Research on the Development of China's Financial IC Card Chips

Jiefu Zhu 1, a
1College of science, Northeastern University, 110819 Shenyang, China

Abstract. Focusing on the financial IC chip technology that is urgently needed in China and the information security of IC card chips which is related to the security of the national financial system, this paper summarizes and researches into the development of China's financial IC card industry, the mainstream module, design standards and specifications, and major technical routes of card chips. In addition, it also centers round the security protection of financial IC card chips. Based on the analysis and introduction of mainstream international and national commercial cipher algorithm it studies the attacking modes and principles of power and electromagnetic analysis attacks and side-channel attack technologies faced by China’s IC card chips, and finally summarizes main protection technologies against various attacks.

1. Introduction
As chip-based bank cards, financial IC cards have excellent computing and storage capabilities compared to traditional magnetic stripe cards, dealing with a variety of financial services through the card operating system and applications. Besides, financial IC cards provide relatively secure financial smart terminal solutions based on various reliable international and state encryption algorithms. Since 2011, in the context of the global promotion of EMV migration in developed countries and the United States as the birthplace of credit cards as well as the leader of the global bank card industry, major financial institutions have begun to “test the water” and issue EMV standard financial IC cards. In China where integrated circuit products have become the largest bulk import trade products, the current research and development of integrated circuit technology with independent intellectual property rights has become a national strategy. Therefore, financial IC card chips, which are used as smart terminals for current and future financial systems, play a crucial role in the security of China’s financial system and are an integral part of the overall security outlook of the country.

1.1 Overview of China’s IC Industry
The Chinese government has given great support to the development of the integrated circuit industry, which is a strategic, basic and leading industry for national economic and social development, and is trying to make it an emerging industry featuring core technological competitiveness. At present, the annual import value of integrated circuit products in China has exceeded that of bulk commodities such as petroleum. According to the statistics released by American Semiconductor Industry Association, from the first quarter of 2014 to the first quarter of 2017, China’s global semiconductor sales market share increased from 26.37% to 32.61%, which was much higher than America’s 19.33%, Japan’s 9.29%, and Europe’s 9.61% in the first quarter of 2017, making China the largest market for semiconductor sales around the world. Relevant data showed that in 2000, China’s IC market consumption scale was only 94.5 billion yuan. In 2014, however, it rose to 1,039.31 billion yuan with an average annual growth rate of 21.4%, accounting for 50.7% of the global market. With the global
integrated circuit market gradually developing to the maturity stage, the growth rate of China's integrated circuit industry has slowed down in the past ten years. Nevertheless, the rapid development of the 3C fast-moving market and emerging industries represented by the Internet of Things and the Internet of Vehicles, and the rise of new technologies such as cloud computing and big data have all brought new growth points to the integrated circuit industry.

1.2 Development of China's Financial IC Card Industry
The financial IC card, a chip-based bank card, is a bank card with a chip as the medium, which includes various information including the storage key, digital certificate, and fingerprint and is equipped with multiple functions such as consumer credit, transfer settlement, cash access. As an important carrier of providing financial services to the people, financial IC cards have realized the upgrading of bank cards from a single payment function to an integrated service featuring information consumption. It is estimated that there are more than 3 billion magnetic bank cards in China to be migrated.

First is about the application of financial IC cards in horizontal industries. In order to implement the Notice of the People's Bank of China on Carrying out the Promotion of Financial IC Cards, the People's Bank of China selected 47 cities across the country to carry out pilot projects of applying financial IC cards in the field of public services as early as June 2011. In the past two years, the application of financial IC cards in the public service sector in both pilot and non-pilot cities has achieved breakthroughs in 28 industries of 7 major categories covering public transportation, social security, health care, culture and education, urban management, life services, and corporate services, which has effectively innovated methods of public services and created a new situation for financial IC cards to improve people’s wellbeing. In the field of public transportation, the financial IC card has realized convenient payment among buses, subways, taxis, highway ETCs, and even high-speed railways. In the field of health care, financial IC cards have the functions of making online appointment with many hospitals, searching medical record information, transferring hospital deposits, and paying medical expenses directly, which have effectively dealt with the difficulties featuring long registration time, long waiting time, long taking time and short consultation time for patients to get medical treatment. In the field of cultural life, functions of campus cards and even citizen cards have been realized, and financial IC cards can be used in multiple aspects of urban management. In the field of life services, many cities promote the use of financial IC cards in “standardized vegetable markets” and the construction of the traceability system for food safety. In the field of corporate services, the “industrial park card” has built a platform for enterprises and their employees to obtain comprehensive financial services.

