Hindawi
Security and Communication Networks
Volume 2023, Article ID 9803063, 1 page
https://doi.org/10.1155/2023/9803063

Retraction

Retracted: Application of Hybrid Encryption Algorithm in Hardware Encryption Interface Card

Security and Communication Networks

Received 13 September 2023; Accepted 13 September 2023; Published 14 September 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] H. Yang, "Application of Hybrid Encryption Algorithm in Hardware Encryption Interface Card," *Security and Communication Networks*, vol. 2022, Article ID 7794209, 11 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 7794209, 11 pages
https://doi.org/10.1155/2022/7794209

Research Article

Application of Hybrid Encryption Algorithm in Hardware Encryption Interface Card

Huiwei Yang

Department of Information and Artificial Intelligence, Wuhu Institute of Technology, Wuhu, Anhui 241000, China

Correspondence should be addressed to Huiwei Yang; 20162103817@mails.imnu.edu.cn

Received 3 April 2022; Revised 23 April 2022; Accepted 3 May 2022; Published 30 May 2022

Academic Editor: C. Venkatesan

In order to effectively solve the increasingly prominent network security problems, cryptographic algorithm is the key factor affecting the effectiveness of IPSec VPN encryption. Therefore, this paper mainly studies cryptographic algorithms and puts forward the following solutions: briefly analyze the concept and function of IPSec VPN, as well as the basic theoretical knowledge of IPSec Security Protocol and cryptography, and analyze the traditional cryptography, modern cryptography, symmetric cryptographic algorithms and asymmetric algorithms, and their security. At the same time, the executable and security performances of AES and DES algorithms are compared and analyzed. This paper studies the elliptic curve encryption algorithm ECC, expounds the mathematical basis of realizing the algorithm, and compares and analyzes the security performance and execution efficiency of ECC. Based on the above two algorithms, a hybrid encryption algorithm is proposed, and the realization mechanism of the hybrid encryption algorithm is studied and discussed. The hybrid encryption algorithm combines the advantages of ECC and AES. The algorithm selects 128-bit AES and 256-bit ECC. In order to better cover up plaintext C, AES is used to encrypt information. While enhancing security, speed is also considered. The improved encryption, decryption, and signature authentication algorithms are relatively safe and fast schemes. ECC algorithm is improved, and on this basis, ECC algorithm and AES algorithm are combined. Moreover, HMAC message authentication algorithm is added, and the performance of the improved algorithm is significantly improved.

1. Introduction

Driven by the tide of global informatization, computer information network has become the infrastructure of people's social life. People's dependence on the network has been comparable to the basic necessities of life such as water and electricity. A large amount of life information, work information, and social information is transmitted, processed, and applied at a high speed in the network. The network supports people's family and social life in all aspects. Property, identity, education, and even the whole social relations also have other problems. The data stored in cyberspace is easy to transmit, process, and share, but the controllability is poor. While cyberspace brings convenience to people, it also brings problems such as the disclosure of privacy information and the disclosure of business and trade information. More and more high-risk problems such as tampering with private information, improper use, and counterfeiting other people's identity make the protection of privacy information urgent; otherwise, it will cause immeasurable losses. There are usually two ways to change the vulnerability of the existing Internet. Method 1: patching based on the existing protocol requires making full use of the existing Internet architecture. Method 2: design a new protocol and take the security part into account, but this method requires a process. How to smoothly transition the existing protocol to the new protocol platform without modification is the biggest problem [1]. With the birth of virtual private networks (VPN) technology, it makes up for the defect of information transmission service security. A virtual private network is an open network that serves as a medium for data transmission and helps build trust among customers, subsidiaries, and business partners at a distance through the integration of encryption, authentication, encapsulation, and key exchange equipment over the Internet and other public networks. And it securely connects to the company's intranet to ensure data security. IP Security (IPSec) is the most widely used protocol family in VPN structure [2]. IPSec explains how to choose the security of peering processes and determine security algorithms and exchange priorities to ensure the privacy, integrity, and accuracy of information published on the Internet [3]. There is no need to modify the upper layer protocol to implement IPSec Protocol on the IP layer. Using IPSec to build VPN can provide transparent security protection for IP layer and upper layer protocols without implementing special security measures [4]. At present, information security on the network mainly depends on two technologies. One is access control and authorization in the traditional sense, such as access control table technology and password verification technology; the other is to use the theory and technology of cryptography to realize information encryption and digital signature [5]. General access control technology and authorization technology are easy to be broken, so information security will still be based on cryptography theory and technology. Cryptography is the most basic and core technology of information security. The encryption of information can ensure the confidentiality of data and prevent unauthorized reading and use of information. Using digital signature can ensure the integrity of data and authenticate the data source and prevent information from being tampered with and user identity from being impersonated. IPSec protocol defines a set of mandatory cryptographic algorithms to provide conventional security protection [6]. However, with the progress of cryptographic technology and the improvement of computing power, the security of these default algorithms continues to decline. It is imperative to find other cryptographic algorithms to replace the default algorithms and provide stronger security protection for data transmission, as shown in Figure 1.

