energies

MDPI

Article

A Certificateless Authenticated Key Agreement Scheme for the Power IoT

Wenchao Cui [1], Rui Cheng [1,*], Kehe Wu [1], Yuling Su [1] and Yuqing Lei [2]

[1] School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China; cuzz@ncepu.edu.cn (W.C.); wkh@ncepu.edu.cn (K.W.); suyuling@ncepu.edu.cn (Y.S.)
[2] China Electric Power Research Institute, No. 15, Qinghe Xiaoying Road, Beijing 100192, China; yuqinglei@epri.sgcc.com.cn
* Correspondence: chengrui@ncepu.edu.cn

Abstract: Power Internet of Things (IoT) is the application of IoT technology in the field of power grid, which can better control all kinds of power equipment, power personnel and operating environment. However, access to mass terminals brings higher requirements for terminal authentication and key management for the power IoT. And the traditional public key infrastructure (PKI) and identity-based public key cryptography (IB-PKC) exist the problems of certificate management and key escrow. Therefore, the paper proposes a novel authenticated key agreement scheme based on the certificateless public key cryptography (CL-PKC) mechanism. In addition, the proposed scheme is proven with the improved extended Canetti-Krawczyk (eCK) security model. Finally, the implementation of the authenticated key agreement protocol is given based on the actual application requirement of the power IoT, and the analysis and comparison of the simulation demonstrates that the proposed scheme has higher efficiency and would be suitable for the power IoT.

Keywords: power IoT; PKI; CL-PKC; authenticated key agreement; eCK security model

Citation: Cui, W.; Cheng, R.; Wu, K.; Su, Y.; Lei, Y. A Certificateless Authenticated Key Agreement Scheme for the Power IoT. *Energies* **2021**, *14*, 6317. https://doi.org/10.3390/en14196317

Academic Editor: Sangheon Pack

Received: 24 September 2021
Accepted: 30 September 2021
Published: 3 October 2021

1. Introduction

Power IoT is the specific application, implementation and evolution direction of the IoT technology in the power grid [1]. The power IoT can dynamically adjust the whole power grid in an all-round way according to the state data of the equipment which locates in all areas of power grid. For example, the traditional power plants can transform into smart power plants by combing with IoT, artificial intelligence and some other technologies to achieve interconnection and information sharing between equipment and equipment, person and equipment [2].

By the end of 2018, State Grid Corporation of China had accessed 540 million power terminals and basically realized the comprehensive information collection of control operation and electricity metering in the grid [3,4]. With the advancement of the construction of the power IoT, A large number of the IoT terminals would be deployed in the whole areas in power plants, transmission line, power substation, distribution station and consumers to realize the real-time monitoring of the grids. Therefore, the process of designing an efficient authenticated key agreement protocol, achieve identity authentication and develop a key agreement that includes the privacy, integrality and undeniability of communication data with massive power IoT terminals has become a focus in current research.

The authenticated key agreement scheme could be implemented by three cipher systems: PKI, IB-PKC and CL-PKC. In the PKI system, the users or the terminals could implement identity authentication by the digital certificate, which contained the public key, and was issued by the certificate authority (CA). However, with the increase of the users or terminals will bring a heavy burden of management certificate such as certificate generation, issuance, savings, verification, and revocation to the PKI system. The IBC system

uses a device's own unique identifier, such as a CPU or disk code, to replace the digital certificate and solve the PKI system's complicated certificate management problem [5]. However, in the IB-PKC system, the user's private key is fully generated by one authoritative private key generator (PKG). Since the PKG has the master key of the system, the entire system is insecure if an attacker obtains the master key of the PKG or the PKG itself is an attacker. The problem of the key escrow existing in the IB-PKC system could be solved in the CL-PKC system. In the CL-PKC system as the users' keys are co generated by the users and the master key of the trusted key generating center (KGC). Therefore, even if the master key of the system is obtained by an attacker, the attacker cannot obtain the user's private key.

Compared with the PKI and IB-PKC, the CL-PKC system has critical advantages in certificate management and key escrow. Therefore, this paper proposes a novel authenticated key agreement scheme that could be suitable for the power IoT, which can effectively improve the security of the power IoT and the grids.

In this paper, our main contributions are as follows:

(1) An efficient authenticated key agreement scheme based on CL-PKC has been proposed, which uses simple point multiplication of elliptic curves to replace complex bilinear pairing to make it simpler and more practical for the terminals with limited computing resources in power IoT.
(2) The security of the proposed authenticated key agreement scheme has been proved by the the e^2CK security model where e^2CK security model is more secure and it have defined the authenticated key agreement protocol is secure as long as any secret value of both parities is not disclosed.
(3) We program and implement the proposed scheme and protocol and make it more applicable for the power IoT, while the performance of other protocols is compared.

In this paper, the introduction and background of the power IoT and CL-PKC are described in Section 1 and some related works has been summarized in Section 2. Section 3 presents some basic knowledge that would need in the paper as the preliminaries. The detailed design and principle of our proposed scheme based on CL-PKC are introduced in Section 4. The analysis and comparison of the simulation are given in Section 5 and our current and upcoming work have been concluded in Section 6.

2. Related Work

Since Al-Riyami et al., put forward the first concept of CL-PKC [6], many works and researches have been raised to enhance the key agreement scheme based on their work. Mandt et al., pointed out that it is unable to resist temporary key leakage attacks and proposed a new scheme. However, the new scheme was at risk of key compromise impersonation (KCI) [7]. Zhang et al., proposed a modified Bellare-Rogaway (mBR) model applicable to certificateless systems and two-party key agreement protocols based on the IB-PKC and proved it under mBR model [8]. He et al., also presented a novel authenticated key agreement protocol with point multiplication and proved it under the mBR model [9]. Sun et al., proved that the two above schemes were vulnerable, meaning that the session key could be calculated by the adversary who could acquire the ephemeral secret keys in the communication between the two parties [10]. Wu et al., proposed a scheme based on the eCK model, but it was also at risk of a KCI attack [11]. Kim et al., Also bring a two-party CLAKA scheme with pairing-free and proved the secure with the eCK model [12]. Bala et al., reminded that the scheme [12] was vulnerable to KCI attacks [13]. Tu et al., proposed a very reliable and secure authenticated key agreement protocol with pairing-free based on CL-PKC. It is suitable for smart media and mobile environment, while proving its security using the eCK model [14]. Sun et al., also proposed a secure pairing-free authenticated key agreement protocol based on CL-PKC, and the strengthened eCK model was used to prove it, but the scheme had heavy communication and calculation costs because the lengths of the users' public and private keys were twice as long as those of other

schemes [15]. Collen et al., improved the eCK model and presented a one-way two-party authenticated key agreement scheme [16]. Lippold et al., enhanced the eCK model to the e^2CK model and proposed an authenticated key agreement scheme under the model to formally prove its security [17]. All of the schemes mentioned above used bilinear pairings; hence, the cost of the calculations was reasonable. Yang et al., proposed a new certificateless model and proposed a two-party agreement scheme under the model [18]. Huang et al., designed a security model of a one-way two-party authentication key agreement that was suitable for the CL-PKC system, and they formally proved its security with the eCK security model. However, the scheme only ensured one-way identity security and exhibited temporary secret value leakage attacks [19].