Second is about the application of financial IC cards in vertical industries. Although current domestic chip manufacturers started late, they have already been equipped with relatively leading competitiveness in some market segments across the world. At present, China has established an independent chip security detection system to provide detection technology and service guarantee for the promotion and application of China's financial IC cards, facilitating domestic production of chips. After passing the safety certification, financial chip cards made by domestic chip manufacturers have entered the bank testing stage.

2. Core Composition of Card Chips and Main Technologies
The core technology of financial IC card chips involves multiple subdivisions such as computing, storage, communications, security, operating system, which is technically challenging and requires demanding craft precision.

2.1 The Core Module of Processor and Technologies Involved
Controlling access to the storage according to demands is realized by sending command analysis to external devices through a microprocessor. When accessed, the microprocessor provides the storage with the address of the accessed data unit and necessary parameters and then processes the
corresponding data transmitted by the processor based on that address. In addition, various operations involved in financial IC cards (such as encryption operations) are also performed by microprocessors.

2.2 The Module of EEPROM and Technologies Involved
The programmable read-only memory, which is point-erasable, is at the critical technology. The EEPROM eraser modifies contents taking Byte as the minimum unit by electronic signals without using other devices, which doesn’t require washing all the data to be able to write, thus completely eliminating the constraints of EPROMEraser and programmer. EEPROM adopts a memory chip that does not lose data after the power is turned off, on which data can not only be stored for at least 10 years, but be erased and written for more than 100,000 times.

2.3 The Module of RFID and Technologies Involved
Radio frequency identification (RFID) is a communications technology used to identify targets, and read and write data by radio signals, and the identified object itself should be equipped with devices receiving and transmitting electromagnetic wave. In recent years, radio frequency identification (RFID) technology has achieved rapid development and found increasingly wide application in various fields which are closely related to people’s production and life. Among them, the IC card, a breakthrough in the field of electronic technology application, is the most widely applied, whose technology realizes terminal communication through radio signals and non-contacts, thus solving the difficulty of passiveness and contactlessness.

2.4 The Module of Encryption and Hardware Implementation of Cryptographic Algorithms
It is advisable to apply various international and state secret algorithms, design cryptographic algorithm circuits, and adopt advanced encryption technology because of their advantages in high security, rigor, feasibility and convenience, and low costs etc. The application data file adopts an independent encryption system, which can not only verify the correctness of the information, but also check the legality of the identity of the two communicating parties, thereby ensuring the security of information transmission. It is realized by the mutual verification of the bank key stored in the card and the bank key stored in the card reader and the black box, thus ensuring that both the card holder and the card reader are legal.

2.5 Card Operating System
The internal operating system of IC cards, which is the management software in the smart card chips, is a system responsible for managing users’ information data and files. When operated, the system receives commands from the IC card reader, and then interprets and executes those commands. The card operating system consists of four smart card modules: communication management, security management, application management, and file management.

The module of communication management accepts commands from the IC card reader and determines their correctness. If the command is correct, it will be sent to the security management module for the next execution; otherwise, a signal requesting command resent will be issued. Communication between the smart card and the terminal device is realized in this way. The module of security management adopts multiple data encryption methods to verify the security of all commands and instructions, and ensures that monitoring communications does not affect data security. The application management module, which is often integrated into security management and file management, judges the feasibility of commands received, mainly controlling the permission for file access. The module of file management serves to manage the internal file data of the IC card which is stored in the IC card in the form of files. Therefore, the file management module is used for reading, writing and changing the internal file data, operations of which can be performed on a file only if the user has previously obtained the permission for doing so in the file system, thereby ensuring that the user's data file can only be legally accessed. There is only one file system on each card. Besides, multiple applications can be integrated into one according to the different needs of users.
2.6 Standards
As early as in the 1990s, the People's Bank of China has closely followed the international EMV migration process and embarked on relevant technical research. In 1997, it released the *China's Financial Integrated Circuit (IC) Card Standards (Version 1.0)*, which was revised in 2005 to form the *China's Financial Integrated Circuit (IC) Card Standards (Version 2.0)*, namely the PBOC2.0., establishing the unified standards for China's financial IC cards. In 2010, *China's Financial Integrated Circuit (IC) Card Standards (Version 2010)* came out. Based on Version 2010, the subsequent *China's Financial Integrated Circuit (IC) Card Standards (Version 3.0)* is compatible with the latest international general technical standards, which improves the function of small contactless payment, supports the application of dual-currency electronic cash payment, standardizes the technical requirements for the Internet terminal of IC cards, and enriches the system of security algorithm.

