A Practical Group Blind Signature Scheme for Privacy Protection in Smart Grid

Wei Kong[a], Jian Shen[a,b], Pandi Vijayakumar[c], Youngju Cho[d,*], Victor Chang[e]

[a] *Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing, China*
[b] *Guangxi Key Laboratory of Cryptography & Information Security, Guilin University of Electronic Technology, China*
[c] *Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tindivanam, Tamil Nadu, India*
[d] *School of the SW Convergence Education Institute at Chosun University, Gwangju, South Korea*
[e] *Xi'an Jiaotong-Liverpool University, Suzhou, China*

Abstract

The leakage of privacy is one of the key factors to restrict the development of smart grid. Currently, researches of protecting privacy in smart grid mainly focused on two aspects: 1) data aggregation based on the mathematical model and algorithm and 2) user anonymous authentication. However, data aggregation is at cost of obtaining fine-grained electricity consumption information to protect privacy. While, anonymous authentication cannot identify the malicious user in previous researches. Hence, in this work, we propose a group blind signature scheme in smart grid to accomplish conditional anonymity. Furthermore, the integrity of consumption data can be verified by homomorphic encryption (HE) which can decrease the communication overhead between control center and smart meter remarkably. From the security analysis and experiment simulation, the results show that our scheme is safety and efficient.

Keywords: Smart grid, anonymous authentication, traceability, data integrity verification, industry 4.0/5.0 for security

*Corresponding author
Email addresses: wei_kongNuist@126.com (Wei Kong), s_shenjian@126.com (Jian Shen), vijibond2000@gmail.com (Pandi Vijayakumar), csjyj@chosun.ac.kr (Youngju Cho), Victor.Chang@xjtlu.edu.cn (Victor Chang)

1. Introduction

Since the American Electric Power Research Institute proposed the concept of "Intelligrid" in 2001, the exploration of next-generation power grid has attached many people's attention. In 2003, the American Department of Energy published a development plan called "Grid2030", which defined the "smart grid" as a full automated electric transmission network that can supervise and control each node [1, 2] [3]. The two-way flow of information and power in the whole transmission and distribution process from power plant to end-user can be ensured. Recently, since the concept of industry 4.0 is proposed, the operation and management of the smart grid can be optimized by connected all kinds of equipment and facilities. While, some concerns have arisen about the security of smart grid in the industrial 4.0, just as shown in Fig. 1, the two-way communication is easy to be eavesdropped by attacker especially at user side. Attackers can obtain different users' power consumption for analysing their lifestyles [4, 5, 6]. So an efficient and safe data transmission scheme is a way to solve the problem.

Recently, researches are seem to focus on the electricity privacy data aggregation scheme [7, 8] [9, 10] [11].The principle is that user sends encrypted electric consumption data to relay nodes which will decrypt them and aggregate data into a multi-dimensional data set. The dataset allows control center to get the sum or average of electricity consumption data, but cannot acquire the particular user's electricity usage data no matter what kind of data aggregation schemes, including one dimensional data aggregation schemes [12, 13, 14] and multi-dimensional data aggregation schemes [15, 16, 17]. These schemes are at cost of acquiring fine-grained electricity usage data, in exchange of privacy-preservation. To realize the multi-granularity electric management, the implicit anonymous authentication protocol is proposed by Tassos [18, 19] which can achieve fine-grained analysis and management to data. However, the terminal devices are needed to exchange information with control center directly which is unrealistic in practice. In addition, there is a limitation for control center to handle up the reporting request from terminal devices. For building IoT

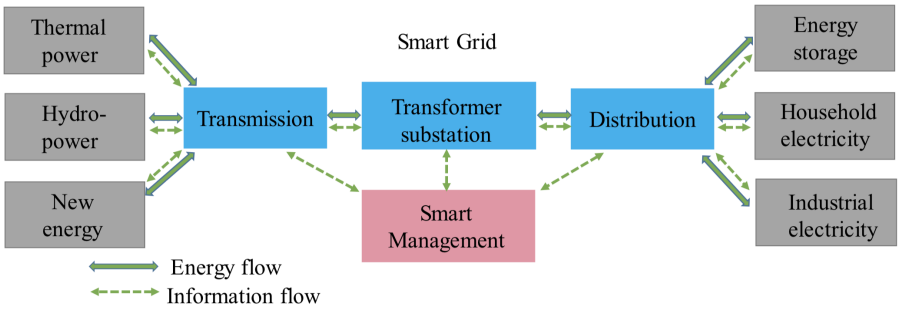


Figure 1: Framework of Smart Grid

collection infrastructure, Chen [20] proposed a web-based monitoring system to monitor household gas consumption, which greatly improved the communication efficiency among nodes. Meanwhile, in the aspect of IoT's identification and recognization, Hsia proposed these methods [21, 22, 23], which not only reduce the system computation time, but also yield real-time requirement and achieve the high rate of recognition.

Hence, a scheme can achieve privacy-preserving is proposed by us which is based on group blind signature [24, 25, 26, 27, 28]. Moreover, our scheme has a good scalability when facing large-scale consumers.

1.1. Related work

According to the aim of smart grid, a more reliable, efficient and controllable power service should be provided to residential and business customers. However, many security and privacy problems are present in smart grid, for example maliciously tampering the electric consumption data, eavesdropping user privacy data. So an efficient scheme that can be applied to resource-constrained environment and privacy-preserving in smart grid needs to be put forward. The related works are summarized as follow:

So far, many researches have focused on developing the data aggregation technology by calculating sum of dimensional data, or using homomorphic operators to masking the original data. In [29], authors successfully extend aggregation concepts from sensor networks into smart grid and use Paillier cryptosys-

tem to aggregate consumption data, but the scheme cannot verify the integrity of data. In [16], a data aggregation scheme that can convert multi-dimensional data for several residential areas into aggregated-data cube. However, CC can only acquire the sum of electricity consumption with coarse-grained data, but cannot restore the original data of single user. In general, these protocols can protect the privacy at cost of sacrificing to acquire fine-grained data.

Hence, an escrow mechanism [30] is proposed by Efthymious that can authenticate anonymous meter's readings. However, it has to assume that the escrow is fully trusted. The protocol [18] proposed by Tassos Dimitriou *et al.* is based on [19] that the allows utility provider to anonymously authenticate SM. In addition, by using anonymous tokens to reward for users in exchange of their fine-grained consumption details. However, both them have the same problem that users are fully anonymity. If some special case happened, the CC cannot get the any information of the user. It's a concern that the user maliciously tampers the consumption but CC cannot revoke its anonymity. Meanwhile, the interaction between users and CC is point-to-point, so that the processing capacity is limited in their experiment.

Furthermore, a privacy-preserving scheme [31] was proposed by T.jeske *et al.* in smart grid based on the group signature. It can not only preserve user's privacy, but also prevent spamming and replay attacks. However, the scheme cannot revoke anonymity of users in case of need. While, double discrete logarithm knowledge signature and discrete logarithm e root knowledge signature is adopted in the protocol [32] which make the whole system in low efficiency.

Note that all the above protocols have been analysed and proofed security, but there are different problems in these papers, such as: the granularity of consumption data, anonymity revoking, processing capacity, data integrity and so on. Motivated by these various weaknesses, an efficient and privacy-friendly scheme in smart grid should have these following features:

1. The fine-grained consumption data can be analysed without revealing user's identify.

2. Anonymity of user can be revoked if in need, such as the consumption

data has been tampered by maliciously user.

3. It's necessary to introduce the middle model. If the participator has been involved in the point-to-point transmission, the delay is inevitable in the process of transmission and will cause great time waste.

4. Data integrity can be verified by CC.

To the best of our knowledge, it's our greatest contribution that apply group blind signature to smart grid. Firstly, based on the features of the group blind signature, the signature and message reveal neither the identity of data owner nor identity of the issuing signer. Then, the scheme is a conditional group blind signature which can identity malicious user if necessary [33].At last, we introduce the homomorphic tag mechanism [34, 35, 36, 37, 38] to verify the integrity of data. We believe that our contributions can widen the application scope of privacy-preserving in smart grid.

1.2. Organization

The remainder of this paper is structured as follows: in section 2, our contributions are elaborated in detail. In Section 3, we precisely present preliminaries and the system model. The system model and security requirements are presented in section 4. In Section 5, we show how our scheme perform from user anonymous authorization to data reporting, which can be achieved by using blind signature and homomorphic verifiable tag mechanism. In Section 6, we analyse the security of all stages in our scheme. In Section 7, we present the performance analysis and evaluation. At last, in Section 8, we conclude the paper and propose the future work, respectively.

