 15%. In Fig. 9b, Homomorphic encryption achieved a maximum processor occupancy rate of 71% during a 1000 s run. During this period, 5% of computing processors had an occupancy rate of over 50%, 30% of computing processors had an occupancy rate of over 30%, and 95% of computing processors had an occupancy rate of over 15%. In Fig. 9c, during the 1000 s run of Elliptic Hash, the highest processor occupancy rate reached 39%. During this period, 5% of computing processors had a usage rate of over 25%, 10% had a usage rate of over 20%, and 95% had a usage rate of over 12%. The research method had a lower burden on hardware devices during runtime and lower performance requirements for the applied devices. Parallel scalar multiplication (PSM), scalar

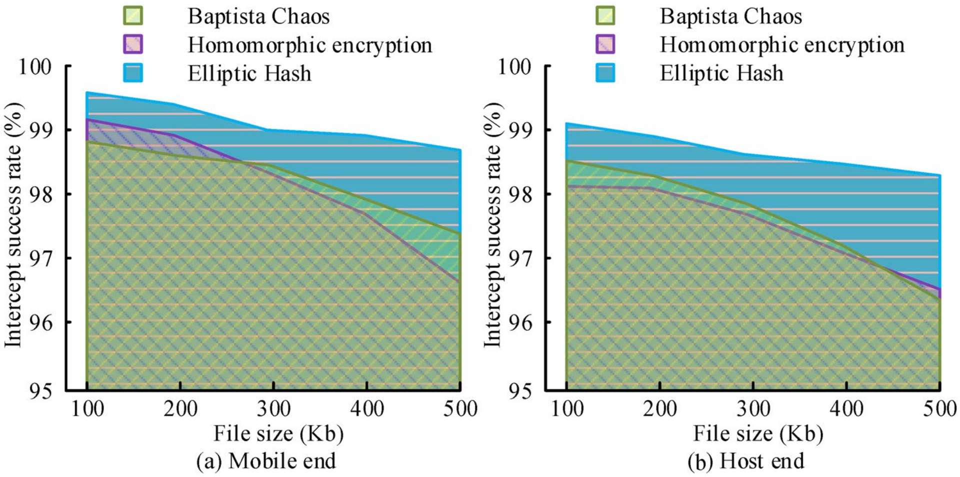


Fig. 8 Success rate of intercepting abnormal data access behavior

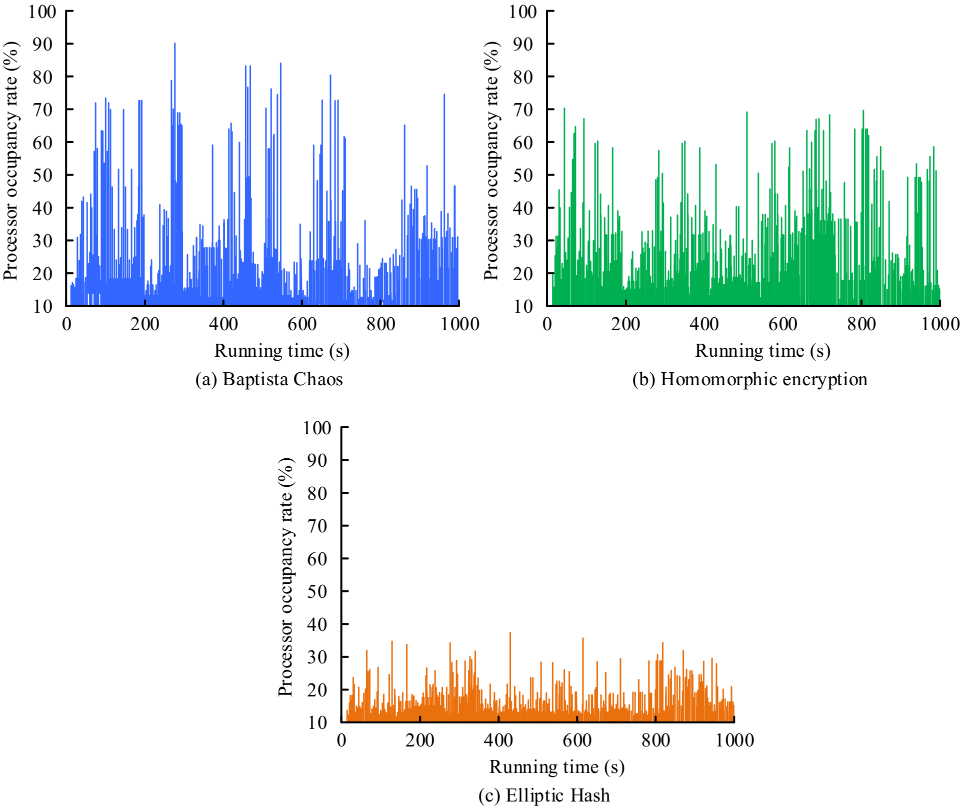


Fig. 9 Hardware operation burden analysis

conversion algorithm (SCA), and parallel scalar multiplication of elliptic curves (PSMEC) were selected for comparison, and the scalar multiplication operation time of the research methods was analyzed, as shown in Fig. 10.