3. Encryption Algorithms
At present, most of the applied encryption technologies are symmetric and asymmetric, among which DES, RSA and AES algorithms are typical.

3.1 DES (Data Encryption Standard)
DES is by far the most widely applied and popular block cipher algorithm across the world, which uses a key of 56 bits in length and a plain text of 64 bits in encrypted length to obtain a 64-bit key.

By using a 56-bit key and an additional 8-bit parity check bit, DES produces a maximum packet size of 64-bit. This is an iterative block cipher, which employs a technique called Feistel to divide the encrypted text block into two halves. The first half is applied to the loop function, whose output and the other half go through the XOR operation together. Then the two halves are swapped, the process of which carries on and then ends at the last loop. DES involves 16 loops and the four basic operations of XOR: permutation, substitution, and shift, whose encryption process is as follows:

First is to decide on a specific plain text x and obtain x0 by permuting x with a fixed initial permutation IP. Let x0 = IP(x) = L0R0, where L0 is the first 32 bits of x0 and R0 represents the last 32 bits.

Second is to perform 16 rounds of operations that are exactly the same, where the data is combined with the key. The calculation rules are as follows:

\[ L_i = R_{i-1}, \quad 1 \leq i \leq 16 \]  
\[ R_i = L_{i-1} \cdot f(R_{i-1}, k_i) \]

Here \( f \) is a function, and \( k_1, k_2, ... k_{16} \) are functions of the key \( k \), each having a length of 48 bits, and together they constitute a key scheme. A round of DES encryption process is shown in Figure 1.

![Figure 1. A round of DES encryption process](image_url)
algorithm to be used for both encryption and decryption.

The first variable \( A \) of the function \( f(A, J) \) is a bit string of 32 bits in length, the second variable \( J \) is a bit string of 48 bits, and the output is bit string of 32 bits. The calculation process of the function is as follows:

a) The first variable \( A \) of the function is expanded to a bit string of 48 bits in length according to a fixed spread function \( E \).

b) \( E(A) \oplus J \) is calculated and the result is divided into 8 bit strings of 6 bits in length, denoted as \( B = B_1B_2B_3B_4B_5B_6B_7B_8 \).

c) Eight S-boxes \( S_1, S_2, S_3, \ldots, S_8 \) are used. Each \( S_j \) is a fixed order matrix of \( 4 \times 16 \), whose elements are integers ranging from 0 to 15. As for a bit string of 6 bits, for example, \( B_j = b_1b_2b_3b_4b_5b_6 \), \( S_j(B_j) \) is calculated with the following method: The row of \( S_j \) is determined with the integer \( r (0 \leq r \leq 3) \) of the two bits of \( b_1b_2 \). The column of \( S_j \) is determined with the integer \( c (0 \leq c \leq 15) \) corresponding to 4 bits. And the value of \( S_j(B_j) \) is the binary representation corresponding to the integer of the row \( r \) and the column \( c \) of \( S_j \). Let \( C_j = S_j(B_j) \), \((1 \leq r \leq 8)\).

d) The 32-bit string \( C = C_1C_2C_3C_4C_5C_6C_7C_8 \) is permute through a fixed \( P \), and the obtained result \( P(C) \) is denoted as \( f(A, J) \). The generation of the function \( f \) is shown in Figure 2.

\[ \text{Figure 2. Generating program of the DES function} \]

### 3.2 RSA (Rivest–Shamir–Adleman)

The public key cryptography RSA is a typical asymmetric cipher, whose theoretical basis is a special reversible modular exponential operation. Its security depends on the difficulty of factorizing large numbers. Description of this algorithm is as follows:

a) A set of big prime numbers \( p \) and \( q \) (decimal digits being over 100 are appropriately selected, namely over \( 10^{100} \)), which is kept private.

b) Let \( n = pq \) (kept public) and compute the Euler function \( \phi(n) = (p-1)(q-1) \) of \( n \) (kept private).

c) A small integer \( e \) (encryption key, public) is randomly selected to ensure that \((e, \phi(n)) = 1\), and \( e < \phi(n) \).

d) Then \( d \) (decryption key) based on \( ed \equiv 1 \mod \phi(n) \) is computed.