2. Main Contributions

In this paper, a privacy-preserving scheme in smart grid based on group blind signature is proposed by us, which enables CC to trace the potential corrupted SS and SM conditional. Moreover, an efficient anonymous authentication scheme and data integrity verification mechanism are provided in our

paper, which can satisfy the need of efficiency and stability in power system. The main contributions of this paper are concluded as follows:

1. Innovatively applying the structure of group blind signature to smart grid. In this paper, to meet the requirements of privacy-preserving, anonymity and traceability, we propose a scheme based on group blind signature. Moreover, to fit resource-constrained and high-efficiency environment, the process of generating blind signature and tracing the malicious users are also improved in terms of efficiency.

2.Anonymous authentication and conditional anonymity can be realized in our scheme. We present an efficient anonymous authentication scheme based on the schnorr identification protocol, which signer only knows it's a legal user without revealing real identity. Once the fault happened, the scheme will perform fault detection to locate the fault. If data has tampered by user, CC will conditionally revoke the anonymity of user, which makes the system more stable.

3. Privacy data can be transmitted securely without being tampered with in our scheme. In the process of data transmission, the homomorphic verification method in the cloud auditing [39, 40] is employed in our scheme. According to the bilinearity properties of the bilinear pairing, CC can make sure that data has been modified as long as the data block has been tampered with.

The contributions mentioned above are applied to the privacy protection in our scheme. In addition, from our simulation results, it's clear that our scheme is efficient when facing large-scale users.

3. Preliminaries

3.1. RSA algorithm

RSA [41] was proposed in the 1977 which is considered as first and widely used asymmetric-key cryptosystem. The security and reliability of RSA algorithm is depend n the hardness of integer factorization problem. The RSA

algorithm consists of four phases: key generation, key distribution, encryption and decryption.

- *Key generation:* The system computes $N = pq$ and Euler's totient function $\varphi(N) = (p-1)(q-1)$, where p and q should be chosen randomly and similar in magnitude but differ in length. Choosing an integer e satisfying the condition that $1 < e < \varphi(N)$ and $gcd(e, \varphi(N)) = 1$. Computing d as the modular multiplicative inverse of $e(\mod \varphi(N))$.

- *Key distribution:* Alice sends her public key (n, e) to Bob by a reliable, but not necessarily secret channel. But Alice always keeps her private key d secret.

- *Encryption:* Bob encrypts m by using Alice's public key e: $c = m^e \mod N$

- *Decryption:* Alice decrypts c by using her private key d : $c^d = m^{e*d} \mod N$,since $e * d \equiv 1 \mod \varphi(N)$.

Although attacks may know the Alice's public key(e,N), but there is a negligible probability to get the p and q because of large integer factorization is a NP-hard problem.

Definition 1. Let g_1 be a generator of group G_1, and let g_2 be a generator of group G_2. G_1 and G_2 are multiplicative cyclic group of prime order q with a additional Group G_T. In this paper, we set $G_1 = G_2$, but in general cases $G_1 \neq G_2$. ψ is a computable isomorphism from G_2 to G_1, with $\psi(g_2) = g_1$. e is a bilinear map which is computable $e : G_1 \times G_2 \to G_T$ with following properties for points:

1. Bilinear: For any $\mathcal{M} \in G_1$, $\mathcal{N} \in G_2$, u, $v \in Z$, we have $e(u\mathcal{M}, v\mathcal{N}) = e(\mathcal{M}, \mathcal{N})^{uv}$.
2. Non-degenerate: $e(g_1, g_2) \neq 1$.
3. commutative: For any $\mathcal{M}, \mathcal{N} \in G_2$, $e(\psi(\mathcal{M}), \mathcal{N}) = e(\psi(\mathcal{N}), \mathcal{M})$.
4. For any $\mathcal{M}_1, \mathcal{M}_2 \in G_1$ and $\mathcal{N} \in G_2$, we have [42]

$$e(\mathcal{M}_1\mathcal{M}_2, \mathcal{N}) = e(\mathcal{M}_1, \mathcal{N}) \cdot e(\mathcal{M}_2, \mathcal{N})$$

3.2. Group Blind Signature

Group blind signature was firstly proposed by Lysyanskaya and Ramzan in 1998 FC conference [43], which adds the blind feature on the basis of group signature. Upon the signer finding signature, he only can ensure that the signature is signed by himself. The signer can neither confirm when he signed the signature nor whom he signed the signature for. The scheme usually has these entities including group manager, group member and external users and consists of five steps:

- *Setup:* Group manager firstly generates group public key y and group private key x in an probability polynomial algorithm.
- *Join:* Group manager interacts with the new group member to generate the new group member's secret/public key pair and certificate.
- *Sign:* An probability polynomial algorithm that input message m and private key of the signer, then output the signature σ.
- *Verify:* Input (m, σ, y), a probability polynomial algorithm judges the correctness of the signature.
- *Open:* A probability polynomial algorithm that output identify of the signer by inputting the signature σ and group manger's private key.

3.3. Schnorr identification protocol

Schnorr identification protocol was proposed by Claus Schnorr in [44] and its security is based on the discrete logarithm problem. We assume that Prover(P) interactive with Verifier(V) in three-rounds protocol to prove that he owns w such that $W = g^{-w} \mod q$. The flowchart of Schnorr identification is following:

- *First round:* P randomly chooses number $r \in Z_q^*$ and calculates $R = g^r \mod q$ then sends R to V.

$$\text{Prover} \xrightarrow{R=g^r \mod q} \text{Verifier}$$

- *Second round:* V randomly picks $e \in [0, 2^t - 1]$, security of the protocol is based on the parameter t, which means the protocol will be more safer with the increase of t, and send e to P.

$$\text{Verifier} \xrightarrow{e} \text{Prover}$$

- *Third round:* P calculates $S = (r + w \cdot e) \mod p$ and sends it to V.

$$\text{Prover} \xrightarrow{S=(r+w\cdot e) \mod p} \text{Verifier}$$

V will verify whether the equation $R = g^s \cdot W^e \mod q$ is set up and accept that P knows w only if the equation holds.

4. System Model and Adversary Model

4.1. System Model

The system model of our scheme is demonstrated in the Fig. 2, which involves three entities' working relationship. Control center(CC), which is responsible for generating the system parameters, entity registration, data verification and tracing other entities conditional. Smart substation(SS), which can interactive with the user directly, verify the identity of user and generate blind signature. Smart meter(SM), which can record data in real time and send a whole period of consumption data regularly, so there is a threat that the data being tampered. In practice, the storage overhead and computing overhead of SM should be taken into consideration, because it's a resource-constrained device.

Moreover, the structure of our scheme is based on the group blind signature. When it comes to communication between three entities, they exchange message

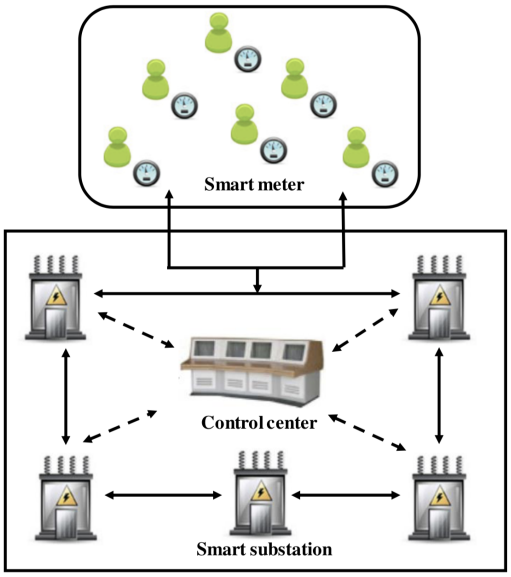


Figure 2: System model

in the tree topology structure which data flow bi-directional propagation in the upper and lower levels. In our scheme, adversary can not only eavesdrop the channel between user and SS, but also attempt to tamper the data and disrupt stability of system. In addition, since the property of traceability in our scheme, CC can acquire the identity of signer or revoke the anonymity of user if failure in signature verification or message verification, respectively.

4.2. Adversary Model

The adversary model determines the capabilities and possible actions of the attacker, adversary model is defined as follows:

1. Adversary can eavesdrop the channel between user and SS to obtain users' consumption information. In addition, spitefully forging and substituting the original or intermediate value can destroy the stability and dependability of system that might result in the threaten to data integrity.

