High-Performance Secure Access and Data Privacy Protection Method for 5G Border Routing Gateway

Yunhui Fang*, Jihua Wang, Xiaolei Ying, Rongli Wang
State Grid Zhejiang Electric Power Co., Ltd. Ningbo Power Supply Company

*Corresponding author e-mail: yunhuifang@qq.com

Abstract. With the substantial increase in the amount of data information and the development of 5G technology, boundary computing technology based on 5G, as a real-time and efficient data processing method, has broad application prospects. The aggregation gateway further aggregates the power injection data of all electric energy storage units and sends it to the power company. The power company uses its own private key to access the aggregated data. Row decryption to obtain the total power data recovered in each time slot. The paper proposes a new solution using Lagrangian interpolation to ensure data privacy and security. The security shows that the algorithm can not only protect the privacy of the electric energy storage unit, but also realize the confidentiality and integrity of the injected data. Efficiency analysis shows that this algorithm can significantly reduce computational complexity and improve communication efficiency.

Keywords: 5G border routing gateway, smart grid, high performance, data security, data privacy protection.

1. Introduction
With the development of 5G network technology, 5G-based boundary computing technology has received widespread attention. Business requirements and network upgrades have further driven the development of boundary computing. Insufficient cloud computing capabilities cannot meet the explosive growth of massive data demands. In addition, the rapid increase in transmission load will lead to longer delays and fail to meet real-time requirements, all of which make boundary computing a research hotspot.

As a key device in network data transmission, the gateway plays the role of protocol conversion and data processing. Through the method of boundary computing, the data can be initially screened and processed in the boundary gateway, and important safety information is sent to the monitoring platform and issued a warning, so that the efficiency of information processing is improved and hidden danger information can be obtained timelier. This paper first studies the characteristics of 5G and boundary computing, applies the scheme to the cloud environment, realizes an identity authentication system that protects user privacy in the cloud environment, and conducts a security analysis of the newly proposed authentication scheme for protecting data privacy in the cloud environment [1]. Performance analysis.
2. Theoretical analysis

2.1. Hash function

2.1.1. Hash function definition and properties. The hash function is to transform an input of any length (also called a pre-mapping) into a fixed-length output through a hashing algorithm, and the output is the hash value. The symbol is represented by h(.). The hash function is mainly used in the field of information security to implement encryption algorithms, generate hash codes, etc., which are mainly reflected in information security applications such as digital signatures, file verification, and authentication protocols. Hash function has the following properties:

   (1) Input parameter information of any length to obtain fixed length information output.

   (2) One-way: If the input parameter is m, it is easy to get the hash value h(m); if the hash value h(m) is known, it is difficult to calculate the parameter m through the hash value. Has an irreversible nature.

   (3) Weak collision resistance: The input parameter is known to be m, if another parameter m' can be calculated to satisfy m≠m', and the hash values h(m) and h(m') are not acceptable OK.

   (4) Strong collision resistance: Given the hash value h(m), calculate another parameter m' to satisfy m≠m', and make the hash value h(m) and h(m') equal is not feasible.

2.1.2. Anti-collision hash function. Given the hash function, defined in the polynomial time of all probabilities, the anti-collision advantage of adversary A can be expressed as:

   \[ Adv_{A}^{TCR} = \Pr \{ y \leftarrow A(H,x); H(x) = H(y) \} \]  

If for any given probability polynomial time is the adversary A, if the advantage of the adversary A for the Hash function H is negligible for \( Adv_{A}^{TCR} \), then the Hash function H is said to be the target anti-collision hash function. Figure 1 shows the principle of the anti-collision hash function [2].

