Cryptanalysis of A Privacy-Preserving Smart Metering Scheme Using Linkable Anonymous Credential

Haipeng Qu, [*]Peng Shang, [†]Xi-Jun Lin [‡]and Lin Sun [§]

November 1, 2015

Abstract: To accomplish effective privacy protection in smart grid systems, various approaches were proposed combining information security technology with the smart grid's new features. Diao et al. proposed a privacy-preserving scheme using linkable anonymous credential based on CL signature, and demonstrated its identity anonymity, message authentication and traceability of broken smart meters. In this paper, a forgery attack is presented to point out the protocol dissatisfies message authentication and unforgeability. We hold the idea that this scheme doesn't have basic safety requirements and application value.

Key words: Smart grid; Privacy protection; Linkable anonymous credential; Message authentication; Forgery attack; Cryptanalysis

1 Introduction

With the ever-increasing demand of electric power supply, traditional centralized power generation cannot satisfy the requirement of industrial production and daily life. On the way to explore a new architecture of power grids, how to reduce costs of power generation and distribution, ease the heavy burden during peak times, and improve utilization of clean energy and information network technology has been a focus of attention among researchers. In these circumstances, the concept of smart grids emerges at a historic moment. Meanwhile the United States, the European Union and other countries have invested heavily in conducting related research and construction.

Smart grids apply two-way communication, information security technology, computer intelligence in the entire process of power transmission, distribution, and consumption. It monitors and schedules all aspects optimally to implement efficient, clean, reliable, secure power supply [11]. Compared with the traditional grids, the most important feature of smart grids is the bidirectional communication of electric power and information. On the one hand, customers can produce electricity using solar panels to offset their power consumption or just transport it back into the grid [21]. This way provides a new economic pattern and

[*] H.Qu is with the Department of Computer Sciences and Technology, Ocean University of China. Qingdao 266100, P.R.China.

[†] P.Shang is with the Department of Computer Sciences and Technology, Ocean University of China. Qingdao 266100, P.R.China.

[‡] X.J.Lin, corresponding author, is with the Department of Computer Sciences and Technology, Ocean University of China. Qingdao 266100, P.R.China. email: linxj77@163.com

[§] L. Sun is with the College of Liberal Arts, Qingdao University. Qingdao 266071, P.R.China.

mode of operation in which customers would have diverse choices. On the other hand, the smart meters collect real-time power consumption data regularly and report back to the utility for analysis and decisions. Conversely, the utility could send time-of-use power price, control commands to users so as to implement energy management more efficiently.

Since the smart grid emerged, security and privacy issues have been widely discussed and studied among researchers. Mainly consider two types of problems listed below [9]:

System Reliability and Failure Protection: Electric power transmission involves every aspect of people's production and living, therefore reliability is the primary factor for us to concern about. How to guarantee the grid system accomplishes expected functions smoothly, diagnose failures and restore effectively needs focused research.

Information Security and Privacy Protection: (1) Fine-grained power consumption data of users are transmitted through the smart grid information system, so that adversaries could obtain these data by means of eavesdropping. And then they would analyze energy consumption and load profiles to get some knowledge of the users' life patterns and habits. (2) Malicious adversaries could compromise users' smart meters in order to tampering with related information or inject false data and control commands into the grid [15]. (3) Some authorities such as the utility are also curious about users' load profiles and privacy information. It is vitally important to minimize privacy information while implementing normal functions such as payment and auditing.

Privacy protection in smart grids is a major concern of our research. For example, Non-Intrusive Load Monitoring (NILM algorithm) proposed in [12] could extract appliances information from load profiles and thus we could infer the user's behaviors. The purpose of NILM was to predict and direct electricity patterns of users. Unauthorized entities or criminals, however, could also take advantage of this algorithm to analyze a user's life patterns and habits for the sake of profit, theft and advertisements. To accomplish effective privacy protection, various approaches were proposed combining information security technology with the smart grid's new features. A brief classification and introduction is summarized as follows.