2.Users have two types, one is honest but curious which they want to get other users' consumption information but don't want to change any data. The

other one is trying to tamper with own consumption data.

3. CC is fully trusted and SS is semi-trusted which as long as SS correctly signs the signature, SS cannot trace to specific users.

5. OUR SCHEME

The scheme we proposed consists of five phases: 1. system initialization, 2. user anonymous authentication and data reporting, 3. message signing, 4. verifying correctness of signature and integrity of data, 5. trace the singer or users. The framework is as shown in Fig. 3. In reality, the number of SS is much less than the number of SM/User. So we plan to use SM_i/U_i to distinguish the different user and use the S_i to indicate the number of SS. At last, we assume that the number of SM is constant $\mathcal{N}$, so i<$\mathcal{N}$. In the phase of data reporting, for simplicity, we only simulate the process of one user generating the tags.

5.1. System Initialization

1) System parameter generation and releasing: The Fig. 4 shows the process of generating the parameter.

- *Step 1:* CC chooses two big distinct prime p and q which satisfying $p|q-1$ and computes $n = pq$.
- *Step 2:* CC calculates the RSA public key pair (e, d) which satisfies $ed \equiv 1($ mod $\phi(n))$, where $\phi(n)$ is Euler function. The group public key and group private key are e and d respectively.
- *Step 3:* CC chooses a cyclic group $G < g >$ which is subgroup of Z_q^*. While, CC randomly chooses the element x and calculates $y = g^x \mod n$. Hence, group manager's public key and private key are y and x respectively.
- *Step 4:* CC publicly chooses secure anti-collision hash function $\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^k$.

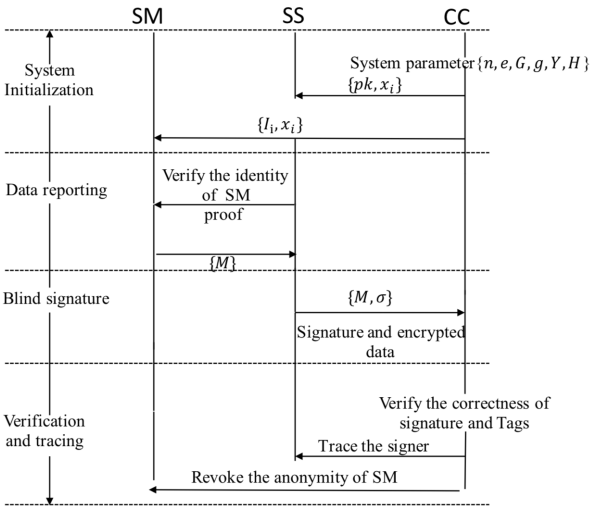


Figure 3: The framework of our scheme

- *Step 5:* CC releases the public parameter $P = \{n, e, G, g, y, \mathcal{H}\}$.

2)The phase of registering: The registering process is shown in Fig. 4.

- *Step 1:* If new group member (SS) wants to join the group, SS randomly chooses the number $x_i \in Z_q^*$ and sends it to the group manger (CC). CC randomly chooses $y_i \in Z_q^*$ and calculates $C = y^{y_i} x_i \mod n$ and $C_1 = g^{y_i} \mod n$. Group manger returns $PK = (C, C_1)$ and group member 's certificate x_i to SS.

- *Step 2:* $User_i$ opens an account in CC and gets $infor_i = (ID_i||address||timestack)$, $User_i$ will save the public value $g_i = (\mathcal{H}(infor_i)^x) \mod n$. CC installs smart meter at user's home. SM_i saves g_i and randomly chooses z_i to calculate $I_i = g^{z_i} \mod n$ as his own id information and sends I_i to CC.

5.2. User anonymous authentication and data reporting

1)user anonymous authentication: Each SM tries to convince SS that he is valid user by using schnorr identification protocol and then transform the encrypted message to SS. The detailed process is shown in the Fig. 5 .

- *Step 1:* SM_i random chooses $t_i \in Z_q^*$ and calculates $T = g^{t_i} \mod n$ and sends to SS.
- *Step 2:* SS calculates $c_b = \mathcal{H}(T||timestack)$ and sends c_b to user.
- *Step 3:* User calculates $S_i = t_i - c_b z_i$ and sends S_i to SS.
- *Step 4:* SS verifies the $c_b = \mathcal{H}(g^{S_i} I_i^{c_b}||timestack)$.

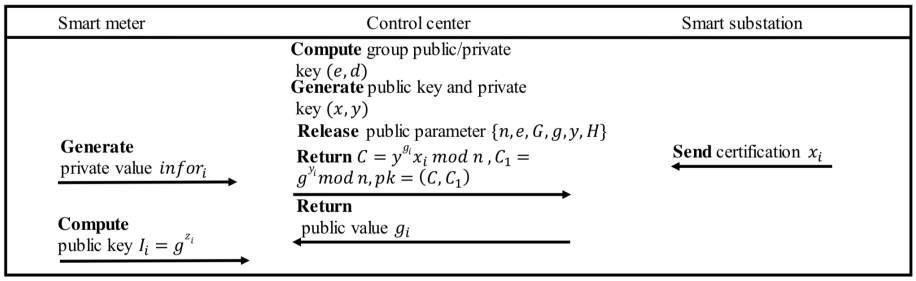


Figure 4: System Initialization

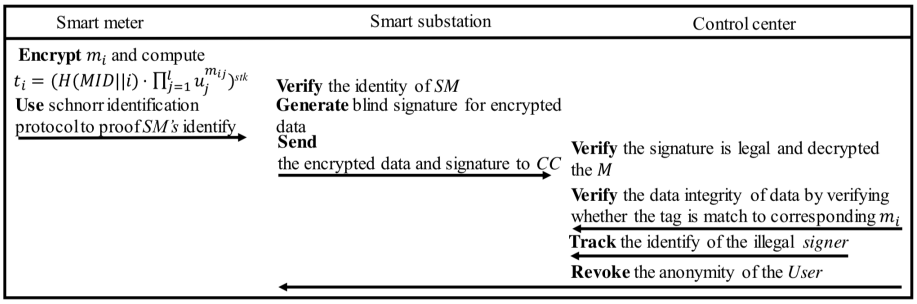


Figure 5: The implement of our scheme

2)data reporting: SS verifies correctness of the meter and receives user's encrypted data. For simplicity, we only simulate one $user_k$ to encrypt information data and report data. $user_k$ encrypts its consumption data and generates tags for every data block. Since every data block m_i is l dimensions, so we generate one data tag t_i for each data block m_i. Then CC acquires all tags with the whole day's electric consumption data $T||m$ and verifies these tags whether match to the corresponding data block. The reporting process is shown in Fig. 5.

- *Step 1:* Due to the security reason, the consumption data components should be restricted by security parameter λ. For example, if security parameter λ is set to 24, SM should generate twenty-four data blocks in a day. So the electric consumption data we collected is in one hour. While, the consumption data is $m = (cons, timestamp)$, in which $cons$ represents l-dimensional user's electricity consumption data $\{L_1, L_2, L_3 \ldots .L_l\}$.

- *Step 2:* SM generates another random number $stk \in Z_q^*$ as the secret tag key. Then SM outputs the public tag key $ptk = g_{SM_k}^{stk} \mod n$ by inputting the security parameter λ .

- *Step 3:* SM_k will generate l random values $\{x_1, x_2, x_3 \ldots .x_l\}$ and calculate $u_j = g_{SM_k}^{x_j} \mod n$ for $j \in [1, l]$. For each data block m_i, it computes a data tag t_i .SM_k will generate tag for every data block$(24/\lambda/day)$ by calculating the $t_i = \left(\mathcal{H}(MID||i) \cdot \prod_{j=1}^{l} u_j^{m_{ij}}\right)^{stk}$, in which MID is the abstract of data and i is the block number of m_i and it outputs the set of data tags $T = \{t_1, t_2, t_3 \ldots .t_i\}$, $i \in [1, 24/\lambda]$.

- *Step 4:* SM encrypts $(m||T)$ by using public key e. By doing so, we ensure that no other entity can learn the consumption information, other than group private key owner CC. Then SM_k calculates $M = (m||T)^e$ and $\mathcal{H}(m)$.