2. Literature Review

The US Data Encryption Standard (DES) is a widely used symmetric encryption algorithm. So far, the only effective method in the attack algorithm against DES is exhaustive and traversing the cipher space [7]. As the computing speed of computer hardware is getting faster and faster, the defect that the length of DES key is too short is exposed, so it is easy to be broken. In 1987, DES algorithm was declared unsafe. Because there is no suitable alternative, it is still widely used in commerce. After entering the 1990s, another algorithm derived from DES, triple DES (3DES), was used. Lekshmy and others said that the encryption and decryption time consumption of 3DES algorithm is large and can not well meet the rapidly growing demand for real-time information encryption [8]. In 2000, DES with an original design life of 10 years was successfully attacked after 23 years of use. In addition, IPSec protocol can also use some other encryption algorithms that have been defined in the standard document. These algorithms include RCS, idea, triple idea, CAS't, and blowfish. Ahmadrufa'i et al. stated that, on January 2, 1997, the National Institute of Standards and Technology (NIST) established an R&D program to adopt a new standard for Advanced Encryption Standard (AES) symmetric block encryption. The purpose is to develop a federal information processing standard that can well protect the encryption algorithm of sensitive government information in the next century to replace the DES algorithm [9]. NIST requires that the published AES algorithm be unprotected, public, and globally free and can support secure packet algorithms with a key length of at least 128 bits. Tamilarasi et al. believed that, after three rounds of screening, the NDAEL algorithm was finally determined as the standard algorithm of AES [10]. The Rijndael algorithm is a packet encryption algorithm that repeats variable packet lengths and key lengths. Its packet length and key length can be independently defined as 128 bits, 192 bits, and 256 bits. It is resistant to all current cryptographic attacks, whether using feedback mode or feedback mode [11]. The key establishment time of Rijndael algorithm is very short and flexible. With very low memory requirements, Rijndael algorithm is very suitable for use in the environment with limited memory and shows good performance. At present, the research of AES algorithm mainly focuses on design principles, security performance analysis, statistical performance analysis, and so on. Both AES algorithm and traditional DES algorithm belong to symmetric encryption algorithm. They have the characteristics of fast implementation speed and are especially suitable for the encryption of massive data. Magsino and others felt that because AES algorithm does not need confidentiality, manufacturers can develop low-cost chips to realize data encryption [12]. Beckham and others think that the simultaneous symmetric encryption algorithm has several disadvantages. The key must be distributed secretly, and the key distribution is difficult. Once the symmetric key is destroyed, the password attacker can easily disguise as the encryption party or decryption party [13]. Symmetric cryptographic algorithm needs to manage a large number of keys. With the continuous increase of network users, the total number of keys will rise rapidly, which will limit the scale of symmetric cryptographic system. In the computer network environment, key distribution and key management have become the main obstacles to the use of symmetric cryptosystems. Wang and others said that, in addition, another disadvantage of symmetric encryption algorithm is that it can not realize digital signature [14]. Asymmetric cryptographic algorithms are produced in such a harsh environment. Almalkawi and others use asymmetric encryption systems with two different keys, one public and one secret. Someone with the public key can encrypt messages, but not decrypt them. Only someone with the private key can decipher it [15]. Asymmetric cryptographic algorithm solves the problem of key distribution and management and can realize digital signature. At present, the popular asymmetric cryptographic algorithms not only have good security performance, but also are relatively easy to implement. Khan and others said that, according to the mathematical problems, they can be divided into three categories: asymmetric cryptographic algorithms based on Large Integer Decomposition (such as RSA); asymmetric cryptographic algorithm based on discrete logarithm problem in finite field (such as DSA); asymmetric encryption algorithm based on elliptic curve discrete logarithm problem

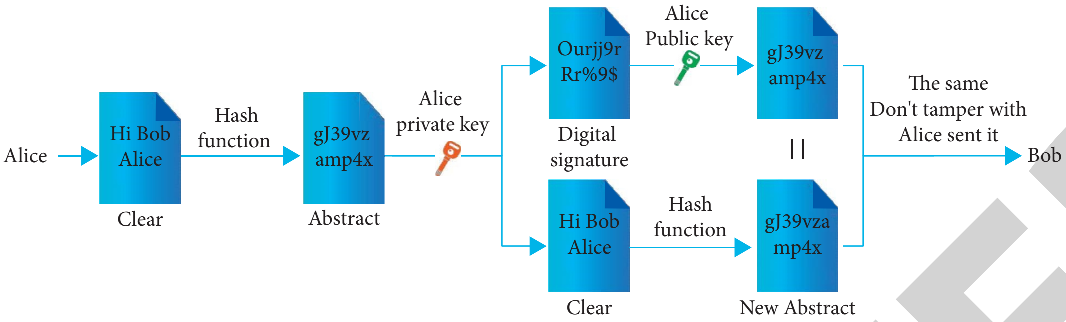

Figure 1: Application Research of hybrid encryption algorithm in hardware encryption bayonet.

(such as RCC). Among the three asymmetric encryption algorithms, the elliptic curve encryption algorithm is an asymmetric encryption algorithm with high security, low processing speed, low storage space, low bandwidth requirements, and high algorithm implementation performance [16].

3. Method

Cryptography is an old and young science with a long history. As early as 4000 years ago, the ancient Egyptians began to use ciphers to encrypt and send messages. Although cryptography is an ancient discipline, from the beginning of cryptography to the end of World War II, it has always been associated with military, secular, inspection, and other businesses, owned and managed by several people. The password is always unknown to the public. The development of information technology has changed all of this. With the rapid development of computer and network communication, more and more secure, private, and sensitive information is being transmitted through public communication sites or computer networks. Especially with the rapid growth and development of e-commerce, more and more personal information is rapidly demanded. Therefore, cryptography has become an important technology to ensure data security. Modern cryptography is no longer limited to politics, military, and diplomacy. It has entered the daily life of the public [17].

Cryptography is a subject that studies cryptography and communication security. Cryptography mainly includes two branches: cryptography and cryptanalysis. Cryptography is a method to ensure the confidentiality and authentication of messages. Cryptanalysis studies the decoding of encrypted information and the forgery of messages. Camouflage the encryptor of a user, encrypt and transform the plaintext of the confidential information to be camouflaged, and get another representation ciphertext that seems to be irrelevant to the original information. If the legitimate user receiver obtains the camouflaged information, he can restore the original confidential information from these information and decrypt and transform it. If the illegal user password analyst attempts to analyze the original confidential information from the camouflaged information, either this analysis is impossible, or the cost is too high to carry out [18–20]. To be exact, a cryptographic system consists of plaintext space, ciphertext space, cryptographic scheme, and key space: (1) the information to be encrypted is called plaintext, and all of the plaintext is called plaintext space. In general, plaintext is represented by M (or m, i.e., message). Plaintext is a source coded symbol, or a text file, a bitmap, a digitally stored voice stream, or a bit stream of a digitized video image. (2) Ciphertext is plaintext after camouflage. All possible ciphertext sets are called ciphertext space. Generally, ciphertext is represented by C (cipher), which can also be considered as character stream or bit string. (3) The cryptographic scheme accurately describes the specific rules of encryption transformation and decryption transformation. This description generally includes a set of rules used when encrypting plaintext, called encryption algorithm, represented by E, and a set of rules used when restoring ciphertext, called decryption algorithm, represented by D. The transformation process of plaintext using encryption algorithm is called encryption transformation, abbreviated as encryption. The transformation process of ciphertext using decryption algorithm is called decryption transformation, which is abbreviated as decryption. (4) The operation of encryption and decryption algorithms is usually done by controlling what is called a key (encryption key and decryption key in most cases). The whole key is called the key space, and the general key is represented by K (or K, i.e., key). Each key symbol is generally independent and appears with equal probability; that is, the key is generally a random sequence. For example, for a plaintext message $m \in M$, under the encryption key $k \in K$, the encryption algorithm $e \in E$ performs encryption transformation e_{k} to obtain the ciphertext message $c \in C$, as shown in the following formula:

$$c = e_k(m). \tag{1}$$

Similarly, the decryption process can be expressed as the following equation:

$$m = d_k(c). \tag{2}$$

One of the communication parties is the sender, and the other is the receiver, as shown in Figure 2:

