World Wide Web (2020) 23:1423–1440
https://doi.org/10.1007/s11280-019-00715-8

Secure limitation analysis of public-key cryptography for smart card settings

Youliang Tian[1] · Qiuxian Li[1] · Jia Hu[2] · Hui Lin[3]

Received: 1 February 2019 / Revised: 22 April 2019 / Accepted: 29 July 2019 /
Published online: 22 August 2019

Abstract
Smart cards are widely used in high security applications due to their self-contained nature. At the same time, the security of smart card has become an urgent problem in the field of intelligent environment. Public-key Cryptography is the main means to solve the security problems based on smart card password authentication and identity authentication protocol. This paper reviews the security issues of public key cryptography used in smart cards from the perspective of information theory. By constructing a attackers channel, we model the Public-key Cryptography process in the way of an adversary to capture the attack ability in the Public-key Cryptography setting. Then, we convert the secure problems of Public-key Cryptography into the attack channels capacity of adversaries that the maximum value of the average mutual information is the secure limitations of a Public-key Cryptography scheme, which is a reachable theoretic limitation of secure communication parties. Finally, we give the bounds of insecure for public-key encryption and signature in different secure levels, and analyze and discuss the secure limitation.

Keywords Public-key cryptography · Smart card · Information theory · Secure limitation · Public-key signature

1 Introduction

The smart card [6] is a miniature electronic device that contains a storage medium and an integrated circuit. It plays two important roles in the application system [22, 30]: identity

This article belongs to the Topical Collection: *Special Issue on Smart Computing and Cyber Technology for Cyberization*
Guest Editors: Xiaokang Zhou, Flavia C. Delicato, Kevin Wang, and Runhe Huang

✉ Youliang Tian
youliangtian@163.com

[1] State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang 550025, China

[2] College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter, EX44QF, UK

[3] College of Mathematics and Informatics, Fujian Normal University, Fuzhou, 350117 China

and security. Due to its low cost, convenient to carry, and the ability to improve security through cryptographic algorithm, it has been widely used in communication, banking, transportation, access control and other fields. In the past few decades, the computing power on smart cards has developed rapidly. Smart cards based on public keys are widely used in various fields, and their applications tend to be diversified. The development of semiconductor technology has improved the capabilities, practicability and accessibility of smart cards. The use of a variety of smart card features, as well as the use of smart cards that are versatile in the future, will make their security, especially user identity authentication and privacy protection become extremely challenging.

In smart card security, there are three main types of attacks. They are: (1) Invasive attacks: These attacks require the microprocessor in the smart card to be removed and attacked directly by physical means. However, these attacks often require very expensive equipment and significant time investment to produce results. (2)Semi-Invasive Attacks: These attacks need to expose the chip surface. Then, the attacker tries to destroy the security of the secure microprocessor without directly modifying the chip. Gandolfi attacks smart cards by analyzing the electromagnetic power radiation of smart cards [11]; Quisquater proves that electromagnetic attacks achieve at least the same results as power consumption [26]. (3) Non-Invasive Attacks: These attacks seek to obtain information without modifying the smart card, i.e. the security microprocessor and the plastic card are not affected. Attackers will attempt to obtain information by observing information leaked during the calculation of a given command or by attempting to inject failures using mechanisms other than light. Kocher found that the time information leaked during the operation of smart card can be used for cryptanalysis, and successfully used time attack to crack the DH key exchange protocol and RSA cryptographic algorithm [16]. After that, Kocher used dozens of power consumption curves to crack DES cryptographic algorithm [17]. Jiang [25] et al have improved the design defects of privacy aware authentication scheme for distributed mobile cloud computing services,including the problem of biometrics misuse, wrong password, and fingerprint login, no user revocation facility when the smart card is lost/stolen. Later, Tian [29] et al have proposed a rational delegation of computation protocol, which is an important technology of mobile Internet at present, which is significant to the construction of intelligent urban computing. In order to close to practical applications, many tasks need cooperation with edge computing and cloud computing.

Although there are many attacks on smart cards, the security of smart cards mainly depends on the complexity of the embedded cryptographic algorithm and authentication protocol, that is, the security of Public-key Cryptography used by smart cards. Public-key cryptography is well suited for applications such as smart cards, which are mobile devices with limited storage and computing power. In recent years, Side channel attack (SCA) is a fast, low-cost and powerful attack method for cryptographic chips, because it can effectively obtain key data and keys in cryptographic chips, which seriously threatens the security of smart card chips. Traditionally, the security of cryptographic chips depends on the complexity of cryptographic algorithms and authentication protocols embedded in them, and most of the chips adopt CMOS technology [21]. Different from existing mathematical analysis methods, Kocher [16] et al. found that the time of operation time leakage of cipher chip could be used for cipher analysis, and successfully used the time attack method to crack Diffie-Hellman key exchange protocol and RSA cipher algorithm. Messerges [19, 20] et al. They have analyzed the power consumption achieved by the public key cryptography algorithm of smart card, and proposed a method to maximize the peak value of differential energy analysis (DPA). At present, many scholars have proposed some anti-power attack