For each \( K = (n, p, q, e, d) \), \( n \) and \( e \) are kept public, but \( p \) and \( q \) are private. The encryption transformation is defined as

\[ E_K(x) = x^e \mod n, x \in Z_n \]  

The encryption transformation is as follows:

\[ D_K(y) = y^d \mod n, y \in Z_n \]  

The security of the RSA encryption algorithm depends on the difficulty of factorizing \( n \) into \( p \) and \( q \). Since the factorization of large numbers is a mathematical challenge and no one has been able to find an effective method, the security of RSA operations can be guaranteed. However, the drawback of RSA is that key generation is cumbersome and the calculation of encryption and decryption is very complicated and time-consuming. What’s more, the computing capability of smart cards is limited due to constraints on their shape and size, which limits the application of RSA encryption algorithms in
smart cards. Nevertheless, as technology advances, this problem has been largely resolved.

3.3 AES (Advanced Encryption Standard)
The AES (Advanced Encryption Standard), also known as the advanced encryption standard Rijndael encryption in cryptography, is a block encryption standard adopted by the US federal government. This standard, which is used to replace the original DES, has been widely analyzed and adopted by many parties around the world. After five years of selection, the Advanced Encryption Standard was published by American National Institute of Standards and Technology (NIST) on FIPS PUB 197 on November 26, 2001, and became an effective standard on May 26, 2002. In 2006, AES became one of the most popular algorithms among symmetric key encryption algorithms.

The length of AES encrypted data block packet must be 128 bits, but the key can be 128 bits, 192 bits, or 256 bits in length (if the data block length and the key length are insufficient, they will be made up). AES encryption has many rounds of repetition and transformation, whose general steps are as follows: 1) Key Expansion; 2) Initial Round; 3) Rounds, each repetition round including SubBytes, ShiftRows, MixColumns, and AddRoundKey; 4) Final Round, which involves no MixColumns.

AES has five modes: ECB, CBC, CFB, OFB, and CTR. ECB is a basic encryption method, whose cipher text is divided into blocks of equal length (insufficient ones will be made up). Those blocks are then encrypted individually, output one by one to form a cipher text. CBC is a cyclic mode, in which encryption is done after the XOR operation of the cipher text of the previous packet and the plain text of the current packet is performed. The purpose is to enhance the difficulty of being cracked. CFB and OFB are actually feedback modes, whose purpose is also to enhance the difficulty of cracking. The encryption results of ECB and CBC are different because they have different modes and CBC will be added an initialization vector in the first cipher block operation.

3.4 SM1 cryptographic algorithm
SM1 (SM1 cryptographic algorithm) is one of the most widely adopted national commercial cipher algorithms which are secure because the encryption process is kept private. The SM1 algorithm, a symmetry algorithm, is a commercial cryptographic group compiled by the National Cryptographic Authority. Besides, it is also the SM1 block cipher algorithm approved by the national password management department, whose packet length and key length are both 128 bits. Since the algorithm is not public, which exists in chips only in the form of IP core, its security strength and related hardware and software implementation performance are equivalent to the AES. The algorithm has already been applied to develop a series of security products such as chips, smart IC cards, smart cipher keys, encryption cards, and encryption machine, finding wild application in every sector of e-government, e-commerce and national economy.

4. Normal Attacking Modes and Main Prevention Techniques

4.1 Power Analysis Attacks
Due to its limited resources, financial IC card chips involve contradictions between efficiency and security when implementing anti-power attack. Currently, among all kinds of mainstream attack technologies, power attack is the most effective and widely adopted, posing serious threats to the security of financial IC card chips.

4.1.1 Security Attack
At present, most integrated circuits are fabricated from CMOS (Complementary Metal Oxide Semiconductor). The power model of CMOS gate-level circuit is as follows.

\[ P_{total} = P_{switch} + P_{short\_circuit} + P_{leakage} \]  

\( P_{switch} \) is the power consumption resulting from the charging and discharging of the load capacitor which is caused by logic gate flipping; \( P_{short\_circuit} \) is the power consumption caused by the short-circuit current; and \( P_{leakage} \) is the power consumption arising from current leakage. Among them, \( P_{switch} \)
accounts for the most of power consumption of the circuit, which is closely related to whether the logic gate is flipped. Therefore, the 0/1 state of the computing data in the circuit must have a certain correlation with power consumption, which is a physical basis of DPA attack.

