Implementation of IC Card Authentication Method Based on Self-defined Algorithm

Jia LIU¹,², Xin KONG³, Yan-fang YUAN¹,², Peng HE¹,², Rui NIE¹,² and Hong ZHANG¹,²

¹State Grid Key Laboratory of Power Industrial Chip Design and Analysis Technology, Beijing Smart-Chip Microelectronics Technology Co., Ltd. Beijing 100192, China
²Beijing Engineering Research Center of High-reliability IC with Power Industrial Grade, Beijing Smart-Chip Microelectronics Technology Co., Ltd. Beijing 100192, China
³Beijing Redlink Information Technology Co., Ltd. Room1-3, South of Deshi Building, 9th East Street of Shangdi, Haidian District, Beijing

Keywords: IC card, Self-defined algorithm, Algorithm packet length, Anti-attack.

Abstract. The traditional IC card authentication method is single, once set, that can not be modified. In this paper, we propose an attack defense authentication method that can be used to define the authentication algorithm. IC card can be set according to the user's own algorithm authentication. This paper supports the algorithm can be divided into 8-byte packet and 16-byte packet algorithm of two algorithms, the certification can be specified by the type of algorithm to complete the IC card authentication in order to achieve a certain security permissions to complete the need Operation of the authority certification. In this paper, we propose an authentication method of attack defense, which can limit the maximum number of external authentication key attempts to ensure the security of the transmitted data in the case of illegal attack.

Introduction

One of the most important reasons for the rapid development and popularity of IC cards is that they provide a higher level of security through COS's security system. While the smart card was authenticated, you can get the security status of the smart card, to a certain extent the use of authority, to carry out some security-related operations.

Traditional smart card authentication is through the smart card and read and write devices at the same time both sides of the same random number for some of the same encryption operation, and then determine the consistency of the results of both operations to verify the legitimacy of smart cards, which also determine a Smart cards are not forged cards. According to the different object of authentication, it is divided into internal authentication and external authentication. The internal authentication is the authentication of the read / write device to the legitimacy of the smart card; the external authentication is the verification of the legitimacy of the read / write device by the smart card [1-2].

Currently used in the authentication algorithm, commonly used 3DES algorithm. But with the 3DES algorithm to break, making the chip's security has been threatened. If there are malicious users to malicious attacks, security problems are at stake. Because the encryption algorithm adopted in the authentication is fixed, the illegal users can adopt the fixed algorithm to attack. In addition, the traditional authentication methods can not adapt to the current and power consumption attacks [3-10]. In order to solve this problem, this paper designs an attack defense authentication method which can customize the algorithm environment. This authentication method allows the user to set the algorithm environment according to their application requirements. When the environment of the algorithm changes, the encryption algorithm adopted for authentication is also variable. At the same time, also provides a means of anti-attack, this means can effectively reduce the number of illegal users to try to attack, thereby increasing the difficulty of illegal users to crack.
Traditional Authentication Methods for IC Cards

The authentication method of traditional IC card is shown in Fig.1. Firstly, the validity of the random number is verified. If the verification is successful, the 3DES algorithm is used to encrypt the random number to get the authentication result. The authentication result is compared with the received authentication result. If the authentication result is the same, the authentication succeeds. If not, the authentication fails. In this case, the number of key attempts corresponding to the authentication needs to be reduced by one.

This authentication method has its own shortcomings, mainly as follows:

(1) the traditional authentication method fixed 3DES algorithm, the attack object can be based on the characteristics of 3DES algorithm, specifically for 3DES algorithm for malicious attacks. Such as: often used SPA, DPA attack means.

(2) the traditional authentication method to verify the results of the first comparison, and then subtract the number of keys that can try. But when the attack object analysis results are calculated and the input authentication results inconsistent, the IC card will automatically power-off operation, this time the program flow can not continue normally, then the corresponding authentication key to try the counter will not be reduced by one, So that the attack object can send an unlimited number of repeated authentication data until the correct key to try to finish the process.

Aiming at the above two shortcomings of common authentication methods, this paper redesigns the authentication order and authentication process, and designs a self-defined algorithm environment anti-attack authentication method.

Figure 1. Traditional IC card external authentication method.
Self-defined Anti-attack Authentication Algorithm Environment

Based on the traditional authentication method, we can get the attack defense authentication method which can be defined in the algorithm environment. As can be seen from the Fig.2, there are two improvements: one is to try to counter a module ahead of random number verification; the second is to provide a custom algorithm environment encryption method that allows the user to select the encryption algorithm, which Provide a variety of authentication algorithms, namely: 3DES algorithm, that is, 8-byte packet length algorithm, 16-byte packet length algorithm. Where: 3DES algorithm is the popular algorithm, 16-byte packet length algorithm can be any algorithm, as long as the packet length of 16 bytes can be. Which algorithm is used for authentication, which is determined by the application user according to their own needs. This increases the application of randomness and uncertainty, increasing the difficulty of attack.

In this paper, the existing authentication methods (internal authentication, external authentication) are improved, respectively, can be certified MF, DDF, ADF directory keys, or master (MK) key, so as to achieve a certain right.

![Diagram of External Authentication](image-url)

Figure 2. Attack against IC card external authentication method.
Self-defined Algorithm Command Design

The two parties use the algorithm specified by P1 bytes to authenticate. Authentication is divided into internal authentication and external authentication [14]. The format is shown in Table 1 and Table 2, respectively.

