Hindawi
Journal of Electrical and Computer Engineering
Volume 2023, Article ID 9762087, 1 page
https://doi.org/10.1155/2023/9762087

Retraction

Retracted: Information Security Protection of Internet of Energy Using Ensemble Public Key Algorithm under Big Data

Journal of Electrical and Computer Engineering

Received 19 December 2023; Accepted 19 December 2023; Published 20 December 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This article has been retracted by Hindawi following an investigation undertaken by the publisher [1].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) Manipulated or compromised peer review

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] B. Lin, Z. Geng, and F. Yu, "Information Security Protection of Internet of Energy Using Ensemble Public Key Algorithm under Big Data," *Journal of Electrical and Computer Engineering*, vol. 2023, Article ID 6853902, 10 pages, 2023.

Hindawi
Journal of Electrical and Computer Engineering
Volume 2023, Article ID 6853902, 10 pages
https://doi.org/10.1155/2023/6853902

Research Article

Information Security Protection of Internet of Energy Using Ensemble Public Key Algorithm under Big Data

Baode Lin,[1] Zhenwei Geng,[1] and Fengrong Yu [2]

[1]*Yunnan Power Grid Co., Ltd. Information Center, Kunming 650217, Yunnan, China*
[2]*Faculty of Metallurgical and Energy Engineering, Kunming University of Science and Technology, Kunming 650093, Yunnan, China*

Correspondence should be addressed to Fengrong Yu; 2018450261126@stu.fzfu.edu.cn

Received 19 April 2022; Accepted 30 May 2022; Published 17 February 2023

Academic Editor: Wei Liu

This work aims to solve the specific problem in the Power Internet of Things (PIoT). PIoT is vulnerable to monitoring, tampering, forgery, and other attacks during frequent data interaction under the background of big data, leading to a severe threat to the power grid's Information Security (ISEC). Cryptosystems can solve ISEC problems, such as confidentiality, data integrity, authentication, identity recognition, data control, and nonrepudiation. Thereupon, this work expounds on cryptography from public-key encryption and digital signature and puts forward the model of network information attack. Then, the security of the two cryptograms is certified against the two cyberattack modes. On this basis, an Identity-based Combined Encryption and Signature (IBCES) ensemble scheme is proposed by combining public-key encryption with the digital signature. Finally, the security of the proposed IBCES's encryption and the signature schemes is verified, and the results prove their feasibility. The results show that the proposed IBCEs are effective and feasible, fully meeting the information confidentiality requirements. Additionally, smart grid against Information Security (ISEC) algorithms must comprehensively consider network resources and computing power. This work creatively combines the two cryptosystems. The proposal breaks the traditional key segmentation principle by applying the same key to different cryptosystems and ensures the independent security of the two cryptosystems. The conclusion provides technical support for future research on cryptography.

1. Introduction

The Power Internet of Things (PIoT) was born as a highly intelligent modern power system in the era of big data based on the Internet of Things (IoT). It uses the most advanced electronic technology, sensing technology, and modern information and communication technology to achieve credibility, effectiveness, safety, and environmental friendliness [1]. Unlike the traditional power grid, the PIoT features two-way communication between smart meters and traditional meters and data systems [2]. To this end, the PIoT system must monitor the power signal in real-time and ensure the Electrical Supply System's (ESS) stability [3]. However, online message exchange also implants threats into the smart grid, such as monitoring, tampering, and counterfeiting [4, 5]. At the same time, with the wide application of new technologies follows more cybersecurity vulnerabilities [6]. Therefore, one of the main objectives of the smart grid is to collect users' power consumption messages for the personal information management center [7]. The information transmission is susceptible to cyberattacks. For example, some malware uses users' power consumption messages for intelligent theft and monitoring [8]. In order to ensure safe communication between the smart meter and Magnetic Domain Matrix Signal (MDMS), the confidentiality and authentication of communication messages in the smart grid have become a hot topic in recent discussion [9]. Indeed, a more secure key communication protocol is needed to address the above problems [10]. As a result, many terms have been coined in cybersecurity fields. As an illustration, the Combined Public Key (CPK) is an encryption algorithm to obtain large-scale encryption with minimal resources [11]. In particular, network resources and computing power must be given full consideration [12]

alongside communication delays to realize instant messaging [13].

Thereupon, against Information Security (ISEC), this work expounds on the Public Key Encryption (PKE) and digital signature systems and defines their importance in maintaining network ISEC. Then, it puts forward an Identity-based Combined Encryption and Signature (IBCES) ensemble scheme by combining encryption and signature. Finally, the security certification of IBCES is carried out from the encryption and signature schemes, respectively. The results clarify the proposed IBCES scheme's feasibility and prove that the power grid ISEC has been protected. The proposed IBCES algorithm plays a positive role in the ISEC protection in PIoT. The innovation of this work on ISEC is to combine the two passwords, which changes the traditional principle of key segmentation. Even different cryptosystems can use the same key pair and ensure that the passwords of different systems are independent and secure. The finding has made a certain contribution to developing ISEC.

This work first analyzes and summarizes the current situation of ISEC in and out of China and introduces the concepts of the PKE system and digital signature system. Then, it analyzes the security target and attack model of the PKE system, the security target, and attack model of the digital signature system and designs the IBCES scheme. Finally, the security and performance of the IBECS are proved and analyzed.

2. Literature Review

The integrity of information, user authentication, and privacy protection are the key issues to protecting the security of the smart grid. More scholars are committed to creating a secure communication environment. Ki-Aries et al. proposed an authentication system using tamper-proof equipment. The protocol had two main purposes: to protect user privacy and smart grid authentication and to detect illegal users [14] ultimately. This system adopted the message authentication code mode based on hash, and the authentication process was swift. However, the proposed protocol could only realize one-way authentication between smart appliances and smart meters and did not consider the authentication between smart meters and Meter Database Management System (MDMS). Shulha et al. proposed broadcast communication and broadcast authentication in a smart grid [15]. A one-time signature technology was used based on broadcast authentication in broadcast communication. The proposed signature technology had unique advantages, including short authentication time and low computing costs. Meanwhile, the existing method demanded high bandwidth and storage overhead. Therefore, a new one-time signature technology was proposed to address the limited environmental issues in the smart grid. Yang et al. designed an effective security protocol to simultaneously realize mutual authentication and confidentiality by using symmetric encryption [16]. The protocol adopted the traditional symmetric encryption system to process messages quickly, ensuring the real-time characteristics of the smart grid. However, in the proposed protocol, key exchange was required between smart meters and MDMS and between smart meters. Therefore, the proposed protocol had become a difficult problem for exchanging and distributing keys flexibly. On the other hand, the protocol used a chain topology to transmit data for the smart meter and reduced the communication delay. The proposed key had some disadvantages: using the smart meter as a node would increase the instability of the whole power grid. Inserting and deleting a node in the topology would regenerate the authentication key and session key, which would cause an excellent maintenance cost.

