Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5566430, 9 pages
https://doi.org/10.1155/2021/5566430

Research Article

Multiauthority Traceable Ring Signature Scheme for Smart Grid Based on Blockchain

Fei Tang, [1,2] Junjie Pang, [1] Kefei Cheng, [2] and Qianhong Gong [3]

[1] *School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[2] *School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[3] *School of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*

Correspondence should be addressed to Fei Tang; tangfei@cqupt.edu.cn

Received 16 January 2021; Revised 26 February 2021; Accepted 22 March 2021; Published 10 April 2021

Academic Editor: Di Zhang

As the next-generation power grid system, the smart grid can realize the balance of supply and demand and help in communication security and privacy protection. However, real-time power consumption data collection might expose the users' privacy information, such as their living habits and economic conditions. In addition, during the process of data transmission, it may lead to data inconsistency between the user side and the storage side. Blockchain provides tamper-resistant and traceable characteristics for solving these problems, and ring signature schemes provide an anonymous authentication mechanism. Therefore, in this work, we consider the applications of ring signature scheme in smart grid based on blockchain. We introduce the notion of multi-authority traceable ring signature (MA-TRS) scheme for distributed setting. In our scheme, there is an auditing node that can distinguish the identity of the real signer from the ring without any secret information. Last but not least, we prove that the proposed scheme is unforgeable, anonymous, and traceable.

1. Introduction

The rapid development of society and economy has driven the increasing demand for electricity of the people, which requires that the power supply system is more convenient, stable, and secure. However, the traditional power grid system has the problems of load imbalance and lack of effective diagnosis of faults in real time. Therefore, a smart grid emerges to cope up with these problems.

Smart grid, combining the traditional power grid system with state-of-the-art information and communication technology, is considered as one of the most significant trends in the next generation power grids [1–4]. In smart grid, different from the one-way communication of the traditional power grid (which just transmits electricity from generation plants to electricity users), it allows two-way communication, which enables the electricity users to easily get their consumption data and intelligently control their use of the domestic electrical equipment properly [5, 6]. In addition, the electricity company can adjust the plan of the power supply to solve the problem of peak power consumption according to the real-time electricity data collection. Compared with traditional power grids, a smart grid system has a lot of significant advantages. However, some researchers have indicated that the malicious attackers or eavesdroppers can infer the users' living habits, financial situations, identity information, or even which household equipment is being used during the process of the real-time power data collection [7, 8]. And it will pose a threat to individual and national security. Hence, how to deal with the leakage of power consumption data and identity information has become the focus of researchers [9].

As the underlying core technology of Bitcoin [10], blockchain is a distributed ledger that maintains the sustainable growth of data records list confirmed by all the participating nodes. Blockchain is a promising and powerful technology, which utilizes cryptography, P2P, and so on to guarantee the security of the system. Due to the properties of decentralization, tamper-resistance, and traceability, blockchain is considered as an alternative option for setting up a trustful platform without a trusted third party. In recent years, it has been widely used in diverse industrial areas, including finance [11, 12], artificial intelligence [13, 14], health care [15, 16], and Internet of Things (IoT) [17–19]. Obviously, it is feasible to utilize blockchain technology into the smart grid system to address the above-mentioned weaknesses. Guan et al. [20] proposed a privacy-preserving and efficient data aggregation scheme based on blockchain for power grid communications. In this study, users are divided into different groups and each group possesses a private blockchain. In order to disguise the users' real identities, every user creates multiple pseudonyms. But this scheme uses a key generation center to generate users' keys, which will lead to key escrow problem, and it lacks of tracing function when data inconsistency.

Although the properties of blockchain can make users' identities anonymous and protect their privacy, it is far from enough to solve the problem of users' information privacy. Ring signature is one of the best methods to tackle it. In order to achieve anonymity of users, Rivest et al. [21] formalized the concept of ring signature in 2001, which is one of the digital signature schemes applied in blockchain. Distinct from group signature [22], ring signature has no group manager and allows any member of the ring to sign on behalf of all ring members as well as protecting the real identity of the true signer.

Identity-based cryptosystem was introduced by Shamir [23], allowing the users to utilize their own identities as the public keys. Zhang and Kim [24] constructed an identity-based ring signature (IDRS) scheme, combining the properties of ring signature and identity-based signature. After that, other researchers have come up with their own ID-based signature schemes, such as [25–27]. Ring signature, however, is not always a best option owing to its full anonymity. Therefore, a traceable ring signature (TRS) scheme [28] was proposed for restricting abusing anonymity. As for group signature, it has a strong ability of traceability, and ring signature has a strong ability of full anonymity. Traceable ring signature keeps the balance between group signature and ring signature. To be specific, traceable ring signature has the characteristics of traceability and anonymity. In a traceable ring signature scheme, not only does it provide anonymity for any signer when he/she signs any message but also provides traceability for verifiers to distinguish whether the signatures are produced by the identical signer on the same transaction while the malicious signer abuses anonymity in some situations. Besides, some researchers have proposed the ring signature schemes with anonymity revocation [29, 30], while it is based on single authority, which is not suitable for blockchain applications.