In terms of the state grid, there has also been much research focused on an authenticated key agreement. For example, State Grid issued a set of standard security access specifications that stipulated that the grid terminals need to use the PKI system and the SM2 digital certificate to complete identity authentication and key agreement in 2014 [20]. Lin et al., proposed an improved safety communication scheme based on [20], which enhanced the security of network communication by adding time stamps and digital signatures to the messages [21]. Tsai et al., proposed a novel authentication protocol which could be applied in the smart grid, but employed bilinear pairing that had a heavy computational cost [22]. Fouda et al., presented a lightweight authentication way for the smart meters in the distributed network with the Diffie-Hellman exchange protocol [23]. However, the scheme leads to high computational complexity. Mahmood et al., pointed out that the scheme is computational expensive and presented one authentication scheme based on the elliptic curve cryptography (ECC) that could implement the mutual identity authentication [24]. Li et al., presented one two-way authentication scheme based on SM2 for the radio frequency identification system and proved it with BAN logic [25]. Li et al., proposed an improved SM2-based key agreement and a mutual identify authentication scheme for smart grid [26]. However, the security schemes above were all achieved by PKI systems, which have complicated certificate management and were not suitable for the power IoT with a large number of terminals. Deng et al., presented a two parties' authenticated key agreement protocol for smart grids based on CL-PCK [27], and Batamuliza et al., introduced a certificateless "signcryption" for a key distribution scheme in a state grid, but he did not give detailed proofs of the scheme's security [28].

According to the above analysis, most of the papers used PKI system to achieve the mutual authenticated key agreement in the state grid, but these schemes were not suited for the power IoT with massive terminals and also some certificateless schemes had heavy communication and calculation costs as they used bilinear pairing and exponential operations. So before introducing the proposed scheme, some basic knowledge will be presented in the following section.

3. Preliminaries

In this section, the basis knowledge of ECC and the computational Diffie–Hellman (CDH) assumption will be described as the preliminaries.

3.1. Elliptic Curve

The elliptic curve on the finite field is the set of points. The equation of elliptic curve E on $FG(p)$ can be expressed as below and p is one prime greater than 3 and $a, b \in FG(p)$.

$$y^2 = x^3 + ax + b \,(\mathrm{mod}\, p) \text{ and } 4a^3 + 27b^2 \neq 0.$$

Based on the elliptic curve, ECC was proposed to implement the asymmetric encryption and decryption as it can use smaller secret keys while ensuring the same security level. And the security of the ECC is defined by the elliptic curve discrete logarithms (ECDLP) which is a hard number theoretic problem. In the ECDLP, it is difficult to assign one integer $r \in [0, n-1]$ to make $Q = [r]P$, where n is the order of the elliptic curve, P

is one point in the elliptic curve and Q belongs to the cyclic group generated by point P [29].

3.2. CDH Assumption

An algorithm that can solve the CDH problem in polynomial time is a probabilistic Turing machine. The algorithm can be presented as below, with the input of a tuple (G, aG, bG) and output the abG according to the input, where G is the generator of the cyclic group P and a, b belongs to Z_r and r is the order of P. The algorithm should be with non-negligible probability. And CDH assumption means that there is no such a probabilistic polynomial time Turing machine to solve the CDH problem [29].

4. Proposed Scheme

In this section, we will introduce the security model and propose a novel authenticated key agreement scheme that can support the two-way authenticated key agreement between the power terminals and management system based on CL-PKC. To prove the security of our proposed scheme under CDH, we now provide the e²CK security model of our proposed scheme based on Lippold [17] before describing the scheme.

4.1. Security Model

The security model defines a security game between adversary ϑ and simulator $\mathcal{B}$. We assume that the set $U = \{U_1, U_2, \ldots, U_n\}$ contains the users participating in the authenticated key agreement. Each user has its own private key and public key. The adversary controls the whole channel, and the simulator generates the public parameters and user information, while simulating the operation of the proposed scheme. Session $\Pi_{i,j}^n$ indicates the n'th time of an authenticated key agreement between i and j, and the ID of session $\Pi_{i,j}^n$ refers to the set of messages transmitted in the connection and the public keys of both parties.

Define 1: Matched session: Sessions $\Pi_{i,j}^n$ and $\Pi_{j,i}^s$ are matched sessions if their session IDs are the same.

The model will be divided into two stages. Stage 1: In the first stage, the adversary can query the following oracle in any order:

Create (ID_i): $\mathcal{B}$ generates the public key and private key for the user ID_i after receiving the oracle;

Reveal_SessionKey ($\Pi_{i,j}^n$): $\mathcal{B}$ returns the session key of $\Pi_{i,j}^n$ or $\perp$ if the session key does not exist and $\perp$ means null;

Reveal_Partial_PrivateKey (ID_i): $\mathcal{B}$ returns the user's partial private key of the user ID_i after receiving the oracle;

Reveal_SecretValue (IDi): $\mathcal{B}$ returns the secret value of the user ID_i after receiving the oracle;

Replace_PublicKey (ID_i, X'): The public key of the user ID_i will be replaced with X' by $\mathcal{B}$;

Reveal_EphemeralKey ($\Pi_{i,j}^n$): $\mathcal{B}$ returns the ephemeral key of session $\Pi_{i,j}^n$ after receiving the oracle;

Send ($\Pi_{i,j}^n$, M): The adversary ϑ sends M message to session $\Pi_{i,j}^n$ and obtains the response message according to the proposed scheme.

Stage 2: In the second stage, the adversary will choose one fresh session $\Pi_{i,j}^n$ and query the oracle of Test ($\Pi_{i,j}^n$) while the first stage is over.