The combination of the PKE system (key generation 1, encryption, and decryption) and public key signature system (key generation 2, signature, and verification) is the CPK cryptosystem (key generation, encryption, decryption, signature, and verification). Here, the encryption and decryption algorithms are the original algorithms of the PKE system before combination [17]. Similarly, the signature and verification algorithm is the original algorithm of the pre-combination public-key signature system. The key generation algorithm is obtained by combining the key generation algorithm of the encryption system and signature system. Regarding the CPK cryptosystem, Li et al. gave its security definition. Suppose that the signature part of a CPK cryptosystem could access the decryption Oracle. In that case, it could ensure the antiexistential forgery under the adaptive selection message attack. The encryption part of the CPK cryptosystem could ensure indistinguishability under the adaptive selection ciphertext attack. When the above two statements held true, the CPK cryptosystem was secure [18]. Ali et al. proposed the attribute-based CPK cryptosystem and gave the security model. Additionally, they also gave the construction method of using a key pair to realize the three cryptosystems of encryption, decryption, and signature by using the attribute-based CPK cryptosystem [19].

At present, the security of the CPK cryptosystem has been proved, and the previous research generally has the defects of low computational efficiency and high communication cost. Therefore, based on the previous research, this work further analyzes the ISEC of the PIoT and tries to devise a new method based on the CPK cryptosystem, namely, the Identity-based Combined Encryption and Signature (IBCES) scheme.

3. Materials and Methods

3.1. Basic Concepts of the PKE System. In 1976, Diffie and Hellman first proposed the concept of the PKE system [20]. PKE system uses different keys to process messages: public keys and private keys [21]. The public key information is public and can be obtained by users, but the decryptor only owns the private key. PKE system is generally divided into encryption system and signature system. Now, the encryption system is first introduced. PKE schemes generally have three algorithms, as detailed below:

(1) Key generation algorithm generates public-private key pairs. The algorithm inputs the security parameter k and outputs a public key pk and a private

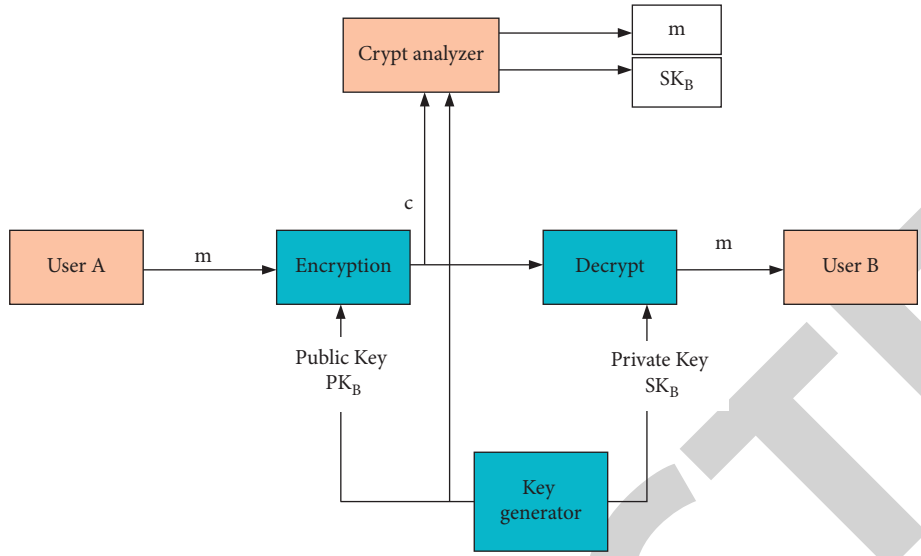

Figure 1: Communication model of PKE system.

key *sk*. The private key *sk* cannot be calculated from the public key *pk*.

(2) Encryption algorithm encrypts messages and generates ciphertext. The algorithm inputs public key *pk* and plaintext message *m* and outputs ciphertext *c*.

(3) Decryption algorithm decrypts the ciphertext and outputs message *m*. The algorithm inputs ciphertext *c* and private key *sk* and outputs plaintext message *m*.

These algorithms must meet the consistency requirements of the encryption system. Suppose $c = Encrypt(pk, m)$. In that case, $m = Decrypt(sk, m)$. *Encrypt* and *Decrypt* represent the encryption and decryption algorithms, respectively [22]. The communication model of the PKE system is shown in Figure 1.

In Figure 1, user *A* is the sender, and user *B* is the receiver. The key generator will generate a (PK_B, SK_B) key pair for user *B*. PK_B is the public key, which everyone can obtain. By comparison, the private key SK_B is only known to user *B*. To send message *m* to user *B*, user *A* first encrypts message *m* with user *B*'s public key PK_B using the encryption algorithm: $c = \text{Encrypt}(PK_B, m)$. Here, *c* is the ciphertext, and Encrypt represents the encryption algorithm. User *A* sends ciphertext *c* to user *B*. After receiving the ciphertext *c*, user *B* decrypts the ciphertext *c* with its private key SK_B based on the decryption algorithm: $m = \text{Decrypt}(SK_B, c)$, where Decrypt stands for the decryption algorithm.

