Proceedings of CECNet 2022
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA220513

Lightweight Application of SM2 Co-Signature Algorithm in the Power IOT

Yanrong ZHANG[1], Feng YANG and Yanfang YUAN
Beijing Smartchip Microelectronics Technology Company Limted, China

Abstract. The access of massive terminal devices at the perception layer poses security threat to the power Internet of Things (IOT) of the State Grid Corporation. Due to lack of computing resources, the IOT perception layer terminal devices cannot embed the security chips. The lightweight authentication technologies are urgently needed to be developed to protect the authentication security of the IOT perception layer terminal devices. This paper proposes a lightweight identity authentication system based on the SM2 co-signature algorithm, which can be applied to the identity authentication of the IOT perception layer terminal devices. This system is implemented in software and characterized by low cost and strong compatibility, and most importantly, it can strengthen the identity authentication security of the power IOT which security protection capability will be improved consequently.

Keywords. SM2 algorithm, co-signature, lightweight, power IOT

1. Introduction

With the continuous deepening construction of the Power Internet of Things (IOT) of the State Grid Corporation, the continuous exploration and expansion of the power business, the continuous innovation of related technologies have brought new risks to the network security. In particular, the massive terminal devices connected to the network participate in the interaction of the power grid and generate a large amount of data, which brings severe challenges to terminal trust management and network access security. The perception layer terminal devices have become potential risks of invading the power IOT from the outside, which forming an important weakness of power grid security [1].

As the important modules for building the power IOT, the perception layer terminal devices are the key factors of the power IOT security. The data sensed by the terminal devices contain various important information such as personal privacy, economic development and national security. It may cause very dangerous consequences once the information is leaked. With the appearance and development of new technologies such as cloud computing, big data, and mobile applications, the network attacks are constantly being upgraded. It is impossible to completely prevent malicious attacks simply relying on the security design of the terminal devices. How to manage the secure access of massive terminal devices is the key issue to solve the current security protection problems of the power IOT. In response to this problem, the

[1] Corresponding author: Yanrong Zhang, Beijing Smartchip Microelectronics Technology Company Limted, China; E-mail: 474123226@qq.com.

existing research result is to make physical isolation among networks to some certain extent, which enhanced the security of information interchange. However, this measure is relatively single, and the power consumption of the physical isolation equipment is relatively large. Besides, the physical isolation equipment requires more computing resources. This cannot meet the requirements of low power consumption, low cost, and multi-distribution. The lightweight identity authentication technologies are urgently needed to be developed to ensure secure access control of terminal devices [1].

The computing resources of the IOT perception layer terminal devices are limited and the security chip cannot be embedded in. Thus, this leads to the existing identity authentication requirements cannot be met. The co-signature technology based on SM2 algorithm proposed in this paper is implemented in software, and it is characterized by low cost and strong compatibility, and can be widely used in the identity authentication of the IOT perception layer terminal devices to achieve secure access control.

2. SM2 Co-Signature Algorithm

2.1. SM2 Algorithm

SM2 algorithm is an elliptic curve public key cryptography standard issued by the State Cryptography Administration of China, and the relevant standard is "GM/T0003-2012 SM2 Elliptic Curve Public Key Cryptography". In 2018, the SM2 digital signature algorithm became an ISO/IEC international standard. Before SM2 algorithm is used, the following conventions are made for the symbols and operations in this paper: if P and Q are elements (elliptic curve points) in the elliptic curve point group, then P+Q represents the point addition of P and Q; $[k]P$ represents the point addition of k times P, that is $P+P+\ldots+P$ (there are k times P in total); mod(n) is the operation of modulo n; "•" represents the multiplication symbol. The public parameters of the SM2 algorithm include q, n, E and G, q is a large prime number; E is an elliptic curve defined on a finite field F_q; $G = (x_G, y_G)$, is the base point of the nth order on E, and e is the message digest obtained by the signature preprocessing of the message M to be signed. SM2 algorithm consists of key generation, signature generation and signature verification [2][3].

2.2. SM2 Co-Signature Algorithm

SM2 co-signature algorithm is based on SM2 digital signature algorithm mentioned in the standard "GM/T0003-2012 SM2 Elliptic Curve Public Key Cryptography". The principle is as follows: a part of the private key is stored in the client and server respectively, and the two parties can only sign the message together. Neither party can obtain any information about the other party's private key. The signature cannot be forged no matter either party is attacked [4][5].

SM2 co-signature process consists of cooperative key generation and cooperative signature.

1.Cooperative key generation

The client and the server generate a private key component independently, the two parties transmit the auxiliary calculation data through interactive communication, and the sever combines the auxiliary calculation data to generate SM2 public key and publishes it.

The process is as follows:

1) The client generates the private key component $D1$.

2) The server generates the private key component $D2$, and then calculates the SM2 public key P according to $D1$ and $D2$. P is taken as the SM2 public key.

Figure 1 shows the detailed process of SM2 cooperative key generation.