![Figure 1. Principle of anti-collision hash function](image)

2.1.3. One-way trapdoor hash function. The one-way trapdoor hash function \( g_{1}(x): R \rightarrow D \) is a one-way hash function, that is, it is easy to calculate in one direction, but it is difficult to calculate in the opposite direction. If you give an arbitrary value \( x \in R \), you can calculate the value \( g_{1}(x) \), and for almost all \( x \in R \) , given the value \( g_{1}(x) \), it is difficult to find the value of \( x \) in reverse. However, if \( g_{1}(x) \) and secret information are given, the value of \( x \) can be easily calculated, and the secret information is called a trapdoor. Figure 2 shows the principle of the one-way trapdoor hash function.
2.2. Lagrangian difference function

2.2.1. Lagrangian interpolation function definition. In many practical problems, such as mathematics, physics, etc., many problems require functions to express certain connections, or mutual laws, but many functions can only be understood through experiments or observations [3]. For example, only by observing a certain physical quantity can we wait for the corresponding observation value in some places, but using Lagrangian interpolation can find a polynomial to get the corresponding value at some observation points. Observations. We call such polynomials Lagrange interpolation polynomials. Mathematically speaking, Lagrangian interpolation can give such a function: it can pass through a number of known point functions, and for a known point \((x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)\), there is only one Lagrangian polynomial \(L\), and its degree cannot exceed \(n\). If you count a higher degree of polynomial, there will be infinitely many, because all polynomials that differ from Lagrangian \(L\) by \(\lambda(x - x_0)(x - x_1)\ldots(x - x_n)\) can satisfy the condition.

Assuming there are any two different \(x_j\), if the Lagrangian interpolation formula is used to transform, the obtained Lagrangian interpolation polynomial can be expressed as:

\[
L(x) := \sum_{j=0}^{k} y_j l_j(x)
\]  

(2)

The \(l_j(x)\) in the formula is called the Lagrangian basic polynomial (also called the Lagrangian interpolation basis function), and the expression is:

\[
l_j(x) = \prod_{i=0, i \neq j}^{k} \frac{x - x_i}{x_j - x_i}
\]

(3)
The characteristic of the basic polynomial \( l_j(x) \) of Lagrangian interpolation is that the value at point \( x_j \) is 1 and the value at other points \( x_i, i \neq j \) is 0.

2.2.2. Properties of Lagrangian interpolation function

\textit{a) Existence}

For the known points: \((x_0, y_0), ..., (x_k, y_k)\), the idea of Lagrangian interpolation is to find a polynomial \( l_j(x) \) whose value is 1 at point \( x_j \) and 0 at other points. In this way, the value of the polynomial \( y_j l_j(x) \) at point \( x_j \) is \( y_j \), and the value at other points is 0. Then the polynomial

\[ L(x) := \sum_{j=0}^{k} y_j l_j(x) \]

satisfies

\[ L(x_j) = \sum_{i=0}^{k} y_i l_i(x_j) = 0 + 0 + ... + y_j + 0 + ... + 0 = y_j \quad (4) \]

Its value at point \( x_j \) is: \((x_j - x_0)(x_j - x_{j-1})(x_j - x_{j+1})... (x_j - x_k) \).

Since \( x_j \) has been assumed to be two different points from each other, the value of the previous polynomial will not be 0. Therefore, by dividing the polynomial by this value, you can obtain a polynomial that satisfies the condition that the value of \( x_j \) is 1, and the value of all other points is 0, as shown below:

\[ l_j(x) = \prod_{i=0, i \neq j}^{k} \frac{x - x_i}{x_j - x_i} \]

\[ = \frac{x - x_0}{x_j - x_0} \cdot \ldots \cdot \frac{x - x_{j-1}}{x_j - x_{j-1}} \cdot \frac{x - x_{j+1}}{x_j - x_{j+1}} \cdots \frac{x - x_k}{x_j - x_k} \quad (5) \]

This polynomial is the basic polynomial of Lagrange interpolation.

\textit{b) Uniqueness}

The uniqueness of Lagrangian polynomials can be obtained by the following proof: given any two Lagrangian interpolation polynomials, their degree cannot be greater than \( k \). At all \( k+1 \) point, the difference the values are all 0, so the difference must be a multiple of polynomial \((x - x_0)(x - x_1)...(x - x_k) \). If the value of this interpolation at \( k+1 \) point is not 0, then the degree of this polynomial must be less than \( k+1 \).