Define 2: Freshness of the session: The session $\Pi_{i,j}^n$ is fresh if

(1) $\Pi_{i,j}^n$ already has the session key;
(2) The adversary does not query the oracle of Reveal_SessionKey in session $\Pi_{i,j}^n$ and matched session $\Pi_{j,i}^s$ of $\Pi_{i,j}^n$;
(3) Neither of the two parties involved in session $\Pi_{i,j}^n$ is fully exposed.

Test ($\Pi_{i,j}^{n}$): The oracle chooses $\beta \in \{0,1\}$ randomly and computes the session key of $\Pi_{i,j}^{n}$ if $\beta = 0$ or one random value as the session key if $\beta = 1$.

The adversary can repeat the above queries, but the session must be kept fresh. After finishing the game, the adversary must submit a guess value $\beta' \in \{0,1\}$. The adversary wins the game if $\beta' = \beta$, with the advantage is defined as $\mathrm{Adv}(k) = \left|\Pr[\beta' = \beta] - \frac{1}{2}\right|$. The authenticated key agreement model could be secure if the advantage Adv (k) is negligible.

4.2. Proposed Scheme

Our proposed scheme consists of five parts as below: initialization, private key generation, public key generation and key agreement. The detailed description of the scheme is as follows.

1. Initialization

This function is mainly responsible for generating some public parameters for the scheme by KGC; KGC chooses one elliptic curve E which has been defined in above and selects one random value $s \in Z_r$ as the master secret key to generate the master public key $P_{pub} = s * G$ and two hash function H_1 and H_2 are chosen for the public parameters where $H_1: \{0,1\}^* \rightarrow Z_r^*$ could map the users' identity to the elements in Z_r, and hash function $H_2: \{0,1\} \rightarrow \{0,1\}^k$ is chosen to compute the session key. The public parameter is $PP = \{GF(q), G, E, P_{pub}, H_1, H_2\}$, and the KGC exposes the PP to all users in the system.

2. Partial Private Key Generation

The KGC computes the partial private key $d_i = sH_1(ID_i)$, while user i sends its ID_i to the KGC and returns the key to the user through the secret channel.

3. Private Key Generation

User i selects one random value $x_i \in Z_r$ and composes the private key $s_i = (x_i, d_i)$ where the partial private key d_i is from the KGC.

4. Public Key Generation

The user i takes $X_i = x_i G$ as its public key.

5. Key Agreement

User A with identity ID_A and user B with identity ID_B can establish the connection and obtain the same session key after finishing the following steps:

(1) User A chooses one random ephemeral key $t_A \in Z_r$ and sends (ID_A, X_A, T_A) to B, where $T_A = t_A G$ and X_A is the public key described above.
(2) After receiving the message (ID_A, X_A, T_A) from A, user B also chooses one random ephemeral key $t_B \in Z_r$ and sends (ID_B, X_B, T_B) to A.
(3) B computes $K_{BA}^1 = (t_B + s_B)(T_A + X_A + H_1(ID_A)P_{pub})$ and $K_{BA}^2 = t_B T_A$, while also obtaining the session key $sk_{BA} = H_2(ID_A||ID_B||T_A||T_B||K_{BA}^1||K_{BA}^2)$.
(4) When receiving the message from B, A will compute $K_{AB}^1 = (t_A + s_A)(T_B + X_B + H_1(ID_B)P_{pub})$ and $K_{AB}^2 = t_A T_B$, while obtaining the session key $sk_{AB} = H_2(ID_A||ID_B||T_A||T_B||K_{AB}^1||K_{AB}^2)$.

Figure 1 shows the complete processes of authentication and key agreement of the proposed scheme.

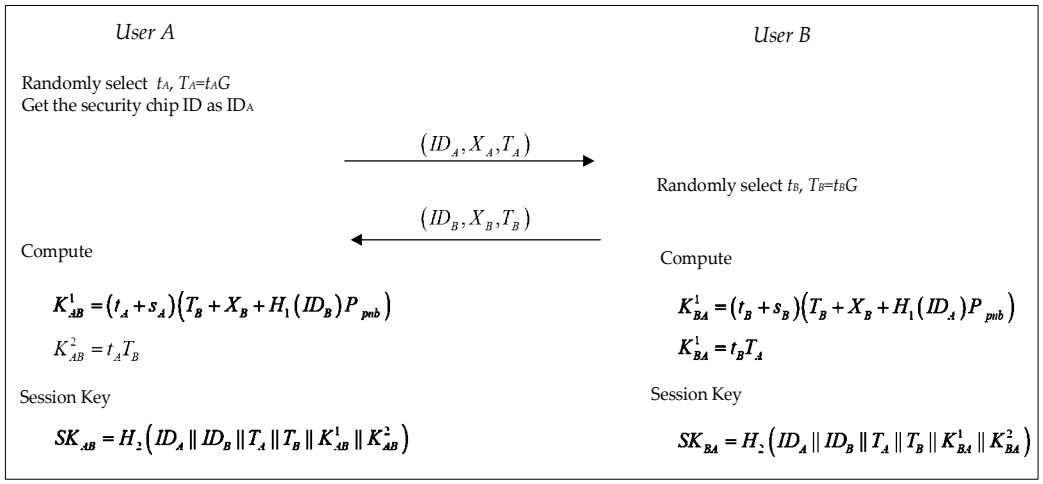

Figure 1. The processes of the proposed scheme.

SK_{AB} and SK_{BA} can be calculated as follows to prove the correctness of the proposed scheme if $SK_{BA} = SK_{AB}$:

$$\begin{aligned} K_{AB}^1 &= (t_A + s_A)(T_B + X_B + H_1(ID_B)P_{pub}) \\ &= (t_A + s_A)(t_B + x_B + H_1(ID_B)s)G \\ &= (t_B + s_B)(T_A + X_A + H_1(ID_A)P_{pub}) \\ &= K_{BA}^1 \end{aligned}$$

$$K_{AB}^2 = t_A T_B = t_A t_B G = t_B T_A = K_{BA}^2$$

Thus, the two parities can transmit data with the same session key for the subsequent communication.

4.3. Security Analysis

We will demonstrate the proposed scheme is secure under the CDH assumption and random oracle, with a security game where the simulator can query the value that cannot be calculated through the CDH assumption and the adversary's interaction with the random oracles in this section. For example, the simulator cannot obtain $x_A T_B$ without x_A, t_B. At this point, the simulator can judge $CDH(X_A, T_B, x_A T_B) = 1$ in K_{AB}^1 by the H_2 oracle queried by the adversary.

