Journal of Electronics and Information Science (2020) 5: 11-16
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2020.51003
ISSN 2371-9524

An efficient revocable ID-Based key insulated signature scheme to achieve authentication of smart meter

Shaomin Zhang, Zejiao Shao, Baoyi Wang

School of control and computer engineering, north China electric power university, Baoding, 071003, China

Keywords: smart meter, identity-based signature, key insulated mechanism, revocable

Abstract: In the smart grid, a large number of smart meters distributed at the edge of the network transmit electricity data to the control center through public network. Therefore, it is crucial to authenticate smart meter. Traditional authentication schemes that based on signature are usually rely on the assumption that the private key is absolutely secure, and private key exposure will endanger the security of the whole scheme. Further, most of these schemes are designed with bilinear pairings, which results in a high cost in computation and communication. So, an efficient revocable ID-based key insulated signature scheme is proposed in this paper. Computational analysis shows that our scheme has less cost than other schemes in computation and communication, which is suitable for smart meters with limited computational capability. Besides, our scheme can revoke the misbehaving or malicious smart meter conveniently and quickly.

1. Introduction

As the next generation of power grid, smart grid can provide more accurate real-time monitoring, higher reliability, more environmentally friendly energy production, and realize bidirectional communication between utility and users [1]. The smart grid brings many benefits while providing users with convenient services. For example, in the demand response phase, users can voluntarily give up part of the planned electricity consumption through rewards, thus ensuring the stability of the power grid at the peak of power consumption. Since the user's electricity data is transmitted over the public network (cellular network or the Internet), making the smart grid more vulnerable to a series of external attacks. Therefore, security becomes the premise of stable operation in smart grid [2]. Confidentiality, integrity and authentication are the three core requirements to ensure security. Authentication is usually the first step in data transmission, which ensures the authenticity of the transmitted data, that is, to confirm that the received messages are actually transmitted by smart meters that claim to do so [3]. Without authentication mechanism, malicious users who gain access to the network can inject false information or modify transmission commands and data that could disrupt the physical power system

In order to ensure the authenticity of the transmitted data, the smart meter needs to sign the transmitted data before sending it. Digital signature is an important function of cryptosystem, which can provide authentication, data integrity and non-repudiation. The security of the Public Key Cryptography (PKC) relies on the assumption that the private key is absolutely secure. In

traditional identity-based signature schemes, private key exposure will affect the security of the whole scheme. Dodis et al. [4] proposed a key insulated scheme for the first time so as to minimize the damage caused by key exposure. Their scheme divides the life time of the private key into several time periods and introduces a physically secure but computation limited device named Helper. The private key is updated every time period with the help of helper, while the public key remains the same. The exposure of the private key for a certain time period cannot derive the private key for different period, thereby ensuring the forward security and backward security of the signature [5]. The identity-based signature scheme that satisfies strong key insulated attribute has been proposed in [6][7].

In the smart grid, we should take misbehaving or malicious smart meters into consider. In the traditional PKI cryptosystem, the user can be revoked by issuing a certificate revocation list (CRL). However, using a similar approach in an identity-based cryptosystem is not an effective solution. In 2017, Jia et al. [8] proposed an efficient revocable ID-based signature scheme which points out the direction for us. In order to improve the security of whole scheme, a secure channel is used between the smart meter and the helper to transmit the updated helper key.

1.1Motivation

In order to effectively monitor and predict the state of the grid, the smart meter needs to send the electricity data to the control center in real time. Most of the existing identity-based signature schemes are designed with bilinear pairing [6][8][9]. However, the reference [10] points out that bilinear pairing operation is 2-10 times slower than the elliptic curve scalar multiplication. Due to the limited computing resources of smart meters, the use of bilinear pairings is computationally expensive and may cause system delays. Therefore, some signature schemes without bilinear pairings have become a research hotspot [7][10][11].

1.2 Our Contribution

This paper presents an efficient revocable identity-based key insulated signature scheme (RIDKIS), so as to ensure the authenticity of the electricity data received by the control center. Our contributions include the following three aspects. First, the proposed scheme reduces the damage of key exposure to the system. Secondly, we use elliptic curve scalar multiplication instead of bilinear pairing, which reduces the authentication cost and is suitable for smart meters with limited computing capability. Finally, we achieve a quick revocation of the misbehaving or malicious smart meter.