- **Homomorphic Encryption and Data Aggregation**

  In the smart grid, data aggregation is an important operation where users' fine-grained power consumption data are collected periodically, and then total or average consumption of some area could be computed by the utility backend system to implement load monitoring and adjusting. To satisfy confidentiality of information transmission as well as aggregation property, homomorphic encryption has been widely studied and applied in the smart grid. It is a semantically secure encryption algorithm that allows algebraic computations on the ciphertext matching some operations on the plaintext. For instance,$D(E(m_1) * E(m_2)) = m_1 + m_2$ describes a simplified additive homomorphic encryption algorithm, in which $E(\cdot)$ and $D(\cdot)$ represent the encryption and the decryption functions. Common homomorphic encryption algorithms include RSA, ElGamal, Paillier Cryptosystem, etc.

  In viewing of the disadvantages of traditional data aggregation, Li et al. introduced a distributed incremental aggregation scheme, in which a balanced aggregation tree was constructed according to the network topology and aggregation tasks were completed in a bottom-up manner. The Paillier Cryptosystem was employed to realize privacy protection [16] . Furthermore, [17] proposed a homomorphic signature algorithm based on the bilinear map, and an incremental verification protocol to preserve data integrity. By means of the anomaly detection mechanism, the aggregator could identify the abnormal position within $O(\log n)$ iterations for n nodes. In addition, Erkin et al. implemented spatial and temporal aggregation with modified Paillier Cryptosystem [8] .

- **Data Perturbation**

  Jelasity et al. applied differentially private techniques to protect users' privacy where small noises were judiciously introduced to mask the load records [14, 27] . In [19] , consumption profiles were blinded with shares summing to zero so that the aggregated results were guaranteed correct while the single reading was protected. [10, 19, 24, 25] implemented data perturbation in terms of load profiles, namely, a rechargeable battery was introduced to level and offset the energy consumption by charging or discharging. In practical application, this method sometimes could not achieve good results in peak times, meanwhile required high efficiency for charge and discharge rate.

- **Secure Multi-Party Computation**

  Secure multi-party computation provides a framework for authorized entities to complete joint functions without revealing their own secret inputs. Danezis et al. proposed an aggregation protocol via secret-sharing, in which the power consumption data were corporately computed by a storage service and some authorized entities that possessed a share of the consumption data. This scheme supported not only linear functions but also some complicated processing such as boolean circuits and binary operations. Nevertheless, multiple entities increased system complexity. And key management, storage and communication overhead should be carefully considered about [5]. Thoma et al. concluded by their surveys that most of the current privacy-preserving works did not involve real-time energy management, and designed a secure multi-party computation based system to implement load management and verifiable billing without loss of privacy. The key of this scheme was the Demand Management Algorithm, in which secure summation based on the Paillier Cryptosystem and secure comparison derived from Yao's millionaire example were utilized to protect fine-grained energy consumption [22] .

- **Zero-knowledge Proof**

  Jawurek et al. proposed a smart metering billing protocol depending on a zero-knowledge proof based on Pedersen Commitments. Distinct from the traditional electricity calculations, a plug-in privacy component was introduced to intercept fine-grained load profiles from the smart meter, complete billing calculations, and submit proofs to the utility [13] . An improved scheme was presented in [1] to implement in-network data aggregation and verifiable billing without a third party. It took full advantage of the aggregation operations to convey proof information. The deficiency of these schemes related to zero-knowledge proof is considerable computational overhead that introduces into the grid systems.

- **Data Anonymization**

  Efthymiou et al. divided electric data into high-frequency and low-frequency metering data, marked with anonymous HFID and attributable LFID. The anonymity of the scheme depended heavily on the third party escrow service, namely, only the authorized third party knew the mapping relation between a valid HFID and LFID [7] . Cheung et al. proposed a credential-based privacy-preserving scheme based on blind signature. The control center blindly signed the credentials generated by the customer and verified the valid customers with anonymous credentials in the power request phase. To complete verifiable billing, however, a traditional kWh meter was introduced and increased deployment cost [4] . In addition, schemes using group signature and ring signature were presented in [23, 26] to implement anonymous operations.