Theorem 1. *In the case of benign adversaries and random oracles, the two matched oracles will always obtain the same session key, and the key is evenly distributed in {0,1}.*

Proof of Theorem 1. A and B can obtain the same session key as the proposed scheme defined in Section 4.2. K^1 and K^2 are randomly generated as the ephemeral keys, while t_A and t_B are random values. Therefore, the session key SK is evenly distributed in {0,1} based on the random H_2 oracle.

Theorem 2. *If the adversary has the advantage Adv (k) to win the game, then we can find a simulator that can solve the CDH problem with the advantage* $\frac{1}{4mp^2}Adv(k)$ *at least. m is the number of sessions and p is the number of users.*

Proof of Theorem 2. The simulator is constructed to solve abG under the CDH problem with the input (aG, bG). Before the game, the simulator needs to choose the two parties A and B, where A and B are the users that query the H_1 oracle for the i'th and j'th times and $i, j \in \{1, \cdots, m\}$ when $i \neq j$. Then, $\mathcal{B}$ generates the public parameters PP and sends them to the adversary ϑ. We complete the security proof by classifying the information that was not disclosed in the game. Thus, the following four cases should be considered:

Case 1: The adversary can not obtain the private key x_A and x_B.

In this case, the simulator $\mathcal{B}$ sets $X_A = aG$ and $X_B = bG$ to guess the test session $\Pi^T_{A,B}$ with an advantage of more than $1/mp^2$. According to the security model, the simulator will answer the queries of the following oracles:

H_1 (ID_i, R_i): $\mathcal{B}$ maintains an empty list L_{H1} (ID_i, R_i, r_i), $\mathcal{B}$ returns r_i if (ID_i, R_i) exists in L_{H1} or returns a random r_i and adds $R_i = r_iG$ to L_{H1}.

Create (ID_i): $\mathcal{B}$ maintains an empty list L_{create} (ID_i, x_i, d_i, X_i); if $ID_i = ID_A$, $\mathcal{B}$ sets $x_A = \perp$ and computes $d_A = sH_1(ID_A)$ and $X_A = aG$; if $ID_i = ID_B$, $\mathcal{B}$ sets $x_B = \perp$ and computes $d_B = sH_1(ID_B)$ and $X_B = bG$. Otherwise, $\mathcal{B}$ chooses the random xi and computes $d_i = sH_1(ID_i)$ and $X_i = x_iG$, then adds (ID_i, x_i, d_i, X_i) to the list L_{create}.

Reveal_Partial_PrivateKey (ID_i): $\mathcal{B}$ looks up the tuple (ID_i, x_i, d_i, X_i) from L_{create} and returns d_i.

Reveal_SecretValue (ID_i): $\mathcal{B}$ looks up the tuple (ID_i, x_i, d_i, X_i) from L_{create} and returns x_i where $ID_i = ID_A$, ID_B and $X_i = x_iG$ or returns $\perp$.

Replace_PublicKey (ID_i, X'): $\mathcal{B}$ looks up the tuple (ID_i, x_i, d_i, X_i) from L_{create} and replaces X' with X_i if $ID_i \neq ID_A$, ID_B or return $\perp$ if it cannot find the tuple.

Reveal_SessionKey ($\Pi^n_{i,j}$): $\mathcal{B}$ looks up the tuple ($\Pi^n_{i,j}$, ID_i, ID_j, X_i, X_j, T_i, T_j, t_{ij}, SK_{ij}) from L_{send} and returns SK_{ij} if SK_{ij} exists. If the $SK_{ij} = \perp$ and the tuple exists, then look up the tuple (ID_i, ID_j, X_i, X_j, T_i, T_j, K^1_{ij}, K^2_{ij}, h_i) from L_{H2} where $ID_i = ID_A$, $ID_j = ID_B$, $X_i = X_A$, $X_j = X_B$, $T_i = T_A$, $T_j = T_B$, which returns h_i as SK_{ij}.

Send ($\Pi^n_{i,j}$, M): $\mathcal{B}$ maintains an empty list L_{send} ($\Pi^n_{i,j}$, ID_i, ID_j, X_i, X_j, T_i, T_j, t_{ij}, SK_{ij}), and the elements (ID_i, X_i, T_i) and (ID_j, X_j, T_j) represent the messages sent and received by ID_i. $\mathcal{B}$ looks up the tuples (ID_i, x_i, d_i, X_i) and (ID_j, x_j, d_j, X_j) from L_{create}. If $M = \lambda$, which means that this is the new session created by $\Pi^n_{i,j}$, $\mathcal{B}$ chooses a random t'_i as t_{ij} and computes $T_i = t'_iG$, and adds ($\Pi^n_{i,j}$, ID_i, ID_j, X_i, X_j, T_i, T_j, t_{ij}, SK_{ij}) into L_{send}, where $SK_{ij} = \perp$. Otherwise, if $M \neq \lambda$, let $SK_{ij} = \perp$ and $t_{ij} = \perp$, $T_j = M$, $ID_i = ID_B$, $ID_j = ID_A$, $X_i = X_B$, $X_j = X_A$, then add the tuple into L_{send}.

Reveal_EphemeralKey ($\Pi^n_{i,j}$): $\mathcal{B}$ looks up the tuple ($\Pi^n_{i,j}$, ID_i, ID_j, X_i, X_j, T_i, T_j, t_{ij}, SK_{ij}) from L_{send} and returns t_{ij}.

H_2 (ID_i, ID_j, X_i, X_j, T_i, T_j, K^1_{ij}, K^2_{ij}, h_i): $\mathcal{B}$ looks up the tuple (ID_i, ID_j, X_i, X_j, T_i, T_j, K^1_{ij}, K^2_{ij}, h_i) in list L_{H2} and returns h_i if the tuple exists, or $\mathcal{B}$ looks up the tuple in L_{send} where $ID_i = ID_A$, $ID_j = ID_B$, $X_i = X_A$, $X_j = X_B$, $T_i = T_A$, $T_j = T_B$, $SK_{AB} \neq \perp$ and returns SK_{AB} as h_i. Otherwise, $\mathcal{B}$ chooses a random h_i and returns it to ϑ.

Test ($\Pi^n_{i,j}$): If $\Pi^n_{i,j} = \Pi^T_{A,B}$, $\mathcal{B}$ outputs a random $\beta \in \{0,1\}$. If ϑ wins the game, the H_2 oracle must have been issued; thus, $\mathcal{B}$ can find the corresponding tuple with the correct elements of K^1 in L_{H2} with a probability of at least 1/4. Then, $\mathcal{B}$ computes $abG = \left(K^1_{AB} - (t_A + s_A)(T_B + X_B + H(B)P_{pub}) - (t_B + s_B)X_A\right)$ with $X_A = aG$ and $X_B = bG$; therefore, the CDH problem can be solved by $\mathcal{B}$ with the non-negligible advantage $\frac{1}{4mp^2}Adv(k)$, which contradicts the CDH assumption.