2. The Proposed RIDKIS Scheme

The RIDKIS scheme is composed of following six algorithms. The process of RIDKIS is shown in Figure 1.

a) System Initialization: Given a security parameter ℓ, PKG runs this algorithm as follows.

① PKG generates an additive cyclic group G of prime order q. Here $q \geq 2^{\ell}$ and P is the generator of G.

②PKG selects three hash functions $H_1: \{0,1\}^* \rightarrow G$, $H_2: \{0,1\}^* \times \{0,1\}^* \rightarrow G$, $H_3: \{0,1\}^* \times G \rightarrow Z_q^*$. PKG also randomly selects $s \in Z_q^*$ as system master key and $t \in Z_q^*$ as helper master key, and compute $P_{pub} = sP, P_T = tP$.

③PKG publishes the system parameter as Params=$\{G, q, P, H_1, H_2, H_3, P_{pub}, P_T\}$ and sends

t to helper via secure channel and keeps s secretly.

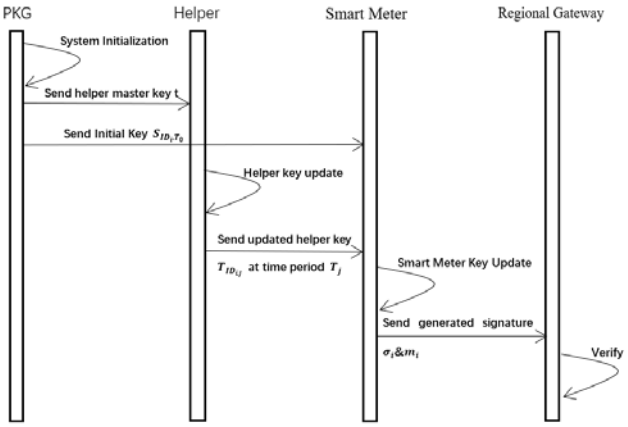

Figure. 1: The process of RIDKIS.

b) Initial Key Extract: This algorithm is run by PKG to generate an initial key for the smart meter. Given $ID_i \in \{0,1\}^*$ $(i \in [1, N])$ of the smart meter, PKG computes:

$$Q_{ID_i} = H_1(ID_i) \tag{1}$$

$$S_{ID_i,T_0} = sQ_{ID_i} + tH_2(ID_i, T_0) \tag{2}$$

Then PKG sends S_{ID_i,T_0} to smart meter.

c) Helper Key Update: This algorithm is run by helper to generate updated helper key for the smart meter. At time period T_j, PKG sends the list of smart meters to helper without revocation, and helper updates the helper key for the smart meters in the list. Helper computes:

$$Q_{ID_{i,j}} = H_2\left(ID_i, T_j\right) \tag{3}$$

$$T_{ID_{i,j}} = t\left(Q_{ID_{i,j}} - Q_{ID_{i,j-1}}\right) \tag{4}$$

Then helper sends $T_{ID_{i,j}}$ to smart meter.

d) Smart Meter Key Update: This algorithm is run by smart meter to update its signing key. At time period T_j, smart meter computes:

$$S_{ID_i,T_j} = S_{ID_i,T_{j-1}} + T_{ID_{i,j}} \tag{5}$$

Then smart meter deletes $S_{ID_i,T_{j-1}}$ and $T_{ID_{i,j}}$.

e) Signature Generation: In order to generate signature σ_i on a message m_i for identity ID_i at time period T_j, the smart meter performs as follows.

①The smart meter randomly selects $r_i \in Z_q^*$, and computes:

$$R_i = r_i P \tag{6}$$

$$h_i = H_3(ID_i, R_i, m_i, T_j) \quad (7)$$

$$V_i = S_{ID_i,T_j} + r_i h_i \quad (8)$$

②The smart meter outputs $\sigma_i = (V_i, R_i)$ as the signature.

f) Signature Verification: At the time period T_j, after receiving the signature sent by the smart meter, the regional gateway verifies the validity of the signature as follows.