DES, or Standard Data Encryption, was developed by IBM. In 1997, the U.S. Department of Commerce approved the release of information as the standard encryption standard for government data. Since its publication, the DES algorithm has crossed national borders and has become the most widely used encryption algorithm in the global

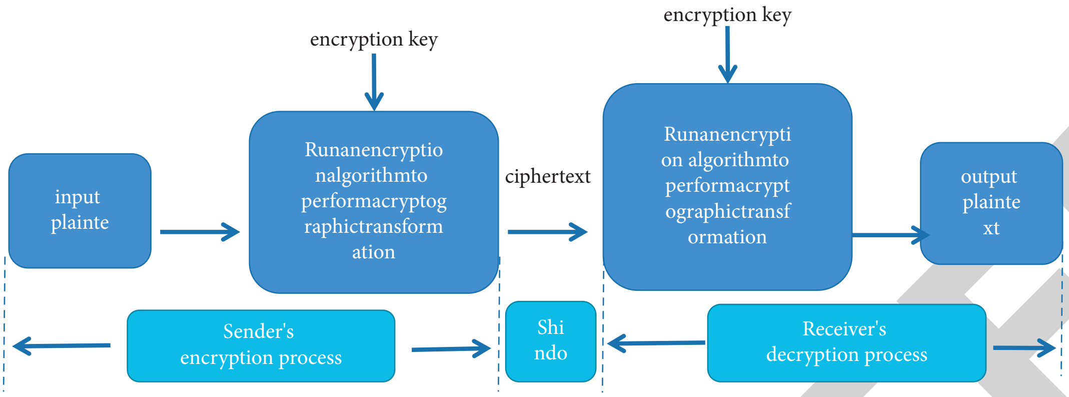
encryption key
encryption key
input plainte
Runanencryptio nalgorithmto performacryptog raphictransform ation
ciphertext
Runanencrypti on algorithmto performacrypt ographictransf ormation
output plainte xt
Sender's encryption process
Shi ndo
Receiver's decryption process

Figure 2: Schematic diagram of encryption decryption.

communication security and computer communication industries. ISO also uses it as standard data encryption. DES is a block encryption algorithm that encrypts data in 64-bit groups. Also, DES is a complex encryption algorithm. DES operates 64-bit plaintext packet m, which is replaced by M_0 through an initial IP, and divides M_0 plaintext into left and right parts $m_0 = (L_0, R_0)$, each 32 bits long. Then, perform the same round of operations, which are called function f transformation. In the operation process, the data is combined with the key. After 16 rounds, the left and right are merged, and after the last change, the ciphertext group C is finally output. The main product is replaced each round, and 48 keys are selected from the 56 keys. Then, through another XOR operation, the output of function f is combined with the left half, the result becomes the new right half, the original right half becomes the new left half, and the operation is repeated 16 times. The specific process is shown in Figure 3.

4. Experiment and Discussion

In Rijndael algorithm, most operations are based on bytes, and bytes are used to represent the elements in the finite field GF (2^8). Definition 4-1$b_7b_6b_5b_4b_3b_2b_1$ constitutes byte B, which can represent a binary polynomial, where $b_1 \in \{0,1\}, i = 0, 1, \ldots, 7$. The addition of formula (3) on GF (2^8) is defined as the addition of binary polynomials, and its coefficient modulus is 2. The multiplication on GF (2^8) is defined as the product module of binary polynomial is an irreducible binary polynomial of degree 8. Irreducible bivariate polynomials cannot be divided by any other bivariate polynomials except by 1 and itself. For Rijndael algorithm, irreducible bivariate polynomial is determined as shown in the following equation:

$$m(x) = x^8 + x^4 + x^3 + x + 1. \tag{3}$$

The coefficients of the polynomials in the finite field GF (2^8) are taken from the polynomials of GF (2^8) elements. Such a 4-byte vector corresponds to a polynomial with a degree less than 4. The AES algorithm is a block encryption algorithm that repeats a variable block length and a variable key length. The length of the key can be 128, 192, and 256 bits. In fact, the key length of Rijndael algorithm can be extended to any integer multiple of 64, but only keys longer than 128, 192, and 256 in AES standard are recognized. AES encryption algorithm has n replacement cycles, where n depends on the key length. If the key length is 128 bits, 9 cycles are required. The length is 192 bits, and 11 cycles are required. If it is 256 bits, 13 cycles are required. The one cycle operation of AES algorithm is very simple, including one replacement, two replacement functions, and a selection function. The 128-bit block of AES can be easily considered as a 4 × 4 matrix, which is called "state." Here, we express the state as a matrix. These states are filled with input data column by column. Some operations in Rijndael algorithm are performed on columns of States, and some are performed on rows. Therefore, this representation realizes a form of column transformation. Whether encryption or decryption, AES algorithm adopts a round transformation mode, which is realized in four steps:

4.1. Bytes Transform. Subbytes transform is a nonlinear byte transform that acts on each byte in the state. This transformation table (or S-box) is reversible. The value of a byte is replaced by its multiplicative inverse in its limit field GF (28). The processed byte value is transformed to construct an S-box. In this transformation, find the polynomial corresponding to this byte by looking up the S-box table, and then replace this byte. Subbytes transformation is also called S-box transformation. This step is very simple. It is through a defined replacement table, that is, S-box. Replace $a\,[i, j]$ with $a'\,[i, j)$.

4.2. Shift Rows. In this step, the row of a is replaced by cyclic left shift, and the first (leftmost, with the largest sequence number) I elements of the first row are moved to the last (rightmost, with the smallest sequence number). In other words, the line shift transformation acts on the line in the intermediate state. The line 0 does not move, the line 1 circulates to the left by 1 byte, the line 2 circulates to the left by 2 bytes, and the line 3 circulates to the left by 3 bytes, that is, the line shift vector $C = (0,\ 1,\ 2,\ 3)$.

