Privacy-Preserving and Dynamic Authentication Scheme for Smart Metering

Xiuxia Tian[1,2], Fuliang Tian[1], Anqin Zhang[1], and Xi Chen[1]
(Corresponding author: Xiuxia Tian)

College of Computer Science and Technology, Shanghai University of Electric Power[1]
No. 2588 Changyang Road, Shanghai 200090, China
College of Data Science and Engineering, East China Normal University[2]
No. 3663 Zhongshan Road, Shanghai 200062, China
(Email: xxtian@fudan.edu.cn.)
(Received Aug. 28, 2017; revised and accepted Dec. 5, 2017)

Abstract

Smart grid has emerged as the next generation of power grid, as a result, the smart meter technology has developed rapidly. However, smart meter faces some critical security challenges such as insufficient authentication and user privacy disclosure. To cope with these challenging issues, a privacy-preserving and dynamic authentication scheme based on Chinese residual theorem is proposed. In the proposed scheme, the smart grid is combined with cloud computing, which solves the problem of key leakage and reduces the burden of data processing in smart grid. Specifically, the proposed scheme not only implements the smart meter authentication, but also makes it impossible for both internal and external attackers to associate the real identity of users with their real-time power. In addition, our scheme supports the dynamic update of smart meter authentication conditions. Compared with the existing schemes, the proposed scheme has higher security and lower communication overhead.

Keywords: Chinese Remainder Theorem; Identity Authentication; Privacy Protection; Smart Meter

1 Introduction

With the development of science and technology, smart grid (SG) [11] has attracted more and more attention. The structure of the SG can be divided into three layers [13]: Power Company (PC), Regional Manager (RM) and Smart Meter (SM). The SM is a power-collecting device with user identity information, which can send the real-time power of the user to the RM and PC. The PC completes power generation planning and remote control operations by analyzing the user's electricity information, and achieve the rational use of resources.

SM has been adopted by more and more countries and regions, but the development of this technology is also has its problems, especially in the sender authentication and user privacy protection [6, 14–16]. According to the report [30], the existing authentication mechanism exist the problem of key exposure and insufficient authentication, the existence of these problems poses a threat to the security of communications in the smart grid. In the process of communication, the information transmitted by smart meter includes many privacy data, such as the user's identity and real-time power. When the attacker obtains these data, especially when the user's identity and real-time power can be associated, the attacker can combine the background knowledge to obtain the user's behavior habit, and makes specific attacks on users. What's more, as the number of SMs increases, calculating keys for each SM is a complex business, as will as the key management and the authentication conditions dynamic update. At the same time, when a large number of users have power requirements, the communication overhead of SMs is also a great challenge.

Fortunately, recent researches [4, 26] shows that cloud computing has a great advantage in terms of flexibility, scalability, and cost investment, and is highly compatible with SG. so we have integrated the SG with cloud computing in the proposed scheme, and migrate master key computing and system data management to cloud computing. In this way, the ability of data calculation and key management for SG is improved, and the problem of key leakage has been solved. In order to solve the problem of SM authentication and user privacy-preserving, we propose a new authentication scheme based on Chinese Remainder Theorem (CRT), it is different from the past.

The contributions of the paper are in the following:

1) The real identity of the user is stored in the cloud computing in an encrypted form, both internal and external attackers cannot associate the real identity of users with their real-time power;

2) The authentication conditions of SMs are calculated

based on the CRT, SMs in the same region have the same authentication conditions, but the authentication process is independent of each other. So we don't have to calculate the authentication conditions for each SM individually, the number of SMs can be dynamic changes, and the authentication conditions can be dynamically updated;

3) We have combined SG with cloud computing to enhance the ability of SG data processing, and solved the problem of key leakage.

The rest of the paper is organized as follows: Related work is reviewed in Section 2. The system model is included in Section 3. The Section 4 explains the proposed scheme, which includes system initialization, smart meter authentication and update operation of authentication condition. In the Section 5, the scheme is verified, and the security and performance are analyzed. Finally, Section 6 concludes the paper.

2 Related Work

The security of information between SMs and servers is a very important issue in the SG [10, 23, 29, 31], facing many types of attacks, such as false data injection attacks [9], data integrity attacks [12], man-in-the-middle attacks [32], DoS attacks [20] and so on. Therefore, the researchers put forward a lot of proposals for SM authentication and user privacy protection.

Jeanno *et al.* [7] used blind signature [5] to generate identity vouchers, in this way, the signer does not know the specific content of the signature information, and then associates the voucher with the request information to complete the authentication of the SM. However, it needs to budget the electricity in advance and generate a large amount of vouchers, which cannot request the quantity of electricity in real time according to the load demand. Yu *et al.* [33] used ring signatures to implement SM authentication and user privacy protection, avoiding the generation of large numbers of credentials, but with greater computational complexity and communication overhead. The certificate verification scheme proposed by Lee *et al.* [17] is authenticated by using a trusted third party to issue a certificate to the SM, but cannot be achieved between the SM and PC certification.