3.2. Security Target and Attack Model of PKE System. In order to prove its security, the security goal of the cryptosystem must be clarified first [23]. According to the opponent's different capabilities and attack targets, the attack modes of the PKE system can include the following three categories: selective plaintext attack, selective ciphertext attack, and adaptive selective secret file attack [24]. Given the security goal and attack and defense modes of the PKE system, people can easily make sense of the security concept of the PKE system. Suppose that a PKE scheme has the Indistinguishability against Adaptive Chosen Ciphertext Attack (IND-CCA2) and meets the polynomial kernel function's security. In that case, the PKE scheme is deemed secure [25]. Next, the specific proof idea of this definition is given. This is a game between opponent and challenger, which has four stages. Initial stage: challenger C runs the system-established algorithm to generate system parameters and a public/private key pair (pk, sk). *C* sends *pk* to opponent *A* and saves *sk*. Phase 1: opponent *A* performs a polynomially bounded decryption query. At this stage, opponent *A* submits a ciphertext *c* to challenger *C*. Challenger *C* runs the decryption algorithm. If the ciphertext is legal, it returns the message *m* to *A*; otherwise, it returns the rejection symbol $\perp$. Challenge phase: opponent *A* decides when to end the decryption query of phase 1 and enter the challenge phase. A generates two plaintexts m_0 and m_1, of the same length and sends them to *C*. *C* randomly selects a bit $b \in \{0, 1\}$ and calculates the ciphertext $c^* = E(pk, mb)$ of mb. *C* sends c^* to *A* as challenge ciphertext. Stage 2: in this stage, opponent *A* can perform a polynomial-time decryption query like stage 1. However, opponent *A* cannot decrypt the ciphertext c^* at this stage. Guess stage: opponent *A* obtains useful information by decrypting the query and outputs a bit *B b*'. If b' = *b*, opponent *A* wins the game. Figure 2 shows a game between opponent *A* and challenger *C*.

Figure 2 summarizes the whole process of the security game. Suppose that no opponent can win the above game with a nonnegligible advantage in polynomial bounded time. In that case, the PKE has polynomial security under CCA2.

3.3. Basic Concepts of the Digital Signature System. Because the signer signs through his own private key and the private key information are only known to the signer, the signature can ensure the signer's data integrity, confirmation, and nonrepudiation. A digital signature system generally consists of key generation, signature, and verification. The above algorithm needs to meet the consistency requirements [26].

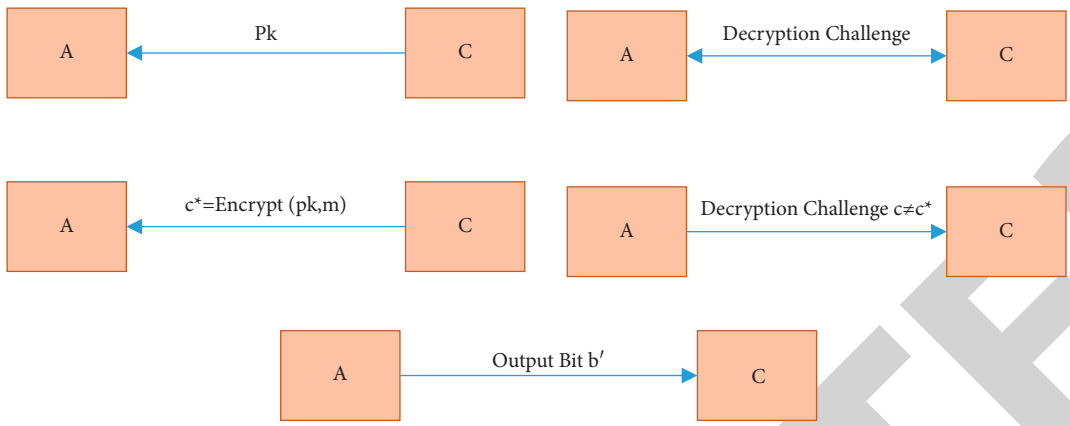

Figure 2: CCA2 security game of PKE system.

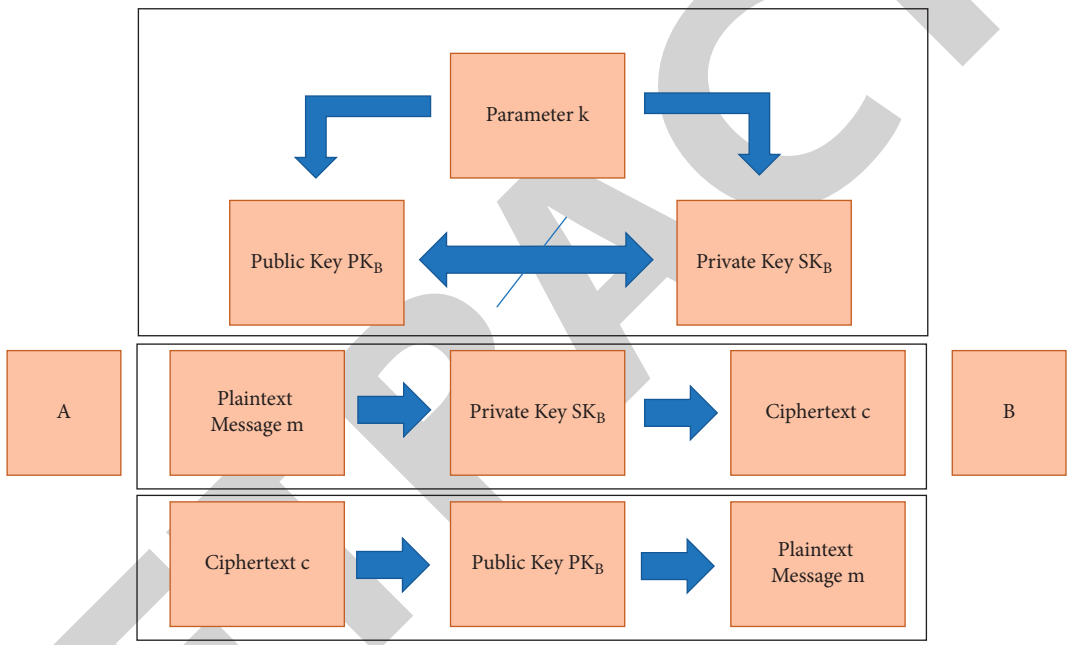

Figure 3: Digital signature communication module.

The communication model of the digital signature system is illustrated in Figure 3.

A and B are the sender and the receiver. The key generator generates a key pair: (PK_B, SK_B) for A, where PK_B is the public key, and SK_B is the private key. To send message m to B, A needs to encrypt m with the private key to obtain ciphertext c. Then, A sends ciphertext c to B. Upon reception, B decrypts c with the public key to obtain message m.

3.4. Security Target and Attack Model of a Digital Signature System. Similar to the PKE system, to verify the security of digital signature methods, there is a need to clarify the security objectives [27]. The digital signature system mainly includes four types of forgery: complete breach, universal forgery, selective forgery, and existential forgery [28].