Taking the DES algorithm as an example, the main steps of the DPA attack are as follows:

a) A large amount of plain text is randomly generated and encrypted, and the power consumption curve of the encryption operation is then recorded.

b) The first bit output from the first S box in the first round are observed. Then the 6-bit key corresponding to the first S box is guessed, whose corresponding plain text is used to compute \( b \).

c) The power consumption curve is divided into two categories of \( b=0 \) and \( b=1 \) based on the value of \( b \).

d) The average power consumption curve of these two categories is calculated, and the differential power consumption curve is then obtained by subtracting the two curves.

e) The power consumption curve obtained in the fourth step is observed. If the guess of the key is correct, the grouping in the third step is correct and a significant peak will appear in the differential power consumption curve. Therefore, the attacker judges whether the guess of the key is correct by observing the peak value.

f) Steps from b) to e) are repeated to obtain other sub-keys.

In this way, the complete 48-bit key information can be determined by the spikes in the differential trace. Then the exhaustive search is adopted or analysis of the next round is continued, which can help easily determine the remaining 8-bit key.

4.1.2 Mainstream protection

The current mainstream protection solutions are based on an asymmetric mask. The core idea of the DES scheme is that the mask values and positions added to the DES in the first and last rounds are different from those of other rounds, so that the mask cannot be eliminated when the Hamming distance model is adopted. The specific process of this scheme is shown in Figure 3.
Figure 3. The protection process of the Mask technology
The asymmetric mask DES algorithm keeps the same process as the original DES process before the first sub key K1 operates on the data. The mask x is introduced after the sub key R_{16} conducts XOR operation on the plain text in the first round. The encryption process of the following 2~15 rounds goes through similar operation, only differing in the random values of XOR, which is designed to maintain the correctness of the P_2 processing in the middle of the algorithm. Finally, conduct XOR operation on mask x before the 16th round is output, which is added with mask 4 to restore the real plain text information after the inverse permutation of IP. It can be seen from this method that the mask is superimposed onto the register only after the information of the key is introduced. And then the random number directly affects the flipping of the register, thereby changing the actual power consumed by the algorithm. If the algorithm also adopts the CPA attack, the value after IP permutation and the value output by the first round are still selected as attack points. Taking the first round as an example, the Hamming distance between the value after IP permutation and the value output by the first round in this scheme is as follows:

\[ H_D = R_y(R_x) = I(M)_{32-63} R_x X_1 \]  \hspace{1cm} (6)

This demonstrates the 32-63 bit part of the data after the plain text goes through initial permutation and the 32-63 bit part of the data output by the first round, which proves that the Hamming distance of this scheme becomes a random number because it goes through the XOR operation with the random number x1. As for the original DES, the Hamming distance is still:

\[ H_D = R_y R_x = I(M)_{32-63} R_x \]  \hspace{1cm} (7)

The effects of random numbers are eliminated. It can be seen that due to the introduction of random numbers, the Hamming distance of this scheme is different from that of the standard DES. That is, the attacker can’t reflect the actual power consumed by use of the Hamming distance model. Therefore, for the CPA attack, correlated coefficients can’t obtain the maximum even if the guess of the key is correct.

4.2 Electromagnetic analysis Attacks

4.2.1 Security Attack

Electromagnetic attacks are powerful side channel attacks, which can detect electromagnetic radiation of cipher chips in a non-invasive way, and can find the best attack area on the surface of the cipher chips to perform differential electromagnetic attacks. Therefore, it can avoid various anti-side channel attacks of cipher chips, posing a great threat to the security of those chips.

Electromagnetic correlation attacks take advantage of the dependence of cipher chips on data when facing electromagnetic leakage, whose core idea is to compute the assumed electromagnetic leakage value at a certain moment through model simulation. This value is highly related to the corresponding intermediate value of electromagnetic leakage processed by the actual cipher chip at a certain moment.

CEMA attacks involve the following five steps.

First is to select an intermediate value of the algorithm executed (in this case, AES). This intermediate value must be a function \( f(d, k) \), where d is generally plain text or cipher text, k is a part of the key (usually a byte), and f is the corresponding function of one or several consecutive operations of the encryption algorithm.