Our Contribution

Recently, Diao et al. proposed a privacy-preserving smart metering scheme using linkable anonymous credential [6] based on Camenisch-Lysyanskaya (CL) signature [2, 3]. The authors claimed that their scheme (PSMLAC) captured the following properties: anonymity, message authentication and traceability of corrupted smart meters.

In this paper, we point out that message authentication property is not captured in the PSMLAC scheme. That is, an attacker can forge the data which will be uploaded to the collector. Hence, Diao et al.'s scheme is insecure.

2 Preliminaries

2.1 Linkable Anonymous Credential System

Here, we recall the framework of the linkable anonymous credential system [3], where three types of entities are involved: users, organizations and verifiers. In such a system, a valid user can get credentials from authorised organizations and anonymously demonstrate to organizations or verifiers that he owns these credentials. One-show credentials provide such a feature that if a user presents his credential only once, the verifier knows nothing more than the fact that he possesses such a credential. If the user shows more than once, however, the verifier gets the ability to link all the credentials of the user.

More in details, a linkable anonymous credential system should satisfy the following properties.

1. *User Privacy*: If a user presents his credential only once, the verifier knows nothing more than the fact that he owns such a credential.
2. *Unforgeability*: It is computationally infeasible to forge a valid user's credential.
3. *Nontransferability*: It is forbidden to share the owner's credentials with other users.
4. *Linkability*: If the user shows his credential more than once, the verifier can link all the user's proofs and find out his identity.

2.2 System Model and Security Requirements

- **System Model**

We have investigated abundant works where different models were established and structured. Here we abstract the commonality from these models and give a general architecture of the smart grid information system as shown in Fig.1.

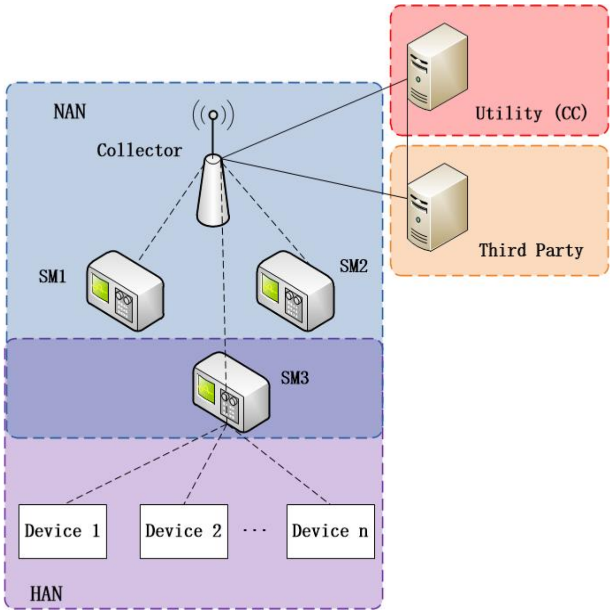

Figure 1: General System Model.

The Home Area Network (HAN): HAN consists of a smart meter (SM) and various electrical appliances such as an intelligent refrigerator. The smart meter supports two-way communication between the utility backend system and those appliances with limited storage and computation capacity. Here in this paper assume the meters are embedded with a trusted platform module (TPM), namely, computations related to the private key are executed in the TPM.

The Neighborhood Area Network(NAN): In the NAN users' smart meters communicate with a collector (C) via a wireless network. The collector acts as a bridge connecting smart meters and the utility, which verifies and transmits users' energy consumption to the utility for payment and real-time monitoring, meanwhile assigns control commands and aggregation plans from the utility to each meter.

The Utility and the Authorized Third Party: The utility represents the electricity service provider in which the data center (DC) and the control center (CC) play vitally important roles. DC completes data analysis and mining of energy consumption while CC adjusts electricity supply plans and ensures the grid system operates normally. To be simplified, the utility is typically researched as a whole. Furthermore, the third party such as PKI aims at providing authorized services for the system operations.