Based on the above analysis, we present a multi-authority traceable ring signature (MA-TRS) scheme for smart grid based on blockchain. The main contributions of this work are listed as follows.

(1) The definition of TRS scheme in the multiple authorities setting is formalized. In our definition, there exist n key-generation nodes, and the electricity user is supposed to interact with at least t out of n key-generation nodes to generate his/her own private keys.

(2) We construct an MA-TRS scheme for blockchain-based smart grid based on ID-based ring signature. And it has the properties of unforgeability, anonymity, and traceability.

(3) In our scheme, the auditing node is responsible for tracing the real signer when the power consumption data of the electricity users is inconsistent with that of the blockchain network, while the auditing node does not possess any secret information.

The rest of this paper is organized as follows. In Section 2, we introduce the preliminary knowledge of our proposed scheme. The system model and security model will be defined in Section 3. Then in Section 4, we present the MA-TRS scheme. In addition, the correctness and security are given in Section 5. Last but not least, we draw a conclusion in Section 6.

2. Preliminaries

In this section, we will introduce the relevant background materials that are utilized in the construction of our scheme.

2.1. Bilinear Map. Let $\mathbb{G}_1, \mathbb{G}_2$ be two multiplicative cyclic groups with the same large prime order q and P be the generator of $\mathbb{G}_1$. A bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ needs to satisfy the following three properties:

(1) *Bilinearity*. For all $a, b \in \mathbb{Z}_q$ and $P, Q \in \mathbb{G}_1$, there is $e(aP, bQ) = e(P, Q)^{ab}$

(2) *Non-degeneracy*. There is $e(P, P) \neq 1_{\mathbb{G}_2}$, where $1_{\mathbb{G}_2}$ is the identity element of the group $\mathbb{G}_2$

(3) *Computability*. There is an efficient algorithm to calculate $e(aP, bP)$ for all $a, b \in \mathbb{Z}_q$

2.2. Complexity Assumption

Definition 1. Discrete logarithm problem (DLP): for all $P, Q \in \mathbb{G}_1$, it is difficult to find $\eta \in \mathbb{Z}_q^*$ to satisfy $Q = \eta P$.

Definition 2. Computational Diffie-Hellman problem (CDHP): given P, aP, bP, it is hard to compute abP.

3. Definitions

In this section, we will formalize the definition of the system model and the security model in our scheme.

3.1. System Model. In the MA-TRS scheme, we design a smart grid network with traceable anonymous authentication mechanism based on blockchain between electricity company and users, in order to guarantee the data privacy of the users. As depicted in Figure 1, our system model is comprised of eight entities: electricity company (EC), data center (DC), smart meter (SM) in the residential area (RA), registration and authentication node (RAN), key-generation node (KGN), data processing node (DPN), blockchain network (BCN), and auditing node (AN).

