Journal of Electronics and Information Science (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2022.070121
ISSN 2371-9524 Vol. 7 Num. 1

An Anti-Quantum Authentication and Key Agreement Scheme of Smart Meter

Baoyi Wang[a,*], Yun Sun[b] and Shaomin Zhang[c]

School of Control and Computer Engineering, North China Electric Power University, HuaDian Road, Baoding, China
a. zhangshaomin@126.com, b. sxsymail@163.com, c. wangbaoyi@126.com
**corresponding author*

Keywords: smart meter, authentication, key agreement, anti-quantum, lattice

Abstract: In order to solve the privacy leakage that may result from the two-way interaction between smart meters and smart grid as well as the quantum attack problem that may arise in the future, a quantum attack-resistant smart meter identity authentication and key agreement scheme is proposed. The scheme eliminates the overhead of certificate management through identity-based cryptography and takes advantage of the fact that the lattice-based problem cannot be solved in the quantum computer, and achieves that the scheme is resistant to quantum attacks by introducing a lattice-based cryptographic. In addition, only multiplication and addition operations of matrices and vectors are involved in this scheme.

1. Introduction

Smart grid combines advanced information, communication and computing technologies to achieve improvements in all aspects of power generation, transmission and distribution in the grid. Electricity users are gradually moving from the original passive electricity consumption mode to intelligent, green and efficient electricity consumption. One of the key components of the smart grid is the smart meter, which can measure and collect electricity consumption data from power users and send it to the control center for electricity consumption monitoring and time-of-use tariff setting. At the same time, it can receive real-time tariffs and other control information from the control center for demand response in the smart grid, and the two-way interaction between the power users and the smart grid is gradually becoming more frequent [1].

However, such frequent information exchange is prone to attract the attention of attackers. For example, the fine-grained electricity consumption data sent periodically by smart meters contains private information such as the user's identity and real-time power consumption. If an attacker obtains this information through active attacks or eavesdropping attacks, he or she can deduce whether someone is in the user's home and thus commit criminal activities. In addition, the control information sent by the power supplier to the customer will cause fluctuations in the power grid if it is tampered with by an attacker, which may cause widespread power outages. Therefore, the security of bi-directional communication of smart meters is very important [2].

The literature [3] proposes a lightweight smart meter authentication and key negotiation scheme that has low computational cost and achieves anonymity and untraceability of smart meters. The literature [4] proposes a PUF-based smart meter authentication scheme that is not only physically secure but also resistant to modeling attacks and has low computational and communication costs. The literature [5] proposed an elliptic curve cipher-based authentication scheme for two-way communication of smart meters, which can achieve secure two-way communication between smart meters and electricity suppliers and resist man-in-the-middle attacks and retransmission attacks. The literature [6] proposes a robust two-way communication scheme for smart meters, which is based on elliptic curve ciphers, enables key negotiation, and provides detailed security proofs that can be implemented in smart meters. The literature [7] proposes a mutual authentication and key negotiation scheme for smart meters based on fog computing and blockchain, which enables three-way communication and has high security. The literature [8] proposes a smart meter authentication protocol based on elliptic curve cipher, which the authors claim has high security and low overhead.

However, the quantum algorithm proposed by Shor [9] shows that none of the current smart meter privacy protection schemes based on discrete logarithm and large number decomposition can resist quantum attacks, and they will be broken with the rapid development of quantum computers. Considering the above problems, this paper designs a quantum attack resistant smart meter authentication and key negotiation scheme, which eliminates the overhead of certificate management by identity-based encryption and combines key negotiation with lattice cipher, and both communication parties generate a session key to achieve secure two-way communication between smart meters and electricity suppliers.

The rest of the paper is as follows. The second part introduces the related technology. The third part establishes the process of our scheme. The fourth part is the summary of this paper.