4.3. Mixed Column. This step performs a complex conversion on column a. That is, the column mixing transformation acts

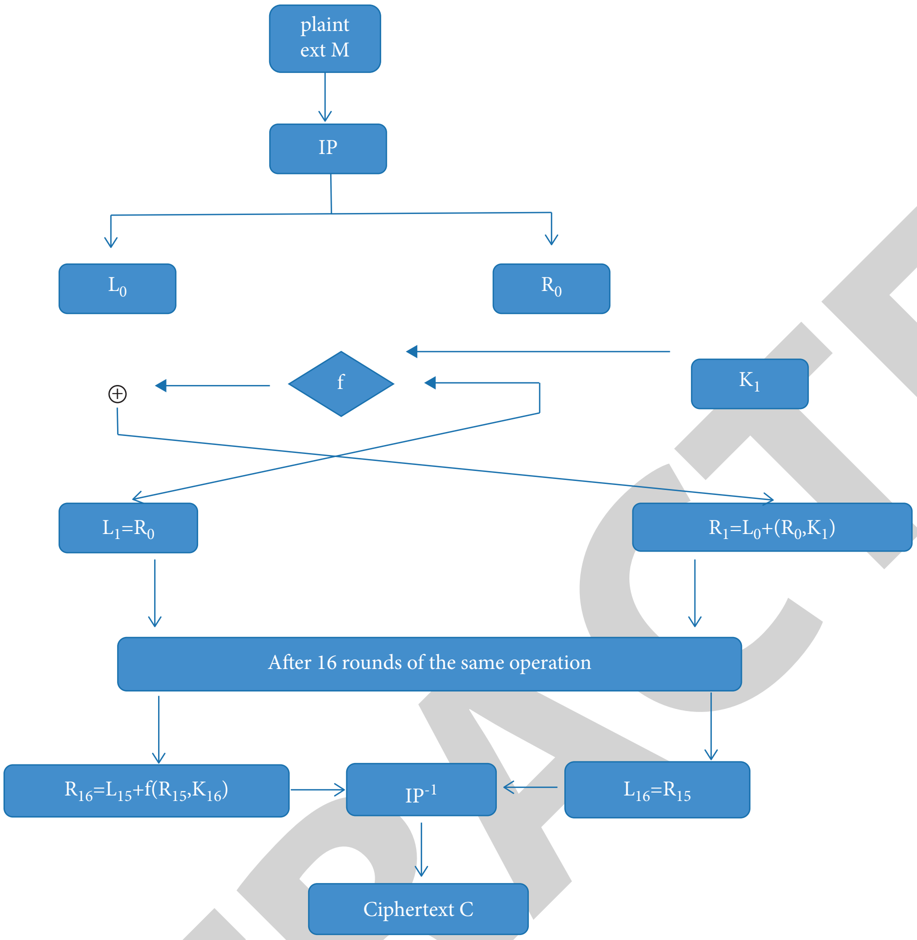

Figure 3: DES flow algorithm diagram.

on the column of the intermediate state. If a column of the intermediate state is recorded as a polynomial on the coefficient GF (2^8): $a(x) = a_3x^3 + a_2x^2 + a_1x + a_0$, the column blending transformation is H_M: $a(x)\mapsto d(x)$, where $d(x) = t(x)a(x)\text{mod}x^4 + 1$. $t(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$, and the multiplication and addition of coefficients are the operations in GF (2^8), which are recorded as $d(x) = d_3x^2 + d_1x + d_0$, and the column blending transformation is $HM(A) = MA$. This “multiplication” is realized by logical operation between bytes. Therefore, multiplying a column by 1 means not to change the column, multiplying by 2 (binary 10) means to shift each byte to the left by one byte, and multiplying by 3 (binary 11) means to shift each byte to the left and add (XOR) 10001011 to the original unmodified value until the meaningful bits in the result do not exceed 8 bits, where $a_{ij} + k_{ij}$ is the operation plus subkey in GF (2^8), which is the last step of a cycle. It is to add (XOR) the current result and a variant of the key. This change is as follows: the first key is itself, and the second key is converted word by word in 4 bytes. The first word circularly shifts one byte to the left, then transforms according to the replacement method of the previous byte replacement step, and then adds it to a variable (XOR). The remaining part of the word in the subkey is obtained by XOR operation between the first word and the word corresponding to the previous key. Security analysis is limited by the length of the key because the computing power of the sensor node is limited, and the storage space is small. ECC encryption algorithm can achieve a better security level through a shorter key. Of course, the required bandwidth is obviously reduced. The storage requirements and computational burden of WSN are reduced. The most famous ECC encryption technology company, Certieom, has done experimental comparison. The results show that the decoding time of ECC algorithm is longer than that of other algorithms. When the key size of the three algorithms is less than 1000 bits, the key size difference of the three encryption algorithms is small by using the same decoding time, indicating that the three algorithms need to achieve the same security and have little difference in spatial complexity requirements, while the spatial complexity of the improved ECC algorithm and ECC algorithm increases slowly. Therefore, big data encryption requires improved ECC algorithms. Therefore, the energy consumption of the three algorithms can be roughly estimated as follows: exponential encryption RSA algorithm consumes the most energy. The traditional ECC algorithm is better than exponential encryption algorithm, and the improved algorithm is better than traditional ECC encryption algorithm. AES encryption algorithm is fast, and its advantages can only be shown when encrypting long plaintext; ECC algorithm has high security and is convenient for key management. The hybrid encryption algorithm combines the two cryptographic algorithms based on their respective strengths; that is, before communication, ECC public key encryption algorithm is used to manage and distribute the randomly generated session key, and then symmetric encryption system is used to encrypt the data packet to be sent with the session key. In this way, private messages can be securely transmitted to the designated area, solving the key management problem caused by the system generating a large number of keys. Hybrid encryption algorithms combine the advantages of ECC and AES. The algorithm selects 128-bit AES and 256-bit ECC. In order to better cover up plaintext C, AES is used to encrypt information. If the invading malicious node chooses to attack ciphertext C, it is extremely difficult to decipher the 128-bit AES encryption algorithm under the existing technical conditions. If you want to start with the decipherment of K, you need to solve the problem of discrete degree, so it is impossible to decipher K. At the same time, HMAC function is added, which adds another layer of protection to the integrity of wireless sensor data packets [21]. Compared with other asymmetric encryption algorithms, the ECC algorithm has the advantages of higher security, smaller storage space, faster operation speed, smaller calculation amount, and lower bandwidth requirements. ECC encryption algorithm has the following advantages: (1) save storage space: under the same security level, the key length of ECC algorithm is shorter than that of other agreed algorithms, which is very important for WSN nodes with limited storage space; (2) save network bandwidth: when encrypting and signing short data packets, ECC encryption algorithm needs to send relatively short encrypted data packets, thus saving network bandwidth; (3) it reduces the time complexity of the algorithm: ECC algorithm has short key length and short data packets to be sent, so it saves time; (4) it can provide higher security: ECC algorithm can provide higher security with a shorter key. Therefore, to improve the security of the system, only increase the length of the key; (5) it can quickly generate key pairs: compared with other public key algorithms, ECC algorithm has shorter key generation time [22]. The algorithm is low, slow, and not suitable for increasing packets. HMAC algorithm is a classic algorithm for message authentication. Its principle is based on SHA-1 and MD-5. The message summary is calculated through secondary hash iteration. The calculation formula is shown in the following formula:

$$\mathrm{HMAC}(K, M) = H(K \oplus \mathrm{opad} | H(k \oplus \mathrm{ipad}) | M), \tag{4}$$