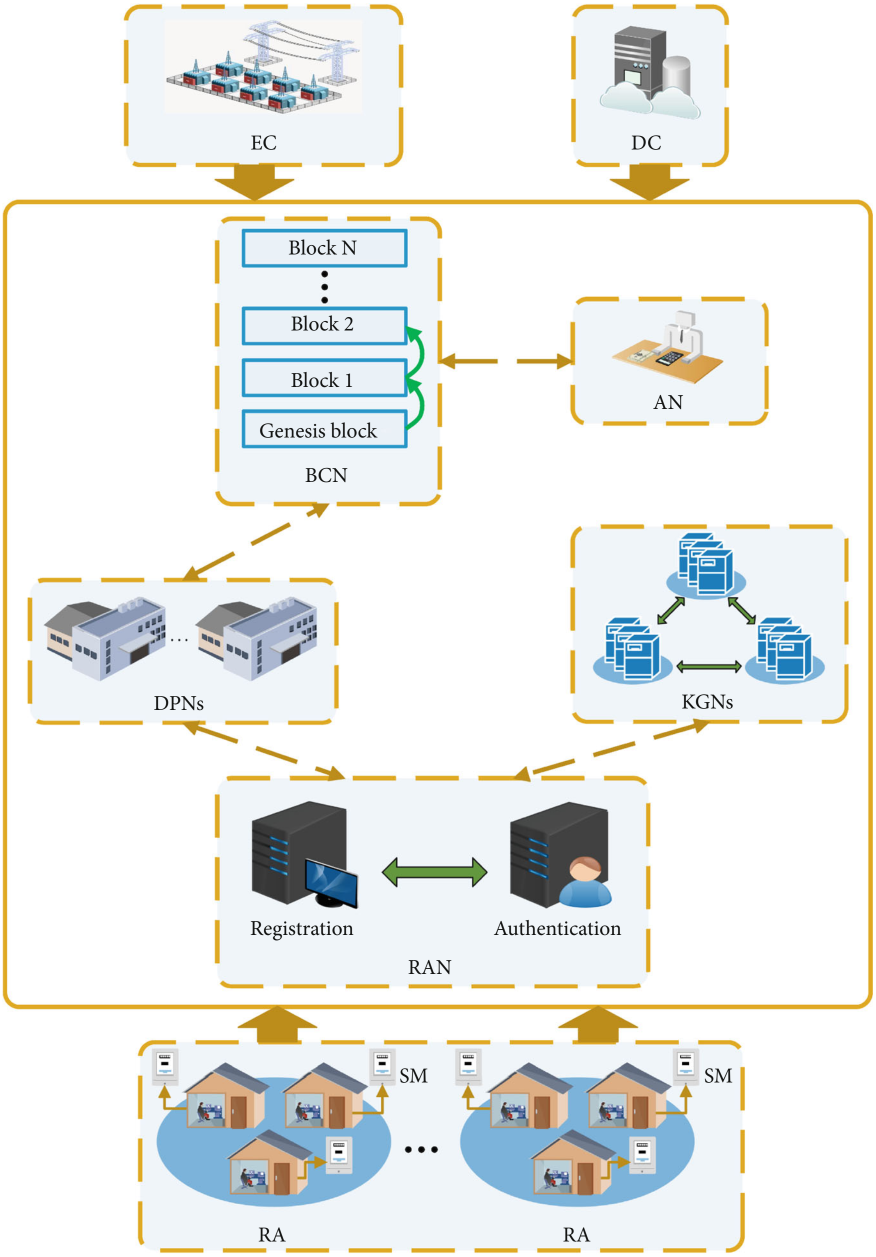

Figure 1: MA-TRS scheme in blockchain-based smart grid.

3.1.1. Electricity Company. In our scheme, the EC is connected to the smart grid network, analyzes the real-time power consumption data, and responds to the electricity demand of the electricity users for providing them with customized services.

3.1.2. Data Center. The DC is in charge of receiving and storing the data copies uploaded by the DPNs to the blockchain network and providing them to the EC or other scientific research institutions for further scientific researches.

3.1.3. Smart Meter. The SM is equipped in the electricity user's house in the residential area to collect the electricity consumption data of his/her household electrical appliance regularly and simultaneously (e.g., 15 minutes). Before uploading the power consumption data to the smart grid network, every smart grid needs to register with the RAN to obtain his/her unique identity. After that, when the electricity user logs in to the smart grid system, the RAN will authenticate the unique identity of the electricity user. Then, the user uses the identities of other users in the same residential area to form the identity set $\mathscr{L}$, generates the ring signature, and sends the power consumption data to the DNPs in the smart grid network.

3.1.4. Registration and Authentication Node. The RAN is responsible for allocating the unique identity to the electricity user who signs up for the smart grid system and authenticating the legitimacy of the user.

3.1.5. Key-Generation Node. The KGNs jointly generate their own key shares when the system is initialized. The electricity user needs to obtain at least t key shares from n KGNs to generate his/her private key.

3.1.6. Data Processing Node. The DPN parses the uploaded power consumption data and packages it to generate the blocks as well as storing the data copy to the DC. Especially, in our scheme, the DPN still records some other operations into the block, such as reading and storage. Because of the strict supervision of every operation via blocks, all kinds of operations of every node can be traced and the interaction of data can be protected, which makes our scheme distinct from the traditional smart grid schemes.

3.1.7. Blockchain Network. The BCN stores the event blocks that the DPNs process, which can achieve the function of data tamper resistance.

3.1.8. Auditing Node. When the electricity consumption data of the electricity user is inconsistent with that of the blockchain network, the AN intervenes to trace the real signer, which makes the data traceable.

3.2. Security Model. The security model of our proposed scheme should meet these three security requirements: unforgeability, anonymity, and traceability.

(1) *Unforgeability*. Unforgeability means that no one can generate a valid ring signature for the identity set $\mathscr{L}$ unless he/she has one of the private keys corresponding to $\mathscr{L}$

(i) *System Setup*. Challenger $\mathscr{C}$ runs the system setup algorithm to produce the system public parameters params and master key shares $sk_1, sk_2, \cdots, sk_n$ for KGNs whose identities are $\text{aid}_1, \text{aid}_2, \cdots, \text{aid}_n$, respectively, then $\mathscr{C}$ returns params to adversary $\mathscr{A}$ who possesses all of the public keys of users but not any private key

(ii) *Queries*. $\mathscr{A}$ can make the following four kinds of queries to $\mathscr{C}$:

(a) *Hash Query*. $\mathscr{A}$ chooses any value, and $\mathscr{C}$ returns him/her the corresponding hash value