Recently, Marmol *et al.* [22] proposed a Homomorphic encryption based solution to protect the privacy of SM, smart meters individually encrypt their requests with an encryption function that allows the energy supplier to decrypt their aggregation result with an aggregated key, no one can decrypt them individually, but it is easily broken by man-in-the-middle attacks. To address the weaknesses resulting from such attacks, Badra *et al.* [2] propose an improved privacy solution which extends the scheme of Marmol *et al.*. Chim *et al.* [8] proposed an authentication scheme by applying the Keyed-Hashing for Message Authentication Code (HMAC). In this scheme, the SM computes the HMAC of the encrypted request information to realizes the authentication and privacy protection, but PC can link the identity information of SM with its real-time power, so they can't defend against internal attacks. In addition, we can also use the zero-proof identity privacy protection schemes [21] to protect user privacy.

Li *et al.* [19] and Liu *et al.* [18] have proposed two efficient schemes for the secure communications of SMs and neighborhood gateways. Li *et al.* [19] proposed an authentication and privacy protection scheme based on Merkle hash tree [24], the real-time electricity consumption report is divided into several parts, the values of the leaf nodes of Merkle tree are the message hashes, the values of internal nodes are derived from their child nodes, finally, the root node value can be obtained. The integrity of the node information is verified by recording the values of the associated nodes, so the Merkle hash tree technique is leveraged to facilitate the authentication implementation. Liu *et al.* [18] have proposed a similar lightweight communication scheme that unlike Li *et al.*'s scheme uses the Lagrange polynomial formula for the message sender authentication, and shows better performance comparing to Li *et al.*'s scheme. But these schemes have not addressed some security requirements, so Abbasinezhad *et al.* [25] propose an extremely lightweight communication scheme that can be applied effectively for the secure bidirectional communications of the SMs and the neighborhood gateways.

Furthermore, key leakage and data processing in smart grid are also concerned by researchers. Baek *et al.* [3] designed a large information data management framework, the literature [1] presents a realistic example of deploying a cloud computing center in an SG system. Saxena *et al.* [27] propose a lightweight cloud-trusted authorities-based integrated distributed authentication protocol that provides mutual authentications among communicated entities in a distributed manner, and combined with cloud computing to achieve the key management. These are the new directions for SG development.

3 System Model

The system designed in this paper can be divided into two parts, the cloud computing part and the smart grid part, as shown in Figure 1. Cloud computing includes central cloud computing (CC) and regional cloud computing (RC), the smart grid section includes Power Company (PC), Regional Manager (RM), and Smart Meter (SM).

CC and RC complete data calculation and preservation during the initialization phase of the system, and can interact with the SG to complete the update operation and SM authentication. The SM records the user's power information and sends the real-time power information to the RM. The RM is used for SM authentication and transmits the electricity consumption report of the area to the PC in encrypted form. The PC responds to the user's electricity demand and completes the billing function.

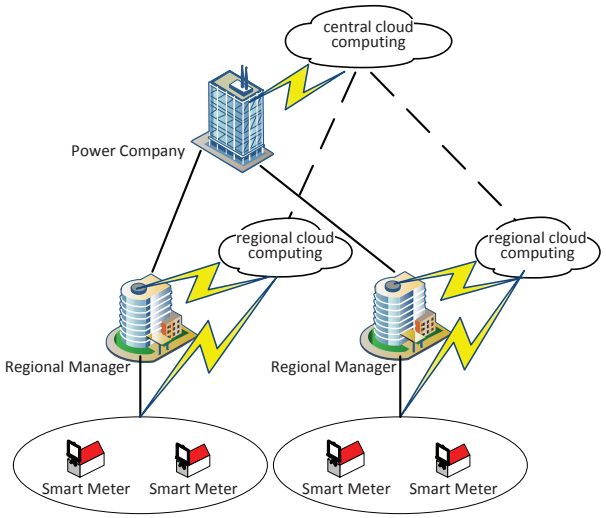

Figure 1: System model

4 Proposed Scheme

This section will introduce the principle and concrete steps of the scheme from three aspects: system initialization, SM authentication and the update operation of authentication condition.

The notations in Table 1 are used throughout this paper.