2. Related technology

2.1 Notations

The security parameter is denoted by k in this paper, and q is an integer that is used as a mode in this paper. Matrices are denoted by uppercase boldface (e.g., $\mathbf{X}$), vectors are denoted by lowercase boldface by default (e.g., $\mathbf{x}$), and the transpose of a matrix $\mathbf{x}$ is denoted as $\mathbf{X^T}$. The Euclidean norm of a given vector $\mathbf{x}$ is denoted as $\|\mathbf{x}\| = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}$, where $x_1, x_2, \cdots, x_n$ is an element of the vector.

2.2 Lattice

A lattice is the set of a class of discrete points in R^m with periodic structure; specifically, a lattice is a linear combination of all the integer coefficients of the set of m linearly independent vectors $\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}$ of the m -dimensional Euclidean space R^m:

$$L(\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}) = \left\{ \sum_{i=1}^{n} a_i \mathbf{b_i} : a_i \in Z \right\}$$

The integers n and m are called the rank and dimension of the lattice, the vector group $\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}$ is called a set of bases of the lattice, the same lattice can be composed of different bases of the lattice, the non-zero shortest vector $\mathbf{b}$ of the lattice is called the shortest distance of the lattice: $D_{min}(L) = min\{\|\mathbf{b}\|, \mathbf{b} \in L \setminus \{0\}\}$.

Any basis of a lattice can be represented as a matrix $\mathbf{B}=\left[\mathbf{b_1},\mathbf{b_2},\cdots,\mathbf{b_n}\right]\in Z^{m\times n}$. $\mathbf{B}$ is called a basis matrix, with basis vectors as columns. The lattice L formed by the basis matrix $\mathbf{B}\in Z^{m\times n}$ is defined as $L(\mathbf{B})=\left[\mathbf{Ba}:\ \mathbf{a}\in Z^n\right]$, where $\mathbf{Ba}$ is the vector matrix multiplication.

The base matrix $\mathbf{B}$ is not unique for any lattice $L(\mathbf{B})$. A matrix is said to be unimodular if its determinant is ± 1, and $\mathbf{BU}$ is a basis of a lattice $L(\mathbf{B})$ for any unimodal matrix $\mathbf{U}\in Z^{n\times n}$.

Small Integer Solution (SIS) problem: Given an $m\times n$ integral matrix $\mathbf{A}\in Z_q^{m\times n}(m\geq n)$ with integer modulo q, a real constant β and a random vector $\mathbf{y}\in Z_q^m$,find a vector $\mathbf{z}\in Z^n\setminus\{0\}$ such that $\mathbf{Az}=\mathbf{y}(\mathrm{mod}\,q)$ and $\|\mathbf{z}\|<\beta$.

3 Scheme implementation

In this section, we propose a quantum attack resistant smart meter authentication and key agreement scheme with two parties in the given network model, i.e., the smart meter and the electricity provider, for the authentication and key agreement scheme. To protect the transmitted data, the smart meter and the service provider need to authenticate each other and secretly negotiate a shared session key. The model of this scheme is shown in Figure 1.

Table 1: Notations and description of the scheme.

Notations	Description
m	Security parameter
n,q	An integer and a prime number
$\mathbf{X}$	A matrix from $Z_q^{m\times n}$
$\mathbf{d}$	Master secret-key of KGC
$\mathbf{P}$	Master public-key of KGC
$H_i(.)$	Cryptographic hash functions, $H_i:\{0,1\}^*\rightarrow Z_q^*, i=1,2,3$
N_i	i^{th} Node
$\mathbf{sk_i}$	private-key of N_i

When a smart meter needs to communicate with an electricity provider, or when an electricity provider needs to communicate with a smart meter, the identity of both parties needs to be verified. Upon successful two-way authentication, a shared session key is generated between the smart meter and the service provider. This session key will be used for subsequent secure communication via encrypted transmitted messages. For convenience, we mark the party initiating the communication as a node N_1, the party receiving the communication as a node N_2, and the key generation center (KGC) as a trusted third party for generating the private keys of the communicating nodes. Our proposed protocol consists of three phases: initialization, private key generation and session key generation, which are described as follows. For the sake of clarity, the notations used in the scheme and their meanings are listed in Table 1.