2.3. 5G technical characteristics

In June 2019, the Ministry of Industry and Information Technology issued a 5G commercial license, marking China's official entry into the first year of 5G commercial use, but the development of 5G technology is still continuing, and it is constantly providing more convenient applications for our lives. 5G stands for fifth-generation communication technology, which is a new generation of cellular mobile communication technology with the following characteristics:

(1) It has a high data transmission rate, up to 10GB/s, which can meet the transmission of large amounts of data; (2) Low latency, the LTE network makes the mobile network delay up to 100ms, but the 5G network can reach 1ms. Satisfy services with very low latency requirements; (3) Improve
system capacity and large-scale device connections to meet the requirements of the Internet of Things and connect various terminals. 5G is not only a great progress for mobile communications, but also a very useful technology for the Internet of Things. The convenience and technological changes it brings will promote economic development.

2.4. Features of boundary computing technology
In boundary computing, the purpose of integrating the data processing process into the boundary device is to reduce the delay, so that the data can be processed quickly without waiting for the data to be transmitted to the traditional data center for processing. After the delay is reduced, the corresponding application can run earlier. At the same time, the cost of data management for local equipment is less than that of cloud and data center networks, which can reduce costs. Specifically, the characteristics of boundary calculation are as follows:

(1) Low time delay: Use boundary equipment to process data, realize real-time data processing, and effectively shorten the response time.
(2) Low cost: Use border devices to filter, calculate and analyze data, reduce data transmission in the backbone network, reduce network bandwidth requirements, and thereby reduce data processing costs and equipment energy consumption.
(3) High reliability: The boundary device itself has computing and processing capabilities, even if there is a problem in the upper data processing center, it will not affect the normal use of users.

Boundary computing is a method proposed to solve the decentralization of cloud computing. At present, cloud computing is to centrally place servers in a data center. Data needs to be transmitted to the data center and then centrally processed. However, as the number of terminal devices continues to increase, the amount of data brought by the gradual increase, the cost of transmitting such a huge amount of data is very high, and the delay has become a bottleneck. Boundary computing is deployed on the device side in a distributed manner, that is, various terminal devices are added with functions such as storage and processing, which can reduce the amount of data transmitted, reduce delays, and reduce costs [4]. At the same time, there may be leakage problems in the process of transmitting private data to the cloud. Using boundary computing can reduce the possibility of data leakage.

3. An anonymous authentication scheme based on provable link layer location privacy

3.1. Secret key distribution stage
The trusted third-party TA completes the following initialization system parameters.

1) Generate a 7-tuple \((q, G, G', G_\tau, e, P, P')\) and \(P_{pub} = sP \in G\) through a bilinear parameter generation function \(\text{Gen}(k)\).

2) Choose a pseudo-random number generation function \(\text{PRNG}(\bullet)\) and hash function \(h, f, H : \{0,1\}^* \rightarrow G',\) and function \(F: G_\tau \rightarrow \{0,1\}^r\) as public parameters.

3) Choose a large prime number \(p \in Z_q^*\) and a random polynomial

\[
f(x) = s + \sum_{i=1}^{n} a_i x^i \pmod{p}
\]  

Among them the coefficient \(a_i \in Z_q^*,\) the constant term is \(s,\) namely \(f(0) = s.\)

4) Calculation:

\[
A_i = f(x_i) \prod_{i=1}^{n-2} \frac{-w_i}{x_A - w_i}
\]  

5
\[ B = \sum_{i=1}^{n-2} f(w_i) \prod_{k \neq i}^{n-2} \frac{-x_k}{w_k - x_k} \]
\[ f(w_i) = \frac{-x_k}{x_i - x_k} \prod_{k \neq i}^{n-2} \frac{-w_j}{x_j - w_j} \]
\[ C_i = \frac{-x_i}{x_A - x_i} \] 

(8)

The trusted third party TA discloses the system parameter \((p, q, G, G', G_r, e, P, P_{pub}, h, f, H, F)\), calculates \(LK = sH(L) \in G'\) for \(L\) the wireless access point \(AP\) at the location, and sends \(LK\) and \(AP\) to E through a secure channel.