- *Step 5:* SM_k chooses an blind factor b to multiply $\mathcal{H}(m)$ and calculates $\mathcal{H}(m)' = b\mathcal{H}(m)$ and $\beta = g^b \mod n$. Then SM_k sends the pair$(\mathcal{H}(m)', \beta)$ to signer.

5.3. Blindly signature on the message

*1)generate the signature :*The process is shown in the Fig. 5.

- *Step 1:* Signer randomly chooses a big prime $k \in Z_q^*$ and calculates k^{-1} which is the multiplicative inverse of k. Then computing the signature $\sigma* = (r, s^*, C, C_1)$,where $s^* = k^{-1}(\mathcal{H}(m)' - ry_i) \mod n$, $r = \beta^k \mod n$, $C_1 = g^{y_i}$, $C = y^{y_i} x_i$.

- *Step 2:* SM_k removes the blind factor b by using $s = s^* b^{-1} = b^{-1}k^{-1}(\mathcal{H}(m)' - ry_i) \mod n$, then gets the signature $\sigma = (r, s, C, C_1)$ and sends σ to CC.

5.4. Verification and traceability

1)verify the signature's correctness and the data's integrity: The detailed process is shown in the Fig. 5.

- *Step 1:* CC decrypts M by using group private key d and gets the consumption information $(m||T)$ and computes $\mathcal{H}(m)$.

- *Step 2:* CC verifies the correctness of signature by judging whether or not the equation (1) is established. If the signature is verified correctly, it is proved that m is not tampered with during transmission.

$$\beta^{\mathcal{H}(m)} = C_1^r r^s \tag{1}$$

- *Step 3:* if signature is legal ,we verify the M by using the Tag T to test whether data has been modified. CC acquires T, m and u_i by decrypted M. Hence, CC can compute following values:

$$TG = \Pi_{i=1}^{24/\lambda} t_i \tag{2}$$

$$MG_j = \sum_{i=1}^{24/\lambda} m_{ij} \tag{3}$$

$$DG = \Pi_{j=1}^{l} e(u_j, ptk)^{MG_j} \tag{4}$$

$$H = \Pi_{i=1}^{24/\lambda} h(MID||i) \tag{5}$$

- *Step 4:* Then CC verifies whether equation(6) is set up:

$$DG \cdot e(H, ptk) = e(TG, g_{SM_k}) \tag{6}$$

- *Step 5:* If equation(6) is setting up, we can sure that the consumer's information has not been modified. If not, CC will revoke the anonymity of user to check whether user or external adversary have changed the consumer's information.

2)trace the identify of signer and revoke the anonymity of user: The detailed process is shown in the Fig. 5.

- *Step 1:* If we find that there is controversy when verifying the signature equation, CC can open the signature to verify signer's identity x_i and find the information of SS by using the CC's private key.

$$\begin{aligned} x_i &= C/C_1^x \\ &= y^{y_i} x_i / g^{y_i x} \end{aligned}$$

- *Step 2:* If equation (6) isn't established, we find that the integrity of m has been destoryed, the anonymity of user will be revoked by CC to check whether adversary or user have changed data. Due to different SM has different g_{SM}, when CC acquires $m||T$ and corresponding g_{SM} .

$$\begin{aligned} g_{SM_i} &= \mathcal{H}(infor_i)^x \mod n \\ &= \mathcal{H}(ID_i||address||timestack)^x \mod n \end{aligned}$$

CC calculates g_{SM_i} by using $infor_i$ in the database and compares to the original g_{SM} , which can insure the identify of user.

6. Security Analysis

Due to our system model has been improved on the basis of Jan Camenisch and Markus Stadler's group blind signature, obviously our scheme is as secure

as their's. The security of our scheme is based on the several difficulty problems assumption, which including discrete logarithm problem, integer factorization problem, and Computational Diffie-Hellman(CDH) problem. In addition, our scheme is based on the security of Schnorr's identification protocol and RSA encryption. In this section, we prove that our scheme has authenticatability, privacy-preserving, traceability, unforgeability and anonymity. The specific analysis is following:

6.1. Authenticatability

Authenticatability means that only legal users can upload their consumption information to SS. In our data reporting protocol, SS will verify the validity of consumers' identity. Only verifying successfully, SS can give a blind signature to data and send encrypted data with signature to CC. In the authenticated process, we use schnorr identification protocol to authenticate the user's identity.

Theorem 1. *The Schnorr identification protocol is an interactive protocol that has two parties, prover A and honest-verifier B. If A and B run the protocol successfully, B is always convinced $A's$ identity.*

Proof.

$$\begin{aligned} c_b &= \mathcal{H}(T||timestack) \\ &= \mathcal{H}(g^{t_i}||timestack) \\ &= \mathcal{H}(g^{S_i+c_b z_i}||timestack) \\ &\stackrel{?}{=} \mathcal{H}(g^{S_i} I_i^{c_b}||timestack) \end{aligned}$$

SS can calculate $g^{S_i} I_i^{c_b}$ and compare it with T. Hence, as long as SS and SM can follow the protocol, SS will accept SM's proof of identity. □

Theorem 2. *The Schnorr identification protocol based on discrete-log related assumption is secure against impersonation under concurrent attack [44].*

Proof. Proof sketch: As the security proof show in the [45], the main idea is to use a "rewinding technique":

1. Suppose there is probabilistic adversary A who interactive with V, so that the probability of V acceptance is ϵ. Assuming that discrete logarithm can be computed in a constant and positive odds by adversary A.
2. A as a prover interacts with an honest verifier V twice. The V chooses different random value c_{b_1} and c_{b_2}, then A calculate $S_1 = t - c_{b_1} z$ and $S_2 = t - c_{b_2} z$. A wins if both S_1 and S_2 accepted by V.
3. Output $z = (S_1 - S_2)/(c_{b_2} - c_{b_1})$ when $c_{b_2} \neq c_{b_1}$. In the first time, the probability of V successfully accepting is ϵ, while the probability that V accepts in the second time is also the polynomial probability of ϵ. Due to the discrete logarithm problem over being hard, so the authentication is security against the impersonation attack.

□

6.2. Unforgeability

Unforgeability refer to the fact that external adversary can't forge or tamper with the file. In our scheme of data reporting, the meter will set security parameter λ in advance to control the times of reporting. If the security parameter is λ, the frequency of sending report is $24h/\lambda$. At the same time, we introduce the homomorphic tag mechanism to verify whether the original data has been modified.

Definition 2. The Computational Diffie-Hellman(CDH) problem is that, consider a cyclic group G of order q, given $\mathcal{G} \in G$ and $(\mathcal{G}, \mathcal{G}^x, \mathcal{G}^y)$ for randomly chosen unknown x and y . It's infeasible to compute $\mathcal{G}^{xy}$ [46].

We define $(\iota - \epsilon) - CDH$consumption as a ι-time algorithm $\mathcal{A}$ has an non-negligible probability ϵ to resolve the CDH-problem.

$$\Pr[\mathcal{A}(\mathcal{G}, \mathcal{G}^x, \mathcal{G}^y) = \mathcal{G}^{xy}] \geq \varepsilon,$$

The CDH assumption indicates that the probability of solving the CDH problem in polynomial time algorithm is negligible, which means that this advantage ϵ is negligible.

Theorem 3. *If our scheme has been correctly performed by all entities, the equation will hold when the CC executes the verification.*

Proof. The correctness of our verification equation (6) is elaborated as follows:

$$
\begin{aligned}
DG \cdot e(H, ptk) =& \Pi_{j=1}^{l} e(u_j, ptk)^{MG_j} \cdot e(H, ptk) \\
e(TG, g_{SM_k}) =& e(\Pi_{i=1}^{24/\lambda} t_i, g_{SM_k}) \\
=& e\Big((\Pi_{i=1}^{24/\lambda} \big(\mathcal{H}(MID||i) \cdot \prod_{j=1}^{l} u_j^{m_{ij}}\big)^{stk}, g_{SM_k} \Big) \\
=& e\Big(\Pi_{i=1}^{24/\lambda} \big(\mathcal{H}(MID||i)^{stk}, g_{SM_k} \Big) \\
& \cdot e\Big(\prod_{j=1}^{l} \Pi_{i=1}^{24/\lambda} u_j^{m_{ij} stk}, g_{SM_k} \Big) \\
=& e(H, g_{SM_k}^{stk}) \cdot e\Big(\prod_{j=1}^{l} u_j^{\sum_{i=1}^{24/\lambda} m_{ij}}, g_{SM_k}^{stk} \Big) \\
=& e(H, g_{SM_k}^{stk}) \cdot e\Big(\prod_{j=1}^{l} u_j, g_{SM_k}^{stk} \Big)^{\sum_{i=1}^{24/\lambda} m_{ij}} \\
\Rightarrow \Pi_{j=1}^{l} e(u_j, ptk)^{MG_j} =& e\big(\prod_{j=1}^{l} u_j^{\sum_{i=1}^{24/\lambda} m_{ij}}, g_{SM_k}^{stk} \big) \\
=& \Pi_{j=1}^{l} e\big(u_j^{\sum_{i=1}^{24/\lambda} m_{ij}}, g_{SM_k}^{stk} \big) \\
=& \Pi_{j=1}^{l} e\big(u_j, g_{SM_k}^{stk} \big)^{\sum_{i=1}^{24/\lambda} m_{ij}}
\end{aligned}
$$