The key agreement protocol is highly secure because of its authentication mechanism, which not only allows the participants to establish a shared session key, but also allows them to authenticate their identity after the session key is constructed, and only after the authentication is passed can they be allowed to use the session key for confidential communication. In addition, the development of the authentication key negotiation protocol is important for enhancing the security of communication networks. Thanks to the good compatibility of the authenticated key agreement, it can play a fundamental role in forming a more secure cryptographic algorithm by combining

digital signature and data encryption technologies to meet the needs of secure communication in data security, key management and confidential communication.

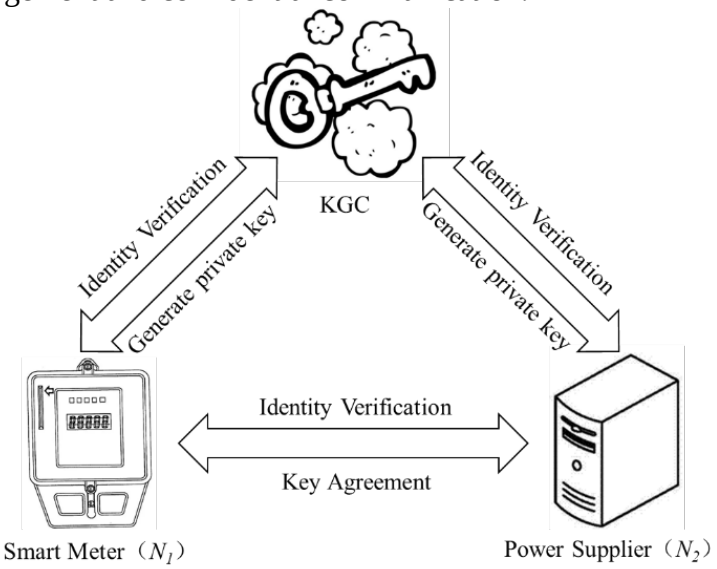

Figure 1: Scheme Model.

3.1 Initialization

The KGC runs the Initialization phase to generate the global system parameters. The input to this phase is a security parameter m. The outputs produced by Initialization are a list containing global parameters. The steps executed by the KGC are:

- Chooses an integer $n \geq 2m\log q$ where $q \geq \alpha \cdot \sqrt{\omega(m\log m)}$ be a prime and a modular matrix $\mathbf{X} \in Z_q^{n\times n}$.
- Selects a random vector $\mathbf{d} \in Z_q^n$ and computes master public-key as $\mathbf{P} = \mathbf{d}^{\mathbf{T}} \cdot \mathbf{X}$.
- Chooses three cryptographic hash functions $H_i : \{0,1\}^* \to Z_q^*, i = 1,2,3$.
- Keeps $\mathbf{d}$ as master secret key and outputs global parameters $\Delta = \{n, q, \mathbf{X}, \mathbf{P}, H_1(\cdot)\}$ publicly.

3.2 Private key extraction

The KGC runs Private key extraction phase to issue the private key $\mathbf{sk_i}$ of each edge node N_i.The steps involved in this phase are as follows.

- The edge node N_i sends its identity $ID_i, i = 1,2$ to the KGC.
- After receipt of ID_i via an offline mode, the KGC verifies the authenticity of N_i and its ID_i
- On successful verification of ID_i, the KGC executes the following steps:
  - Picks a random vector $\mathbf{r_i} \in Z_q^n$ and calculates $\mathbf{P_i} = \mathbf{r_i}^{\mathbf{T}} \cdot \mathbf{X}$.
  - Computes $h_i = H_1(ID_i \| \mathbf{P_i})$ and calculates the private key of edge node N_i as $\mathbf{sk_i} = (\mathbf{r_i} + h_i \cdot \mathbf{d}) \bmod q$
  - Sends $(\mathbf{sk_i}, \mathbf{P_i})$ to edge node N_i via secure channel.

3.3 Session key generation

The Session key generation phase is executed by both the edge nodes- N_1 and N_2. This phase negotiates a common session key between them. The steps of this phase are as follows.