Table 1: Notations and definitions

Notation	Definition
CRT	Chinese Remainder Theorem
PC	Power Company
CC	Central cloud computing
RC	Regional cloud computing
RM	Regional Manager
SM	Smart Meter
SG	Smart grid
MPU	Main public key
MPR	Main private key
PU	Public key
PR	Private key
γ	A random number
C_r	Secret value
f()	Key calculation formula
H()	Hash function (MD5) for computing h
$E_{PU}()$	Encrypting message using PU
$D_{PR}()$	Decrypting message using PR
h	Hash value
ID	Real identity information of SM
MSG	Ciphertext information
T	time stamp
PW	SM power information
X	Solution of CRT
n_i	A prime number

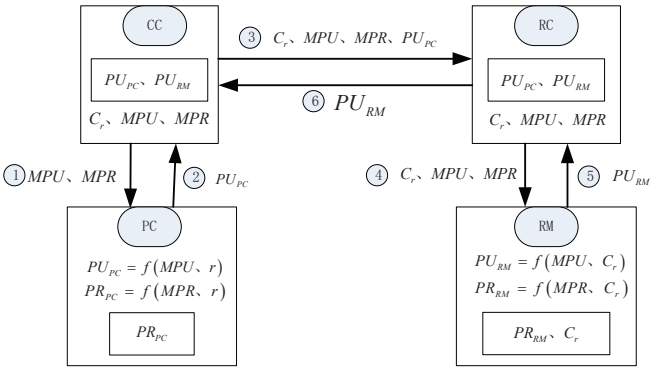

Figure 2: Keys generation and distribution

4.1 System Initialization

System initialization includes the generation and distribution of keys and the identity registration of SM. In order to reduce the overhead of SG, system initialization is completed in cloud computing.

4.1.1 Keys Generation and Distribution

Since the calculation and generation of the key has a high cost, in our scheme, the CC calculates the main public key and the main private key, PC and RM calculate their own keys according to the main public key and the main private key. In this way, the computational cost of the SG is reduced, and the private key of each part of the SG is only known by itself, avoiding the risk of key leakage, specific steps as shown in Figure 2.

Step 1. The CC generates a pair of key MPU and MPR , where MPU is the main public key, MPR is the main private key, and then CC sends MPU and MPR to the PC;

Step 2. The PC uses a random number γ and (MPU, MPR) to generate its own public key $PU_{PC} = f(MPU, \gamma)$ and private key $PR_{PC} = f(MPR, \gamma)$, and upload the public key PU_{PC} to the CC, and save the private key PR_{PC};

Step 3. CC selects different secret value C_r for each RC, and send $\{C_r, MPU, MPR, PU_{PC}\}$ to the RC;

Step 4. The RC sends $\{PU_{PC}, C_r, MPU, MPR\}$ to the RM;

Step 5. The RM uses the secret value C_r and (MPU, MPR) to compute the public key $PU_{RM} = f(MPU, C_r)$ and the private key $PR_{RM} = f(MPR, C_r)$, and uploads the public key PU_{RM} to the RC, and save the private key PR_{RM}.

4.1.2 SM Registration

The SM should register authentication information in the RC before they are used. In order to protect the real identity information of the users, we propose a new scheme for SM identity authentication based on the CRT, and use the secret value C_r as the SM authentication condition, the user's real identity is encrypted with the PC's public key, and saved in the RC.

The basic principle of CRT [28] is: If integers $m_1, m_2, \ldots, m_n$ are pairwise relatively prime, then for any integer $a_1, a_2, \ldots, a_n$, the following system of simultaneous congruence has a unique solution x.

$$\begin{cases} x \equiv a_1(modm_1) \\ x \equiv a_2(modm_2) \\ \quad\vdots \\ x \equiv a_n(modm_n) \end{cases} \tag{1}$$

The general solution can be constructed as follows. Let $M = \prod_{i=1}^{n} m_i$ be the product of integers $m_1, m_2, \ldots, m_n$, and set $M_i = M/m_i$, $M_i t_i \equiv 1(modm_i), i \in 1, 2, ..., n$, the general solution of the equations is $x = kM + \sum_{i=1}^{n} a_i t_i M_i$, in the sense of M, there is only one solution to the equations: $x = (\sum_{i=1}^{n} a_i t_i M_i) modM$.

As shown in Figure 3, the SM identity registration process is as follows:

Step 1. The RC selects a group of coprime integers $n_1, n_2, \ldots, n_i$, the number of coprime integers should be sufficient for the users to use. Then, RC uses the secret value C_r issued by the CC to obtain the only solution X according to Equation (2);

$$\begin{cases} X \equiv (C_r + n_1)(modn_1) \\ X \equiv (C_r + n_2)(modn_2) \\ \quad\vdots \\ X \equiv (C_r + n_i)(modn_i) \end{cases} \tag{2}$$

Step 2. The RC sends $\{PU_{PC}, PU_{RM}, X, n_i\}$ to the SM after passing the user's application information, in this step, the communication channel is private;

Step 3. SM encrypts the real identity information ID with the PC's public key, then return $\{E_{PU_{PC}}(ID), n_i\}$ to the RC and save (X, n_i) for identity authentication;

Step 4. The encrypted SM identity information $(E_{PU_{PC}}(ID), n_i)$ saved in RC. Where the relationship between $E_{PU_{PC}}(ID)$ and n_i is corresponding.