Hence , we ensure that the equation $DG \cdot e(H, ptk) = e(TG, g_{SM_k})$ will establish through the formula if all participants follow as our scheme. □

Theorem 4. *The verification tag is unforgeable for the possibility of any adversary A win the verification game is negligible ϵ in the polynomial time.*

Proof. We assume that adversary A can forge the tag and construct a challenger C. When A queries C, C will respond A correctly. The game is illustrated below.

- *Setup:* Define set $B = \{m_1, m_2, \ldots, m_{24/\lambda\}}$ is the challenged block message. Challenger C performs $Setup$ algorithm to generate system parameter to adversary A, which includes $P = \{n, e, G, g, y, h\}$. Then C randomly choose $x \in Z_q^*$.

- *Hash queries:* A sends the message's ID m_i to the challenger C. Only if m_i exists in set B, C can return the corresponding value $h(MID||i)^{stk}$ to A .

- *Extract queries:* A queries the block's private key by sending the ID of block message m_i. If m_i is in the set B, C randomly chooses $x_j \in Z_q^*$ and calculates $u_j = g_{SM_k}^{x_j}$.

- *KeyGen queries:* A queries meter's secret tag key by sending sequence of smart meter k. C returns $ptk = g^{stk}$ to A if the SM exist.

- *Tag queries:* A sends the data block m_i to query the verification tag from C. C calculates tag as following

$$t_i = \mathcal{H}(MID||i)^{stk} \cdot \prod_{j=1}^{l} u_j^{m_{ij}stk}$$

and returns to A.

- *Outputs:* A finally outputs t_{i^*} at data block m_{i^*} with the abstract of m_{i^*} MID^*. We can obtain following equation:

$$\begin{aligned} t_{i^*} &= \left(\mathcal{H}(MID^*||i^*)\right)^{stk} \cdot \prod_{j=1}^{l} u_j^{m_{i^*j}stk} \\ &= (\mathcal{H}(MID^*||i^*))^{stk} \cdot \prod_{j=1}^{l} g_{SM_k}^{x_j m_{i^*j}stk} \end{aligned}$$

It is easy to see the conclusions described in the following from this equa-

tion.

$$\prod_{j=1}^{l} g^{x_j stk} = \left(\mathcal{H}(MID^*||i^*)^{-skt}\right)^{1/m_{i*j}} \tag{7}$$

We can draw a conclusion that A solves the $CDH - assumption$ in the polynomial time algorithm with the non-negligible possibility, which contradicts with the hardness of $CDH - assumption$. Hence, the adversary can't forge the valid tag.

□

6.3. Privacy-Preserving

Theorem 5. *Adversary cannot get the user's consumption information in the initial and intermediate phrase.*

Proof. In two phrases of data reporting and blind signature, adversary and SS have ability to get the encrypted user's consumption information M and can't get private key of CC directly. So the possible way is to divide the big prime number into p and q. We assume that factorizing N into correct p and q is an non-negligible possibility ϵ in the polynomial time algorithm. However, there is no efficient algorithm to resolve the problem of prime factorization. Hence, our scheme can efficiently protect the privacy of users' consumption information.

□

6.4. Anonymity

The scheme is anonymity if m is leaked, but the *Adversary* cannot get the identity of the information owner.

Theorem 6. *Even if the adversary can crawl into the private database of CC and steal the decrypted information m and T, A can't infer the identity of the user by analysing the consumption information m.*

Proof. If *Adversary* tries to infer the identify of data owner, the only way is to get g_{SM_k} from $t_i = \left(\mathcal{H}(MID||i) \cdot \prod_{j=1}^{l} g_{SM_i}^{x_j \cdot m_{ij}}\right)^{stk}$ and compare to $\mathcal{H}(infor_i)^x$

mod n. However, $Adversary$ has no capacity for getting g_{SM_k} because of solving the discrete logarithm problem is hard.

For experiment $Exp(b)$ is for giving g_{SM},the $adversary$ choose the correct corresponding $infro_{b_i}$ from $infro_{b_0}$ and $infro_{b_1}$ for $i = 0, 1$.

Algorithm 1 *Experiment* $Exp^{Anon-b}_{GBS,\mathcal{A}}(b)$

- $Exp(b) \leftarrow \mathcal{A}_{find}(g_{SM})$

- $(infro_{b_o}, infro_{b_1}) \leftarrow Exp(b)$

- $b_i \leftarrow \mathcal{A}_{guess}(g_{SM}, infro_{b_o}, infro_{b_1})$

- $return \quad b_i$

More formally, we define that all PPT adversaries $\mathcal{A}$ have a negligible advantage $Adv^{Anon-b}_{GBS,\mathcal{A}}$, where the advantage is defined as follows:

$$\begin{aligned} Adv^{Anon}_{GBS,\mathcal{A}} &= Pr|Exp^{Anon-0}_{GBS,\mathcal{A}}(b_0) = 1 - Exp^{Anon-1}_{GBS,\mathcal{A}}(b_1) = 1| \\ &= \epsilon \end{aligned}$$

Hence, we can draw a conclusion that the true probability of identifying the correct user identity from the set $\{infro_i\}$ is $1/\mathcal{N} + \epsilon$ after the adversary steals the user's information. We define the probaility as following:

$$\begin{aligned} Adv^{Iden}_{GBS,\mathcal{A}} &= Pr|Exp^{Iden-infor_i}_{GBS,\mathcal{A}}(b_{infor_i}) = 1| \\ &= 1/\mathcal{N} + \epsilon \end{aligned}$$

,when the number of user $\mathcal{N}$ approaches a large integer, $1/\mathcal{N}+\epsilon$ will converge to a negligible probability. It is clear that such a game captures the requirement

that adversary can't link the m to identify of the user, so anonymity can be guaranteed. □

6.5. Traceability

Theorem 7. *If the equation (1) is not established, the CC executes tracking operation to get the signer's information by using $x_i = C/C_1^x$. Next, CC will revoke the anonymity of user, if the equation (6) isn't established.*

Proof. Correctness:

$$\begin{aligned}
\beta^{\mathcal{H}(m)} &\stackrel{?}{=} C_1^r r^s \\
&= g^{y_i r} \cdot \beta^{ks} \\
&= g^{y_i r} \cdot g^{bks} \\
&= g^{y_i r + bkb^{-1}k^{-1}(\mathcal{H}(m)' - ry^i)} \\
&= g^{\mathcal{H}(m)'}
\end{aligned}$$

By verifying the correctness of equation (1), CC can check the signature issuing from SS.

$$\begin{aligned}
x_i &= C/C_1^x \\
&= y^{y_i} x_i / g^{y_i x} \\
&= x_i
\end{aligned}$$

CC can get identity of signer by using group private key x which only group manager owns.

$$\begin{aligned}
g_{SM_i} &= \mathcal{H}(infor_i)^x \mod n \\
&= \mathcal{H}(ID_i||address||timestack)^x \mod n
\end{aligned}$$

Finally, by utilizing registration information in the database, CC can calculate $\mathcal{H}(infor_i)^x$ one by one to match the result with corresponding g_{SM_i}. □

Table 1: Features Comparison

Schemes	Ours	[18]	[47]	[48]
Fine-grained Data	√	√	√	√
Anonymous Authentication	√	√	√	√
Unforgeability	√	×	√	√
Data Integrity	√	×	×	√
Traceability	√	×	×	×
Scalability	√	×	√	×

† √: Support the feature

† ×: Dot not support the feature

7. Performance Analysis and Evaluation

In the section, the proposed scheme is analysed in the aspects of features, computational cost and performance evaluation. From results of analysis and comparison, our scheme not only has more functionality and features, but also can be more practical in reality.