Case 2: The adversary ϑ cann not obtain the ephemeral key t_A and the private key x_B.

In this case, the simulator $\mathcal{B}$ sets the ephemeral public key $T_A = aG$ and public key of B $X_B = bG$ to guess the test session $\Pi^T_{A,B}$ with an advantage of more than $1/mp^2$. According to the security model, the simulator will answer the queries of the following oracles:

H_1 (ID_i, R_i): Same as the H_1 oracle in case 1.

H_2 (ID_i, ID_j, X_i, X_j, T_i, T_j, K^1_{ij}, K^2_{ij}, h_i): Same as the the H_2 oracle in case 1.

Reveal_Partial_PrivateKey (ID_i): Same as the Reveal_Partial_PrivateKey oracle in case 1.

Reveal_SessionKey ($\Pi^n_{i,j}$): Same as the Reveal_SessionKey oracle in case 1.

Create (ID_i): $\mathcal{B}$ maintains an empty list L_{create} (ID_i, x_i, d_i, X_i). If $ID_i \neq ID_B$, $\mathcal{B}$ chooses the random x_i and computes $d_i = sH_1(ID_i)$ and $X_i = x_iG$, or lets $x_B = \perp$ and computes $d_B = sH_1(ID_B)$, $X_B = bG$ if $ID_i = ID_B$, then adds (ID_i, x_i, d_i, X_i) into the list L_{create}.

Reveal_SecretValue (ID_i): $\mathcal{B}$ looks up the tuple (ID_i, x_i, d_i, X_i) from L_{create} and returns x_i, where $ID_i \neq ID_B$ and $X_i = x_iG$.

Replace_PublicKey (ID_i, X'): $\mathcal{B}$ looks up the tuple (ID_i, x_i, d_i, X_i) from L_{create} and replaces X' with X_i if $ID_i \neq ID_B$.

Send ($\Pi_{i,j}^n$, M): $\mathcal{B}$ looks up the tuples (ID_i, x_i, d_i, X_i) and (ID_j, x_j, d_j, X_j) from L_{create}. If $\Pi_{i,j}^n = \Pi_{A,B}^T$, let $t_{ij} = \perp$, $SK_{ij} = \perp$ and $T_i = aG$, then add ($\Pi_{i,j}^n$, ID_i, ID_j, X_i, X_j, T_i, T_j, t_{ij}, SK_{ij}) into L_{send}; or if $\Pi_{i,j}^n \neq \Pi_{A,B}^T$, with the case $M = \lambda$, $\mathcal{B}$ chooses a random t_i' as t_{ij} and computes $T_i = t_i'G$, then adds ($\Pi_{i,j}^n$, ID_i, ID_j, X_i, X_j, T_i, T_j, t_{ij}, SK_{ij}) into L_{send}, where $SK_{ij} = \perp$, $ID_i = ID_A$, $ID_j = ID_B$, $X_i = X_A$, $X_j = X_B$. Otherwise, if $M \neq \lambda$, let $SK_{ij} = \perp$, $t_{ij} = \perp$, $T_j = M$, $ID_i = ID_B$, $ID_j = ID_A$, $X_i = X_B$, $X_j = X_A$, then add the tuple into L_{send}.

Reveal_EphemeralKey ($\Pi_{i,j}^n$): If $\Pi_{i,j}^n \neq \Pi_{A,B}^T$, $\mathcal{B}$ looks up the tuple ($\Pi_{i,j}^n$, ID_i, ID_j, X_i, X_j, T_i, T_j, t_{ij}, SK_i) from L_{send} and returns t_{ij}.

Test ($\Pi_{i,j}^n$): If $\Pi_{i,j}^n = \Pi_{A,B}^T$, $\mathcal{B}$ outputs a random $\beta \in \{0,1\}$. If ϑ wins the game, the H_2 oracle must have been issued; thus, $\mathcal{B}$ can find the corresponding tuple with the correct elements of K^1 in L_{H2} with a probability of at least 1/4. Then, $\mathcal{B}$ computes $abG = \left(K_{AB}^1 - (x_A + s_A)\left(T_B + X_B + H(B)P_{pub}\right) - (x_B + s_B)T_A\right)$ with $T_A = aG$ and $X_B = bG$; therefore, the CDH problem can be solved by $\mathcal{B}$ with the non-negligible advantage $\frac{1}{4mp^2}Adv(k)$, which contradicts the CDH assumption.

Case 3: The adversary can not obtain the private key x_A and the ephemeral key t_B.

Case 3 is symmetric to case 2, and we will not give the details here to save space.

Case 4: The adversary can not obtain the ephemeral key t_A and t_B.

In this case, the simulator $\mathcal{B}$ sets the ephemeral public key $T_A = aG$ and $T_B = bG$ to guess the test session $\Pi_{A,B}^T$ with an advantage of more than $1/mp^2$. According to the security model, the simulator will answer the queries of the following oracles.

H_1 (ID_i, R_i): Same as the H_1 oracle in case 1.

H_2 (ID_i, ID_j, X_i, X_j, T_i, T_j, K_{ij}^1, K_{ij}^2, h_i): Same as the the H_2 oracle in case 1.

Reveal_Partial_PrivateKey (ID_i): Same as the Reveal_Partial_PrivateKey oracle in case 1.

Reveal_SessionKey ($\Pi_{i,j}^n$): Same as the Reveal_SessionKey oracle in case 1.

Replace_PublicKey (ID_i, X'): Same as the Replace_PublicKey oracle in case 1.

Create (ID_i): $\mathcal{B}$ maintains an empty list L_{create} (ID_i, x_i, d_i, X_i); if $ID_i \neq ID_A$, IDB, $\mathcal{B}$ chooses the random x_i and computes $d_i = sH_1(ID_i)$ and $X_i = x_iG$; if $ID_i = ID_A$, $\mathcal{B}$ chooses the random x_i and computes $d_A = sH_1(ID_i)$ and $X_A = x_iG$; if $ID_i = ID_B$, $\mathcal{B}$ chooses the random x_i and computes $d_B = sH_1(ID_i)$ and $X_B = x_iG$; then, adds (ID_i, x_i, d_i, X_i) into the list L_{create}.