For example, one of the secret values chosen by CC is $C_r = -1$, CC sends the secret value to RC_1. RC_1 expects that there will be three SMs can be used, so the RC_1 selects a group of coprime integers $n_1 = 3, n_2 = 5, n_3 = 7$, and produce Equation (3) according to Equation (2).

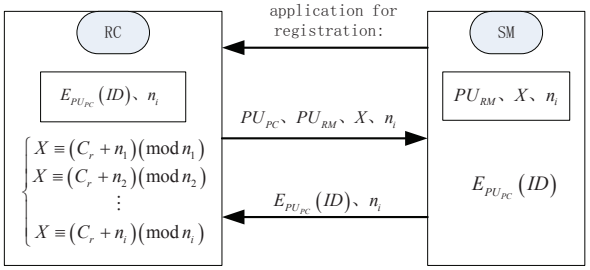

Figure 3: The registration of SM

$$\begin{cases} X \equiv 2(mod3) \\ X \equiv 4(mod5) \\ X \equiv 6(mod7) \end{cases} \tag{3}$$

RC_1 calculates X according to solving process. $M = n_1 \cdot n_2 \cdot n_3 = 105$, and $M_i = M/n_i$. t_i is a solution of an equation $M_i t_i \equiv 1(modn_i)$, so the value of M_1 and t_1 is calculated as follows:

$$\begin{aligned} M_1 &= M/n_1 = 105/3 = 35 \\ M_1 t_1 &= 1(modn_1) \\ 35 \cdot t_1 &= 1(mod3) \\ t_1 &= 2 \end{aligned}$$

In the same way, $M_2 = 21$, $t_2 = 1$, $M_3 = 15$, $t_3 = 1$. Then, the solution X for the given CRT equation is calculated by Equation (4).

$$X = (\sum_{i=1}^{n} a_i t_i M_i) modM \tag{4}$$

So $X = (2 \cdot 2 \cdot 35 + 4 \cdot 1 \cdot 21 + 6 \cdot 1 \cdot 15) mod105 = 104$.

Assume that RC_1 has passed the registration requests for SMs, RC_1 sends $\{X = 104, n_1 = 3\}$ to SM_1 as the information of authentication, and the real identity of SM_1 is saved in RC_1 as $(E_{PU_{PC}}(ID), n_i = 3)$. In the same way, RC_1 sends $\{X = 104, n_2 = 5\}$ to SM_2, and sends $\{X = 104, n_3 = 7\}$ to SM_3.

4.2 SM Authentication

With one SM as an example, we explain the identity authentication and charging process of SM, as shown in Figure 4. During this process, MD5 and Elliptic Curves Cryptography (ECC) are used as cryptographic hash function and encryption/decryption algorithm. Compared with other public key cryptosystems based on RSA, ECC achieves the same level of security strength with smaller key size and less computational cost. Therefore, ECC is more suitable for devices with limited computing resources such as smart meters.

Firstly, the SM encrypts the authentication information (X, n_i) and the electricity consumption report

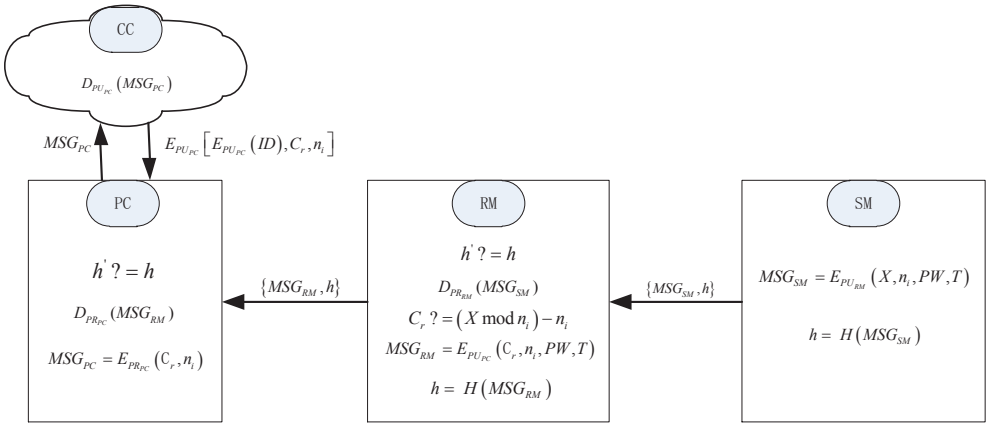

Figure 4: Authentication of SM

PW with the public key of RM to get the ciphertext $MSG_{SM} = E_{PU_{RM}}(X, n_i, PW, T)$, SM adds the timestamp T of the current system when encrypting the message to prevent replay attacks. In order to ensure the integrity of the information, SM computes $h = H(MSG_{SM})$, which is the hash value of the ciphertext MSG_{SM}. Finally, the SM sends the message $\{MSG_{SM}, h\}$ to the RM.