- N_1 chooses $\mathbf{x_1} \in Z_q^n$ at random in such a way that $\|\mathbf{x_1}\| \le \alpha, \alpha \in Z^+$, and computes $\mathbf{A_1} = \mathbf{X} \cdot \mathbf{x_1}$ and $\mathbf{B_1} = \mathbf{x_1^T} \cdot \mathbf{X}$.
- N_1 computes $\delta_1 = H_2(\mathbf{B_1} \| \mathbf{P_1} \| T_1)$ where T_1 represents the timestamp and calculates $\mathbf{S_1} = (\mathbf{sk_1} + \delta_1 \cdot \mathbf{x_1}) \bmod q$.
- Now, N_1 sends the tuple $\{\mathbf{A_1}, \mathbf{B_1}, T_1, \mathbf{S_1}, \mathbf{P_1}\}$ to N_2 over a public channel.
- On receiving $\{\mathbf{A_1}, \mathbf{B_1}, T_1, \mathbf{S_1}, \mathbf{P_1}\}$ from N_1, N_2 checks whether $\mathbf{S_1^T} \cdot \mathbf{X} = \mathbf{P_1} + h_1 \cdot \mathbf{P} + \delta_1 \cdot \mathbf{B_1}$.
- On successful verification, N_2 chooses $\mathbf{x_2} \in Z_q^n$ at random in such a way that $\|\mathbf{x_2}\| \le \alpha, \alpha \in Z^+$, and computes $\mathbf{k_2} = \mathbf{x_2^T} \cdot \mathbf{A_1}$ and $\mathbf{B_2} = \mathbf{x_2^T} \cdot \mathbf{X}$.
- N_2 computes $\delta_2 = H_2(\mathbf{B_2} \| \mathbf{P_2} \| T_2)$ where T_2 represents the timestamp and calculates $\mathbf{S_2} = (\mathbf{sk_2} + \delta_2 \cdot \mathbf{x_2}) \bmod q$.
- Now, N_2 compute the session key as $\mathrm{K}_2 = H_3(\mathbf{k_2} \| ID_1 \| ID_1 \| T_1 \| T_2 \| \mathbf{P_1} \| \mathbf{P_2} \|)$ and sends the tuple $\{\mathbf{B_2}, T_2, \mathbf{S_2}, \mathbf{P_2}\}$ to N_1 over a public channel.
- On receiving $\{\mathbf{B_2}, T_2, \mathbf{S_2}, \mathbf{P_2}\}$ from N_2, N_1 checks whether $\mathbf{S_2^T} \cdot \mathbf{X} = \mathbf{P_2} + h_2 \cdot \mathbf{P} + \delta_2 \cdot \mathbf{B_2}$.
- On successful verification, N_1 computes $\mathbf{k_1} = \mathbf{B_2} \cdot \mathbf{x_1}$ and computes the session key as $\mathrm{K}_2 = H_3(\mathbf{k_1} \| ID_1 \| ID_1 \| T_1 \| T_2 \| \mathbf{P_1} \| \mathbf{P_2} \|)$

Note that in the generation of session key, the values of $\mathbf{k_1}$ and $\mathbf{k_2}$ are same as $\mathbf{k_1} = \mathbf{k_2} = \mathbf{x_2^T} \cdot \mathbf{X} \cdot \mathbf{x_1}$.

4 Correctness verification

Theorem 4.1 If the scheme is correct, i.e., the validating node can verify the authenticity of the incoming message by the formula, then the following equation holds.

$$\mathbf{S_i^T} \cdot \mathbf{X} = \mathbf{P_i} + h_i \cdot \mathbf{P} + \delta_i \cdot \mathbf{B_i}, i = 1, 2.$$

Proof:

$$\begin{aligned} \mathbf{S_i^T} \cdot \mathbf{X} &= (\mathbf{sk_i} + \delta_i \cdot \mathbf{x_i})^{\mathbf{T}} \cdot \mathbf{X} \\ &= \left((\mathbf{r_i} + h_i \cdot \mathbf{d}) + \delta_i \cdot \mathbf{x_i}\right)^{\mathbf{T}} \cdot \mathbf{X} \\ &= \mathbf{r_i^T} \cdot \mathbf{X} + h_i \cdot \mathbf{d^T} \cdot \mathbf{X} + \delta_i \cdot \mathbf{x_i^T} \cdot \mathbf{X} \\ &= \mathbf{P_i} + h_i \cdot \mathbf{P} + \delta_i \cdot \mathbf{B_i} \end{aligned}$$

Hence, it is proved.