where K represents the key, M represents the message, H represents the hash function, and the length of the key is 64 bytes. If it is less than 64 bytes, it is supplemented with 0. IPad and opal are sequences composed of 0×36 and $0 \times 5c$, respectively, which indicates a connection operation. (1) Create a sequence group with a length of b bits. If it is less than b bits, fill it with 0. (2) Use the sequence in (1) and iPad for XOR operation. (3) Put message M into the result sequence of (2). (4) Put the result of (3) into the hash function to generate the summary value. (5) XOR the sequence in (1) with OPAD. (6) Put the message summary generated in (4) into (5). (7) Put the result of (6) into the hash function. The most general result is that the construction of HMAC algorithm takes into account the defects of hash function. Under the action of key, the value range of function is greatly increased, so it also greatly enhances the anti attack. The key of HMAC algorithm can be any length, and the selection of key is random and will be updated irregularly. The main purpose of this is to prevent malicious nodes from stealing the corresponding relationship between key and function, which can improve the security of the system. Principle of digital envelope: the so-called digital envelope uses the public key of the receiving node to encrypt the private key of the symmetric algorithm, and the ciphertext data formed is called digital envelope. The steps of digital envelope are as follows: (1) the sending node encrypts the WSN packet with a randomly generated AES key; (2) encrypting the AES key with the generated ECC public key of the receiving node; (3) the receiving node restores the encrypted AES session key with its ECC private key; (4) the receiving node decrypts the data packet with the obtained AES key to obtain plaintext. The expression is as follows, where formula (5) is the encryption formula of the sending node, and formula (6) is the decryption formula of the receiving node:

$$\begin{cases} C_1 = E_{\mathrm{KAES}}(M), \\ C_2 = E_{\mathrm{KPB}}(K_{\mathrm{AES}}), \end{cases} \tag{5}$$

$$\begin{cases} K_{\mathrm{AES}} = D_{\mathrm{KSB}}(C_2), \\ M = D_{\mathrm{KAES}}(C_1). \end{cases} \tag{6}$$

Design of hybrid encryption algorithm: encryption module: (1) plaintext encryption: encrypt plaintext m with AES algorithm to obtain ciphertext C, and the encryption key used is KAC; (2) key encryption: encrypt Ka with ECC to obtain AES key block; (3) digital envelope: (1) the digest value of plaintext m is obtained by signing plaintext m with HMAC algorithm; (4) send ciphertext C, signature, and AES key block to the receiver Bo. The encryption process of the sender is shown in Figure 4.

(1) Key decryption: decrypt the AES key block with ECC to obtain Ka; (2) ciphertext decryption: decrypt ciphertext C with Ka to obtain plaintext m; (3) signature verification: use ECC private key to authenticate the signature block and compare whether the calculated summary value is the same as the sent summary. If it is the same, it means that the ciphertext has not been tampered with. If not, it means that the ciphertext has been tampered with. The decryption process of the receiver is shown in Figure 5.

Hybrid encryption algorithms combine the advantages of private key encryption and public key encryption. In the communication process, in addition to effectively ensuring security, it also significantly improves the efficiency of the encryption algorithm. The hybrid encryption algorithm uses a one-time session key, even if a malicious node steals the session key when exchanging keys. In sensor networks, the network nodes use hybrid encryption algorithm, the confidential information is double-layer encrypted by two efficient algorithms, and the data is signed and authenticated, which not only improves the security of the system, but also ensures the integrity of the data [23]. Implementation of

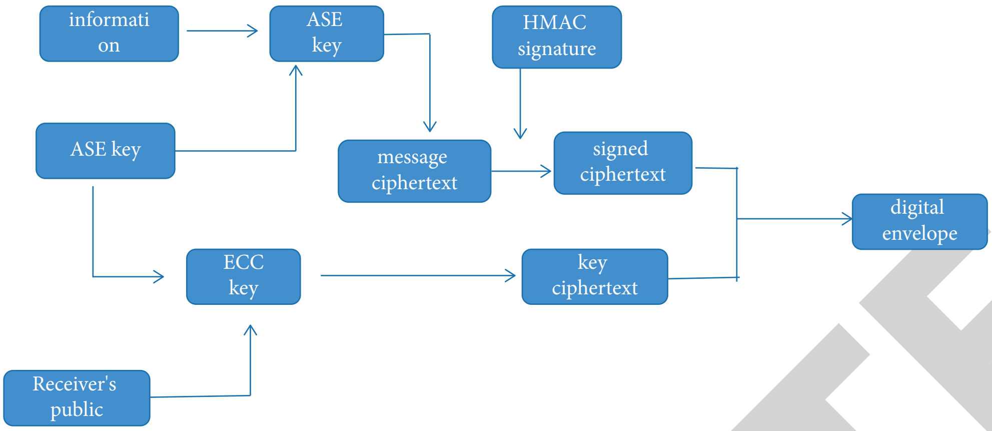

Figure 4: Sender encryption diagram.

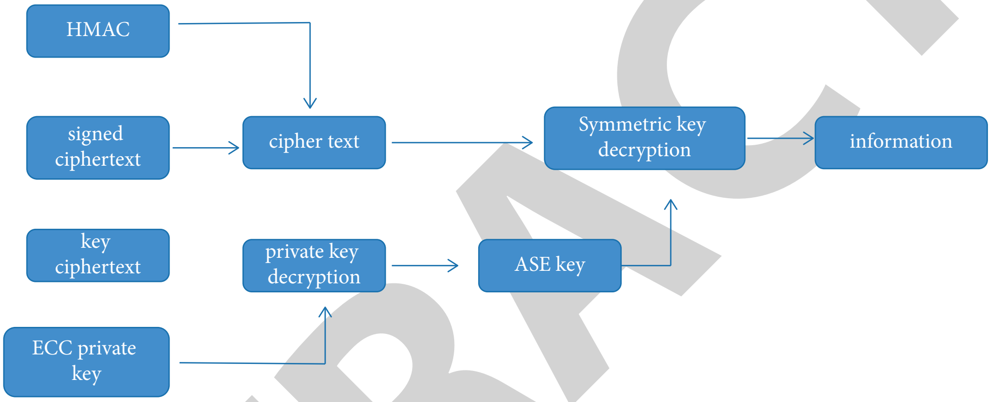

Figure 5: Receiver decryption diagram.

hybrid encryption algorithm: Hardware Platform: PC Intel x86/x64 main frequency: 1.8 GHz, memory: 3G; Software platform: Win7 flagship 64 bit; Development platform: Ms Visual Studio 2008 (c + +); Third party reference implementation library: Crypto + 5.6.20 hybrid encryption algorithm uses symmetric encryption algorithms such as AES to encrypt information data, and asymmetric encryption algorithms such as ECC to encrypt the random key used by AES. At the same time, information authentication code technologies such as HMAC are used for data integrity authentication and message source authentication. The system framework is shown in Figure 6.