On receiving $\{MSG_{SM}, h\}$, the RM computes $h' = H(MSG_{SM})$ and checks if $h' = h$. If it is verified, the RM uses its private key to decrypt the ciphertext $D_{PR_{RM}}(MSG_{SM}) = (X, n_i, PW, T)$, and checks whether timestamp T is valid. If it is verified, RM computes the secret value $C'_r = (Xmodn_i) - n_i$. The RM checks if $C'_r = C_r$, here C_r is the secret value of the RC allocation. If identical, indicating that the identity of SM is legal. Then, the RM uses the public key of the PC to encrypt the relevant information of the SM and adds the timestamp T, obtain the ciphertext $MSG_{RM} = E_{PU_{PC}}(C_r, n_i, PW, T)$. Then, the RM computes $h = H(MSG_{RM})$ and sends the message $\{MSG_{RM}, h\}$ to the PC.

On receiving $\{MSG_{RM}, h\}$, the PC computes $h' = H(MSG_{RM})$ and checks if $h' = h$. If it is verified, the PC uses its private key to decrypt the ciphertext $D_{PR_{PC}}(MSG_{RM}) = (C_r, n_i, PW, T)$ and checks whether timestamp T is valid. If it is verified, the information is accepted. After a billing cycle, the PC computes the total charge of the user with the mark (C_r, n_i) and sends $MSG_{PC} = E_{PR_{PC}}(C_r, n_i)$ to the CC. The CC uses the public key of the PC to decrypt the ciphertext MSG_{PC}, and according to the secret value C_r to find out the corresponding RC, and then find out the real identity of the SM according to n_i, CC returns $\{E_{PU_{PC}}(ID), C_r, n_i\}$ to PC. After decrypting the information, the PC obtains the user's real identity and completes the billing function.

Take SM_1 as an example, SM_1 adds $(X = 104, n_1 = 3)$ to the information and sends to RM. In order to complete the authentication of SM_1, when RM receives the information from SM_1, RM calculates the secret value of SM_1 by using the following equation:

$$\begin{aligned} C'_r &= (Xmodn_1) - n_1 \\ C'_r &= (104mod3) - 3 \\ C'_r &= 2 - 3 \\ C'_r &= -1 \end{aligned}$$

The value of C'_r from the SM_1 is the same as the C_r from RC_1, it indicates that the SM_1 is legally valid.

RM adds $(C_r = -1, n_1 = 3)$ to the information and sends it to PC. after a billing cycle, PC sends $MSG_{PC} = E_{PR_{PC}}(C_r = -1, n_1 = 3)$ to the CC. The CC uses the public key of the PC to decrypt the ciphertext MSG_{PC}, and according to the secret value $C_r = -1$ to find out the RC_1, and then find out the $E_{PU_{PC}}(ID)$ of the SM_1 according to $n_1 = 3$, CC returns $\{E_{PU_{PC}}(ID), C_r = -1, n_1 = 3\}$ to PC. After decrypting the information, the PC obtains the real identity ID of SM_1 and completes the billing function.

4.3 Dynamic Update of Authentication Conditions

The security of key and authentication conditions is decreasing with time, so the key of each entity in SG and the authentication condition of SM need to be updated dynamically. In our scheme, all SMs belonging to the same RM have the same authentication conditions X and C_r, therefore, it is not necessary to calculate the authentication conditions for each SM individually. The authentication conditions can be updated uniformly, and it has an absolute advantage in the actual implementation and operation.

When updating, CC selects new secret values C'_r for each RC, the RC gets the new X' according to the Equation (5).

$$\begin{cases} X' \equiv (C'_r + n_1)(modn_1) \\ X' \equiv (C'_r + n_2)(modn_2) \\ \qquad\qquad \vdots \\ X' \equiv (C'_r + n_i)(modn_i) \end{cases} \tag{5}$$

The RC sends C'_r to the RM, and sends X' to all SMs, the SM uses X' to replace the previous X, that the dynamic update of authentication conditions has been completed.

Continue with the example above, CC selects new secret value $C'_r = -2$ for RC_1, the RC_1 gets the new X' according to the Equation (6).

$$\begin{cases} X' \equiv 1(mod3) \\ X' \equiv 3(mod5) \\ X' \equiv 5(mod7) \end{cases} \tag{6}$$

According to the solving process, $X' = (1 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 5 \cdot 1 \cdot 15) mod 105 = 103$. RC_1 sends $C'_r = -2$ to the RM, and sends $X' = 103$ to all SMs. The SM_1 uses $X' = 103$ to replace the previous $X = 104$, and sends $\{X = 103, n_1 = 3\}$ to RM, RM calculates secret value of SM_1 by using $C''_r = (X mod n_1) - n_1 = -2$, and it is the same as the secret value $C'_r = -2$ from RC_1, so SM_1 completed the authentication under the new authentication conditions.