3.2. Anonymous mutual authentication phase

1) \(N_i\) first selects a random number \(r_j, j \in Z_q^*\), calculates \(C_i = r_iP, N_i\) and uses position information \(L\) to calculate

\[ R_1 = F(e(P_{pub}, H(L))^5) \] 
\[ C_2 = R_1 \oplus M \] 

(10)

Get

\[ M = j \| h(r_i) \| C_i \| Timestamp \| r_iA_C_iP \] 

(11)

2) After receiving information \(C\) at \(AP\), first use \(LK\) to calculate

\[ R' = F(e(C_1, LK)), C_2 \oplus R'_1 \] 
\[ M = j \| h(r_i) \| C_i \| Timestamp \| r_iA_C_iP \] 

(12)

(13)

Where \(M' = r_2P \| L \| Timestamp'\). \(AP\) Calculate the shared session key \(K_j = r_1C_i = r_1r_2P\).

\[ M' = C_4 \oplus R_3' \] 

(14)

among them

\[ R_3' = F(e(r_1P_{pub}, H(L)h(r_i) \| C_i)) \] 
\[ M' = r_2P \| L \| Timestamp \] 

(15)

(16)

Get \(r_2P\), and calculate the session key \(K_j = r_1r_2P\).

3.3. Scheme security analysis

We analyze the performance of this program from two aspects: space efficiency and time efficiency.
Space efficiency: Compared with the solution in literature [1], our solution does not increase the number of information exchanges between users and wireless access points. The amount of information stored on the user side is the same as the original solution. The information storage of the wireless access point is increased by a message $B$ compared to the original solution. However, the information $B$ is only a parameter and has a negligible impact on the storage space of the wireless access point.

In terms of the amount of calculation on the mobile client side, our solution is compared with the solution in [1]. When generating information $M = j || h(r_i || C_r) || Timestamp || r_i A_r C_r P$, one hash calculation and two dot product calculations are required, and the hash and dot product calculations are fast, the computational consumption of the mobile client is also acceptable. When wireless access point $AP$ authenticates mobile users, our solution needs to verify whether the calculation $D^2 F(e(C_r, LK)^{h(r_i || |C_r|)})$ is equal. If it does not wait, the authentication is unsuccessful and the user exits and the user is determined to be illegal. This avoids the wireless access point from performing subsequent calculations and reduces calculation consumption. If the authentication is successful, $R_i = D^j$ is calculated, and the follow-up operation is performed. In the solution in, the wireless access point authenticates the user through the entire authentication process until the user can access the service. In this process, the wireless access point needs to perform all the preset calculations regardless of whether the mobile user can be successfully authenticated. If the authentication is unsuccessful, it will greatly consume the computing resources of the wireless access point. Therefore, our scheme is relatively efficient in terms of wireless access point authentication.

In terms of time efficiency, the time of the scheme is mainly consumed in the element operations of hash calculation, linear pair calculation, modular multiplication calculation, and XOR calculation. This scheme and the scheme of $R$ literature are included in the certification process stage. The number of these meta-operations is analyzed and compared, see Table 1.

|             | Hash function | Bilinear pair | Modular multiplication | XOR | Modulus index |
|-------------|---------------|---------------|------------------------|-----|---------------|
| Literature  | $AP$          | 4             | 2                      | 2   | 1             |
|             | $Mu$          | 4             | 2                      | 3   | 2             |
| This article| $AP$          | 4             | 2                      | 2   | 1             |
|             | $Mu$          | 3             | 2                      | 3   | 1             |

It can be seen from the table that the number of these element operations in this paper is the same as the number of bilinear pairings, modular multiplications, and exclusive OR operations compared with the solution in literature [5]. However, hash functions and modular exponential operations are more the scheme of is even less, and it can be seen that the efficiency of this scheme is higher than that of the scheme of literature.

3.4. G secure access to data privacy protection system

3.4.1. Development environment

a) Operating System

The Windows 7 operating system is a well-known operating system with a good graphical user interface. The core version number is Windows NT 6.1. Windows 7 can be used for laptops, home and business working environments, multimedia centers, tablets, etc.