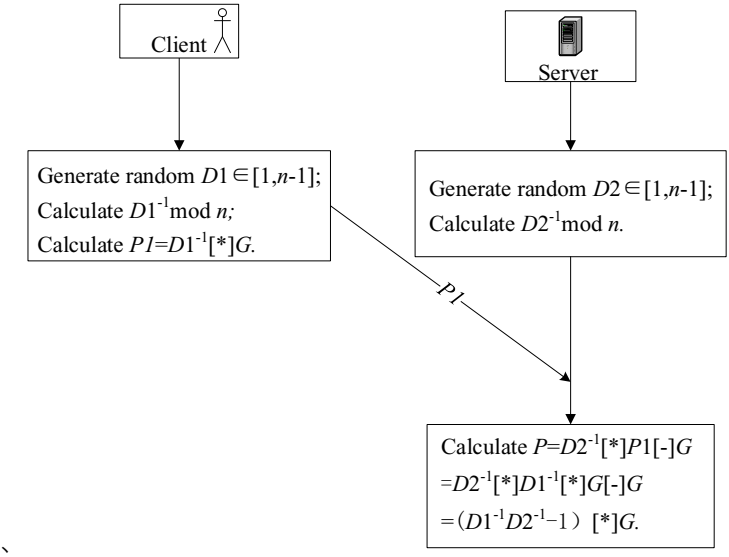

Figure 1 SM2 cooperative key generation

2. Cooperative signature

When the message needs to be signed, the two parties use their respective private key component to calculate the signature component, and then the two parties transmit auxiliary calculation data such as the signature component, and finally, the client combines and calculates the received data to get SM2 co-signature.

The process is as follows:

1) The client calculates the digest e of the message M to be signed and the first part of the signature $Q1$, then sends e and $Q1$ to the server;

2) The server calculates the second part of the signature r according to $Q1$ and e, and calculates the third part of the signature $s2$ and the fourth part of the signature $s3$ according to $D2$, then sends r, $s2$ and $s3$ to the client;

3) The client calculates the complete signature (r, s) according to $D1$, r, $s2$ and $s3$, then outputs it as SM2 co-signature;

Figure 2 shows the detailed process of SM2 co-signature.

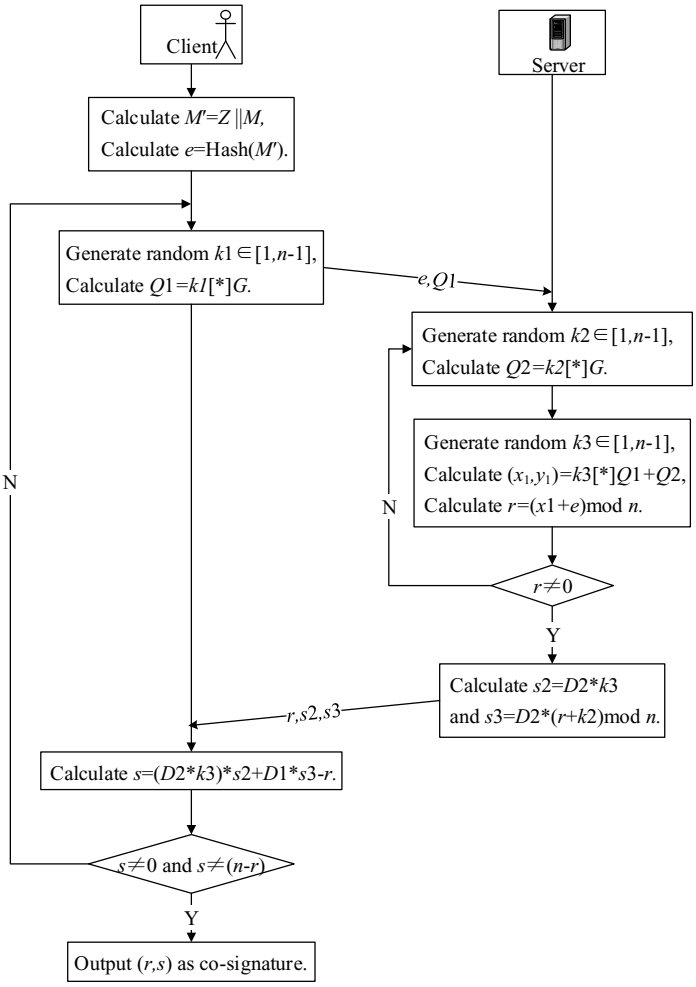

Figure 2 SM2 co-signature

3. Identity Authentication System Based on SM2 Co-signature

3.1. The System Model

The identity authentication system based on SM2 co-signature does not rely on the hardware cryptographic chip, and implements all functions such as reliable cryptographic operation and CA digital certificate operation in software, thereby it can replace the traditional USBKEY technology which implements the above functions in hardware. The system runs in the of the power IOT terminal devices and provides cryptographic computing support for the power IOT application. This system requires the integration of the software development kit (SDK) on the client and server, and the SDK provides the related functions of SM2 co-signature cryptographic operation [6][7].