(b) *Master Secret Key Query*. $\mathscr{A}$ initiates a request for some KGNs aid_i for their master key shares. For such a query, $\mathscr{C}$ transmits sk_i to $\mathscr{A}$

(c) *Key Generation Query*. Upon receiving an identity of a user uid_i, $\mathscr{C}$ then returns the relevant secret key C_i to $\mathscr{A}$

(d) *Ring Signature Query*. $\mathscr{A}$ chooses and submits the message m and the identity set of users in the same residential area $\mathscr{L}$. After that, $\mathscr{C}$ returns the relevant ring signature σ to $\mathscr{A}$

(iii) *Forgery*. At last, $\mathscr{A}$ outputs the signature σ^* of another message m^* and the identity set of users in the same residential area $\mathscr{L}$ that satisfy the following three conditions:

(a) σ^* is a valid signature produced by $\mathscr{A}$

(b) $(m^*, \mathscr{L}^*)$ does not appear in the phase of ring signature query

(c) $\mathscr{A}$ never inquiries the private key of the members of $\mathscr{L}^*$

(2) *Anonymity*. Anonymity means that given a signature, no one can determine the real signer unless all of the ring members (the users in the same residential area as the signer) launch collusion attacks

(i) *System Setup*. Challenger $\mathscr{C}$ executes the system setup algorithm to compute the system public parameters params and returns it to adversary $\mathscr{A}$

(ii) *Queries*. $\mathscr{A}$ adaptively executes polynomial times ring signature queries

(iii) *Challenge*. In the phase of challenge, $\mathscr{A}$ outputs a message m, the identity set $\mathscr{L}$ of ℓ users, two different public key $Y_1, Y_2 \in \mathscr{L}$, and transmits them to $\mathscr{C}$. $\mathscr{C}$ randomly chooses a bit $y \in \{0, 1\}$ and runs the signature generation algorithm with the real signer uid_y, then returns σ to $\mathscr{A}$

(iv) *Queries*. $\mathscr{A}$ adaptively executes polynomial times ring signature queries

(v) *Challenge*. Finally, $\mathscr{A}$ outputs a bit $y' \in \{0, 1\}$. $\mathscr{A}$ will succeed if and only if $y = y'$.

(3) *Traceability*. Different from the ring signature schemes [31], whose anonymity cannot be revoked, the property of the anonymity of TRS schemes is conditional. The property of traceability of TRS schemes means that for any valid ring signature, there exists someone who can determine the real signer from the ring (all users in the same residential area including the signer)

Definition 3. The MA-TRS scheme is unforgeable for any $\mathscr{A}$, because the advantage of him/her is negligible.

Definition 4. The advantage of any polynomial time adversary $\mathscr{A}$ is defined as $\text{Adv} = |\Pr[y = y'] - 1/2|$. We say that an MA-TRS scheme is anonymous if the advantage of $\mathscr{A}$ is negligible.

4. Multiauthority Traceable Ring Signature Scheme

In this section, we construct a multi-authority traceable ring signature (MA-TRS) scheme for smart grid based on blockchain, which is mainly comprised of the following five parts: system setup, user registration, user report generation, data storage, and user data tracing.

4.1. System Setup. The system setup phase is divided into two subprocesses: system initialization and key-generation nodes initialization.

(1) System initialization is responsible for generating all system public parameters by the DPNs

(a) The DPNs select two multiplicative cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ with the same large prime order q and define a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Let P be the generator of $\mathbb{G}_1$

(b) The DPNs choose two hash functions: $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$

(c) According to the whole number n of KGNs, the DPNs decide the threshold value t of KGNs that participate in the generation of user's secret key

(d) The DPNs publish the system public parameters $\text{params} = \{q, P, e, \mathbb{G}_1, \mathbb{G}_2, H_1, H_2, t, n\}$

(2) During key-generation nodes initialization subprocess, all the KGNs cooperate with each other to generate their own master key shares

(a) Each KGN $\text{aid}_i \in \mathbb{Z}_q^*$ chooses randomly a polynomial $f_i(z) \in \mathbb{Z}_q^*$ of degree $t-1$

$$f_i(z) = f_{i0} + f_{i1}z + \cdots + f_{i(t-1)}z^{t-1}, \tag{1}$$

where $f_i(0) = f_{i0} = s_i$.