In the PSMLAC scheme, the grid system consists of a control center (utility), a collector and multiple smart meters. So in the next sections we mainly focus on these entities.

- **Security Requirements**

Diao et al. assume that CC and C are physically safe and semi-honest. Namely, they are assumed to follow the protocol properly while actively inferring information about others. SM installed in a user's home is vulnerable to various attacks. The security requirements are listed as follows.

1. *Identity Anonymity*: To achieve privacy protection,when a valid SM sends a message to C only once in each time interval, C can only verify that the message comes from a valid user, but doesn't know the user's identity.
2. *Message Authentication*: Messages transmitted in the grid need to be effectively authenticated to ensure they are from authorised users.
3. *Traceability of Broken SM*: A broken SM means that it would send multiple messages in some time interval. And C could locate it effectively.

3 PSMLAC Scheme

In this section, we recall the PSMLAC scheme. In their scheme, a user's power consumption data can be uploaded to C anonymously. The data is uploaded with the corresponding signature signed by the smart meter with its credentials. If the received signature is valid, C accepts the data. More in details, their scheme consists of the following six phases. Note that the *Trace* phrase is omitted here since it has nothing to do with our cryptanalysis.

- *Setup*

  1. Generate an RSA modulus $N = pq$ where $p = (2p' + 1)$, $q = (2q' + 1)$ such that p, p', q, q' are primes and N has l_n bits.
  2. Choose a cyclic group G_s, and order$(G_s) > N$.
  3. A user list UL, which is initially empty, records the information of the SM which obtains the credential.
  4. Hash functions $H_1 : \{0,1\}^* \to \{0,1\}^{k_2}, H_2 : \{0,1\}^* \to G_s$.
  5. Pick $h_i \in QR_N$ randomly, where $0 \leq i \leq 3$.
  6. k_1, k_2 are the security parameters, and their lengths ranges are $(160, l_n/8)$.
  7. The public parameters are $(N, G_s, H_1, H_2, h_i(0 \leq i \leq 3), k_1, k_2)$.
  8. An SM's public/private key pair is (h_1^x, x), where x has k_1 bits.

- *Join*

  When a new SM joins the network, it interacts with C as follows.

  1. The SM randomly chooses v' of $k_1 - 1$ bits, and sends $h_1^x, h_2^{v'}$ to C. Then the SM proves that it has x, v' by means of zero-knowledge proofs.
  2. After C verifies these proofs, it randomly chooses v'' of $k_1 - 1$ bits. Then it generates credential (A, e) that satisfies $A^e h_1^x h_2^v = h_0 \in QR_N$, where $v = v' + v''$, e is a prime number of k_1 bits. C sends v'' and (A, e) to the SM, and adds $(id, xpk_{id} = (h_1^x, h_2^v), Cred = (A, e))$ to the UL afterwards.
  3. The SM computes $v = v' + v''$ and obtains the private signing key $xsk_{id} = (A, e, x, v)$.

- *Data Upload*

  To protect the privacy of valid SM, the discrete logarithm base $H_2(T)$ is updated in every interval, where T represents a timestamp. Then the SM could upload data M to C anonymously as follows.

  1. Pick $s_0 \in \{0,1\}^{k_1}$, $r_1 \in \{0,1\}^{2k_1+k_2+1}$, $\{r_0, r_e, r_x, r_v\} \in \{0,1\}^{k_1+k_2+1}$ randomly.
  2. Compute
  $$\begin{aligned} T_0 &= h_0^{s_0} \\ T_1 &= A h_3^{s_0} \\ h_0 &= T_1^e h_1^x h_2^v h_3^{-s_1}, where\ s_1 = es_0 \\ T_2 &= H_2(T)^x \\ D_0 &= h_0^{r_0} \\ D_1 &= T_1^{r_e} h_1^{r_x} h_2^{r_v} h_3^{-r_1} \\ D_2 &= H_2(T)^{r_x} \end{aligned}$$
  3. Compute $c = H_1(M, T, T_0, T_1, T_2, D_0, D_1, D_2)$.
  4. Compute
  $$\begin{aligned} z_e &= r_e - ce \\ z_i &= r_i - cs_i, where\ i = 0, 1 \\ z_x &= r_x - cx \\ z_v &= r_v - cv \end{aligned}$$
  5. The signature is
  $\sigma = (M, T, T_0, T_1, T_2, c, z_e, z_0, z_1, z_x, z_v)$.