The system randomly generates an AES session key and a start vector IV and uses the AES session key to encrypt plain text data; the system randomly generates an ECC key combination for both parties; the AES session key and ciphertext are sent to the receiving node in the WSN; the receiving node of the WSN decrypts the AES session key and initialization vector IV with its own private key to obtain the AES key and uses the decrypted AES key to decrypt the encrypted file. Compare the average cost of encrypting different data packets 100 times for different levels of wireless sensor devices. The results are as follows: Time Complexity Analysis in Table 1 shows the key generation time for the three main algorithms. ECC algorithm always owns and improves ECC hybrid encryption algorithm that has a short key generation time, while RSA hybrid encryption algorithm key generation time increases with the number of packets.

When the packets are increased from 1 m to SOM, the time increases from 17.4 ms to 23.8 ms. This indicates that the RSA hybrid encryption algorithm is not suitable for encrypting small packets. Table 1 shows the encryption time of the three key algorithms for wireless sensor data packets of different sizes. The traditional ECC algorithm takes the longest time, and the other two hybrid encryption algorithms have almost the same encryption time. As the data packet becomes larger, the time complexity of the three algorithms becomes longer, as shown in Table 2.

It can be seen from Table 2 that the encryption time of the encryption algorithm is similar to that of the large data packet of the wireless sensor network. In the data encryption stage, the hybrid encryption algorithm saves more time than the traditional algorithm. When the packet size is 1 m, the ECC hybrid encryption algorithm is 59070 higher than the traditional algorithm, and the RSA hybrid encryption algorithm is 68070 higher than the traditional ECC algorithm. When the data packet is greater than 1 m and less than or equal to SOM, the time used by the two hybrid algorithms in the encryption phase is not much different. There are often confidential data in the network. It is extremely necessary to use signature technology to verify the integrity of confidential

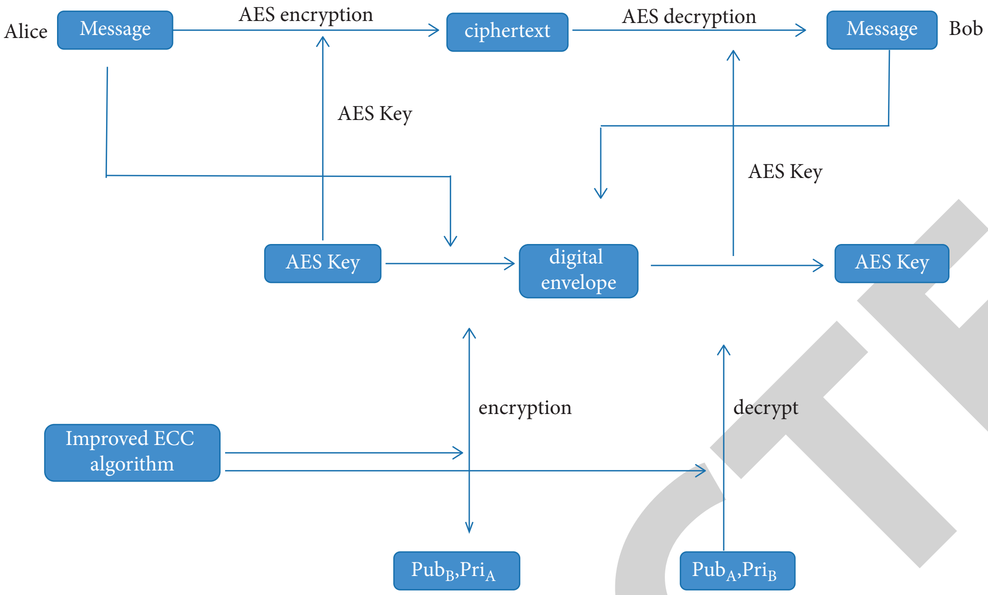

Figure 6: System framework.

Table 1: Comparison of key generation time between hybrid encryption algorithm and traditional elliptic curve algorithm.

Data packet (M)	ECC (ms)	RSA + AES (ms)	ECC + AES (ms)
1	1	17.4	1
10	1	18.1	1
20	1	18.8	1
30	1	21.7	1
40	1	23.2	1
50	1	23.8	1

Table 2: Comparison of encryption time between hybrid encryption algorithm and traditional elliptic curve algorithm.

Data packet (M)	ECC (ms)	RSA + AES (ms)	Higher than ECC (%)	ECC + AES (ms)	Higher than ECC (%)
1	38.7	12.3	68	15.7	59
10	298.9	85.3	71	89.3	70
20	588.8	196.2	67	188.3	68
30	881.3	255.1	71	267.3	70
40	1192.3	352	70	351.1	71
50	1476.4	429.3	71	437.7	71

data. Table 3 shows the time of signing wireless sensor data packets of different sizes by two hybrid encryption algorithms [24].

In the case of RSA encryption algorithm, the length of the mixed key should be shorter than that of the plaintext encryption algorithm. Table 3 shows the decryption time of three key algorithms for various variants of wireless sensor packets. The traditional ECC algorithm takes the longest time, and the encryption time of the other two hybrid encryption algorithms is almost the same, as shown in Table 4.

As shown in Table 4, the decoding time of the encryption algorithm is similar to the size of the wireless sensor dataset. The hybrid encryption algorithm saves more time than the traditional process when decrypting data, and there is no difference between the two hybrid encryption algorithms in the encryption stage. Here is a comparison of the total running time of our base algorithm. Table 5 shows that the encryption time of our algorithm increases with the amount of packet data. The conversion diagram is shown in Figure 7.

Table 3: Comparison of signature time of two encryption algorithms.

Data packet (M)	RSA + AES (ms)	ECC (ms)
1	7.2	6.1
10	54.7	54.6
20	117.3	116.8
30	172.2	168.3
40	212.9	202
50	269.6	263

As shown in Figure 7 and Table 5 above, the encryption time of the encryption algorithm correlates well with the size

Table 4: Comparison of decryption time between hybrid encryption algorithm and traditional elliptic curve algorithm.

Data packet (M)	ECC (ms)	RSA + AES (ms)	Higher than ECC (%)	ECC + AES (ms)	Higher than ECC (%)
1	39.1	15.4	61	15.2	61
10	300.3	88.6	70	88.1	71
20	591.7	185.3	69	190.1	68
30	883.3	261.4	70	264.6	70
40	1183.8	345.4	71	348.9	71
50	1475.6	429.7	71	432.3	71

Table 5: Comparison of total time complexity between hybrid encryption algorithm and traditional elliptic curve algorithm.