Different opponents have different attack capabilities. The digital signature system mainly includes three attack models: key only attack, known message attack, and adaptive Chosen Message Attack (CMA) [29]. Once the security target and attack model are determined, the security definition can be given to the digital signature system. A digital signature scheme with Existential Unforgeability Against Adaptive Chosen Messages Attack (EUF-CMA) is defined as secure. Figure 4 is the security game between opponent A and Challenger C [30]. The adaptive choice message-based attack game of the digital signature system consists of three stages similar to that in Figure 4.

Figure 4 summarizes the entire game process of the signature scheme under the adaptive CMA. Suppose that no opponent wins the game with a nonnegligible advantage in polynomially bounded time. In that case, this digital signature scheme is EUF-CMA [6].

3.5. Identity-Based CPK Scheme. Two or more encryption and signature schemes are combined such that they share the same key generation algorithm, while the existing encrypt/

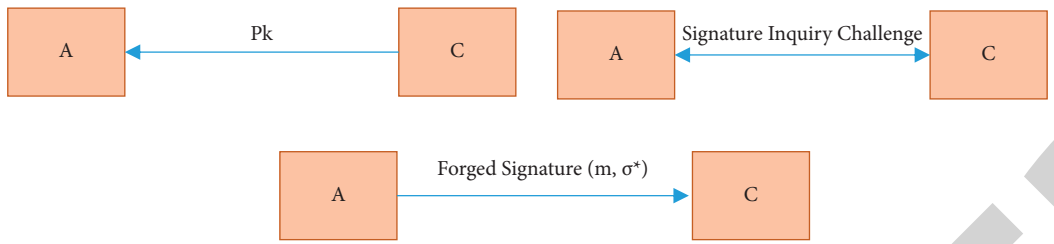

Figure 4: Adaptive CMA game of digital signature system.

decrypt and sign/verify algorithms are reserved. This is called the CPK scheme [31]. The basic structure of the CPK scheme is demonstrated in Figure 5.

The CPK system has several advantages. Consider a scenario in which each party can only save one public/private key pair. In that case, in Public Key Infrastructure-(PKI-) based cryptosystem, the encryption and signature systems can significantly reduce the encryption space, public-key certificate space, and certification time. By comparison, the application only needs to retain one identity information in identity-based or certificate-less cryptosystems, thus reducing the storage space and encryption acquisition time.

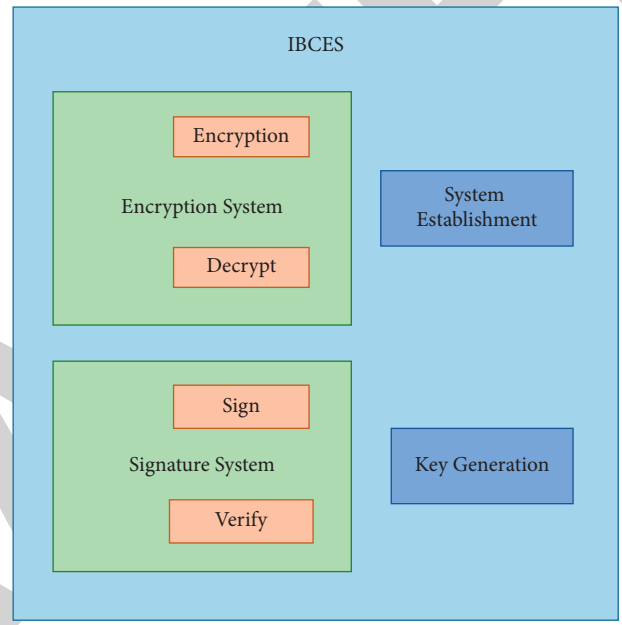

Figure 5: CPK system.

3.6. Algorithm Composition of the Formal Model

(1) System establishment

The algorithm is completed by the Private Key Generator (PKG). It sets the initial basic parameters for the encryption method, including the system public parameter param and the master key s used to generate the user's private key. PKG saves the master key s and makes other information public [32].

(2) Key extraction

The algorithm is completed by PKG. According to the initial system parameters and the user's Identity Document (ID), PKG uses this method to obtain the corresponding public key Q_{ID} and private key S_{ID}.

(3) Encryption

The algorithm is completed by the encryptor. The algorithm encrypts the message m and outputs a ciphertext c according to the system public parameters and the receiver's public key Q_{ID}.

(4) Decryption

The algorithm is completed by the decryptor. The decryptor decrypts the ciphertext c according to its own private key S_{ID}. If the decryption is successful, it outputs the plaintext message m or symbol-$\times$(indicates decryption failure).

(5) Signature

The algorithm is completed by the signer. The algorithm signs the message m according to the system public parameters and its own private key S_{ID} and outputs a signature σ.

(6) Verification

Upon receiving signature σ, the receiver verifies whether the signature is legal according to the public system parameters and the sender's public key Q_{ID}. The algorithm outputs the symbol $\surd$ or $\times$. If the verification is successful, the receiver will receive the message m; otherwise, it will refuse to receive.

3.7. The Security Concept of the Identity-Based Combined Encryption and Signature (IBCES) Ensemble Scheme. An identity-based encryption system should meet IND-ID-CCA2, and an identity-based signature system should meet EUF-ID-CMA. Next, the security model of Identity-based Combined Encryption and Signature (IBCES) is proposed [33].

3.7.1. IND-IBCES-CCA2. Suppose that (key generation, encryption, decryption, signature, and verification) is a combined encryption and signature method. In that case, the security definition of the IBCES encryption system is given as follows. This is a game between Challenger C and opponent A. Figure 6 is a schematic diagram of the IBCES encryption system under CCA2. The whole process is divided into the initial stage, stage 1, the challenge stage, stage 2, and the guess stage.