Table 1. Internal authentication command format.

| Code | Data | Le |
|------|------|----|
| Value | 00 88 | B8=0: the key in the current directory B7~b1: Key ID Le=08H, 3DES algorithm: 8 bytes after encrypting the authentication data; 16-byte packet length algorithm: the output of the encrypted "authentication data + inversion of authentication data", the first 8 bytes and the following 8-byte XOR result |

Table 2. External authentication command format.

| Code | Data | Le |
|------|------|----|
| Value | 00 82 | B8=0: the key in the current directory B7~b1: Key ID P2=0, The MK under the current DF Le does not exist |

(1) P1 indicates the user-defined algorithm environment. For example, '00' means SM1 algorithm, '01' means AES algorithm and '02' means 3DES algorithm.

(2) b1 ~ b7 of P2 are the key identification of the internal authentication key;

(3) Regardless of the authentication algorithm packet length used is 8 or 16, followed by the authentication data length Lc are 8;

(4) Regardless of the length of the authentication algorithm packet used is 8 or 16, the returned encrypted authentication data length Le is 8.

Authentication Procedure

In this paper, we propose an improved method for authentication against attack based on user-defined algorithm environment, which includes the following steps:

Step 1 The IC card generates a random number, which is encrypted according to the 3DES algorithm or the 16-byte packet length algorithm according to the user's designation, with the identification code, key, and random number generated by the card reader. Obtaining an encrypted stream;

Step 2 When using 16-byte packet length algorithm for internal authentication, since the packet length of the algorithm is 16 bytes and the input authentication data is only 8 bytes, and the input needs to be increased to 16 bytes, And 8 bytes of the 8-byte authentication data are combined together
to form 16 bytes, and the encrypted ciphertext length is 16 bytes. Since the output authentication data of the transmitted internal authentication command The length of 8 bytes, the need to get the results of 16 bytes, the first 8 bytes of data and the last 8 bytes of data XOR operation to get the final 8 bytes of authentication data, and then sent out;

Step 3 When the 16-byte packet length algorithm is used for external authentication, the received data format is the same as that of the above-mentioned internal authentication, and the IC card is required to use the "8-byte random number + 8-byte random number" After the external authentication key is encrypted, the 8 bytes are XORed before and after the 8-byte external authentication data. If the authentication is the same, the external device is valid; otherwise, the external device is considered illegal and the subsequent process is rejected.

When an external authentication is used, a counter for restricting the external authentication key is set to prevent malicious attack from the user. When the external authentication key is used for encryption, the designated external authentication key It can not be used for external authentication. If the number of times of using the key is greater than 0, it means that the key can be used for external authentication. Otherwise, the key is locked and can not be used for external authentication. The number of available external authentication keys is reduced by one. If the final external authentication succeeds, the number of times of using the specified external authentication key is restored to the maximum, so that the subsequent authentication can be continued.

Comparison of the Advantages of Authentication Methods

The advantages of the proposed authentication method, compared with the traditional authentication method, are shown in Table 3. As can be seen from Table 3, the proposed authentication scheme has higher security and applicability.

| Security attributes                  | The authentication scheme proposed in this paper | traditional authentication schemes |
|-------------------------------------|-------------------------------------------------|------------------------------------|
| Authentication method diversity     | Support multiple algorithms                      | only supports 3DES algorithm       |
| 16-byte authentication method       | support                                         | not support                        |
| Number of external authentication attempts | You can try up to 15 times                      | Can be numerous times              |
| Whether anti-attack                 | Anti-attack                                     | Not anti-attack                    |

Summary

In this paper, an improved IC card authentication method based on the user-defined algorithm environment is proposed, which enables the card to be authenticated according to different algorithms according to the user-defined algorithm environment, so as to change the value of the global security status register or local security state machine, Thus ensuring the diversity of authentication algorithms, but also improve the complexity of the command processing. In addition, in this paper, an attack prevention method is proposed, which can guarantee the security of data transmission in case of malicious attack by restricting the number of times of using external authentication key.

References

[1] Wang Ai-ying. Smart card technology [M]. Tsinghua University press, 2009.

[2] Xue Feng, Wang Ting, Wang Li-ping. Two smart card-based password authentication protocol security analysis [J]. Journal of Computer Applications, 2012, 32 (7): 2007-2009, 2021.
[3] Wang Ya-fei. Based smart card password authentication scheme [J]. Computer application and software, 2011, 28 (9): 295-297.

[4] Yang Li, Ma Jian-feng. Trusted smart card password mutual authentication scheme [J]. Journal of University of Electronic Science and Technology of China, 2011, 40 (1): 128-133.

[5] Gao Liang, Fang Yong, A smart card-based mutual authentication scheme [J]. Sichuan University Institute of Information Security, 2011, 2 (44): 85-86, 90.

[6] Wu Jian-wu. Remote password authentication scheme based on smart card [J]. Computer Engineering & Applications, 2007, 43 (33): 158-160.

[7] Zhang Xin, Feng Quan-yuan. Dynamic ID-based remote user authentication scheme [J]. Computer Engineering & Design, 2007, 28-3: 545-546, 557.

[8] Adleman L. Molecular Computation of Solutions to Combinatorial Problems [J]. Science, 1994, 266 (11): 1021-1024.

[9] Chen Liang; Cui Yong-quan; Tian Miao-miao; Fu Xiao-qing; Xu Peng; False Attack on Two Identity-Based Signature Schemes [J]; Journal of China Institute of Communication; 2013-02.

[10] Fu Qing-qin, Ang Zheng-quan, Yuan Yan-fang; An improved security strategy of smart card data transmission [J]; Computer Engineering & Science, 2014, 11(30): 2229-2233.