Data packet (M)	ECC (ms)	RSA + AES (ms)	Higher than ECC (%)	ECC + AES (ms)	Higher than ECC (%)
1	78.7	64.3	18	38	52
10	600.2	246.7	59	233	61
20	1181.3	517.6	56	496.2	58
30	1765.6	700.4	60	701.2	60
40	2377.6	933.5	61	923	61
50	2953	1152.4	61	1144	61

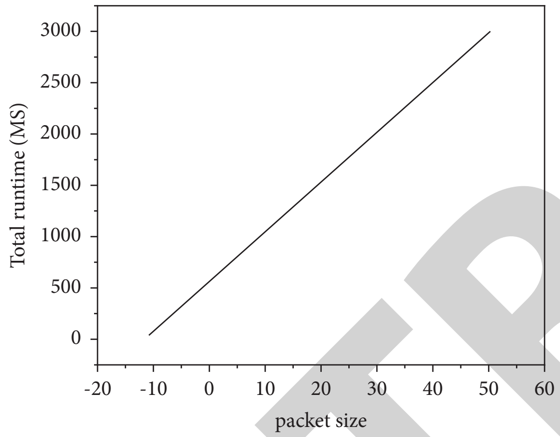

Figure 7: Comparison of total running time.

of the wireless sensor package. The difficulty time of the hybrid encryption algorithm is lower than that of the traditional algorithm. When the data packet size is between 1 m and 30 m, the performance of ECC hybrid encryption algorithm is more improved than that of RSA hybrid encryption algorithm. With the increase of wireless sensor data packets, the time complexity of the two hybrid algorithms is getting closer and closer. ECC mixed cipher algorithm uses AES symmetric encryption algorithm to encrypt information. Therefore, in terms of data security, ECC mixed cipher algorithm has good security of AES algorithm. In terms of key security, ECC asymmetric encryption algorithm is used to encrypt the key of AES, so the security of the key is equal to that of ECC algorithm [25]. Theoretically, assuming that a computer can perform about 4×10^4 ECC addition points per second, the maximum number of ECC addition points that this computer can run in a year $(4\times 10^4)\times(60\times 60\times 24\times 365)\}2^{40}$. Therefore, even if 10000 units are calculated simultaneously at the speed of 1000 mips, $n\approx 2^{160}$, the time required to solve the discrete logarithm problem is 6000 years. Therefore, in the current situation, it is not feasible to solve the ECC discrete logarithm problem, so the security of the algorithm is guaranteed. In the aspect of key management, the symmetric key encryption algorithm is abandoned, and the asymmetric key encryption algorithm is selected because the symmetric encryption algorithm is difficult to manage and update.

In symmetric cryptosystem, both parties share a key during communication, and it is required that each two nodes can only use one key without repetition. Therefore, assuming that N nodes communicate with each other, each node should save $n-1$ keys, and the total number of keys required by N nodes is $N = n(n-1)/2$. It can be seen that, with the increase of the number of nodes, the total number of keys increases accordingly, which makes it difficult to update and manage the keys. Energy consumption analysis: theoretically, the energy consumption of the algorithm is related to the number of nodes in WSN and the running time of the algorithm system. The larger the number of nodes, the faster the energy consumption. The higher the time complexity of the algorithm, the faster the energy consumption. Therefore, in the same wireless sensor network, it can be roughly estimated that the energy consumption ranking of the three algorithms should be that ECC hybrid encryption algorithm has the lowest energy consumption, traditional ECC encryption algorithm has the highest energy consumption, and RSA hybrid encryption algorithm is in the middle [26].

To sum up, the hybrid encryption algorithm has the following advantages: (1) since the AES key used for data communication is encrypted by ECC encryption algorithm, it is not necessary to send the key secretly before communication. (2) The key management method of the hybrid algorithm is similar to the traditional ECC encryption algorithm, as long as it manages the private key used to decrypt the AES key. (3) Compared with the traditional ECC algorithm, the hybrid encryption algorithm has less time complexity. The algorithm uses the more time-consuming ECC algorithm to manage only the 128-bit key of AES algorithm. If the encrypted data is long enough, using the public key encryption system to manage the key can be ignored. (4) Hybrid encryption algorithm can not only send the key, but also carry out digital signature.

Limitations and next steps: (1) due to limited conditions, this research can not be simulated and tested on the actual wireless sensor network platform, and all the research is completed on the PC platform. The system simulates the key processes such as encryption, decryption, signature, and verification in the process of end-to-end data communication but does not simulate the process of data transmission. The system implements the encryption and signature process based on asymmetric encryption algorithm but does not design and implement public key distribution mechanism [27, 28]. (2) The system implementation is based on an open source algorithm library on a PC platform, without considering the optimization of embedded system used in wireless sensor networks. The optimization of ECC algorithm is simply compared and analyzed, and the running environment is not fully considered for in-depth research. (3) Based on the simulation system, some design and performance comparison evaluations are carried out, but limited to the simulation environment, it can not carry out very accurate analysis. For example, system energy consumption is very important to network nodes. But we can only make some rough estimation and analysis of energy consumption. In this paper, ECC encryption algorithm, AES symmetric encryption algorithm, and HMAC signature algorithm are combined to obtain ECC hybrid encryption algorithm. The algorithm uses AES symmetric encryption algorithm to encrypt data packets, ECC algorithm to encrypt AES key, and hash function to ensure the integrity of data transmission. At the same time, the ECC hybrid encryption algorithm is compared with the RSA hybrid encryption algorithm, and it is determined that the ECC encryption algorithm has better performance and higher security when sending small files.

5. Conclusion

In this paper, the secure communication based on hybrid encryption algorithm is studied, the encryption algorithm of wireless sensor networks is improved, and an encryption scheme combining the advantages of AES and ECC is proposed. This paper adopts hybrid encryption technology and selects AES symmetric encryption algorithm to encrypt data, ECC algorithm to encrypt key, HMAC algorithm to authenticate message and ensure the integrity of message. Through simulation verification, it can be seen that the hybrid encryption algorithm can encrypt confidential data and verify identity more efficiently and safely, which solves the problem that the encryption speed and encryption and decryption security can not be considered at the same time in the current password coding system. When studying each link of WSN encryption and decryption, this paper not only enhances the security, but also considers the speed problem. The improved encryption, decryption, and signature authentication algorithms are relatively safe and fast schemes. Firstly, the ECC algorithm is improved, and on this basis, the ECC algorithm and AES algorithm are combined. Moreover, HMAC message authentication algorithm is added, and the performance of the improved algorithm is significantly improved.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Anhui University Natural Science Research Project (no. KJ2021A1316) and “Anhui University Excellent Talents Support Program (no. gxyq2020120).”

References

[1] G. D. Belga, “Hybrid encryption algorithm towards secured instant messaging application,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 2, pp. 236–242, 2020.