Second is to measure the electromagnetic leakage. As for encryption or decryption for D times, the attacker first needs to know the corresponding value in order to calculate the intermediate value in the first step. These known values are denoted as vectors \( d = (d_1, \ldots, d_D) \), which represent the data value (plain text or cipher text) corresponding to the encryption and decryption at the time of \( i \). During each encryption or decryption, the attacker logs a trace of electromagnetic leakage. The energy trace corresponding to the data is formulated as follows.

\[ \rightarrow (t_{i1}, \ldots, t_{iT}) \]  \hspace{1cm} (8)

Here \( T \) represents the length of the electromagnetic trace (the number of sampling points). When
the operation going through for D times, a D * T sized matrix is obtained to represent D (the number) electromagnetic leakage traces. DFDDDD

Third is to calculate the assumed intermediate value. The next step of the attack is to calculate the corresponding assumed intermediate value for each possible k value, and record these possible values as k(k1, .., kk ), which are named as the key assumption. Once the data vector d and the key assumption k are decided, the attacker can calculate the assumed intermediate value f(d, k) for all operations of D times and all key assumptions, and obtain a D*K sized matrix v of the intermediate value.

Fourth is to map the intermediate value to the electromagnetic leakage value. The electromagnetic leakage value here refers to the assumed value. The attacker selects a model and then maps the assumed intermediate value matrix to the matrix H of the assumed value of electromagnetic leakage.

Fifth is to compare the assumed electromagnetic leakage value with the electromagnetic leakage trace collected in the second step. Compare each column of H (K columns in total) with each column of T (T columns in total), and then conduct a correlation analysis to obtain correlated K*T sized matrix R, whose element r_{ij} represents the correlation degree of columns h_i and t_j. The correlation coefficient is calculated with the following equation:

\[ r_{ij} = \frac{\sum_{d=1}^{D} (h_{d,i} - \bar{h}_i)(t_{d,j} - \bar{t}_j)}{\sqrt{\sum_{d=1}^{D} (h_{d,i} - \bar{h}_i)^2} \times \sqrt{\sum_{d=1}^{D} (t_{d,j} - \bar{t}_j)^2}} \] (9)

Here \( \bar{h}_i \) and \( \bar{t}_j \) represent the average of \( h_i \) and \( t_j \). The larger the value of \( R_{ij} \) is, the better the matching of columns \( h_i \) and \( t_j \) is. Finding the largest element \( r_{ck,ct} \) of the matrix \( R \) can help get the correct key index \( ck \) and then process the time point \( cd \) of the corresponding intermediate value.

4.2.2 Mainstream protection

S-box is the only nonlinear component in the AES algorithm and demonstrates high utilization rate, directly determining the function, performance, and anti-side channel attack capability of cipher chips that adopt the AES algorithm. The key to resisting side channel attacks is to eliminate the correlation between data and side channel information. Currently, researchers have proposed some logic circuits that can reduce such data correlation, representative of which include dynamic differential cascade voltage switch logic (DDCVSL), dual-rail random switching logic (DRSL) mask.

References

[1] KOCHER P, JAFFE J, JUN B. Differential power analysis[C].Proceeding of Advances in cryptography (CRYPTO’99).1999: 388—397.
[2] BIHAME E, SHAMIR A. Differential fault analysis of secret key cryptosystems[C]. Proceeding of Advances in Cryptology, 1997, 1294: 513—525
[3] Ji fang Jin, Er hong Lu, Xian wei. GaoAn Efficient Algorith for DPA resistent RSA[C]. APCCAS, 2006: 1659- 1662.
[4] Yang Aiyun, Research on the Countermeasures to Promote the Development of China's Financial IC Card [J]. Financial Development Review, 2010: 10.
[5] Wang Aiyin, Smart Card Technology, Beijing: Tsinghua University Press: 2000.
[6] Xu Zhikai, Application and Expansion of Financial IC Card in Hainan [D]. Hainan Finance, 2000: 08.
[7] Xu Zhijie & Leijing & Li Yongbin, Study on the Security Technologies of the Smart Card [J]. Modern Electronics Technique, 20.
[8] Chen Zuobing & Chen Yan, Research on CPU Card Technology and Its Application System Design [J]. Journal of Wuhan University of Technology, 2002(9): 85-8.
[9] Wang Zhen, System Design Based on Embedded Implementation of SM1 Algorithm [J]. Electronics World, 2012(3): 119-120.
[10] Pang Jinxiang, Design and Construction of Campus Card Accounting System [J]. China Management Informationization, 2017, 20(17): 56-57.
[11] Han Jun & Zeng Xiaoyang & Tang Tingao, VLSI Design of Anti-Attack DES Circuits [J]. Journal of Semiconductors, 2005, 26(8): 1646.
[12] Chen Zhimin, Side Channel Power Analysis on Secure Integrated Circuits and Countermeasures [D]. Shanghai: Shanghai Jiao Tong University, 2007.