  The process of submitting the signature is equivalent to presenting the credential to C anonymously, which is actually a noninteractive zero-knowledge signature on M.

- *Link*

  On receiving all signatures from the SM, C checks whether T_2 of these signatures are all different. If it is the case, C performs the *Verify* algorithm; otherwise it performs the *Trace* algorithm to locate the corrupted SM.

- *Verify*

  1. For each signature, compute
  $$\begin{aligned} \tilde{D}_0 &= h_0^{z_0} T_0^c \\ \tilde{D}_1 &= T_1^{z_e} h_1^{z_x} h_2^{z_v} h_3^{-z_1} h_0^c \\ \tilde{D}_2 &= H_2(T)^{z_x} T_2^c \\ \tilde{c} &= H_1(M, T, T_0, T_1, T_2, \tilde{D}_0, \tilde{D}_1, \tilde{D}_2) \end{aligned}$$
  2. Verify whether or not $\tilde{c} = c$. If it is the case, output *Accept*; otherwise *Reject*.

  The validness of the verification is shown as follows:

$$\begin{aligned} \tilde{D}_0 &= h_0^{z_0} T_0^c \\ &= h_0^{z_0} h_0^{cs_0} \\ &= h_0^{z_0 + cs_0} \\ &= h_0^{r_0} \\ &= D_0 \end{aligned}$$

$$\begin{aligned}
\tilde{D}_1 &= T_1^{z_e} h_1^{z_x} h_2^{z_v} h_3^{-z_1} h_0^c \\
&= T_1^{z_e} h_1^{z_x} h_2^{z_v} h_3^{-z_1} * T_1^{ce} h_1^{cx} h_2^{cv} h_3^{-cs_1} \\
&= T_1^{z_e+ce} h_1^{z_x+cx} h_2^{z_v+cv} h_3^{-(z_1+cs_1)} \\
&= T_1^{r_e} h_1^{r_x} h_2^{r_v} h_3^{-r_1} \\
&= D_1
\end{aligned}$$

$$\begin{aligned}
\tilde{D}_2 &= H_2(T)^{z_x} T_2^c \\
&= H_2(T)^{z_x} H_2(T)^{cx} \\
&= H_2(T)^{z_x+cx} \\
&= H_2(T)^{r_x} \\
&= D_2
\end{aligned}$$

$$\begin{aligned}
\tilde{c} &= H_1(M, T, T_0, T_1, T_2, \tilde{D}_0, \tilde{D}_1, \tilde{D}_2) \\
&= H_1(M, T, T_0, T_1, T_2, D_0, D_1, D_2) \\
&= c
\end{aligned}$$

4 Cryptanalysis

In this section, we present our attack on the PSMLAC scheme. That is, an attacker can forge the corresponding signature of the uploaded data. More in details, in the *Data Upload* phase, an attacker can choose the data M^* which he wants to upload to C and forge its signature σ^* by performing the following steps:

1. Pick $r_0, r'_0, r_1, r'_1, r'_2, r'_3$ randomly.
2. Compute $D_0 = h_0^{r_0}$ and $T_0 = h_0^{r'_0}$.
3. Compute $D_1 = h_0^{r_1}$ and $T_1 = h_0 h_1^{r'_1} h_2^{r'_2} h_3^{r'_3}$.
4. Compute $D_2 = H_2(T)^{-r'_1 r_1}$ and $T_2 = H_2(T)^{-r'_1}$.
5. Compute $c = H_1(M^*, T, T_0, T_1, T_2, D_0, D_1, D_2)$.
6. Compute $z_0 = r_0 - r'_0 c$, $z_e = r_1 - c$, $z_x = -r'_1 z_e$, $z_v = -r'_2 z_e$, $z_1 = r'_3 z_e$.
7. Outputs the forged signature
   $\sigma^* = (M^*, T, T_0, T_1, T_2, c, z_e, z_0, z_1, z_x, z_v)$.