Reveal_SecretValue (ID_i): $\mathcal{B}$ looks up the tuple (ID_i, x_i, d_i, X_i) from L_{create} and returns x_i.

Send ($\Pi_{i,j}^n$, M): $\mathcal{B}$ looks up the tuples (ID_i, x_i, d_i, X_i) and (ID_j, x_j, d_j, X_j) from L_{create}. If $\Pi_{i,j}^n = \Pi_{A,B}^T$, let $t_{ij} = \perp$, $SK_{ij} = \perp$ and $T_i = aG$, then add ($\Pi_{i,j}^n$, ID_i, ID_j, X_i, X_j, T_i, T_j, t_{ij}, SK_{ij}) into L_{send}; or if $\Pi_{i,j}^n$ is the matched session of $\Pi_{A,B}^T$, let $t_{ji} = \perp$, $SK_{ji} = \perp$ and $T_j = bG$, then add ($\Pi_{i,j}^n$, ID_i, ID_j, X_i, X_j, T_i, T_j, t_{ij}, SK_{ij}) into L_{send}.

Test ($\Pi_{i,j}^n$): If $\Pi_{i,j}^n = \Pi_{A,B}^T$, $\mathcal{B}$ outputs a random $\beta \in \{0,1\}$. If ϑ wins the game, the H_2 oracle must have been issued; thus, $\mathcal{B}$ can find the corresponding tuple with the correct elements of K^2 in L_{H2} with a probability of at least 1/4. Then, $\mathcal{B}$ computes $abG = (K_{AB}^2 - t_AT_B)$ with $T_A = aG$ and $T_B = bG$; therefore, the CDH problem can be solved by $\mathcal{B}$ with the non-negligible advantage $\frac{1}{4mp^2}Adv(k)$, which contradicts the CDH assumption. From the above theories, we can conclude that the proposed scheme is a secure authenticated key agreement model based on CL-PKC.

5. Performance Analysis

The terminals of power IoT need to carry a lot of data acquisition and business computing and most of them are embedded systems with limited CPU and memory resource.

The performance of the proposed scheme should be considered according to the actual application scenarios. So in this section, the comparison and analysis of the security model and computation and communication cost with the previous schemes and the proposed scheme will be presented in a detailed account in Table 1.

Table 1. Comparison of the schemes.

Scheme	Computation Cost	Communication Cost	Security Model
Zhang [8]	1P + 5S + 1H	$\|ID\| + 2\|G\|$	mBR
He [9]	5S + 2H	$\|ID\| + 3\|G\|$	mBR
Wu [11]	7S + 2H	$\|ID\| + 4\|G\|$	e^2CK
Tu [14]	5S + 4H	$\|ID\| + 2\|G\|$	e^2CK
Sun [15]	12S + 7H	$\|ID\| + 2\|G\|$	eCK
Lippold [17]	10P + 6S + 4E + 3H	$\|ID\| + 2\|G\|$	e^2CK
Deng [27]	4S + 3H	$\|ID\| + 2\|G\|$	eCK
Our scheme	3S + 1H	$\|ID\| + 2\|G'\|$	e^2CK

The computational cost is measured by point multiplication S, exponential operation E, bilinear pairing P and hash operation H. And as a comparison, the computation cost of P operation is two or three times higher than S operation with the same elliptic curve [30]. The proposed scheme only needs three S operations and one hash operation in one round, and it has obvious advantages over other schemes.

As the both parties of the schemes need to communicate and exchange data, the communication cost should consider the length of the necessary messages and the integrity of the communication. In the above schemes, we summarize the message as IDs, public keys and ephemeral keys. The other schemes choose a 1024 bits Group G with order r, where r is 512 bits and we use $|G|$ to identify the size of Group G. Consequently, the size of the point is $2|G|$ and $|ID|$ has 16 bits. However, the elliptic curve used in the proposed schemes is 256 bits, and the size of the point is $2|G'|$ (512 bits) where $|G'|$ is the size of the group in our elliptic curve.

In addition, in order to meet the application requirements of the power IoT, we use three gateways with Intel Xeon E3 CPU at 3.4 GHz and 8 GB memory to build the test network topology that depicted in Figure 2. The terminal simulator server and security gateway are the two parities of the communication and we program the test routines with C programming language and Openssl libraries which have implemented the algorithms of point multiplication. The power IoT management system is designed to be responsible for the interaction of business data with the terminals that have completed the authentication. As a comparison, we also implement the key agreement protocol used in the voltage monitoring device of the state grid, as well as some of the other improved versions based on it.

Figure 2. Network topology of the experimental evaluation.

To ensure the integrity and the confidentiality of the proposed scheme and the communications, we encrypt and sign the messages with the standard SM2 algorithm [31,32]. A confirmation step is added to ensure the reliability of the session key. In addition, we add the time stamps in the message to keep the freshness of the session, thus resisting replay attacks and making protocols more robust with some other flags. The pseudo codes are below:

(1) Terminal A sends the request of a key agreement to a security gateway B;

```
//Encrypt data
Create_EcPoint (PP, tA, TA);
Get_CurrentTime (TimeA);
Sm2_Encrypt (IDB, IDA + XA + TA + TimeA, Buffer + 40);
//Pack data
Buffer [TYPE] = 0x01; Buffer[SUBTYPE] = 0x01;
* ((u16 *) (Buffer + LENGTH)) = Change_Int (Length);
* ((u16 *) (Buffer + VER)) = Change_Int (0x0100);
* ((u16 *) (Buffer + SN_REQ)) = Change_Int (8000);
memcpy (Buffer + IDX_SIM_CARD_ID, SIM_ID, 16);
memcpy (Buffer + IDX_DEVICE_ID, CHIP_ID, 16);
TempBuffer = Buffer + Length—64;
//Signature data
Hash (Buffer, Length—64, TempBuffer);
Sm2_Sign (PriA,TempBuffer, Buffer + 165);
```