In Fig. 10, the scalar multiplication time of different methods in different types of networks increased with the output length of the Hash function. Figure 10a showed that in a local area network environment, the computation time of PSM increased to 57 ms when the output length of the hash function reached 340bits. The computation time of SCA increased to 63 ms when the output length of Hash function reached 340bits. The computation time of PSMEC increased to 46 ms when the output length of the Hash function reached 340bits. The increase in computation time of Elliptic Hash was slower compared to other methods, with a computation time of only 18 ms when the output length of the Hash function reached 340bits. In Fig. 10b, in an open network environment, the computation time of Elliptic Hash significantly increased compared to the computation speed in a local area network, but it was still lower than other methods. The computation time was 5 ms when the output length of the Hash function was 600bits, and it increased to 48 ms when

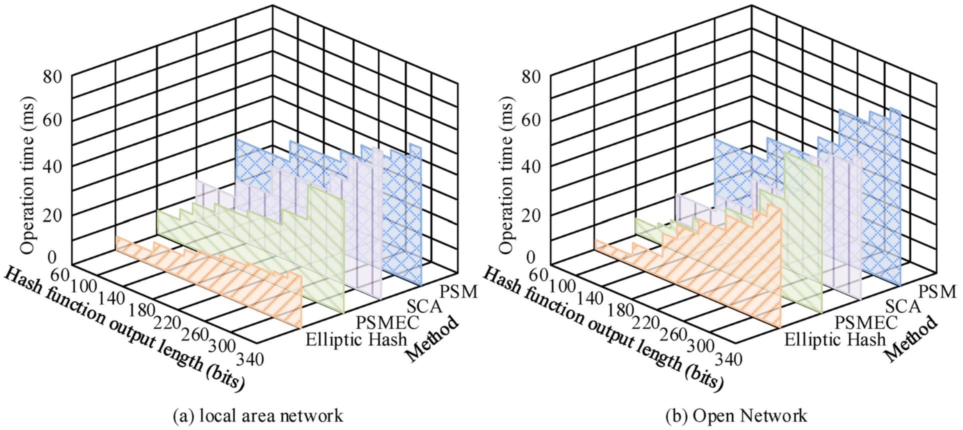


Fig. 10 Scalar multiplication operation time

the output length of the Hash function reached 340bits. This indicates that the research has faster scalar multiplication operation speed and can respond more quickly to IoT protection tasks.

5 Conclusion

A study designed an encryption technique using non-adjacent scalar forms in ECC to improve the data security of IoT RFID. During the process, the Non-Adjacent Form scalar multiplication algorithm was introduced to optimize and improve elliptic curve scalar multiplication. The scalar multiplication algorithm replaced modular operations with bit operations and division operations with shift operations, treating the central data system and reader as a whole. Burrows, Abadi, and Needham logic were introduced for protocol formal analysis, and freshness rules were employed to verify the freshness of messages. The experiment outcomes illustrated that the research method could effectively cover five key security indicators in the comparison of protocol security performance indicators. In the analysis of the success rate of intercepting abnormal data access behavior, the success rate of intercepting files with a size of 500 Kb on mobile devices remained above 98.8%. When conducting hardware operation burden analysis, the research method only achieved a maximum processor occupancy rate of 39% during a 1000 s run. In the analysis of scalar multiplication operation time, the research method showed that in an open network environment, when the output length of the Hash function reached 340bits, the operation time was only 48 ms. This denotes that the research method has good operational performance and can effectively improve the data security of the IoT. However, the impact of network fluctuations and electromagnetic interference has not been considered in the method design of the study. More interference factors will be added in the future to optimize the method and enhance its applicability.

Author contributions Bin Zheng made all the contributions in this research.

Funding There is no Funding in this manuscript.

Data availability All data generated or analyzed during this study are included in this article. Further enquiries can be directed to the corresponding author.

Declarations

Ethics approval and consent to participate An ethics statement was not required for this study type, no human or animal subjects or materials were used.