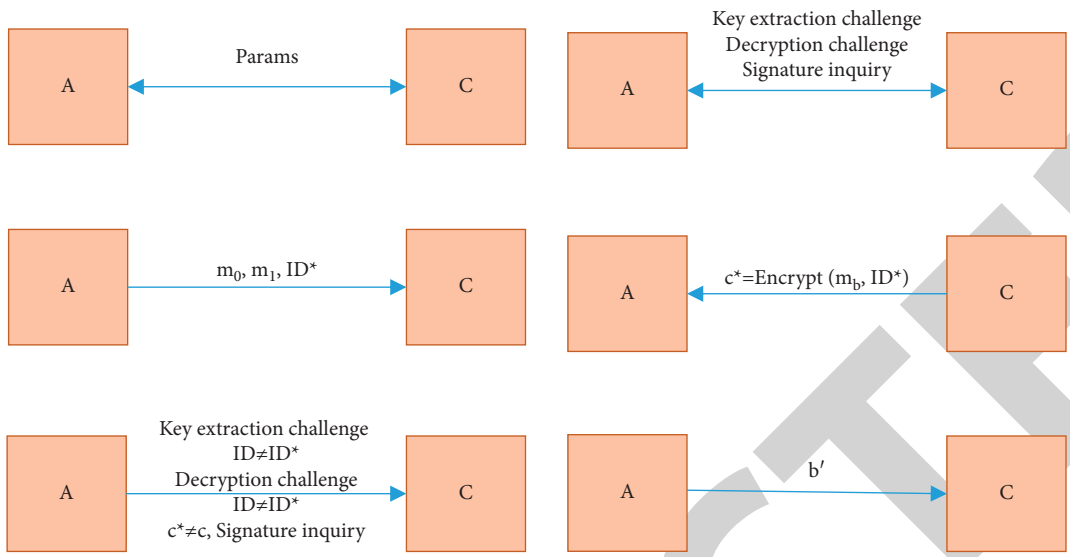

Figure 6: Schematic diagram of IBCES encryption system under CCA2.

According to Figure 6, IND-IBCES-CCA2 is defined as follows. Suppose that no opponent A can win the above game with a nonnegligible advantage after q key extraction, decryption, and signature queries in a polynomial bounded time. In that case, the IBCES encryption system is secure against CCA2, namely, IND-IBCES-CCA2.

3.7.2. EUF-IBCES-CMA. Suppose that (key generation, encryption, decryption, signature, and verification) is a combined encryption-signature system. In that case, the security definition of existence forgery of its IBCES signature system is given as follows. This is a game between challenger C and opponent A. Figure 7 draws the certificate flow of the IBCES signature system.

According to Figure 7, EUF-IBCES-CMA is defined as follows. Suppose that no opponent can win the above games with a nonnegligible advantage after q key extraction, signature, and decryption queries in a polynomial bounded time. In that case, the IBCES signature system is secure against CMA, namely, EUF-IBCES-CMA.

3.8. Design of IBCES Ensemble Scheme. The main content here is to propose an IBCES scheme [13].

3.8.1. System Establishment Stage. With a cyclic additive group G_1, the order is a prime number q. G_2 is a cyclic multiplication group, and G and G_2 have the same order. P is a generator in the group $G_1 1$, and there is a bilinear mapping e: $G_1 \times G_1 \longrightarrow G$. Define four secure hash functions: H_1: $\{0,1\}^* \longrightarrow Z_q^*, H_2$: $\{0,1\}^* \times G_2 \times G_1^4 \longrightarrow Z_q^*, H_3$: $\{0,1\}^* \longrightarrow \{0,1\}^M, H_4$: $\{0,1\}^* \times G_1 \times G_2 \longrightarrow Z_q^*$. M is the plaintext length, and Z_q^* means the multiplicative cyclic group modulo q (the elements in the group do not include 0). PKG randomly selects $s \in Z_q^*$ as the master key and computes $P_{pub} = sP$, $g = e(p, p)$. PKG exposes system parameters $(G_1, G_2, P, P_{pub}, g, e, H1, H2, H3, H4)$ and saves the master key s.

3.8.2. Key Extraction. Given an identity ID, PKG generates a public-private key pair $(Q_{\mathrm{ID}}, S_{\mathrm{ID}})$ according to the system parameters generated above and the master key s, the private key $S_{ID} = (Q_{I\,D} + s)^{-1}P$, and public key $Q_{I\,D} = H_1(I\,D)$. Finally, PKG transfers the private key through a secure channel to the corresponding user.

3.8.3. Offline Encryption. Given the public system parameters, the offline encryption algorithm randomly selects $x, a \in Z_q^*$ and calculates according to equations (1)–(3):

$$R = g^x, \tag{1}$$

$$T_0 = aP, \tag{2}$$

$$T_1 = x\left(aP + P_{pub}\right). \tag{3}$$

In equations (1)–(3), R is a new bit parameter generated about x. T_0 and T_1 are new time parameters, and the final generated offline ciphertext is $\varnothing = \{a, x, R, T_0, T_1\}$.

3.8.4. Online Encryption. Given $(m, I\,D, \varnothing)$, the online encryption algorithm is calculated by equations (4)–(6).

$$u = x\left(H_1(I\,D) - a\right)\mathrm{modq}, \tag{4}$$

$$c_1 = H_2(m, R, T_0, T_1, u)x - a\mathrm{modq}, \tag{5}$$

$$c_2 = m \otimes H_3(R). \tag{6}$$

Equations (4)–(6), u is a new bit parameter generated by x. c_1 and c_2 are the new ciphertext. Finally, the generated online ciphertext is $c = (T_0, T_1, u, c_1, c_2)$.

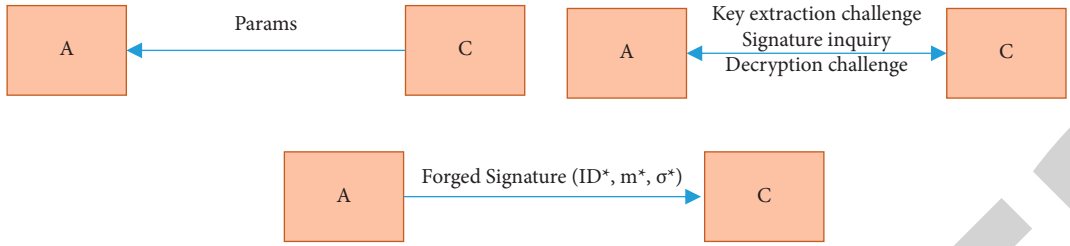

Figure 7: Schematic diagram of IBCES signature system under CMA.

3.8.5. Decryption. Given $(c, I\ D, S_{I\ D})$, the decryption algorithm is counted by equations (7) and (8).

$$R = e\left(uP + T_1, S_{ID}\right), \tag{7}$$

$$m = c_2 \otimes H_3(R). \tag{8}$$

Suppose that $R^{H_2(m,R,T_0,T_1,u)} = e(c_1P + T_0, P)$ holds. In that case, the message m is output; otherwise, the symbol $\times$ is output.