Theorem 4.2 After successful execution of the scheme, node N_1 and node N_2 can exchange an identical session key between them.

Proof: During key negotiation, N_1 computes $\mathbf{k_1} = \mathbf{B_2} \cdot \mathbf{x_1} = \mathbf{x_2^T} \cdot \mathbf{X} \cdot \mathbf{x_1}$ and N_2 computes $\mathbf{k_2} = \mathbf{x_2^T} \cdot \mathbf{A_1} = \mathbf{x_2^T} \cdot \mathbf{X} \cdot \mathbf{x_1}$. Therefore, $\mathbf{k_1}$ and $\mathbf{k_2}$ have the same value, and node N_1 and node N_2 can negotiate an identical session key $\mathrm{K} = H_3\left(\mathbf{k_1} \| ID_1 \| ID_1 \| T_1 \| T_2 \| \mathbf{P_1} \| \mathbf{P_2} \| \right) = H_3\left(\mathbf{k_2} \| ID_1 \| ID_1 \| T_1 \| T_2 \| \mathbf{P_1} \| \mathbf{P_2} \| \right)$.

Hence, it is proved.

5 Conclusion

In order to address the privacy leakage that may result from the two-way interaction between smart meters and the grid and the quantum attacks that may arise in the future, a lattice based smart meter authentication and key negotiation scheme that is resistant to quantum attacks is proposed in this paper. The scheme eliminates the overhead of certificate management by identity-based encryption and improves the traditional scheme based on DH key exchange protocol by taking advantage of the fact that Bi-SIS and Bi-ISIS problems cannot be solved even in the quantum environment, solving its disadvantages of inefficiency and inability to resist quantum attacks. In addition, the scheme can resist man-in-the-middle attacks, unknown key sharing attacks, and known key security attacks, and has perfect forward security with quantum security.

References

[1] Tufail S, Parvez I, Batool S, Sarwat A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid[J]. Energies. 2021; 14(18):5894.

[2] Desai S, Alhadad R, Chilamkurti N, et al. A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure[J]. Cluster Computing, 2019, 22(3).

[3] Zhang L, Zhao L, Yin S, et al. A lightweight authentication scheme with privacy protection for smart grid communications[J]. Future generation computer systems, 2019, 100(Nov.):770-778.

[4] P. Gope and B. Sikdar, "A Privacy-Aware Reconfigurable Authenticated Key Exchange Scheme for Secure Communication in Smart Grids," in IEEE Transactions on Smart Grid, vol. 12, no. 6, pp. 5335-5348, Nov. 2021.

[5] Tc A, Xy A, Gw B. Securing communications between smart grids and real users; providing a methodology based on user authentication[J]. Energy Reports, 2021.

[6] Sadhukhan D , Ray S , et al. A Secure and Privacy Preserving Lightweight Authentication Scheme for Smart-Grid Communication using Elliptic Curve Cryptography[J]. Journal of Systems Architecture, 2020, 114(11):101938.

[7] Tomar A, Tripathi S. Blockchain-assisted authentication and key agreement scheme for fog-based smart grid[J]. Cluster Computing, 2022, 25(4).

[8] Sureshkumar V , Anandhi S , Amin R , et al. Design of Robust Mutual Authentication and Key Establishment Security Protocol for Cloud-Enabled Smart Grid Communication[J]. IEEE Systems Journal, 2020, PP(99):1-8.

[9] Shor, Peter, W. POLYNOMIAL-TIME ALGORITHMS FOR PRIME FACTORIZATION AND DISCRETE LOGARITHMS ON A QUANTUM COMPUTER.[J]. Siam Journal on Computing, 1997.