Consent for publication Not applicable.

Conflicts of interest The authors declare no competing interests.

References

1. Gupta M, Singh VP, Gupta KK, Shukla PK. An efficient image encryption technique based on two-level security for internet of things. Multimedia Tools Applicat. 2023;82(4):5091–111.
2. Pu L, Lin C, Chen B, He D. User-friendly public-key authenticated encryption with keyword search for industrial internet of things. IEEE Internet Things J. 2023;10(15):13544–55.
3. Hedayati R, Mostafavi S. A lightweight image encryption algorithm for secure communications in multimedia Internet of Things. Wireless Pers Commun. 2022;123(2):1121–43.

4. Feng J, Wang J, Zhu Y, Han K. A hybrid chaotic encryption ASIC with dynamic precision for internet of things. IEEE Int Things J. 2023;11(1):1148–63.
5. Liu C, Zhang Y, Xu J, Zhao J, Xiang S. Ensuring the security and performance of IoT communication by improving encryption and decryption with the lightweight cipher uBlock. IEEE Syst J. 2022;16(4):5489–500.
6. Zhu S, Xu X, Gao H, Xiao F. CMTSNN: A deep learning model for multiclassification of abnormal and encrypted traffic of Internet of Things. IEEE Int Things J. 2023;10(13):11773–91.
7. Khayyat MM, Khayyat MM, Abdel-Khalek S, Mansour RF. Blockchain enabled optimal Hopfield Chaotic Neural network based secure encryption technique for industrial internet of things environment. Alex Eng J. 2022;61(12):11377–89.
8. Kalaiarasi M, Venkatasubramani VR, Vinoth Thyagarajan V, Rajaram S. A parallel elliptic curve crypto-processor architecture with reduced clock cycle for FPGA platforms. J Supercomput. 2022;78(13):15567–97.
9. Bashir Z, Malik MGA, Hussain M, Iqbal N. Multiple RGB images encryption algorithm based on elliptic curve, improved Diffie Hellman protocol. Multimedia Tools Applicat. 2022;81(3):3867–97.
10. Ametepe AFX, Ahouandjinou ASRM, Ezin EC. Robust encryption method based on AES-CBC using elliptic curves Diffie-Hellman to secure data in wireless sensor networks. Wireless Netw. 2022;28(3):991–1001.
11. Ye G, Liu M, Wu M. Double image encryption algorithm based on compressive sensing and elliptic curve. Alex Eng J. 2022;61(9):6785–95.
12. Prasad DSV, Sekhar PS, Prasanth AVV, Ganesh KNS, Madhuri KR, Prasad TVVD. Digital image encryption algorithm based on elliptic curve public cryptosystem. Mathe Statistian Eng Applicat. 2022;71(4):644–55.
13. Gao M, Lu YB. URAP: a new ultra-lightweight RFID authentication protocol in passive RFID system. J Supercomput. 2022;78(8):10893–905.
14. Lee TF, Lin KW, Hsieh YP, Lee KC. Lightweight cloud computing-based RFID authentication protocols using PUF for e-healthcare systems. IEEE Sens J. 2023;23(6):6338–49.
15. Kumar S, Banka H, Kaushik B. Ultra-lightweight blockchain-enabled RFID authentication protocol for supply chain in the domain of 5G mobile edge computing. Wireless Netw. 2023;29(5):2105–26.
16. Krishna SN, Madnani K, Mazo M Jr, Pandya P. From non-punctuality to non-adjacency: a quest for decidability of timed temporal logics with quantifiers. Formal Aspects Comput. 2023;35(2):1–50.
17. Cheng L, Meng F. Certificateless public key authenticated searchable encryption with enhanced security model in IIoT applications. IEEE Internet Things J. 2022;10(2):1391–400.
18. De Dieu NJ, Ruben FSV, Nestor T, Zeric NT, Jacques K. Dynamic analysis of a novel chaotic system with no linear terms and use for DNA-based image encryption. Multimedia Tools Applicat. 2022;81(8):10907–34.
19. Munjal K, Bhatia R. A systematic review of homomorphic encryption and its contributions in healthcare industry. Complex Intell Syst. 2023;9(4):3759–86.
20. Chen S, Li J, Zhang Y, Han J. Efficient revocable attribute-based encryption with verifiable data integrity. IEEE Int Things J. 2023;11(6):10441–51.
21. Gowda NC, Manvi SS, Malakreddy AB, Buyya R. TAKM-FC: two-way authentication with efficient key management in fog computing environments. J Supercomput. 2024;80(5):6855–90.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.