3.8.6. Offline Signature. Given $(I\ D, S_{I\ D})$, the offline signature algorithm randomly selects l, $\alpha \in Z_q^*$ and calculates according to equations (9) and (10):

$$r = g^l, \tag{9}$$

$$S' = \alpha S_{ID}. \tag{10}$$

In equations (9) and (10), r is a new bit parameter generated by l. S' denotes a randomly generated pseudokey. Finally, the offline signature is $\delta = (l, \alpha^{-1}, r, S\prime)$.

3.8.7. Online Signature. Given $(I\ D, \delta)$, the online signature algorithm is calculated by equations (11) and (12):

$$h = H_4\left(m, r, S'\right), \tag{11}$$

$$\theta = (l + h)\alpha^{-1}\ mod q. \tag{12}$$

In equations (11) and (12), h is the newly defined hash function. θ signifies the key factor to verify the master key and the pseudokey. Finally, the online signature is generated as $\sigma = (h, \theta, S\prime)$.

3.8.8. Verification. Given $(m, I\ D, \sigma)$, the verification algorithm is specified in equations (13) and (14).

$$S = \theta S', \tag{13}$$

$$r = e\left(S, H_1(I\ D)P + P_{pub}\right)g^{-h}. \tag{14}$$

Suppose that $h = H_4(m, r, S')$ holds. In that case, the receiver accepts the signature; otherwise, it outputs symbol $\times$.

4. Results and Discussion

4.1. Security Certification of IBCES Ensemble Scheme. First, it is proved that the IBCES encryption scheme satisfies the IND-IBCES-CCA2 security, as exhibited in Figure 8. There is only one difference between the encryption part of the IBCES scheme and the traditional security proof method of identity-based encryption scheme. Opponent A can access both the decryption Oracle and the signature Oracle. The challenger can simulate a signature Oracle. Suppose that the simulated Oracle can respond to the challenge of the opponent like a real signature Oracle. In that case, it can be said that the opponent can access the signature Oracle or not has zero impact. In the proof process, challenger C is the challenger of the IBCES encryption part. C can ask its challenger B for key extraction and decryption and send the result returned by B to opponent A.

Opponent A performs polynomially bounded key extraction, decryption, and signature queries. In the key extraction and query stage, A provides a set of IDs to C. C sends the ID to its own Oracle B and feeds back the response results to A. In the decryption query stage, A submits a set of IDs and ciphertext C. Similarly, C can call his own Oracle and send the response to A. Therefore, in addition to the signature inquiry, C can correctly answer all A's challenges. When A asks for a signature, C needs to construct a signature simulator SIG to respond to A's challenge because C has no signature Oracle. At this time, when A submits a set of IDs and a message m to C, C first selects randomly in order to output a signature θ, $h \in Z_q^*$, $S' \in G_1$. Then, it calculates $S = \theta S'$, $r = e(S, H_1(I\ D)P + P_{pub})g^{-h}$ and defines $h = H_4(m, r, S')$. Finally, C will send $(h, \theta, S\prime)$ to A. According to the verification algorithm, the signature verification results of all SIG outputs are legal. It shows that the error probability of C is negligible. That is, even if Challenger C does not have a signature Oracle, a signature Oracle can be simulated to answer A's challenge when the opponent asks for a signature. Therefore, whether opponent A can access the signature Oracle or not has no impact on the security of the IBCES encryption scheme. The IBCES encryption scheme can meet the IND-IBCES-CCA2 security.

Furthermore, the security of the IBCES signature scheme is proved, as in Figure 9. Similar to encryption, there is only one difference between the signature security proof of the IBCES scheme and the security proof of the traditional identity-based signature scheme. Opponent A can access both the signature Oracle and the decryption Oracle. Suppose that the challenger can simulate a decryption Oracle to respond to the opponent's challenge. Even if the opponent