The Linux system is a POSIX and UNIX-based multi-tasking, multi-user, multi-CPU operating system that supports multi-threading. The core design idea is based on the UNIX network, which can
run application software, network protocols, and UNIX tool software. With 32-bit and 64-bit hardware support, it is a relatively stable network operating system.

b) **Hadoop distributed computing platform**

Hadoop is an open source distributed computing platform under the Apache Software Foundation. Users do not need to understand the underlying details of the distribution to be able to develop distributed programs. Hadoop has great storage performance and cluster high-speed computing capabilities. The core is mainly composed of Hadoop distributed file system (referred to as HDFS) and MapReduce programming model consists of two parts. HDFS is characterized by high scalability, high fault tolerance, and can be deployed on inexpensive equipment. The test results of this article will use Hadoop to simulate a cloud environment platform, deploy the system on the platform for verification, and prove the feasibility and correctness of the scheme.

c) **eclipse integrated development tools**

Eclipse provides a highly integrated development tool with commercial quality and complete functions. It is an open source integrated software development tool. It has three projects and four components. The three components are the Eclipse technology project, the Eclipse project and the Eclipse tool project. The four components include: JDT, PDE, CDT and Eclipse Platform. For Java developers, Eclipse is a very good graphical interface development tool.

d) **Java programming language**

This article chooses Java language as the main programming language. Java is a completely object-oriented programming language launched by SUN in 1995. It has the advantages of platform independence, security, object-oriented, distributed and robustness.

1. Platform independence means that Java applications can run on different operating platforms that can run the Java virtual machine. The Java virtual machine is built on the basis of hardware and operating systems. The Java virtual machine mainly interprets Java programs as Binary, providing a unified interface for different platforms.

2. Object-oriented means that Java encapsulates data, and adopts the object-oriented thinking of C++ language, so that Java programs can be used repeatedly only after being compiled once, and the programmer's work is concentrated on the realization of classes and interfaces.

3. Distributed means that Java is built on the TCP/IP network communication platform. The Java function library provides a large number of methods of HTTP protocol transmission and reception of information, which makes programmers use network files like native files.

3.5. **Design of anonymous authentication system based on cloud environment**

3.5.1. **System architecture design**. This section first introduces the architecture and implementation of the authentication system from an overall perspective. The authentication system mainly includes a client, a trusted third party and an authentication server. The authentication server is placed in the cloud. The client mainly completes registration and login. The trusted third party mainly generates initialization parameters during the system establishment phase and generates authentication credentials for the user during the user registration phase. The authentication server mainly implements interactive authentication with the user [7]. This system adopts C/S architecture. The system architecture of the entire authentication system is shown in Figure 3.
Figure 3. System structure of the two-way authentication system

It can be seen from Figure 3 that the operations in the solution are mainly concentrated between the user end and the service provider. Since the cloud environment is an open and insecure environment, in this article, in order to realize the two-way anonymous authentication between the user and the cloud, a system is required. The information agency performs parameter generation in the system initialization phase.

In this authentication system, the trusted organization mainly completes the acquisition of authentication credentials in the user registration phase and the generation of parameters in the system initialization phase. After the establishment of the system is completed, the implementation of authentication is completely handed over to the user and the cloud service provider. The user registers with a trusted organization to generate an authentication certificate, and then sends the certificate to the authentication server of the cloud service provider [8]. The cloud authentication server uses the system to establish in the stage, the credential obtained from a trusted institution verifies the legitimacy of the user. After passing, the credential of the cloud authentication server is returned to the user to allow the user to verify the legitimacy of the server. After passing, the user can use the services provided by the cloud service provider. In the entire authentication process, any user-related information that the cloud service provider cannot obtain, realizes anonymous authentication and is two-way authentication.

3.5.2. The design of the server-side module of the system trusted organization. The trusted organization server-side program mainly implements the following functions: (1) System initialization parameter generation: the generation of the entire system parameters. (2) Data transmission function: When a user makes a registration request, an authentication certificate is generated for the user, and the authentication certificate is sent to the cloud authentication server during the system establishment phase. (3) Registered user management function: In order to realize the cancellation of user authority, there is a registered user information table on the server side. This table can not only check the user's registered user name, but also in the table for each registered user Set a timestamp. The timestamp value is specified by the rules of user registration to realize the function of revoking user permissions. (4) Monitoring function: It is mainly realized to monitor the request access from registered users, analyze the user's request information, and complete the user registration according to the user's request information. Through the above analysis, the trusted organization server mainly has the following modules as shown in Figure 4.
3.5.3. System client module design. The main functions of the system client program are as follows: Registration function: realizes the user's registration function. At this stage, the user registers with a trusted organization to obtain credential information during authentication. Login function: The authentication is successfully logged into the system. At this stage, the user and the cloud authentication server complete the mutual authentication process, and the legal user logs in. Data transmission function: Users register with trusted institutions and send authentication information to the cloud authentication server to access cloud resources. Authentication function: It mainly completes the authentication of the client to the cloud server [9]. Through the above analysis, the client mainly has the following modules as shown in Figure 5.