(b) KGN aid_i calculates $F_{ik} = f_{ik}P$ for $k = 1, 2, \cdots, t-1$, then broadcasts F_{ik}

(c) KGN aid_i computes the subshare $s_{ij} = f_i(\text{aid}_j)$ for every other KGN aid_j for $j = 1, 2, \cdots, i-1, i+1, n$ and sends s_{ij} to KGN aid_j via secure channel. Simultaneously, KGN aid_i computes and keeps $s_{ii} = f_i(\text{aid}_i)$ for himself/herself

(d) Upon receiving the sub-share $s_{ji}(j = 1, 2, \cdots, i-1, i+1, \cdots, n)$ from all other $n-1$ KGN aid_j for $j = 1, 2, \cdots, i-1, i+1, n$, KGN aid_i verifies whether the equation $s_{ji}P = \sum_{k=0}^{t-1} F_{jk}\text{aid}_i^k$ holds. If it holds, the sub-share from KGN aid_j is valid. Otherwise, KGN aid_i broadcasts a complaint against KGN aid_j. Then, KGN aid_j is obliged to retransmit value s_{ji} that satisfies the equation so as to pass the verification

(e) After finishing the above interactions, KGN aid_i calculates its own master key share $sk_i = \sum_{j=1}^{n} s_{ji}$ and computes its corresponding public key share $pk_i = sk_iP$. Note that the master secret key s can be recovered by at least t out of n master key shares sk_i

(f) For the purpose of computing the master public key, any one of the KGNs can select at random t out of n KGNs' public key shares. Suppose Ω is the set of qualified KGNs to generate master keys. Therefore, it calculates the master public key as

$$P_{\text{pub}} = sP = \sum_{i \in \Omega} \left(\prod_{j \in \Omega, j \neq i} \frac{\text{aid}_j}{\text{aid}_j - \text{aid}_i} \right) pk_i. \tag{2}$$

(g) All the KGNs append P_{pub} and their own $\{\text{aid}_i, pk_i\}_{i=1}^{n}$ to params as $\text{params} = \{q, P, e, \mathbb{G}_1, \mathbb{G}_2, H_1, H_2, t, n, P_{\text{pub}}, \{\text{aid}_i, pk_i\}_{i=1}^{n}\}$

4.2. User Registration. If the electricity user intends to join the smart grid, he/she is supposed to submit the registration information to the RAN. Then, the RAN will assign him/her a unique identity. After that, the electricity user needs to interact with at least t out of n KGNs to generate his/her private key. In other words, when there are less than t KGNs, the user cannot generate his/her own private key. There do not exist any two of t KGNs interacting with each other in this phase. Consequently, the user can choose any t KGNs according to his/her preference. After the interaction with KGNs, the user computes his/her own private key with the secret key shares from t KGNs.

(1) Each user initiates a registration request to the RAN. Subsequently, the RAN allocates him/her a unique identity $\text{uid}_i \in \mathbb{Z}_q^*$. Next, the DPNs calculate and publish $B_i = H_1(\text{uid}_i)$.

(2) Every KGN aid_j computes $psk_{ij} = sk_iB_i$ and transmits it to user uid_i securely

(3) When receiving the secret key share psk_{ij} from KGN aid_j, user uid_i verifies whether the equation $e(psk_{ij}, P) = e(B_i, pk_j)$ holds. If it holds, the secret key share is valid. Conversely, the user discards the invalid secret key share and KGN aid_j has to resend the value that satisfies the equation

(4) When collecting t secret key shares, user uid_i can generate his/her secret key as follows:

$$C_i = sH_1(\text{uid}_i) = \sum_{j\in\Omega}\left(\prod_{k\in\Omega,k\neq j}\frac{\text{aid}_k}{\text{aid}_k - \text{aid}_j}\right)psk_{ij}. \tag{3}$$

(5) Every user selects a random number $x_i \in \mathbb{Z}_q^*$, then calculates $X_i = x_i C_i$ and $Y_i = x_i(P + B_i)$. After that, the user keeps (x_i, C_i) as his/her private key and regards (Y_i, uid_i) as his/her public key. At last, the user broadcasts (Y_i, uid_i).

4.3. User Report Generation. In this phase, every electricity user utilizes the SM to collect power consumption data $m \in \{0, 1\}^*$, generates ring signature of it, and sends the data to the smart grid network regularly, e.g., every 15 minutes. Let $\mathcal{L} = \{\text{uid}_1, \text{uid}_2, \cdots, \text{uid}_\ell\}$ be the identity set of all ℓ users in the same residential area. Assume that the real signer, indexed by $\mathcal{S}$, keeps $(Y_\mathcal{S}, \text{uid}_\mathcal{S})$ as his/her public key and $(x_\mathcal{S}, C_\mathcal{S})$ as his/her private key, where $Y_\mathcal{S} = x_\mathcal{S}(P + B_\mathcal{S})$.