(2) The gateway decrypts and verifies the received message, and then sends the response message to A, while the gateway computes the session key using the proposed model.

```
//Decrypt data
Sm2_Decrypt (PriB, Buffer,IDA + XA + TA + TimeA);
//Compare freshness
strcmp (TimeA,Get_CurrentTime (Time));
//Verify
Hash (Buffer, Length—64, TempBuffer);
Sm2_Verify (IDA, TempBuffer, Buffer + 165);
//Encrypt data
Create_EcPoint (PP, tB,TB) ;
Get_CurrentTime (TimeB);
Sm2_Encrypt (IDB, IDB + XB + TB + TimeB, Buffer + 40);
//Pack data
Buffer [TYPE] = 0x01; Buffer [SUBTYPE] = 0 x 02;
* ((u16 *) (Buffer + LENGTH)) = Change_Int (Length);
* ((u16 *) (Buffer + VER)) = Change_Int (0x0100);
* ((u16 *) (Buffer + SN_REQ)) = Change_Int (8001);
TempBuffer = Buffer + Length—64;
//Signature data
Hash (Buffer, Length—64, TempBuffer);
Sm2_Sign (PriB, TempBuffer, Buffer + 133);
//Compute the session key
DK = Hash (IDA + XA + TA + K1BA + K2BA, 16);
```

(3) The terminal decrypts and verifies the received message and computes the session key, sending the acknowledged message, including the hash value of the session key, to B.

```
//Decrypt data
Sm2_Decrypt (PriA, Buffer, IDB + XB + TB + TimeB);
//Compare freshness
strcmp (TimeB, Get_CurrentTime (Time));
//Verify
Hash (Buffer, Length—64, TempBuffer);
```

Sm2_Verify (ID_B, TempBuffer, Buffer + 133);
//Compute the session key
DK = Hash (ID_B + X_B + T_B + K^1_{AB} + K^2_{AB}, 16);
//Pack data
Buffer [TYPE] = 0x01;Buffer [SUBTYPE] = 0x03;
* ((u16 *) (Buffer + LENGTH)) = Change_Int (Length);
* ((u16 *) (Buffer + VER)) = Change_Int (0 x 0100);
* ((u16 *) (Buffer + SN_REQ)) = Change_Int (8002);
//Hash
Hash (Buffer, Length—32, TempBuffer);
memcpy (Buffer + Length—64, TempBuffer, 32);

(4) The gateway compares the received hash value and the hash of its own session. The session key will be established if the results are consistent, else the gateway will close the connection.

Figure 3 shows the comparison of the execution time in the proposed scheme and schemes [20,21,26]. We calculate the processing time of security gateway by increasing the number of the simulated concurrency from 1 to 10,000. As the authenticated key agreement protocols used in the other three schemes are implemented by the traditional digital certificates, their execution time and computation cost are much greater than our proposed scheme. Conversely, it also shows that the proposed authenticated key agreement has higher efficiency.

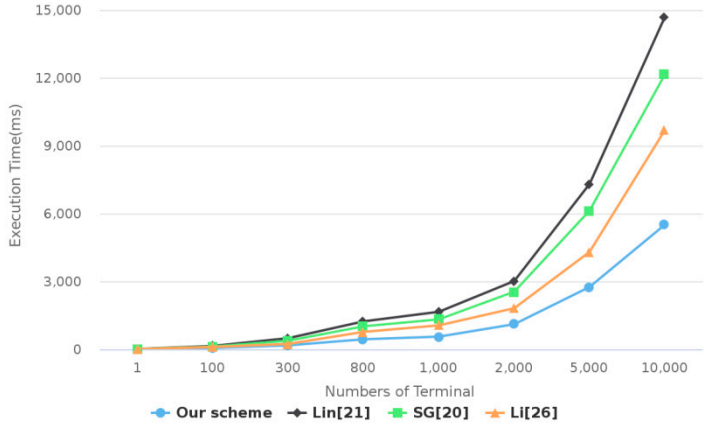

Figure 3. Comparison of the schemes' execution time.

In contrast, the proposed scheme only needs approximately 500 bytes to implement the whole authenticated key agreement, while the other three schemes need at least 1500 bytes for communication. This scheme consumes fewer communication and computing resources, which makes the execution time relatively low, the efficiency higher, and it becomes more suitable for the secure access of mass power IoT terminals.

6. Conclusions

In order to protect the security of the communication in power IoT, this paper proposes a novel authenticated key agreement model based on CL-PKC and simplify the communications to improve the performance of the key agreement protocol according the requirement of power IoT and by uses simple point multiplication of elliptic curves to replace complex bilinear pairing make it is simpler and more practical for the terminals with limited computing resources in power IoT. The proposed scheme has provable security with the e^2CK security model under the CDH assumption with detailed proof thereof. Finally, the authenticated key agreement protocol based on the proposed scheme has been

programmed and implemented, then the analysis and comparison of the simulation proves that our scheme has higher efficiency.

However, there is also some work that needs to be improved in our scheme. We use the standard SM2 algorithm to perform asymmetric encryption and signature in the key agreement protocol of the test routine. In the future, we could design a certificateless public key encryption and digital signature algorithm based on SM2 and a certificateless key agreement based on SM2, which will be our upcoming research.