3.5.4. Cloud authentication server module design. The function of the cloud authentication server program is mainly: the function of authenticating the user: receiving the authentication information sent by the user and verifying the legitimacy of the user. Data transmission function: Send the generated verification information to the user, allowing the user to verify the legitimacy of the service provider. Monitoring function: It mainly monitors the request information of the logged-in user, and starts the mutual authentication process after receiving the login request. If the requested information is wrong, the communication is terminated, otherwise the required information is sent to the client.
Access service function: After mutual authentication is completed, the user can access the application or jump to the application server.

3.6. Implementation of anonymous privacy authentication system based on cloud environment

The system is divided into three entities: the client, the trusted organization server and the cloud authentication server. This section mainly describes the main classes and methods involved in the system implementation process, and analyzes some encountered in the implementation process Key issues and solutions, and finally the main operating interface of the system is given.

One of the main functions of the trusted organization server is to initialize the parameters of the entire system and generate master key information. The main structure of the operation design is shown in Figure 6 below:

**Figure 6.** System parameter initialization

Another main function implemented by the trusted organization server is to distribute authentication credentials to registered users and issue authentication information to the cloud authentication server when users log in to apply for access to cloud resources. The main structure of this class is shown in Figure 7 below:
4. Conclusion
This article discusses the 5G-based edge computing gateway and its application in the power grid, and introduces the application of 5G network and edge computing in substations in combination with substation business. The paper uses Lagrangian interpolation to propose a new solution. The security shows that the solution not only fully realizes security, but also requires less calculations on the client and server through performance analysis. Although 5G technology is still in its infancy, the initial deployment also uses non-independent networking, which cannot fully demonstrate its characteristics (such as low latency). I believe that with the continuous improvement of 5G and edge computing technology systems, independent networking deployment of 5G technology Gradually mature, it can process more data information more accurately, conveniently and quickly, and truly achieve the purpose of increasing data transmission rate and reducing delay.

Acknowledgments
This work is supported by the State Grid Zhejiang Electric Power Co., Ltd. Science and Technology Project “Study on 5G information security boundary access module for ubiquitous power Internet of Things”

References
[1] Weber, A., Reith, S., Kasper, M., Kuhlmann, D., Seifert, J. P., & Krauß, C. Souveränität und die IT-Wertschöpfungskette. Datenschutz und Datensicherheit-DuD, vol. 42, pp. 291-293, May 2018.
[2] Hoberg, F. Stau auf der Datenautobahn. ATZ-Automobiltechnische Zeitschrift, vol. 118, pp. 8-13, February 2016.
[3] Berg, S., & Thiels, T. Widerstand und die Formierung von Ordnung in der digitalen Konstellation. ZPTh-Zeitschrift für Politische Theorie, vol. 10, pp. 67-86, January 2019.
[4] Henseler-Unger, I. Hochleistungsfähige Kommunikationsnetze: Wer investiert?. Wirtschaftsdienst, vol. 97, pp. 28-33, January 2017.
[5] von Lucke, J. Wie smart darf Polizeiarbeit eigentlich werden?. VM Verwaltung & Management, vol. 26, pp. 107-124, March 2020.
[6] Christen, M., Gordijn, B., Weber, K., van de Poel, I., & Yaghmaei, E. A review of value-conflicts in cybersecurity: an assessment based on quantitative and qualitative literature analysis. Orbit Journal, vol. 1, pp. 28-32, January 2017.

[7] Weber, K., Christen, M., & Herrmann, D. Cybersicherheit. TATuP-Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis, vol. 29, pp. 10-43, January 2020.

[8] Calliess, C., & Baumgarten, A. Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective. German Law Journal, vol. 21, pp. 1149-1179, June 2020.

[9] Clarke, R., & Wigan, M. The information infrastructures of 1985 and 2018: The sociotechnical context of computer law & security. Computer Law & Security Review, vol. 34, pp. 677-700, April 2018.