(1) Signer chooses $r_i, u_i \in \mathbb{Z}_q^*$, respectively, and calculates the following equations:

$$U_i = u_i P(i = 1, 2, \cdots, \ell, i \neq \mathcal{S}), \tag{4}$$

$$R_i = r_i(P + B_i)(i = 1, 2, \cdots, \ell), \tag{5}$$

$$R_i' = r_i Y_i(i = 1, 2, \cdots, \ell), \tag{6}$$

$$R = x_\mathcal{S}\sum_{i=1}^{\ell} R_i, \tag{7}$$

$$h_i = H_2(m\|U_i\|R\|\mathcal{L})(i = 1, 2, \cdots, \ell, i \neq \mathcal{S}). \tag{8}$$

(2) Signer selects a random $u_\mathcal{S} \in \mathbb{Z}_q^*$ and computes:

$$U_\mathcal{S} = u_\mathcal{S} B_\mathcal{S} - \sum_{i=1, i\neq\mathcal{S}}^{\ell}(U_i + h_i Y_i), \tag{9}$$

where $U_\mathcal{S} \neq U_i$. If $U_\mathcal{S} = U_i$, $u_\mathcal{S}$ needs to be reselected.

$$h_\mathcal{S} = H_2(m\|U_\mathcal{S}\|R\|\mathcal{L}), \tag{10}$$

$$D = h_\mathcal{S} x_\mathcal{S} P_{pub} + h_\mathcal{S} X_\mathcal{S} + u_\mathcal{S} C_\mathcal{S}. \tag{11}$$

(3) The ring signature of power consumption data m signed by signer $\mathcal{S}$ outputs as

$$\sigma = \left(m, U_1, U_2, \cdots, U_\ell, R_1', R_2', \cdots, R_\ell', R, D, \mathcal{L}\right). \tag{12}$$

(4) The user reports the signed electricity data $m\|\sigma\|T$ to the DPN, where T is the current time stamp

4.4. Data Storage. Any one of the DPNs can serve as the verifier who verifies the validity of the signature σ of power consumption data m.

(1) After receiving the signed electricity data, the DPN computes the following equation if $|T' - T| \leq \Delta T$:

$$h_i = H_2(m\|U_i\|R\|\mathcal{L})\ (i = 1, 2, \cdots, \ell), \tag{13}$$

where T' is the current time stamp, and ΔT is a predefined time threshold value.

(2) The DPN checks the validity of the signature by examining whether

$$e\left(P_{\text{pub}}, \sum_{i=1}^{\ell}(U_i + h_i Y_i)\right) = e(P, D), \tag{14}$$

holds. If it holds, accept the signature. Otherwise, reject it.

(3) The DPN packages the signed electricity data into block and broadcasts it to other DNPs. After most DNPs verify and accept the block, the DPN uploads it into the blockchain network. At the same time, the DPN sends the data copies to the DC for further scientific researches. Besides, the DPN will also record the operation of uploading data in the blockchain, which makes every operation traceable and data interaction protected

4.5. User Data Tracing. When the user finds that the electricity consumption data is inconsistent with that stored in the blockchain network, he/she can initiate an audit request. Then, the AN intervenes to solve it. During this process, the AN only needs to interact with all the users in the same residential area once to trace the real signer $\mathcal{S}$. What the AN executes is as follows.

(1) The AN firstly parses the operation recorded in the blockchain to trace which operation of the data inconsistency

(2) In accordance with R_i' and the set of identities of the electricity users in the same residential area $\mathcal{L}$ in ring signature σ, the AN collects the value of R_i from the relevant user uid$_i$in the same residential area by calculating $R_i = R_i' x_i^{-1}$

(3) After finishing the collection of all of the R_i, the AN needs to verify the validity of R_i one by one through checking whether the equation $e(R_i', P + B_i) = e(R_i, Y_i)$ holds. On condition that all R_i are true, the AN computes $W = \sum_{i=1}^{\ell} R_i$. After that, the real signer $\mathcal{S}$ can be determined by $e(R, P + B_i) = e(W, Y_i)$

(4) The AN will solve this problem of data inconsistency according to the tracking results

5. Correctness and Security

This section proves the correctness and security of our proposed scheme.

5.1. Correctness

Theorem 5. *If $e(P_{pub}, \sum_{i=1}^{\ell}(U_i + h_i Y_i)) = e(P, D)$, the signature of the power consumption data is valid.*

Proof.

$$\begin{aligned} e\left(P_{\text{pub}}, \sum_{i=1}^{\ell}(U_i + h_i Y_i)\right) &= e\left(sP, U_{\mathcal{S}} + h_{\mathcal{S}} Y_{\mathcal{S}} + \sum_{i=1, i \neq \mathcal{S}}^{\ell} (U_i + h_i Y_i)\right) \\ &= e\left(sP, u_{\mathcal{S}} B_{\mathcal{S}} - \sum_{i=1, i \neq \mathcal{S}}^{\ell} (U_i + h_i Y_i)\right. \\ &\quad \left. + \sum_{i=1, i \neq \mathcal{S}}^{\ell} (U_i + h_i Y_i) + h_{\mathcal{S}} Y_{\mathcal{S}}\right) \\ &= e(P, s(u_{\mathcal{S}} B_{\mathcal{S}} + h_{\mathcal{S}} Y_{\mathcal{S}})) \\ &= e(P, u_{\mathcal{S}} C_{\mathcal{S}} + s h_{\mathcal{S}} x_{\mathcal{S}} (P + B_{\mathcal{S}})) \\ &= e\left(P, u_{\mathcal{S}} C_{\mathcal{S}} + h_{\mathcal{S}} x_{\mathcal{S}} P_{pub} + h_{\mathcal{S}} X_{\mathcal{S}}\right) \\ &= e(P, D). \end{aligned} \tag{15}$$