5 Security and Performance Analysis

This section presents the security and performance analysis of our scheme in comparison with existing programs.

5.1 Security Analysis

When the messages is transmitted in the SG, it may be possible for an attacker to save them for later use. However, in the proposed scheme, the senders adds a timestamp T when sending messages and computes the hash value of ciphertext $h = H(MSG)$. When the recipient receives the message, he will check the hash value and the timestamp, only $h' = h$ and in the effective time that the message will be processed. Therefore, the proposed authentication scheme can resist the replay attack.

In the proposed scheme, The user's real identity ID is encrypted into $E_{PU_{PC}}(ID)$ and stored in the RC, the SM uses (X, n_i) for authentication. Only the PC has completed the electricity statistics, can the user's identity be queried by PC and decrypted with its private key. In the whole process of SM authentication, any participant cannot associate the real identity of SM with its real time power, so it can prevent internal and external attackers to analyze the user's behavior.

Furthermore, in the proposed scheme, the CC produces the main public key MPU and the main private key MPR, each member of the SG calculates its own public and private key based on (MPU, MPR). In this way, the private key is only known to itself, so it can avoid the problem of key exposure. In addition, the authentication conditions can be dynamic update in the proposed scheme, it is harder for attackers to get the authentication conditions.

Our scheme is compared with other schemes in security, the results are shown in Table 2. where "yes" means that it can resist the attack, "no" means that it cannot resist the type of attack.

5.2 Communication Overhead

The proposed scheme mainly considers the communication overhead between SMs and RM. Because a RM corresponds to a lot of SMs, when multiple SMs communicate with the RM at the same time, the communication overhead of the channel is an area that needs to be paid attention to. We choose to compare with the existing schemes to illustrate that the proposed scheme has more advantages in communication overhead when multiple SMs communicate with the RM at the same time.

In the Li *et al.*'s scheme [19], the communication traffic between the RM and the SM includes $\{U_i, C_j, S_j, API_j\}$, we know that the messages (U_i, C_j, S_j) are $128 \cdot 3 = 384$ bits, and the API_j is the authentication path information which includes seven 128-bit cryptographic hash values. So the total communication overhead of each SM in once communication is $128 \cdot 3 + 128 \cdot 7 = 1280$ bits.

In the Liu *et al.*'s scheme [18], the SM sends $\{ID_i, C_j, S_j\}$ and the coefficient of $f(x)$ to the RM, the messages (ID_i, C_j, S_j) are $128 \cdot 3 = 384$ bits, and the communication overhead of $f(x)$ is 128-bit. therefore, in total the communication overhead of each SM in once communication is $128 \cdot 3 + 128 = 512$ bits.

The communication overhead of Abbasinezhad *et al.*'s scheme [25] includes the messages $\{ID_i, V_j^i, M_j^i\}$ which are 128+256+256=640 bits, so the total communication overhead of each SM in once communication is 640 bits.

In the proposed scheme, SM sends information $\{MSG_{SM}, h\}$ to the RM, the encrypted information MSG_{SM} is 256 bits, and h is 128 bits. So the communication overhead of each smart meter is 256+128=384 bits. As shown in Figure 5, When the number of SMs communicating with the RM at the same time is increasing, the proposed scheme uses less resources for SM communication overhead.

5.3 Storage Cost

In the Li *et al.*'s scheme [19], the SM needs to store (r_j, C_j, API_j), where j=1,2,3,...,128, The storage space of r_j is $128 \cdot 128$ bits, the storage space of C_j is $256 \cdot 128$ bits, and the storage space of API_j, where each API_j contains seven hash values, is $128 \cdot 7 \cdot 128$ bits, so the total required storage space is 34 KB.

In the Liu *et al.*'s scheme [18], the SM needs to store (r_j, C_j, R_j), where j=1,2,3,...,96. The needed storage space for r_j is $128 \cdot 96$ bits, the storage space of C_j is $128 \cdot 96$ bits, and the storage space of R_j is $128 \cdot 96$ bits, so the total required storage space is 4.5 KB.

In Abbasinezhad *et al.*'s scheme [25], the SM needs to store E_i^{SM}, which takes 256 bits.

In our scheme, the SM only needs to store (X, n_i), which takes 64+64=128 bits. Table 3 demonstrates the storage space comparison.