The validness of the forged signature is shown as follows:

$$\begin{aligned}
\tilde{D}_0 &= h_0^{z_0} T_0^c \\
&= h_0^{z_0+r'_0 c} \\
&= h_0^{r_0} \\
&= D_0
\end{aligned}$$

$$\begin{aligned}
\tilde{D}_1 &= T_1^{z_e} h_1^{z_x} h_2^{z_v} h_3^{-z_1} h_0^c \\
&= (h_0 h_1^{r'_1} h_2^{r'_2} h_3^{r'_3})^{z_e} h_1^{z_x} h_2^{z_v} h_3^{-z_1} h_0^c \\
&= (h_0^{z_e} h_1^{r'_1 z_e} h_2^{r'_2 z_e} h_3^{r'_3 z_e}) h_1^{z_x} h_2^{z_v} h_3^{-z_1} h_0^c \\
&= (h_0^{z_e} h_1^{-z_x} h_2^{-z_v} h_3^{z_1}) h_1^{z_x} h_2^{z_v} h_3^{-z_1} h_0^c \\
&= h_0^{z_e} h_0^c \\
&= h_0^{z_e+c} \\
&= h_0^{r_1} \\
&= D_1
\end{aligned}$$

$$
\begin{aligned}
\tilde{D}_2 &= H_2(T)^{z_x} T_2^c \\
&= H_2(T)^{z_x} H_2(T)^{-r_1' c} \\
&= H_2(T)^{z_x - r_1' c} \\
&= H_2(T)^{-r_1' z_e - r_1' c} \\
&= H_2(T)^{-r_1'(r_1 - c) - r_1' c} \\
&= H_2(T)^{-r_1' r_1 + r_1' c - r_1' c} \\
&= H_2(T)^{-r_1' r_1} \\
&= D_2
\end{aligned}
$$

$$
\begin{aligned}
\tilde{c} &= H_1(M^*, T, T_0, T_1, T_2, \tilde{D}_0, \tilde{D}_1, \tilde{D}_2) \\
&= H_1(M^*, T, T_0, T_1, T_2, D_0, D_1, D_2) \\
&= c
\end{aligned}
$$

Hence, the forged message/signature pair (M^*, σ^*) can make the *Verify* algorithm output *Accept*. That is, an attacker is able to inject forged data into the gird correctly. In other words, Diao et al.'s scheme does not capture the message authentication property.

5 Conclusions

In this paper, we present a forgery attack to show that the PSMLAC scheme dissatisfies unforgeability and a malicious attacker could inject false data into the gird in order to influence the normal performance of the grid system. Lin et al. also pointed out that the scheme was vulnerable to heavy computation or even denial of service [18]. In addition, the PSMLAC scheme only considered about anonymous data uploading and could not combine with verifiable billing. We conclude that this scheme doesn't have basic safety requirements and application value.

Acknowledgment

This work was supported by Chinese Ministry of Education, Humanities and Social Sciences Research Project (No. 14YJCZH136).

References

[1] Borges F, Demirel D, Bock L, et al. A Privacy-Enhancing protocol that provides In-Network data aggregation and verifiable smart meter billing[C].Computers and Communication (ISCC), 2014 IEEE Symposium on. IEEE, 2014: 1-6.

[2] Camenisch J, Lysyanskaya A. A signature scheme with efficient protocols[M].Security in communication networks. Springer Berlin Heidelberg, 2003: 268-289.

[3] Camenisch J, Lysyanskaya A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation[M].Advances in CryptologyEUROCRYPT 2001. Springer Berlin Heidelberg, 2001: 93-118.