[2] M. Omid, F. Eshghi, and A. Zamani, “A hybrid encryption algorithm for security enhancement of wireless sensor networks: a supervisory approach to pipelines,” *Computer Modeling in Engineering and Sciences*, vol. 122, no. 1, pp. 323–349, 2020.

[3] A. Vahi and S. J. Jassbi, “Separ: A new lightweight hybrid encryption algorithm with a novel design approach for IoT,” *Wireless Personal Communications*, vol. 114, no. 10, pp. 1–32, 2020.

[4] D. Rachmawati, A. Sharif, and Ericko, “Hybrid cryptosystem combination algorithm of hill cipher 3 × 3 and Elgamal to secure instant messaging for Android,” *Journal of Physics: Conference Series*, vol. 1235, no. 1, Article ID 012074, 2019.

[5] M. Zarebnia, H. Pakmanesh, and R. Parvaz, “A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images,” *Optik*, vol. 179, pp. 761–773, 2019.

[6] Z. Cao and O. Markowitch, “Comment on “circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing”,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 2, pp. 392-393, 2021.

[7] Y. Tang, “Security design and application of internet of things based on asymmetric encryption algorithm and neural network for Covid-19,” *Journal of Intelligent and Fuzzy Systems*, vol. 39, no. 6, pp. 8703–8711, 2020.

[8] P. L. Lekshmy and M. Abdul Rahiman, “Hybrid approach to speed-up the privacy preserving kernel k-means clustering and its application in social distributed environment,” *Journal of Network and Systems Management*, vol. 28, no. 2, pp. 398–422, 2020.

[9] Ahmadrufa’i, A. T. Balarabe, I. Muazu, and M. Sirajo, “Formulation of an improved hybrid cipher system,” *International Journal of Innovative Research in Science Engineering and Technology*, vol. 5, no. 12, pp. 605–611, 2020.

[10] K. Tamilarasi and A. Jawahar, “Medical data security for healthcare applications using hybrid lightweight encryption and swarm optimization algorithm,” *Wireless Personal Communications*, vol. 114, no. 3, pp. 1865–1886, 2020.

[11] L. B. Rivera, J. A. Bay, E. R. Arboleda, M. R. Perea, and R. M. Dellosa, “Hybrid cryptosystem using RSA, DSA, Elgamal, and AES,” *International Journal of Scientific & Technology Research*, vol. 8, no. 10, pp. 1777–1781, 2019.

[12] J. P. Magsino, E. R. Arboleda, and R. R. Corpuz, “Enhancing security of Elgamal encryption scheme using RSA and Chaos algorithm for e- commerce application,” *International Journal of Scientific & Technology Research*, vol. 8, no. 11, pp. 1343–1347, 2019.

[13] O. Beckham, G. Oldman, J. Karrie, and D. Craig, “Techniques used to formulate confidential data by means of fragmentation and hybrid encryption,” *International Research Journal of Management, IT and Social Sciences*, vol. 6, no. 6, pp. 68–86, 2019.

[14] X. Wang, Y. Su, H. Zhang, and C. Zou, “A new hybrid image encryption algorithm based on Gray code transformation and snake-like diffusion,” *The Visual Computer*, vol. 2021, pp. 1–22, 2021.

[15] I. T. Almalkawi, R. Halloush, A. Alsarhan, A. Al-Dubai, and J. N. Al-Karaki, “A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications,” *Journal of Information Security and Applications*, vol. 49, pp. 102384.1–102384.13, 2019.

[16] S. Khan, L. Han, H. Lu, K. K. Butt, and N. U. Khan, “A new hybrid image encryption algorithm based on 2d-ca, fsm-dna rule generator, and fsbi,” *IEEE Access*, vol. 2019, no. 99, p. 1, 2019.

[17] A. Babbar, C. Prakash, S. Singh, M. K. Gupta, M. Mia, and C. I. Pruncu, “Application of hybrid nature-inspired algorithm: single and bi-objective constrained optimization of magnetic abrasive finishing process parameters,” *Journal of Materials Research and Technology*, vol. 9, no. 4, pp. 7961–7974, 2020.

[18] H. D. J. R. H. Utami, R. Arifudin, and A. Alamsyah, “Security login system on mobile application with implementation of advanced encryption standard (AES) using 3 keys variation 128-bit, 192-bit, and 256-bit,” *Scientific Journal of Informatics*, vol. 6, no. 1, pp. 34–44, 2019.

[19] R. F. S. L. Et.al, “Image encryption using rk-rsa algorithm in aadhaar card,” *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 3, pp. 4683–4693, 2021.

[20] G. Shrividya, “Application of hybrid genetic algorithm for successful cs-mri reconstruction,” *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, no. 3, pp. 408–414, 2020.

[21] J. Jayakumar, B. Nagaraj, S. Chacko, and P. Ajay, “Conceptual implementation of artificial intelligent based E-mobility controller in smart city environment,” *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5325116, 8 pages, 2021.

[22] M. Bradha, N. Balakrishnan, S. Suvi et al., “Experimental, computational analysis of Butein and Lanceoletin for natural dye-sensitized solar cells and stabilizing efficiency by IoT,” *Environment, Development and Sustainability*, vol. 24, no. 6, pp. 8807–8822, 2021.

[23] N. Yuvaraj, K. Srihari, G. Dhiman et al., “Nature-inspired-based approach for automated cyberbullying classification on multimedia social networking,” *Mathematical Problems in Engineering*, vol. 2021, Article ID 6644652, 12 pages, 2021.

[24] R. Huang, S. Zhang, W. Zhang, and X. Yang, “Progress of zinc oxide-based nanocomposites in the textile industry,” *IET Collaborative Intelligent Manufacturing*, vol. 3, no. 3, pp. 281–289, 2021.

[25] D. Selva, B. Nagaraj, D. Pelusi, R. Arunkumar, and A. Nair, “Intelligent network intrusion prevention feature collection and classification algorithms,” *Algorithms*, vol. 14, no. 8, p. 224, 2021.

[26] Q. W. A. Et.al, “Energetic data security management scheme using hybrid encryption algorithm over cloud environment,” *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 6, pp. 201–208, 2021.

[27] X. Liu, J. Liu, J. Chen, F. Zhong, and C. Ma, “Study on treatment of printing and dyeing waste gas in the atmosphere with Ce-Mn/GF catalyst,” *Arabian Journal of sciences*, vol. 14, no. 8, pp. 1–6, 2021.

[28] A. Hafsa, A. Sghaier, J. Malek, and M. Machhout, “Image encryption method based on improved ECC and modified aes algorithm,” *Multimedia Tools and Applications*, vol. 2021, no. 2, pp. 1–33, 2021.