Theorem 6. *If $e(R_i', P + B_i) = e(R_i, Y_i)$ and $e(R, P + B_i) = e(W, Y_i)$, the user data can be traced correctly.*

Proof.

$$\begin{gathered} e\left(R_i', P + B_i\right) = e(r_i Y_i, P + B_i) = e(r_i x_i (P + B_i), P + B_i) = e(r_i (P + B_i), x_i (P + B_i)) = e(R_i, Y_i) \\ e(R, P + B_i) = e\left(x_i \sum_{i=1}^{\ell} R_i, P + B_i\right) = e\left(\sum_{i=1}^{\ell} R_i, x_i (P + B_i)\right) = e(W, Y_i). \end{gathered} \tag{16}$$

5.2. Unforgeability

Theorem 7. *The proposed MA-TRS scheme is unforgeable.*

Proof. Because the master secret key s is jointly generated by at least t key-generation nodes and the private key of the user is produced after interacting with at least t key-generation nodes, it is infeasible for anyone who does not belong to the signature ring to obtain the part of the private key C_i of the user. Additionally, another part of user's private key x_i cannot be computed by $Y_i = x_i(P + B_i)$ due to DLP. Namely, it is difficult to forge any valid private key of the ring members. The values U_i, R_i, R_i' of one signature can be produced by anyone. However, the calculation of the values R, D requires at least one of the private keys of the ring members. According to the security model of unforgeability, the adversary cannot obtain any private key of the ring. And it is impossible to compute D by U_i, h_i owing to CDHP. Therefore, it is impossible for anyone who is not a member of the ring to forge a valid signature.

5.3. Anonymity

Theorem 8. *The ring signature is anonymity of the signer in our proposed MA-TRS scheme.*

Proof. The values of r_i, u_i are chosen at random from $\mathbb{Z}_q^*$, so the values of U_i, R_i, R_i' are evenly distributed in the group $\mathbb{G}_1$, and the same is the value of h_i. In addition, the value $u_{\mathcal{S}}$ is selected randomly by the real signer, and the value $U_{\mathcal{S}}$ computed by $U_{\mathcal{S}} = u_{\mathcal{S}} B_{\mathcal{S}} - \sum_{i=1, i \neq \mathcal{S}}^{\ell} (U_i + h_i Y_i)$ is evenly distributed. Therefore, the values R and D will not reveal the information of the signer. In another word, it is computationally distinguishable unless all the ring members cooperate to compute. So, it is anonymous for the signer in our MA-TRS scheme.

5.4. Traceability

Theorem 9. *The proposed MA-TRS scheme can trace the real signer if necessary.*

Proof. When the user or the electricity company finds the power consumption data is different from the data stored in the blockchain network, the auditing node will execute the tracing program to trace the real signer. The auditing node can obtain the value of R_i after interacting with every user in the same residential area. After collecting ℓR_i, the auditing node verifies their validity, then traces the real signer by the public parameters. In the whole process of tracing, it is impossible for any member to leak his/her private key. That means the auditing node possesses nothing concerning the secret but the published information. Only the ring member who satisfies the equation $e(R, P + B_i) = e(W, Y_i)$ is the real signer. Hence, the proposed MA-TRS scheme is traceable.

6. Conclusion

In this paper, we propose a multi-authority traceable ring signature scheme for smart grid based on blockchain, combining ring signature scheme and blockchain technology. In addition, our scheme takes advantage of distributed key generation technology to address the problem of key escrow. A responsible user can generate his/her secret key by interacting with t out of n key-generation nodes, and no one knows the master secret key. When the power consumption data of the user is inconsistent with that of the blockchain network, the auditing node can trace the real signer and solve this data inconsistency, which makes our scheme different from other smart grid schemes. Compared with other ring signature schemes, our scheme has the properties of unforgeability, anonymity, and traceability. At last, we discuss the security proof of our scheme.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (No. 61702067), and in part by the Natural Science Foundation of Chongqing (No. cstc2020jcyj-msxmX0343).

References

[1] S. Bera, S. Misra, and J. J. P. C. Rodrigues, "Cloud computing applications for smart grid: a survey," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1477–1494, 2015.

[2] H. Liang, B. Choi, W. Zhuang, and X. Shen, "Towards optimal energy store-carry-and-deliver for PHEVs via V2G system," in *2012 Proceedings IEEE INFOCOM*, pp. 25–30, Orlando, FL, USA, 2012.