7.1. Features Comparison

In this subsection, our scheme is compared with Dimitriou [18] and Zargar [47] in terms of fine-gained data, anonymous authentication, unforgeability, data integrity, traceability and scalability. As shown in Table 1, [18] can get the fine-grained usage data and achieve anonymous authentication, but it cannot sure that the file is modified by the external adversary. In addition, both [18] and [47] cannot achieve data integrity in the transmission process and trace malicious participants when signature or data are corrupted. Finally, although [48] can efficiently protect the privacy of consumer, it cannot trace malicious participants and use widely.

7.2. Computational cost

In the subsection, we can divide it into three stages including System setup, anonymous authentication, blind signature generating and verification. Note

that we count modular multiplication operation M, modular exponentiation operation E, Weil Pairing operation W and hash operation H for every phase. In addition, these operations are positively related to the participants, hence, we assume that the number of SM is v and the number of SS is s. Computational cost comparison is demonstrated in Table 2 in terms of setup phase, authentication phase, sigGen phase and proof phase.

In the setup phase, CC needs to calculate y, C, $C1$, g_i, I_i and a hash $h(infor_i)$. Hence, $M = s, E = s + 2v + 1, H = v$. Then the identify of SM will be authenticated by SS in the second phase, $T = g^{t_i}$ will be obtained by SM to compute v times of exponentiation operation. While, for providing authentication service, SS will compute $2v$ times of exponentiation operation g^{s_i} and I^{c_b}, $2v$ times of modular multiplication operation and v times of modular multiplication operation. In the third phase, $H(m)$, $(m||T)^e$ and β will be calculated by using $2v$ modular exponentiation and v hash function. To verify the correctness of the equation(1), CC will compute $C_1^r r^s$, $\beta^{h(m)}$ by using $4v$ modular exponentiation and v modular multiplication. In summary, $M = v$, $E = 6v$, $H = v$. The experimental comparison results are shown in Fig. 6(a),6(b), time cost increases linearly with the number of users and substations, but increases more slowly than [47, 31, 48].

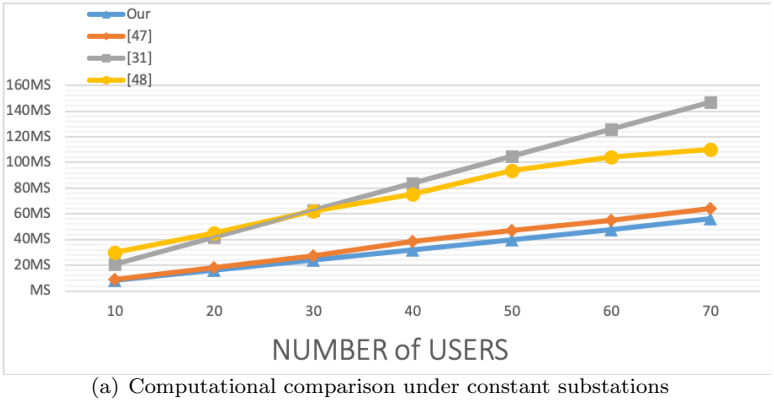
Specially, in the report generating phase homomorphic tag mechanism has been firstly used in smart grid to verify the integrity of data. Before reporting consumption message, ptk, u_j, and t_i should be computed by SM_k with $1 + l + 24/\lambda(l+1)$ modular exponentiation, $24/\lambda$ modular multiplication and $24/\lambda$ hash in a day. When CC decrypts messages m, l Weil pairing operations and $24/\lambda$ Hash operations are needed for computing DG and H. At the same time, $e(H, ptk)$ and $e(TG, g_{SM_k})$ are 2 Weil pairing operations. Hence, we totally need M= $24/\lambda$, $E = 1 + l + 24/\lambda(l + 1)$, H= $24/\lambda$, $W = l + 2$ in the report generating and verifying phase in a day for one user and CC.

Table 2: Computational cost comparison

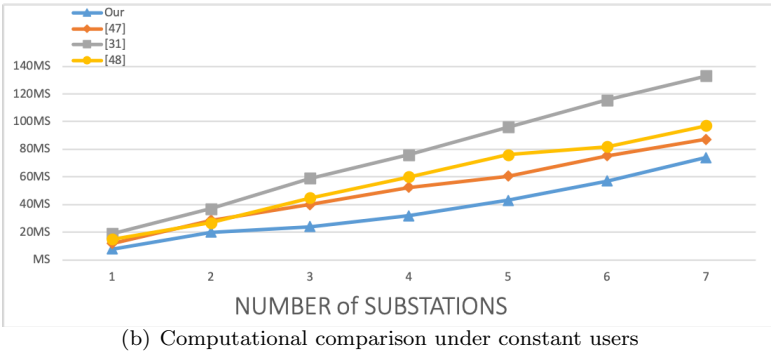
Protocol	Setup	Authentication	SigGen	Proof
Ours	$s(M+E)+v(2E)+vH$	$v(M+2E)$	$v(E+H)$	$v(6E+M+H)$
[47]	$sW+v(3M+2E+H)$	$v(3E+W)$	$v(2E+M)$	$v(5E+5M+2W)$
[31]	$v(4M+4E)$	$v(3E+5M)$	$v(6E+4M)$	$v(5E+5M)$
[48]	$v(M+4W)$	$v(2W+3M)$	$3vM$	$10vM$

† M, E, W, H: Operations of modular multiplication operation, modular exponentiation, Weil Pairing and hash

† $\times$: v, s: The number of SM and SS



(a) Computational comparison under constant substations



(b) Computational comparison under constant users

Figure 6: The computational cost comparison

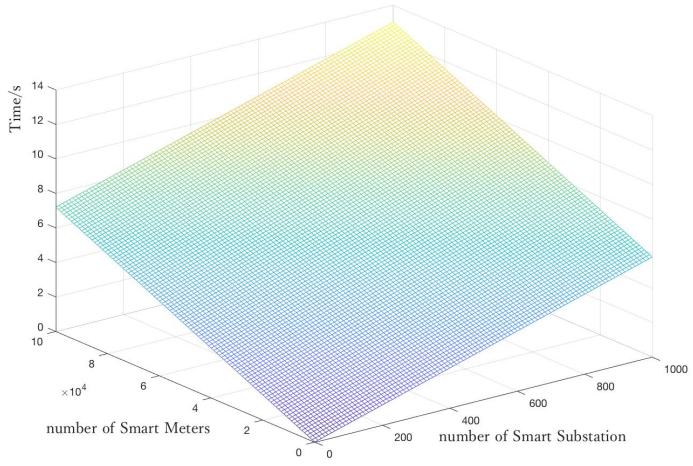
7.3. Performance Evaluation

To simulate the efficient our scheme in reality, we perform on a desktop installed Ubuntu16.04 with Intel Core i3-3120 CPU and 4GB memory. The simulation experiment is carried out by C language, in which pairing-based cryptography(PBC) library and GUN multiply precision arithmetic(GMP) library are used. The experimental results are obtained from the terminal of the Linux and calculated the average value of twenty times. At the same time, we acquire the graph by using MATLAB 2017a.

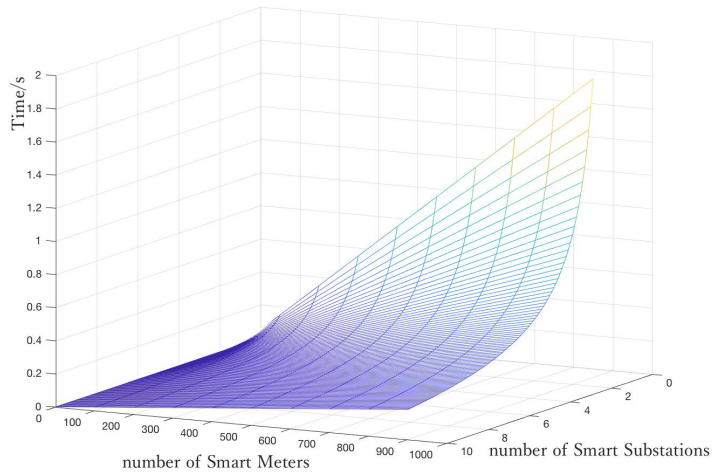
The simulation is made up by four stage. In the first stage, setup time overhead is presented by increasing of the number of smart meters and smart substations. It is clearly that time cost is linear with the two variables. When the number of smart meters is up to 1000 and the number of smart substation is up to 10, the time cost is $13.005s$ in Fig. 7(a). In Fig. 7(b), the simulation result shows that the time cost will increase with the smart meters and decrease with the number of smart substations. As shown in the Fig. 7(b), the time overhead is 0.202s when the number of SM and SS up to 1000 and 10, respectively. The reason is that, load balance technology [49] will assign different SM authentication services to different SS to increase data processing capability. Ideally, with the increase of SM and SS, time consumption will be stable within a certain range. Just as shown in Fig. 7(c), the time consumption of blind signature also satisfies this rule. The time cost will decline rapidly with the increase of SS.