[4] Cheung J C L, Chim T W, Yiu S M, et al. Credential-based privacy-preserving power request scheme for smart grid network[C].Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE. IEEE, 2011: 1-5.

[5] Danezis G, Fournet C, Kohlweiss M, et al. Smart meter aggregation via secret-sharing[C].Proceedings of the first ACM workshop on Smart energy grid security. ACM, 2013: 75-80.

[6] Diao F, Zhang F, Cheng X. A Privacy-Preserving Smart Metering Scheme Using Linkable Anonymous Credential[J]. Smart Grid, IEEE Transactions on, 2015, 6(1): 461-467.

[7] Efthymiou C, Kalogridis G. Smart grid privacy via anonymization of smart metering data[C].Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on. IEEE, 2010: 238-243.

[8] Erkin Z, Tsudik G. Private computation of spatial and temporal power consumption with smart meters[C].Applied Cryptography and Network Security. Springer Berlin Heidelberg, 2012: 561-577.

[9] Fang X, Misra S, Xue G, et al. Smart gridThe new and improved power grid: A survey[J]. Communications Surveys & Tutorials, IEEE, 2012, 14(4): 944-980.

[10] Ge B, Zhu W T. Preserving User Privacy in the Smart Grid by Hiding Appliance Load Characteristics[M].Cyberspace Safety and Security. Springer International Publishing, 2013: 67-80.

[11] Ghafurian R. Smart grid: The electric energy system of the future[M]. IEEE, 2011.

[12] Hart G W. Nonintrusive appliance load monitoring[J]. Proceedings of the IEEE, 1992, 80(12): 1870-1891.

[13] Jawurek M, Johns M, Kerschbaum F. Plug-in privacy for smart metering billing[C].Privacy Enhancing Technologies. Springer Berlin Heidelberg, 2011: 192-210.

[14] Jelasity M, Birman K P. Distributional differential privacy for large-scale smart metering[C].Proceedings of the 2nd ACM workshop on Information hiding and multimedia security. ACM, 2014: 141-146.

[15] Khurana H, Hadley M, Lu N, et al. Smart-grid security issues[J]. IEEE Security & Privacy, 2010 (1): 81-85.

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

[17] Li F, Luo B. Preserving data integrity for smart grid data aggregation[C].Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on. IEEE, 2012: 366-371.

[18] Lin J, Zhao X. A New Privacy-Preserving Smart Grid System[J]. 2015.

[19] McLaughlin S, McDaniel P, Aiello W. Protecting consumer privacy from electric load monitoring[C].Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011: 87-98.

[20] Shi E, Chan T H H, Rieffel E G, et al. Privacy-Preserving Aggregation of Time-Series Data[C].NDSS. 2011, 2(3): 4.

[21] Smith S W. Security and privacy challenges in the smart grid[J]. 2009.

[22] Thoma C, Cui T, Franchetti F. Secure multiparty computation based privacy preserving smart metering system[C].North American Power Symposium (NAPS), 2012. IEEE, 2012: 1-6.

[23] Wang W, Qu H, Shang P, et al. Smart Grid Payment Scheme Based on Ring Signature and Certificateless Signature[J]. 2015.

[24] Yang L, Chen X, Zhang J, et al. Optimal privacy-preserving energy management for smart meters[C].INFOCOM, 2014 Proceedings IEEE. IEEE, 2014: 513-521.

[25] Yang W, Li N, Qi Y, et al. Minimizing private data disclosures in the smart grid[C].Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012: 415-427.

[26] Zargar S H M, Yaghmaee M H. Privacy preserving via group signature in smart grid[C].Proceedings of the 1st Electric Industry Automation Congress, EIAC 2013. 2013: 1-5.

[27] Zhao J, Jung T, Wang Y, et al. Achieving differential privacy of data disclosure in the smart grid[C].INFOCOM, 2014 Proceedings IEEE. IEEE, 2014: 504-512.