The application process is as follows:

1) The application system initiates a signature request, and meanwhile pushes the signature request to the client and the server. The client and the server cooperate to calculate the user's public key and SM2 co-signature.

2) The server uses the public key to apply for a user certificate through the CA system, and then uses the user certificate to verify SM2 co-signature, and thus the identity of the client is confirmed.

It has been proved by practice that the SM2 co-signature result is correctly verified by the traditional SM2 signature verification method mentioned in the standard "GM/T0003-2012 SM2 Elliptic Curve Public Key Cryptography". So, the identity authentication system based on SM2 co-signature is reliable [8].

The application process is shown in Figure 3.

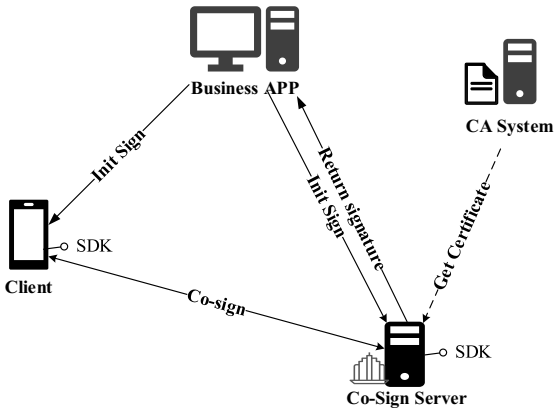

Figure 3 The identity authentication system based on SM2 co-signature

3.2. The System Features

1. Key split

The security design of the identity authentication system based on SM2 co-signature relies on the key split technology. The private key of the traditional SM2 algorithm is split into two parts: the client private key component and the server private key component. The client and the server store their own private key component separately so as to ensure the safe storage.

2. Two parties cooperate to sign

The client and the server calculate their own signature independently. Both of the signatures are used as intermediate results. No signature information can be deduced from the intermediate results. The server transmits the intermediate results to the client, and the client finally completes the final co-signature. The verification of the SM2 co-signature is completed by the server through the user certificate according to the traditional SM2 signature verification method mentioned in the standard "GM/T0003-2012 SM2 Elliptic Curve Public Key Cryptography".

3. Online signature

During the SM2 co-signature process, the client must maintain real-time interaction with the server, and both of them need to be online synchronously, thus the signature performance depends on the network environment.

4. Conclusions

Now the scale of the Power IOT terminal devices connected to the State Grid Corporation reaches tens of millions, and the terminal devices have the characteristics of wide variety, huge scale, wide application, diverse scenarios and complex networks. The identity authentication system based on SM2 co-signature does not rely on any additional hardware cryptographic module. It has strong compatibility, and can solve the security access problem of the diverse perception layer devices with limited computing resources effectively, thereby, an open, efficient and flexible power IOT cryptographic protection system will be built.

Compared with the traditional UKEY authentication technology, the security level of the lightweight identity authentication system based on SM2 co-signature is lower, because UKEY relies on the hardware cryptographic module. However, the authentication system based on SM2 co-signature adopts key split technique and various risk control measures. Only a part of the private key appears on the client or the server, and the complete private key does not appear at any time in the key cycle, which is different from UKEY authentication technology. This prevents the private key from the risk of exposure, and also there is no need for additional chip to store the private key. The chips are more expensive, especially when the number of devices is large, and this system is only to integrate SDK in the device. So, if this system is adopted, the cost will be reduced to a great extent, moreover, the application scenarios of the authentication system will be expanded greatly. The authentication system can also be applied to other fields such as finance, electronics and so on.

References

[1] HU Zhaohui, LIANG Zhiqiang. Research on authentication technique in electric power information system [J]. Computer Applications and Software, 2013, 30 (12): 318-321

[2] State Cryptography Administration. GM-T 0003-2012 Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves[S]. Beijing: Standards Press of China, 2010.

[3] Wang Zhaohui, Zhang Zhenfeng. Overview on public key cryptographic algorithm SM2 based on elliptic curves[J]. Journal of Information Security Research, 2016, 2 (11): 972-982.

[4] Feng Qi, He DeBiao. Efficient Two-Party SM2 Signing Protocol for Mobile Internet. Journal of Computer Research and Development. 2020, 57 (10): 2136-2146.

[5] Lin Jingqiang, Ma Yuan. Signature and decryption method and system based on SM2 algorithm suitable for cloud computing. Patent CN 104243456 B, 2014.

[6] Zhang Yong, Zhang Huan. Secret sharing scheme based on elliptic curve[J]. Computer Engineering and Applications, 2014, 50 (8): 90-92.

[7] Shang Ming, Ma Yuan, Lin Jingqiang. SM2 Elliptic Curve Threshold Cryptographic Algorithm [J]. Journal of Cryptography, 2014, 1(2): 155-166.

[8] Zhang QiuPu, Peng Zhu. A method system of SM2 Cooperative Signature which can verify the client's identity. CN 109246129 A, 2019.