Specially in Fig. 7(d),we present the time consumption on the tag generation phase and tag verification phase. From the experimental result, it's clear that time consumption is positively related to the number of data blocks and the dimensions of data. When the number of data dimension and data block are both up to 1000, the time cost of tag generation and tag verification are 0.071835s and 0.000009s respectively.

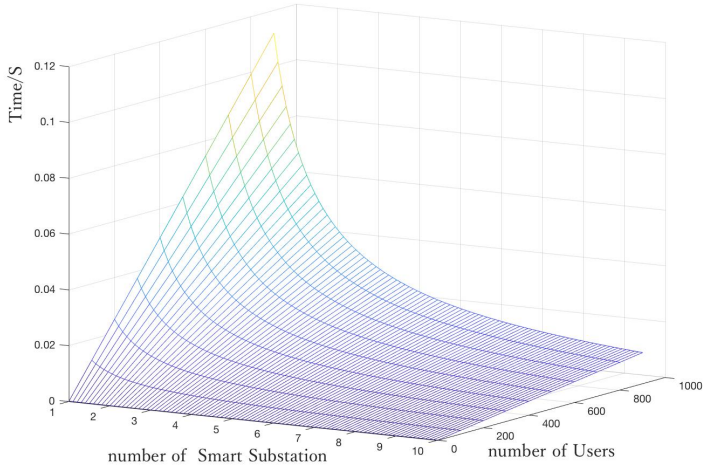
Through all above experiments, our scheme has proofed efficient and performed well when facing large-scale users. Hence, the scheme not only can be proved secure, but also has a good scalability.



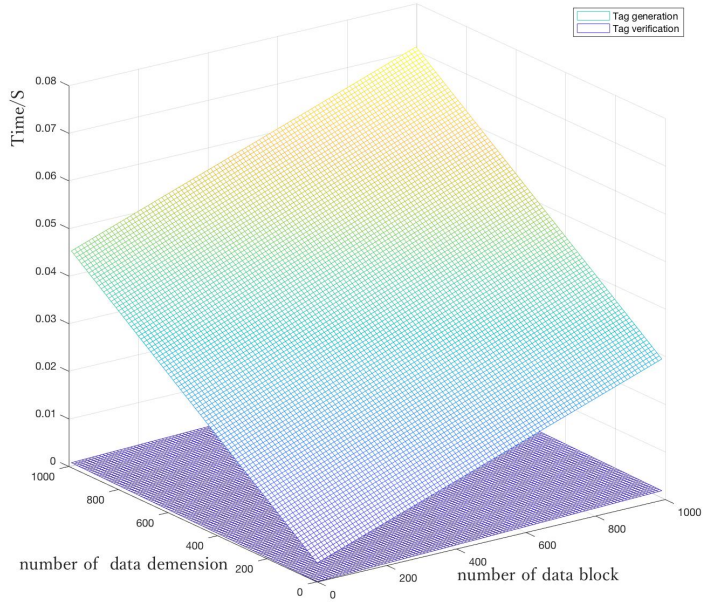
(a) Setup time



(b) Time of anonymous authentication



(c) Time of blind signature



(d) Time of tag generation and verification

Figure 7: Efficiency simulation for different phases.

8. Conclusion

In the paper, we have proposed a practical group blind signature scheme with anonymous authentication and privacy-preservation for smart grid. Four phases are included into the proposed scheme: the phase-I, where, SMs, SSs finish registration after CC generates system parameters. In phase-II, SMs anonymously authenticate with SS by employing the schnorr identification. Subsequently, the homomorphic tags are generated by SMs for verifying the integrity of data. Phase-III, where SS generates group blind signature for data from authenticated SM. In Phase-IV, the correctness of signature and the integrity of data are verified by CC. The experiment simulation shows that our scheme is scalable and efficient. In our future work, we plan to expand our scheme to accomplish the anonymous rewarding when consumer's power consumption meets certain standards by using block chain.

Acknowledgements

This work is supported by the National Science Foundation of China under Grant No.U1836115, No. 61672295, No. 61672290, the Natural Science Foundation of Jiangsu Province under Grant No.BK20181408, the State Key Laboratory of Cryptology Foundation, the Guangxi Key Laboratory of Cryptography and information Security under Grant No.GCIS201715, the CICAEET fund, and the PAPD fund.

References

[1] F. Xi, M. Satyajayant, G. Xue, D. Yang, Smart grid-the new and improved power grid: A survey, IEEE Communications Surveys and Tutorials 14 (4) (2012) 944–980.

[2] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, T. Basar, Dependable demand response management in the smart grid: A stackelberg game approach, IEEE Transactions on Smart Grid 4 (1) (2013) 120–132.

[3] M. H. Rehmani, A. Davy, B. Jennings, C. Assi, Software defined networks based smart grid communication: A comprehensive survey, IEEE Communications Surveys & Tutorialsdoi:S10.1109/COMST.2019.2908266.

[4] Y. Zhang, R. Yu, N. Maziar, Y. Liu, S. Xie, S. Gjessing, Cognitive machine-to-machine communications: visions and potentials for the smart grid, IEEE Network 26 (3) (2012) 6–13.

[5] D. Seo, H. Lee, A. Perrig, Secure and efficient capability-based power management in the smart grid, IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops 42 (4) (2011) 119–126.

[6] X. Wang, P. Yi, Security framework for wireless communications in smart distribution grid, IEEE Transactions on Smart Grid 2 (4) (2011) 809–818.

[7] Y.-H. Lin, S.-Y. Chang, H.-M. Sun, Cdama: Concealed data aggregation scheme for multiple applications in wireless sensor networks, IEEE Transactions on Knowledge and Data Engineering 25 (7) (2013) 1471 – 1483.

[8] K.-A. Shim, C.-M. Park, A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems 26 (8).

[9] M. A. Mustafa, S. Cleemput, A. Aly, A. Abidin, A secure and privacy-preserving protocol for smart metering operational data collection, IEEE Transactions on Smart Griddoi:10.1109/TSG.2019.2906016.

[10] P. Gope, B. Sikdar, Lightweight and privacy-friendly spatial data aggregation for secure power supply and demand management in smart grids, IEEE Transactions on Information Forensics and Security 14 (6) (2019) 1554–1566.

[11] J. Zhang, L. Liu, Y. Cui, Z. Chen, Sp2das: Self-certified pkc-based privacy-preserving data aggregation scheme in smart grid, International Journal of Distributed Sensor Networks 2013 (9) (2013) 56–64.

[12] E. Vahedi, M. Bayat, M. Pakravan, A secure ecc-based privacy preserving data aggregation scheme for smart grids, Computer Networksdoi:10.1016/j.comnet.2017.08.025.

[13] D. He, N. Kumar, S. Zeadally, A. Vinel, L. T. Yang, Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversarie, IEEE Transactions on Smart Grid 18 (4) (2017) 628–639.

[14] L. Chenm, R. Lu, Z. Cao, Lpda: A lightweight privacy-preserving data aggregation scheme for smart grid, Peer-to-Peer Networking and Applications 8 (6) (2015) 1122–1132.

[15] C. Li, R. Lu, H. Li, L. Chen, J. Chen, Pda: A privacy-preserving dual-functional aggregation scheme for smart grid communications secur, Security and Communication Networks 8 (15) (2015) 2494–2506.

[16] H. Shen, M. Zhang, J. Shen, Efficient privacy-preserving cube-data aggregation scheme for smart grids, IEEE Transactions on Information Forensics and Security 12 (6) (2017) 1369–1381.

[17] R. Lu, X. Liang, X. Li, X. Lin, X. Shen, Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications, IEEE Transactions on Parallel and Distributed Systems 23 (9) (2012) 1621–1631.