Table 2: Security comparison

Scheme	Malicious user	Power company	Man in the middle	The third party	Replay attack	Data integrity attack
Chim *et al.* [8]	yes	no	yes	yes	yes	yes
Lee *et al.* [17]	no	no	yes	no	yes	yes
Li *et al.* [19]	yes	no	yes	yes	yes	no
Liu *et al.* [18]	yes	no	yes	yes	yes	no
Abbasinezhad *et al.* [25]	yes	no	yes	yes	yes	yes
Saxena *et al.* [27]	yes	no	no	yes	no	yes
Proposed Scheme	yes	yes	yes	yes	yes	yes

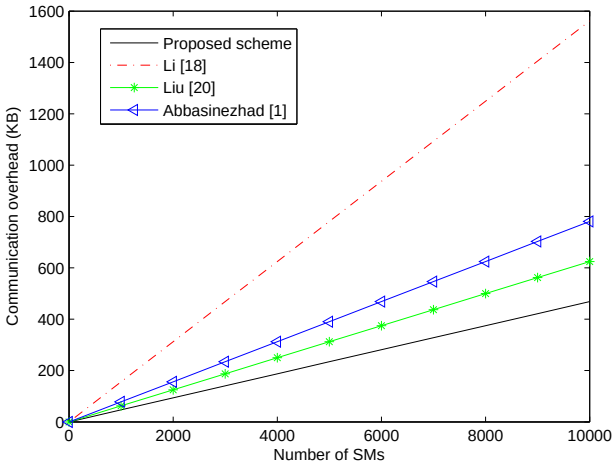

Figure 5: Comparison of communication overhead

Table 3: Storage cost

Scheme	Storage cost
Li *et al.* [19]	34 KB
Liu *et al.* [18]	4.5 KB
Abbasinezhad *et al.* [25]	256 bits
Proposed Scheme	128 bits

5.4 Computational Cost

we only consider the computation cost of a SM in each day, we divide 24 hours into small time intervals and set the length of the time interval to be 15 minutes, a SM collects the usage data with a pre-defined format during every time interval.

In the Li *et al.*'s scheme [19], a SM needs to execute 255 hash operations to construct the Merkle hash tree, 128 encryptions with two inputs for computing the C_j, 128 random generations, and 1 encryption for the root node value.

In the Liu *et al.*'s scheme [18], each SM needs to execute 96 hash operations, one decryption, 96 encryptions for the $f(x)$ coefficients, 96 random generations, and 1 polynomial generation.

In Abbasinezhad *et al.*'s scheme [25], each SM needs to perform 200 one-input hash functions and 96 random generations.

In our scheme, the calculation of authentication information of SMs is completed by cloud computing, and each SM only needs to execute 96 encryption operations and 96 hash operations.

6 Conclusion

In this paper, we have proposed a privacy-preserving and dynamic authentication scheme for smart meter, it solves the problem of smart meter authentication and user privacy-preserving, and avoids the leakage of key. What's more, the authentication conditions of smart meter are dynamic update. Detailed security analysis shows that the proposed authentication scheme can resist the internal and external attack, and has a stronger security than the existing scheme. Performance analysis demonstrates its efficiency in terms of communication overhead and storage cost.

Acknowledgments

This work was supported by NSFC Grants (No. 61772327No. 61202020No. 61532021), Project of Shanghai Science and Technology Committee Grant (No.

15110500700) and CCF-Tencent Open Fund Grant (No. IAGR20150109, RAGR20150114). We would like to express our gratitude to the anonymous reviewers for their valuable feedback and comments which helped us to improve the quality and presentation of this paper.

References

[1] B. A. Akyol, *Cyber Security Challenges in Using Cloud Computing in the Electric Utility Industry*, 2012.

[2] M. Badra and S. Zeadally, "An improved privacy solution for the smart grid," *International Journal of Network Security*, vol. 18, no. 3, pp. 529–537, 2016.

[3] J. Baek, Q. H. Vu, J. K. Liu, X. Huang and Y. Xiang, "A secure cloud computing based framework for big data information management of smart grid," *IEEE Transactions on Cloud Computing*, vol. 3, no. 2, pp. 233–244, 2015.

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

[5] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, pp. 199–203, 1983.

[6] M. Y. Chen, C. C. Yang and M. S. Hwang, "Privacy protection data access control," *International Journal of Network Security*, vol. 15, no. 6, pp. 411–419, 2013.

[7] J. C. Cheung, T. W. Chim, S. M. Yiu, V. O. Li and L. C. Hui, "Credential-based privacy-preserving power request scheme for smart grid network," in *IEEE Global Telecommunications Conference (GLOBECOM'11)*, pp. 1–5. IEEE, 2011.

[8] T. W. Chim, S. M. Yiu, L. C. Hui and V. O. Li, "Pass: Privacy-preserving authentication scheme for smart grid network," in *IEEE International Conference on Smart Grid Communications*, pp. 196–201, 2011.

[9] M. Esmalifalak, G. Shi, Z. Han and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 160–169, 2013.

[10] S. Finster, "Smart meter speed dating, short-term relationships for improved privacy in smart metering," in *IEEE International Conference on Smart Grid Communications*, pp. 426–431, 2013.