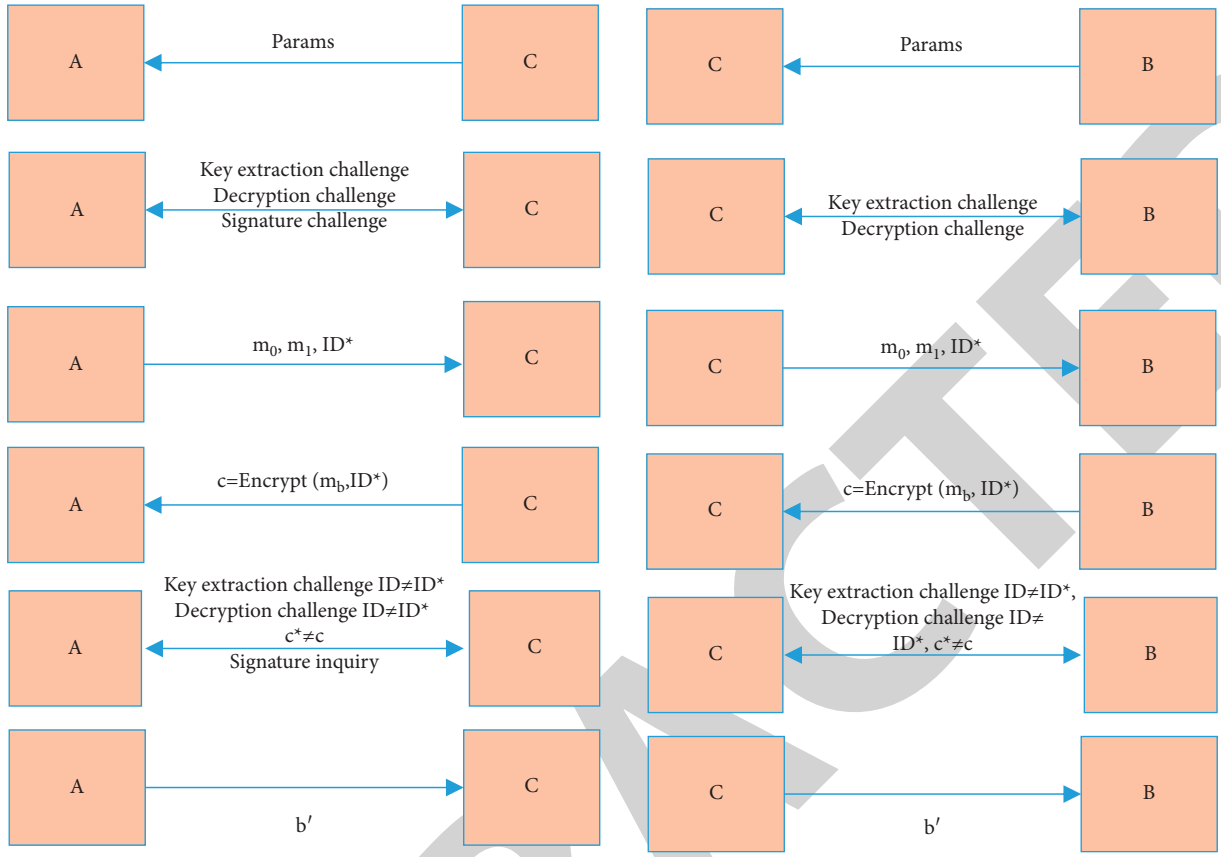

Figure 8: IBCES encryption scheme certification.

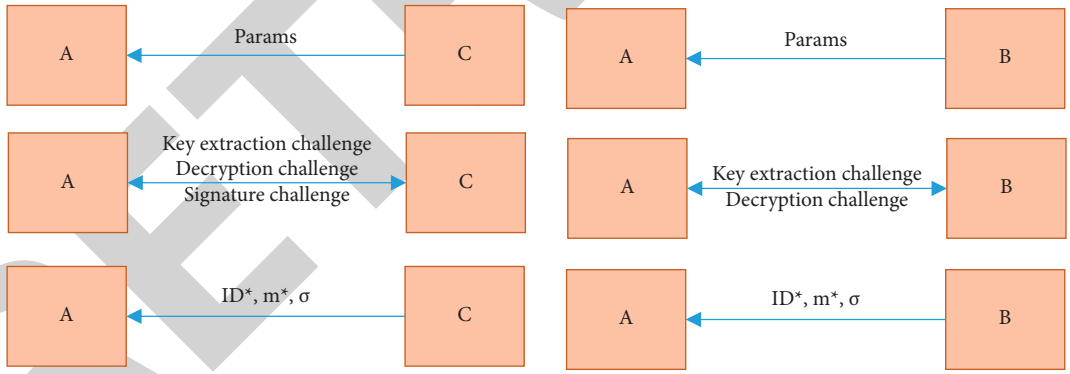

Figure 9: IBCES signature scheme certification.

can access the decryption Oracle, it is not helpful. In this way, the EUF-CMA security proof of the signature part of the IBCES scheme can be transformed into the security proof of the original signature scheme. In this game, C is both a challenger and an opponent. C performs a key extraction query and signature query like its challenger B and sends the result returned by B to opponent A.

When A is in the decryption challenge phase, C needs to construct a decryption simulator DEC to answer A's challenge. There is a difference between the decryption simulator DEC and the real decryption Oracle. When the DEC outputs ×, the real decryption Oracle can correctly return a message m. This error between the two is actually the probability that A does not perform a (m, R, T_0, T_1, u) hash query on H_2. Thus, the probability that C can succeed is close to 1. In other words, even if challenger C does not have a decryption Oracle, a simulated signature Oracle can cope with the challenge from A. Therefore, whether opponent A can access the signature Oracle or not does not affect the security of the IBCES signature scheme. Now, it is derived that the IBCES signature scheme meets the EUF-CMA security.

4.2. Performance Analysis of IBCES Ensemble Scheme. There are two main security performance concerns: the computational cost and the signature scheme's communication

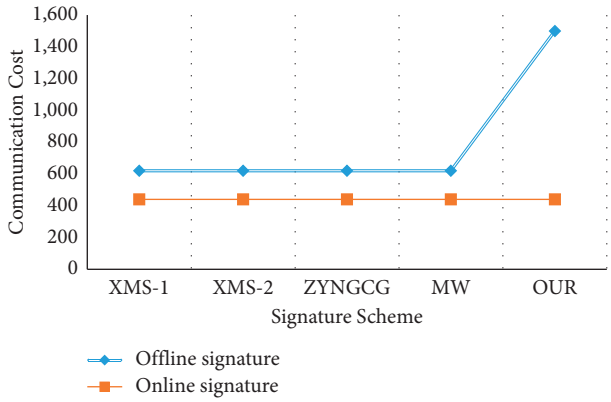

Figure 10: Communication cost comparison.

cost. The proposed IBCES ensemble scheme is compared with four other online/offline signature schemes by factoring in the computational cost and ciphertext length, as plotted in Figure 10.

Given the same security level, the proposed IBCES ensemble scheme's performance is faster in the offline signature stage because the exponential operation is faster than the point-to-point operation. Meanwhile, it is faster than the other four schemes in the decryption stage because the pair operation is more time-consuming than the dot product operation. Figure 10 proves that the computational cost of the proposed IBCES ensemble scheme is the lowest.

5. Conclusions

This work proves the security of the combined encryption and signature system. The encryption part of the proposed IBCES scheme meets the IND-IBCES-CCA2 security. The security is also proved for the signature part of the IBCES scheme. Meanwhile, this work compares the performance of different combined encryption-signature systems. The computational cost of the signature scheme selected in this work is the lowest. Although this work has made some efforts in the security of the smart grid, there are still some shortcomings. All the security verification methods are verified under the random prediction model. All hash functions are regarded as ideal. However, verifying security under the random prediction model is not necessarily safe and reliable in the real environment. Therefore, future works will design a protocol with higher security and a faster communication rate for the system. The research finding provides a reference for the maintenance and stability of the power system. It provides an improvement direction for the further development of the smart grid under the PIoT.

Data Availability

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

Conflicts of Interest

The authors declare no potential conflicts of interest.

References

[1] W. Hu, W. Yao, Y. Hu, and H. Li, "Selection of cluster heads for wireless sensor network in ubiquitous power internet of things," *International Journal of Computers, Communications & Control*, vol. 14, no. 3, pp. 344–358, 2019.

[2] S. Shim, M. C. Belanger, A. R. Harris, J. M. Munson, and R. R. Pompano, "Two-way communication between ex vivo tissues on a microfluidic chip: application to tumor–lymph node interaction," *Lab on a Chip*, vol. 19, no. 6, pp. 1013–1026, 2019.