[18] T. Dimitriou, K. Karame, Enabling anonymous authorization and rewarding in the smart grid, IEEE Transactions on Dependable and Secure Computing 14 (5) (2017) 565–572.

[19] T. Dimitriou, K. Karame, Privacy-friendly tasking and trading of energy in smart grids, ACM Symposium on Applied Computing 21 (6) (2013) 652–659.

[20] C.-H. Chen, C.-Y. Chen, C.-H. Hsia, G.-X. Wu, Efficient vision-based smart meter reading network, International Journal of Web Services Research (IJWSR) 14 (1) (2017) 44–58.

[21] C. Hsia, Hsien, Improved finger-vein patternmethod usingwavelet-based for real-time personal identification system, Journal of Imaging Science and Technology 62 (3).

[22] C.-H. Hsia, Y.-J. Dai, S.-L. Chen, T.-L. Lin, J. Shen, A gait sequence analysis for ip camera using a modified lbp, Journal of Internet Technology 19 (2) (2018) 451–458.

[23] C.-H. Hsia, New verification strategy for finger-vein recognition system, IEEE Sensors Journal 18 (2) (2018) 790–797.

[24] E. Ghadafi, Formalizing group blind signatures and practical constructions without random oracles, Information Security and Privacy (2013) 330–346.

[25] R. Rivest, A. C. Smith, Z. A. Ramzan, Group blind digital signatures theory and applications, Master Thesis Mit (1999) 199–203.

[26] A. Lysyanskaya, Z. Ramzan, Group blind digital signatures: A scalable solution to electronic cash, International Conference on Financial Cryptography 1465 (1998) 184–197.

[27] J. Shen, A. Wang, C. Wang, J. Li, Y. Zhang, Content-centric group user authentication for secure social networks, IEEE Transactions on Emerging Topics in Computingdoi:10.1109/TETC.2017.2779163.

[28] S. Tang, L. Xu, L. Niu, J. Ding, Z. Yang, Provably secure group key management approach based upon hyper-sphere, IEEE Transactions on Parallel and Distributed Systems 25 (12) (2014) 3253–3263.

[29] F. Li, B. Luo, P. Liu, Secure information aggregation for smart grids using homomorphic encryption, First IEEE International Conference on Smart Grid Communications (2010) 327–332.

[30] C. Efthymiou, G. Kalogridis, Smart grid privacy via anonymization of smart metering data, in: First IEEE International Conference on Smart Grid Communications, 2010.

[31] T. Jeske, Privacy-preserving smart metering without a trusted-third-party, Proceedings of the International Conference on Security and Cryptography 6585 (1) (2014) 114–123.

[32] J. Camenisch, A. Lysyanskaya, A signature scheme with efficient protocols, International Conference on Security in Communication Networks 2576 (1) (2002) 268–289.

[33] X. Li, S. Tang, L. Xu, H. Wang, C. Jie, Two-factor data access control with efficient revocation for multi-authority cloud storage systems, IEEE Access 5 (99) (2017) 393–405.

[34] J. Shen, D. Liu, M. Z. Alam Bhuiyan, J. Shen, X. Sun, A. Castiglione, Secure verifiable database supporting efficient dynamic operations in cloud computing, IEEE Transactions on Emerging Topics in Computingdoi:10.1109/TETC.2017.2776402.

[35] X. Chen, J. Li, J. Ma, Q. Tang, W. Luo, New algorithms for secure outsourcing of modular exponentiations, IEEE Transactions on Parallel and Distributed Systems 25 (9) (2014) 2386–2396.

[36] X. Chen, X. Huang, J. Li, J. Ma, W. Luo, D. S. Wong, New algorithm for secure outsourcing of largescale systems of linear equations, IEEE transactions on information forensics and security 10 (1) (2015) 69–78.

[37] J. Shen, C. Wang, A. Wang, S. Ji, Y. Zhang, A searchable and verifiable data protection scheme for scholarly big data, IEEE Transactions on Emerging Topics in Computingdoi:10.1109/TETC.2018.2830368.

[38] S. Tang, X. Li, X. Huang, X. Yang, L. Xu, Achieving simple, secure and efficient hierarchical access control in cloud computing, IEEE Transactions on Computers 65 (7) (2016) 2325–2331.

[39] X. Chen, L. Jin, X. Huang, J. Ma, W. Lou, New publicly verifiable databases with efficient updates, IEEE Transactions on Dependable and Secure Computing 12 (5) (2015) 546–556.

[40] X. Chen, J. Li, X. Huang, J. Li, Y. Xiang, D. S. Wong, Secure outsourced attribute-based signatures, IEEE Transactions on Parallel and Distributed Systems 25 (12) (2014) 3285–3294.

[41] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the Acm 26 (2) (1978) 96–99.

[42] D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and verifiably encrypted signatures from bilinear maps, Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic techniques (Eurocrypt'03) 2656 (1) (2003) 416–432.

[43] A. Lysyanskaya, Z. Ramzan, Group blind digital signatures: A scalable solution to electronic cash, Financial Cryptography 1465 (1998) 184–197.

[44] C. Schnorr, Efficient identification and signatures for smart cards, Advances in Cryptology EUROCRYPT (1989) 688–689.

[45] M. Bellare, A. Palacio, Gq and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks, Proc of Crypto 2442 (2002) 149–162.

[46] M. Ueli, W. Stefan, The relationship between breaking the diffie-hellman protocol and computing discrete logarithms, Siam Journal on Computing 28 (5) (1998) 1689–1721.

[47] S. H. M. Zargar, M. H. Yaghmaee, Privacy preserving via group signature in smart grid, in: Proceedings of the Electric Industry Automation Congress (EIAC), Mashhad, Iran, 2013, pp. 13–14.

[48] Z. Sui, M. Niedermeier, et al., Tai: a threshold-based anonymous identification scheme for demand-response in smart grids, IEEE Transactions on Smart Grid 9 (4) (2018) 3496–3506.

[49] S. Lu, H. Fang, Y. Wei, Distributed clustering algorithm for energy efficiency and load-balance in large-scale multi-agent systems, Journal of Systems Science and Complexity 31 (1) (2018) 234–243.

Biographies

Wei Kong received the B.E. degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2017. He is currently a postgraduate with the School of Nanjing University of Information Science and Technology, Nanjing, China. His research interests include computer and network security, privacy-preserving and cryptography.

Jian Shen received the M.E. and Ph.D. degrees in Computer Science from Chosun University, South Korea, in 2009 and 2012, respectively. Since late 2012, he has been a professor at Nanjing University of Information Science and Technology, Nanjing, China. His research interests include public key cryptography, secure data sharing and data auditing in cloud.

Pandi Vijayakumar completed his Ph.D in Computer Science and Engineering in Anna University Chennai in the year 2013. He completed Master of Engineering in the field of Computer Science and Engineering in Karunya Institute of Technology in the year 2005. He completed his Bachelor of Engineering under Madurai Kamarajar University in the year 2002. He is presently working as Assistant Professor at University College of Engineering, Tindivanam. He is

guiding for many Ph.D scholars in the field of network and cloud security. He has published various quality papers in the reputed journals like IEEE Transactions, Elsevier, Springer, IET, Taylor and Francis, Wiley etc. His main thrust research areas are Key management in Network Security and Multicasting in Computer Networks.

Youngju Cho is the SW education research professor of the SW Convergence Education Institute at Chosun University and is a head researcher of an annex research institute owned by the SCG corporation. She received her master's degree and PhD both in electronic calculation from Chosun University, specializing in information technologies, education, and mobile ad hoc networks. Her interests include network security, IOT, information protection, mobile ad hoc networks, Internet ethics, VR, and AR.

Victor Chang is a Senior Associate Professor, Director of Ph.D. (June 2016 – May 2018) and Director of MRes (September 2017 - February 2019) at International Business School Suzhou (IBSS), Xi'an Jiaotong-Liverpool University (XJTLU), Suzhou, China, since June 2016. He is also a very active and contributing key member at Research Institute of Big Data Analytics (RIBDA), XJTLU. He's an Honorary Associate Professor at the University of Liverpool and Visiting Researcher at the University of Southampton, UK. Previously he worked as a Senior Lecturer at Leeds Beckett University, UK, for 3.5 years. Within 4 years, he completed Ph.D. (CS, Southampton) and PGCert (Higher Education, Fellow, Greenwich) while working for several projects at the same time. He has published 3 books as sole

authors and the editor of 2 books on Cloud Computing and related technologies.