[11] C. W. Gellings, *The Smart Grid: Enabling Energy Efficiency and Demand Response*, 2009.

[12] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar and K. Poolla, "Smart grid data integrity attacks," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1244–1253, 2013.

[13] J. N. Green and R. G. Wilson, *Control and Automation of Electrical Power Distribution Systems*, vol. 28, 2006.

[14] Q. Jiang, J. Ma, G. Li and L. Yang, "Robust two-factor authentication and key agreement preserving user privacy," *International Journal of Network Security*, vol. 16, no. 3, pp. 229–240, 2014.

[15] W. S. Juang and J. L. Wu, "Efficient user authentication and key agreement with user privacy protection," *International Journal of Network Security*, vol. 7, no. 1, pp. 120–129, 2008.

[16] H. Khurana, M. Hadley, N. Lu and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, 2010.

[17] S. Lee, J. Bong, S. Shin and Y. Shin, "A security mechanism of smart grid ami network through smart device mutual authentication," in *International Conference on Information Networking (ICOIN'14)*, pp. 592–595, 2014.

[18] Y. Liu, C. Cheng, T. Gu, T. Jiang and X. Li, "A lightweight authenticated communication scheme for smart grid," *IEEE Sensors Journal*, vol. 16, no. 3, pp. 836–842, 2016.

[19] H. Li, R. Lu, L. Zhou, B. Yang and X. Shen, "An efficient merkle-tree-based authentication scheme for smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 655–663, 2014.

[20] S. Liu, X. P. Liu and A. E. Saddik, "Denial-of-service (dos) attacks on load frequency control in smart grids," in *IEEE PES on Innovative Smart Grid Technologies (ISGT'13)*, pp. 1–6, 2013.

[21] A. M. Markham, P. Shenoy, K. Fu, E. Cecchet and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, pp. 61–66, 2010.

[22] F. G. Marmol, C. Sorge, O. Ugus and G. Martínez Pérez, "Do not snoop my habits: Preserving privacy in the smart grid," *IEEE Communications Magazine*, vol. 50, no. 5, 2012.

[23] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, vol. 7, no. 3, 2009.

[24] R. C. Merkle, "Protocols for public key cryptosystems," in *IEEE Symposium on Security and Privacy*, pp. 122–122, 1980.

[25] D. A. Mood and M. Nikooghadam, "An ultra-lightweight and secure scheme for communications of smart meters and neighborhood gateways by utilization of an arm cortex-m microcontroller," *IEEE Transactions on Smart Grid*, pp. 1, 2017.

[26] S. Rusitschka, K. Eger and C. Gerdes, "Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain," in *First IEEE International Conference on Smart Grid Communications*, pp. 483–488, 2010.

[27] N. Saxena and B. J. Choi, "Integrated distributed authentication protocol for smart grid communications," *IEEE Systems Journal*, no. 99, pp. 1-12, 2016.

[28] W. Stallings and M. P. Tahiliani, *Cryptography and Network Security: Principles and Practice*, vol. 6, Pearson London, 2014.

[29] Y. Strengers, "Smart metering demand management programs: Challenging the comfort and cleanliness habitus of households," in *Proceedings of the 20th Australasian Conference on Computer-Human Interaction: Designing for Habitus and Habitat*, pp. 9–16, 2008.

[30] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[31] X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 809–818, 2011.

[32] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Yao, B. Pranggono and H.F. Wang, "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid scada systems," *International Conference on Sustainable Power Generation and Supply (SUPERGEN'12)*, 2012.

[33] C. M. Yu, C. Y. Chen, S. Y. Kuo and H. C. Chao, "Privacy-preserving power request in smart grid networks," *IEEE Systems Journal*, vol. 8, no. 2, pp. 441–449, 2014.

Biography

Xiuxia Tian received the MS degree in applied cryptography-based information security from Shanghai Jiaotong University in 2005, and the PhD degree in database security and privacy preserving in cloud computing from Fudan University in 2011. She is currently a professor in the College of Computer Science and Technology, Shanghai University of Electric Power. She is a visiting scholar of two years at UC Berkeley working with groups of SCRUB and SecML. She has published more than 40 papers and some papers are published in international conferences and journals such as DASFAA, ICWS, CLOUD, and SCN. Her main research interests include database security, privacy preserving (large data and cloud computing), applied cryptography, and secure machine learning.

Fuliang Tian Graduate. College of Computer Science and Technology in Shanghai University of Electric Power. He research interests mainly focus on the security and privacy protection for the smart meter (Email:tianflxs@163.com).

Anqin Zhang female, born in April 1974, teacher in College of Computer Science and Technology at Shanghai University of Electric Power, Ph. D., associate professor.She is a member of Chinese Computer Federation.Her main research interest is: Data Mining and social computing.

Xi Chen Graduate. College of Computer Science and Technology in Shanghai University of Electric Power.