[3] M. Chen, Y. Cheng, Z. Cheng, D. Zhang, Y. Lv, and R. Liu, "Energy storage traction power supply system and control strategy for an electrified railway," *IET Generation, Transmission & Distribution*, vol. 14, no. 12, pp. 2304–2314, 2020.

[4] M. Weiss and M. Weiss, "An assessment of threats to the American power grid," *Energy, Sustainability and Society*, vol. 9, no. 1, p. 18, 2019.

[5] H. T. Reda, A. Anwar, and A. Mahmood, "Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts," *Renewable and Sustainable Energy Reviews*, vol. 163, Article ID 112423, 2022.

[6] S. Gurung, M. Kanti Ghose, and A. Subedi, "Deep learning approach on network intrusion detection system using NSL-KDD dataset," *International Journal of Computer Network and Information Security*, vol. 11, no. 3, pp. 8–14, 2019.

[7] S. Whittaker and C. Massey, "Mood and personal information management: how we feel influences how we organize our information," *Personal and Ubiquitous Computing*, vol. 24, no. 5, pp. 695–707, 2020.

[8] X. L. Yu, O. Al-Bataineh, D. Lo, and A. Roychoudhury, "Smart contract repair," *ACM Transactions on Software Engineering and Methodology*, vol. 29, no. 4, pp. 1–32, 2020.

[9] S. M. S. Hussain, S. M. Farooq, and T. S. Ustun, "A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages," *IEEE Transactions on Power Delivery*, vol. 35, no. 5, pp. 2565–2567, 2020.

[10] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: authentication and key generation," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 92–98, 2019.

[11] P. S. N∗, A. V. Kumar, and A. C. R, "On the sanctuary of a combined confusion and diffusion based scheme for image encryption," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 1, pp. 3258–3263, 2019.

[12] D. Muyizere, L. K. Letting, and B. B. Munyazikwiye, "Effects of communication signal delay on the power grid: a review," *Electronics*, vol. 11, no. 6, p. 874, 2022.

[13] G. Ye, K. Jiao, X. Huang, B. M. Goi, and W. S. Yap, "An image encryption scheme based on public key cryptosystem and quantum logistic map," *Scientific Reports*, vol. 10, no. 1, p. 21044, 2020.

[14] D. Ki-Aries, S. Faily, H. Dogan, and C. Williams, "Assessing system of systems information security risk with oasosis," *Computers & Security*, vol. 117, 2022.

[15] O. Shulha, I. Yanenkova, M. Kuzub, I. Muda, and V. Nazarenko, "Banking information resource cybersecurity system modeling," *JOItmC*, vol. 8, no. 2, p. 80, 2022.

[16] Y. Yang, L. Zhang, Y. Zhao, K. K. R. Choo, and Y. Zhang, "Privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based vanet," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 317–331, 2022.

[17] M. Shaohui, G. Tuerhong, M. Wushouer, and T. Yibulayin, "Pca mix-based hotelling's t2 multivariate control charts for intrusion detection system," *IET Information Security*, vol. 16, no. 3, pp. 161–177, 2022.
[18] B. Li, Q. Zhou, Y. Cao, and X. Si, "Cognitively reconfigurable mimic-based heterogeneous password recovery system," *Computers & Security*, vol. 116, 2022.
[19] S. M. Ali, S. M. N. Hoq, A. B. M. M. Bari, G. Kabir, and S. K. Paul, "Evaluating factors contributing to the failure of information system in the banking industry," *PLoS One*, vol. 17, no. 3, p. e0265674, 2022.
[20] N. A. Kako, H. T. Sadeeq, and A. R. Abrahim, "New symmetric key cipher capable of digraph to single letter conversion utilizing binary system," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, p. 1028, 2020.
[21] S. M. Aldossari and K. C. Chen, "Machine learning for wireless communication channel modeling: an overview," *Wireless Personal Communications*, vol. 106, no. 1, pp. 41–70, 2019.
[22] A. M. Hinkes, "Throw away the key, or the key holder? coercive contempt for lost or forgotten cryptocurrency private keys, or obstinate holders," *Northwestern Journal of Technology and Intellectual Property*, vol. 16, no. 4, p. 225, 2019.
[23] J. Al-Azzeh, B. Zahran, and Z. Alqadi, "A novel based on image blocking method to encrypt-decrypt color," *JOIV: International Journal on Informatics Visualization*, vol. 3, no. 1, pp. 86–93, 2019.
[24] O. A. Alzubi, J. A. Alzubi, O. Dorgham, and M. Alsayyed, "Cryptosystem design based on Hermitian curves for IoT security," *The Journal of Supercomputing*, vol. 76, no. 11, pp. 8566–8589, 2020.
[25] O. Zaki, M. Dunnigan, V. Robu, and D. Flynn, "Reliability and safety of autonomous systems based on semantic modelling for self-certification," *Robotics*, vol. 10, no. 1, 2021.
[26] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, no. 2, pp. 943–961, 2019.
[27] C. Chen, X. Li, A. N. Belkacem et al., "The mixed kernel function SVM-based point cloud classification," *International Journal of Precision Engineering and Manufacturing*, vol. 20, no. 5, pp. 737–747, 2019.
[28] A. K. Wong, R. S. G. Sealfon, C. L. Theesfeld, and O. G. Troyanskaya, "Decoding disease: from genomes to networks to phenotypes," *Nature Reviews Genetics*, vol. 22, no. 12, pp. 774–790, 2021.
[29] I. Lubis, "The validity of the electronic signature in electronic general meeting of shareholders S of the limited company's," *Kanun Jurnal Ilmu Hukum*, vol. 23, no. 2, pp. 257–273, 2021.
[30] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, "Digital signature scheme for information non-repudiation in blockchain: a state of the art review," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, p. 56, 2020.
[31] X. Yao, H. Kong, H. Liu, T. Qiu, and H. Ning, "An attribute credential based public key scheme for fog computing in digital manufacturing," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 4, pp. 2297–2307, 2019.
[32] B. Raj, I. Ahmedy, M. Y. I. Idris, and R. Md. Noor, "A survey on cluster head selection and cluster formation methods in wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–53, 2022.
[33] T. Y. Wu, C. M. Chen, K. H. Wang, C. Meng, and E. K. Wang, "A provably secure certificateless public key encryption with keyword search," *Journal of the Chinese Institute of Engineers*, vol. 42, no. 1, pp. 20–28, 2019.