[3] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *Journal of Internet Technology*, vol. 16, no. 1, pp. 171–178, 2015.

[4] H. Shen, M. Zhang, and J. Shen, "Efficient privacy-preserving cube-data aggregation scheme for smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1369–1381, 2017.

[5] Y. Ming, X. Zhang, and X. Shen, "Efficient privacy-preserving multi-dimensional data aggregation scheme in smart grid," *IEEE Access*, vol. 7, pp. 32907–32921, 2019.

[6] F. Rahimi and A. Ipakchi, "Demand response as a market resource under the smart grid paradigm," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 82–88, 2010.

[7] R. Anderson and S. Fuloria, "Who controls the off switch," in *2010 First IEEE International Conference on Smart Grid Communications*, pp. 96–101, Gaithersburg, MD, USA, 2010.

[8] S. Finster and I. Baumgart, "Privacy-aware smart metering: a survey," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 2, pp. 1732–1745, 2015.

[9] M. R. Asghar, G. Dan, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: a survey," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, pp. 2820–2835, 2017.

[10] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BN Publishing, New York City, NY, USA, 2008.

[11] S. Anwar, V. K. Shukla, S. S. Rao, B. K. Sharma, and P. Sharma, "Framework for financial auditing process through blockchain technology, using identity based cryptography," in *2019 Sixth HCT Information Technology Trends (ITT)*, pp. 99–103, Ras Al Khaimah, United Arab Emirates, 2019.

[12] N. A. Popova and N. G. Butakova, "Research of a possibility of using blockchain technology without tokens to protect banking transactions," in *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 1764–1768, Saint Petersburg and Moscow, Russia, 2019.

[13] J. D. Harris and B. Waggoner, "Decentralized and collaborative AI on blockchain," *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 368–375, Atlanta, GA, USA, 2019.

[14] N. B. Somy, K. Kannan, V. Arya et al., "Ownership preserving AI market places using blockchain," in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 156–165, Atlanta, GA, USA, 2019.

[15] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019.

[16] F. Tang, S. Ma, Y. Xiang, and C. Lin, "An efficient authentication scheme for blockchain-based electronic health records," *IEEE Access*, vol. 7, pp. 41678–41689, 2019.

[17] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: a distributed and trusted authentication system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, 2020.

[18] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, 2018.

[19] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3602–3609, 2019.

[20] Z. Guan, G. Si, X. Zhang et al., "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[21] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology — ASIACRYPT 2001. ASIACRYPT 2001*, C. Boyd, Ed., vol. 2248 of Lecture Notes in Computer Science, pp. 552–565, Springer, Berlin, Heidelberg, 2001.

[22] D. Chaum and V. Eugene, "Group signatures," in *Advances in Cryptology-EUROCRYPT '91*, pp. 257–265, Springer, Berlin, Heidelberg, 1991.

[23] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology. CRYPTO 1984*, G. R. Blakley and D. Chaum, Eds., vol. 196 of Lecture Notes in Computer Science, pp. 47–53, Springer, Berlin, Heidelberg, 1984.

[24] F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," in *Advances in Cryptology — ASIACRYPT 2002. ASIACRYPT 2002*, Y. Zheng, Ed., vol. 2501 of Lecture Notes in Computer Science, pp. 533–547, Springer, Berlin, Heidelberg, 2002.

[25] J. Chang, B. Shao, Y. Ji, M. Xu, and X. Rui, "Secure network coding from secure proof of retrievability," *Science China Information Sciences*.

[26] J. Chang, H. Wang, and F. Wang, "RKA security for identity-based signature scheme," *IEEE Access*, vol. 8, pp. 17833–17841, 2020.

[27] C. Lin and T. Wu, "An identity-based ring signature scheme from bilinear pairings," in *18th International Conference on Advanced Information Networking and Applications, 2004. AINA 2004*, pp. 182–185, Fukuoka, Japan, 2004.

[28] E. Fujisaki and K. Suzuki, "Traceable ring signature," in *Public Key Cryptography – PKC 2007. PKC 2007*, T. Okamoto and X.

Wang, Eds., vol. 4450 of Lecture Notes in Computer Science, pp. 181–200, Springer, Berlin, Heidelberg, 2007.

[29] D. Huang, X. Yang, and H. Chen, "Ring signature scheme with revocable anonymity," *Computer Engineering and Applications*, pp. 88-89, 2010.

[30] H. Yang, X. Miao, H. Zhu, and Y. Li, "Efficient certificateless ring signature scheme with identity tracing," *Information Security and Technology*, pp. 32–35, 2014.

[31] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, "A blockchain privacy protection scheme based on ring signature," *IEEE Access*, vol. 8, pp. 76765–76772, 2020.