①The regional gateway computes:

$$h_i = H_3(ID_i, R_i, m_i, T_j) \quad (9)$$

$$Q_{ID_i} = H_1(ID_i) \quad (10)$$

$$Q_{ID_{i,j}} = H_2(ID_i, T_j) \quad (11)$$

②The regional gateway checks whether the verification equation holds or not, and outputs "Accept" if it does, or "Reject" if not.

$$V_i P = P_{pub} Q_{ID_i} + P_T Q_{ID_{i,j}} + R_i h_i \quad (12)$$

3. Performance Evaluation

In this section, we compare the proposed scheme with the schemes in [7][8][9][11] in terms of computation cost, communication cost, and functions. In order to achieve the same security level as 1024 bits RSA, the bilinear pairing is defined over the super singular elliptic curve E/F_p : $y^2 = x^3 + x^2$ with embedding degree 2. q is a 160-bit prime number that satisfies $q = 2^{159} + 2^{17} + 1$, and P is a 512-bit prime number that satisfies $P + 1 = 12qr$. In order to effectively evaluate the performance of each scheme, the cryptographic operation results in references [7][11] are used in this paper and expressed by modular multiplication as shown in Table 1.

Table 1: Description and Conversion of Cryptographic Operations.

Symbol	Description	Conversion
T_{mm}	Modular multiplication operation	$1T_{mm}$
T_{sm}	Elliptic curve scalar multiplication	$T_{sm} = 29T_{mm}$
T_e	Modular exponentiation operation	$T_e = 240T_{mm}$
T_{pe}	Pairing based exponentiation	$T_{pe} = 43.5T_{mm}$
T_p	Bilinear pairing	$T_p = 87T_{mm}$
T_h	Simple hash function	negligible
T_{MH}	Map to point hash function	$T_{MH} = 29T_{mm}$
T_{PA}	Elliptic curve point addition	$T_{PA} = 0.12T_{mm}$
T_{INV}	Modular inversion operation	$T_{INV} = 11.6T_{mm}$

3.1 Computation Cost

In reference [7], the computation cost of generating a signature is $T_{sm} + T_{INV} + T_{PA} + T_h + T_{mm} = 41.72T_{mm}$. The computation cost of verifying a signature is $3T_h + 4T_{sm} + 3T_{PA} = 116.36T_{mm}$. Thus, the total computation cost is $158.08T_{mm}$.

In reference [8], the computation cost of generating signatures is $T_{pe} + 2T_{sm} + T_h + 2T_{PA} = 101.74T_{mm}$. In the verification phase, since two of the two bilinear pairing operations can be calculated in advance, the computation cost of verifying a signature is $2T_{pe} + T_p + T_h + 2T_{mm} = 176T_{mm}$. Thus, the total computation cost is $277.74T_{mm}$.

In reference [9], the computational cost of generating a signature is $T_e + T_{mm} + T_h = 241T_{mm}$. The computation cost of verifying a signature is $3T_p + T_{MH} + T_h = 290T_{mm}$. Thus, the total computation cost is $531T_{mm}$.

In reference [11], the computation cost of generating signatures is $T_{sm} + T_{INV} + T_h + T_{mm} = 41.6T_{mm}$. The computation cost of verifying a signature is $2T_h + 3T_{sm} + 2T_{PA} = 87.24T_{mm}$. The total computation cost is $128.84T_{mm}$.

In our scheme, the computational cost of generating a signature is $2T_{sm} + T_h + T_{PA} = 58.12T_{mm}$. Since $P_{pub}Q_{ID_i}$ and $P_TQ_{ID_{i,j}}$ can be calculated in advance, the computation cost of verifying the signature is $2T_{sm} + T_h + 2T_{PA} = 58.24T_{mm}$. Thus, the total computation cost is $116.36T_{mm}$.

The computation cost of different schemes are shown in Figure 2. We can see that the computation cost of our scheme is about 26.39% less than the reference [7], about 58.11% less than the reference [8], about 78.09% less than the reference [9], and about 9.69% less than the reference [11].

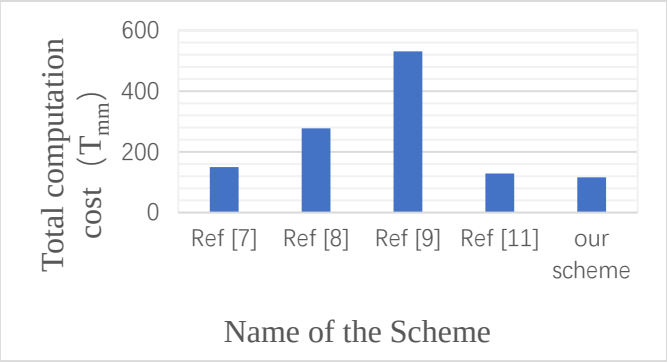

Figure. 2: Comparison of computation cost.