Author Contributions: Methodology, R.C. and W.C.; project administration, K.W.; writing—original draft, Y.S.; writing—review and editing, R.C. and W.C.; funding acquisition, Y.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key R&D Program of China, grant number 2020YFB0905900.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cornel-Cristian, A.; Gabriel, T.; Calin-Arhip, M.; Zamfirescu, A. Smart grid integration of IoT. In Proceedings of the 2019 54th International Universities Power Engineering Conference (UPEC), Bucharest, Romania, 3–6 September 2019; Institute of Electrical and Electronics Engineers (IEEE): San Diego, CA, USA, 2019; pp. 1–5.
2. Capizzi, G.; Lo Sciuto, G.; Napoli, C.; Tramontana, E. Advanced and adaptive dispatch for smart grids by means of predictive models. *IEEE Trans. Smart Grid* **2018**, *9*, 6684–6691.
3. Shahinzadeh, H.; Moradi, J.; Gharehpetian, Gevork, B.; Nafisi, H.; Abedi, M. IoT Architecture for smart grids. In Proceedings of the 2019 International Conference on Protection and Automation of Power System (IPAPS), Tehran, Iran, 8–9 Janaury 2019; Electrical and Electronics Engineers (IEEE): San Diego, CA, USA, 2019; pp. 22–30.
4. Zhao, M.; Tang, P.; Sun, K.; Cheng, R.; Chen, G. Development and prospect of ubiquitous electric internet of things. *J. North China Electr. Power Univ.* **2020**, *47*, 63–74.
5. Shamir, A. Identity-based cryptosystems and signature schemes. *Lect. Notes Comput. Sci.* **1985**, *196*, 47–53, doi:10.1007/3–540-39568-7_5.
6. Al-Riyami, S.S.; Paterson, K.G. Certificateless public key cryptography. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, 30 November–4 December 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 452–473.
7. Mandt, T.K.; Tan, C.H. Certificateless authenticated two-party key agreement protocols. In Proceedings of the 11th Asian Computing Science Conference, Tokyo, Japan, 6–8 December 2006; Springer: Berlin/Heidelberg, Germany, 2007; pp. 37–44.
8. Zhang, L.; Zhang, F.; Wu, Q.; Domingo-Ferrera, J. Simulatable certificateless two-party authenticated key agreement protocol. *Inf. Sci.* **2010**, *180*, 1020–1030, doi:10.1016/j.ins.2009.11.036.
9. He, D.; Chen, Y. Chen, J. Zhang, R. Han, W. A new two-round certifificateless authenticated key agreement protocol without bilinear pairings. *Math. Comput. Model* **2011**, *54*, 3143–3152, doi:10.1016/j.mcm.2011.08.004.
10. Sun, H.; Wen, Q.; Zhang, H.; Jin, Z. A strongly secure pairing-free certificateless authenticated key agreement protocol for low-power devices. *Info. Technol. Control* **2013**, *42*, 113–123, doi:10.5755/j01.itc.42.2.1689.
11. Wu, T.; Jing, X. Two-party certificateless authenticated key agreement protocol with enhanced security. *J. China Univ. Posts Telecommun.* **2019**, *26*, 12–20.
12. Bala, S.; Sharma, G.; Verma, A.K. Impersonation attack on CertificateLess key agreement protocol. *Int. J. Ad Hoc Ubiq Co* **2018**, *27*, 108–120, doi:10.1504/IJAHUC.2018.089580.
13. Kim, Y.J.; Kim, Y.M.; Choe, Y.J.; Choe, Y.J. An efficient bilinear pairing-free certificateless two-party authenticated key agreement protocol in the eck model. *Theor. Phys. Cryptogr* **2013**, *3*, 1–10.
14. Tu, H.; Kumar, N.; Kim, J.; Seo, J. A strongly secure pairing-free certificateless authenticated key agreement protocol suitable for smart media and mobile environments. *Multimed. Tools Appl.* **2015**, *74*, 6365–6377, doi:10.1007/s11042-015-2470-3.
15. Sun, H.; Wen, Q.; Li, W. A strongly secure pairing-free certificateless authenticated key agreement protocol under the CDH assumption. *Sci. China Inf. Sci.* **2016**, *59*, 103–118, doi:10.1007/s11432-015-5303-0.
16. Swanson, C.; Jao, D. A study of two-party certificateless authenticated key-agreement protocols. In Proceedings of the 10th International Conference on Cryptology in India, New Delhi, India, 13–16 December 2009; Roy, B.; Sendrier, N., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 57–71.

17. Lippold, G.; Boyd, C.; Nieto, J. Strongly secure certificateless key agreement. In Proceedings of 3rd International Conference on Paring-Based Cryptography; Stanford University, Palo Alto, CA, USA, 12–14 August 2009; Shacham, H.; Waters, B., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 206–230.
18. Yang, G.; Tan, C. Strongly secure certificateless key exchange without pairing. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011; Association for Computing Machinery: New York, NY, USA, 2011; pp. 71–79.
19. Huang, B.; Tu, H. Strongly secure certificateless one-pass authenticated key agreement scheme. *Kuwait J. Sci.* **2015**, *42*, 91–108.
20. Q/GDW11118-2013 *Specification for Information Security Access of Voltage Monitoring Devices Based on Wireless APN Virtual Private Network[S]*; National Standard Press: Beijing, China, 2014.
21. Lin, N.; Chen, Z.; Zuo, L.; Wang, L. Security analysis and improvement of access protocol for voltage monitoring device in power network. *Comput. Eng. Des.* **2019**, *40*, 3085–3089.
22. Tsai, J.L.; Lo, N.W. Secure anonymous key distribution scheme for smart grid. *IEEE Trans. Smart Grid* **2016**, *7*, 906–914, doi:10.1109/TSG.2015.2440658.
23. Fouda, M.M.; Fadlullah, Z.M.; Kato, N.; Lu, R.; Shen, X. A lightweight message authentication scheme for smart grid communications. *IEEE Trans. Smart Grid* **2011**, *2*, 675–685, doi:10.1109/TSG.2011.2160661.
24. Mahmood, K.; Chaudhry, S.A.; Naqvi, H.; Kumari, S.; Li, X.; Sangaiah, A.K. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Gener. Comput. Syst.* **2018**, *81*, 557–565, doi:0.1016/j.future.2017.05.002.
25. Li, Z.; Liu, B.; Wang, P.; Yang, Y. Two-way authentication protocol based on sm2 and zero knowledge for radio frequency identification. *Comput. Eng.* **2017**, *43*, 97–100, doi:10.3969/j.issn.1000-3428.2017.06.016.
26. Li, W.; Li, R.; Wu, K.; Cheng, R.; Su, L.; Cui, W. Design and implementation of an SM2-based security authentication scheme with the key agreement for smart grid communications. *IEEE Access* **2018**, *6*, 71194–71207, doi:10.1109/ACCESS.2018.2875681.
27. Deng, L.; Gao, R. Certificateless two-party authenticated key agreement scheme for smart grid. *Inf. Sci.* **2021**, *543*, 143–156, doi:10.1016/j.ins.2020.07.025.
28. Batamuliza, J.; Hanyurwimfura, D. A secure and efficient anonymous certificateless signcryption for Key Distribution Scheme for Smart Grid. In Proceedings of the 2020 21st International Arab Conference on Information Technology (ACIT), Giza, Egypt, 28–30 November 2020; Institute of Electrical and Electronics Engineers (IEEE): San Diego, CA, USA, 2020.
29. Cheng, R.; Wu, K.; Su, Y.; Li, W.; Cui, W.; Tong, J. An Efficient ECC-Based CP-ABE Scheme for Power IoT. *Processes* **2021**, *9*, 1176. https://doi.org/10.3390/pr9071176.
30. Ding, S.; Li, C.; Li, H. A Novel Efficient Pairing-Free CP-ABE based on elliptic curve cryptography for IoT. *IEEE Access* **2018**, *6*, 27336–27345, doi:10.1109/ACCESS.2018.2836350.
31. State Cryptography Administration. *GM/T 0003.4-2012. Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves—Part 4: Public Key Encryption Algorithm*; China Quality and Standards Publishing & Media Co., Ltd.: Beijing, China, 2012.
32. State Cryptography Administration. *GM/T 0003.4-2012. Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves—Part 2: Digital Signature Algorithm*; China Quality and Standards Publishing & Media Co., Ltd.: Beijing, China, 2012.