3.2 Communication Cost

In order to achieve the security level of 80bits in the bilinear pairing operation, given $\hat{e}: G_1 \times G_1 \to G_T$, G_1 is an additive cycle group of order $\hat{q}$, and the generator is $\hat{P}$。 $\hat{E}: y^2 = x^3 + x^2 \ mod \ \hat{P}$, $|\hat{P}| = 512\text{bits}$, $\hat{q} = 160\text{bits}$, $|G_1| = 1024\text{bits}$. In order to achieve the same security level in the elliptic curve, let G be an additive cyclic group of order q, and the generator is P. E: $y^2 = x^3 + ax + b \bmod P$, $a, b \in Z_q^*$. $|P| = 160\text{bits}$, $q = 160\text{bits}$, $|G| = 320\text{bits}$.

The signature lengths of both [7] and [11] are $2|G| + |Z_q^*|$, and the communication cost is $(320 \times 2 + 160)/8 = 100\text{byte}$. The signature length of reference [8] is $|G_1| + |Z_q^*|$, and the communication cost is $(1024 + 160)/8 = 148\text{byte}$. The signature length of reference [9] is $|G_1|$,

and the communication cost is $(1024)/8 = 128$byte. The signature length of our scheme is $2|G|$, and the communication cost is $(2 \times 320)/8 = 80$byte. It can be seen that the communication cost of our scheme is lower than that of other schemes, and is applicable to low bandwidth data links.

4. Conclusion

In order to ensure the authenticity of transmitted data send by the smart meter and reduce the damage caused by the exposure of signing key to the system, an efficient revocable identity-based key insulated scheme that can achieve authentication of smart meter is proposed in this paper. Also, scalar multiplication instead of bilinear pairing operation are adopted in the scheme, which improves the authentication efficiency effectively. Finally, the computational analysis shows that RIDKIS has less cost in computation and communication than other schemes, which is suitable for smart meters with limited computational capability.

Reference

[1] *Nikos Komninos, Eleni Philippou, Andreas Pitsillides. Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures[J]. IEEE COMMUNICATION SURVEYS & TUTORIALS, 2014, 16(4): 1933-1954.*

[2] *Amin Mohammadali, Mohammad Sayad Haghighi, Mohammad Hesam Tadayon, and Alireza Mohammadi-Nodooshan. A Novel Identity-Based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid[J]. IEEE TRANSACTIONS ON SMART GRID, 2018, 9(4): 2834- 2842.*

[3] *Liehuang Zhu, Meng Li, Zijian Zhang, et al. Privacy-preserving Authentication and Data Aggregation for Fog-based Smart Grid[J]. IEEE Communications Magazine, 2019, 1-6.*

[4] *Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, and Moti Yung. Key-Insulated Public Key Cryptosystems[J]. Proceedings of the Eurocrypt 2002. Amsterdam. 2002: 65-82.*

[5] *QIN zhiguang, LIU jingjing, ZHAO yang, et al. Research Status of Key Insulation Cryptography [J]. CHINESE JOURNAL OF COMPUTER, 2015, 38(4): 760-774(in Chinese).*

[6] *P. Vasudeva Reddy, P.V.S.S.N. Gopal. Identity-based key-insulated aggregate signature scheme[J]. Journal of King Saud University – Computer and Information Sciences, (2017), 29: 303–310.*

[7] *P. Vasudeva Reddy, A. Ramesh Babu b, Gayathri. Efficient and Secure Identity-based Strong Key-Insulated Signature Scheme without Pairings[J]. Journal of King Saud University – Computer and Information Sciences, 2018, 1-8.*

[8] *XiaoYing Jia, DeBiao He, Sherali Zeadally, Li Li. Efficient Revocable ID-Based Signature With Cloud Revocation Server[J]. IEEE Access, 2017, 5: 2945-2954.*

[9] *Zhiwei Wang. An Identity-Based Data Aggregation Protocol for the Smart Grid[J]. IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, 2017, 13(5): 2428-2435.*

[10] *Kyung-Ah Shim，Cheol-Min Park. A Secure Data Aggregation Scheme Based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks[J]. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 2015, 26(8): 2128-2139.*

[11] *Gowri Thumbur, SMIEEE, N.B. Gayathri, P. Vasudeva Reddy, et al. Efficient Pairing-Free Identity-Based ADS-B Authentication Scheme with Batch Verification[J]. IEEE Transactions on Aerospace and Electronic Systems, 2018, 1-15.*