schemes [7, 18]. Jiang [14] et al propose an integrated AKA framework for public key cryptosystem that integrates the single-server 3-factor AKA protocol and the non-interactive identity-based key establishment protocol, and evaluate its performance based on a simulated experimental platform. However, smart cards are often sensitive to the implementation cost and efficiency of schemes due to the limitations of their internal resources and computing speed. In order to improve the performance and security of smart card products, we need to design algorithms with higher efficiency and security, among which the elliptic curve scalar multiplication technology [13, 15] has become a current research hotspot. With the standardization and standardization of smart card development, the future development of smart card field has provided a huge power [5, 12]. Figure 1 is the smart cards security and application scenario diagram.

Public-key Cryptography is the most important invention and development of modern cryptography. Since Diffie and Hellman proposed the public key cryptography in 1976 [10], scholars have come up with a number of public key cryptography schemes, such as RSA [27], ElGamal system [4, 28], McEliece [23], backpack system, etc [1, 24]. Many researches has been done into methods for designing encryption schemes that are both practical and could be analyzed formally [2]. Bellare and Rogaway proposed the stochastic prediction model. In this model, the cryptographic hash function is assumed to be completely random. In provable secure public key cryptosystems, the traditional Chosen Plaintext Attack (IND-CPA) [31] model has a relatively low security level. Naor and Yung [9] propose Adaptive Chosen Ciphertext Indiscernibility (IND-CCA2) is the model with the highest level of security in provable security theory. In 1998, Cramer and Shoup (CS98) constructed a public-key encryption algorithm for Adaptive Chosen Ciphertext Attack (CCA) security based on standard model [8]. In 2005, Boyen, Mei and Waters (BMW) gave a secure encryption algorithm [3] for CCA using Waters identity-based encryption algorithm [32]. The BMW algorithm has a prominent feature: before decryption of ciphertext, there is a verification algorithm that can determine the integrity of ciphertext without inputting any private key, and it can

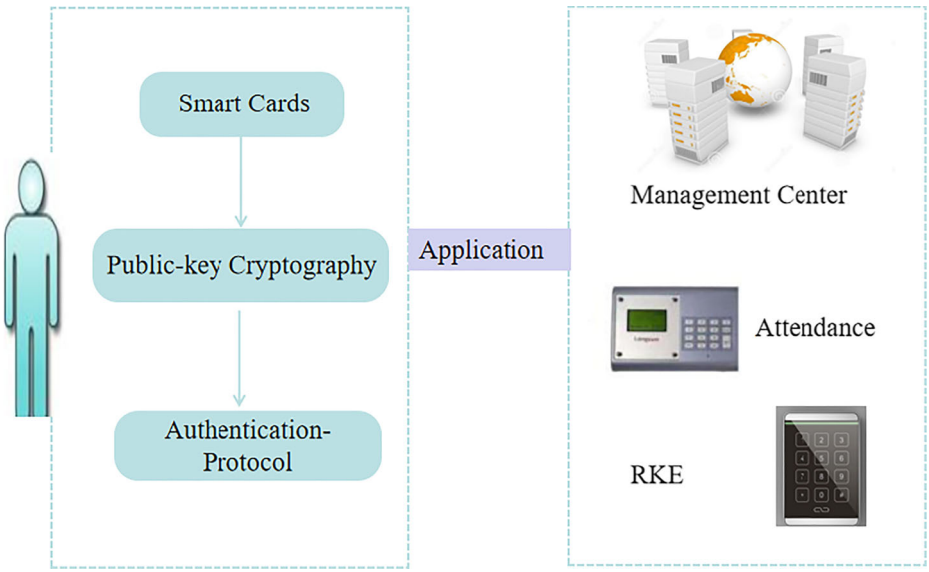

Figure 1 Smart cards security and applications

ensure the correctness of the plaintext message after decryption. The verification algorithm is called public ciphertext integrity verification because it does not need to input the private key. In the above public-key cryptography based on the adversary attack model, the security of the scheme is proved, but the quantization of the security limit is not considered. This paper is motivated by the goal of finding *secure/insecure limitation* of Public-key Cryptography schemes in the standard model, in perspective of the convertible attack channels capacity of adversaries. We mainly analyze the security of common public cipher algorithm used in smart cards and its security, and give the security boundaries of different cipher algorithms and their mathematical relations.

Our contribution We transform the security problem of smart card into the security problem of its PKC algorithm. One may hope to obtain secure or insecure limitation of a Public-key Cryptography algorithm by using naive construction of the convertible attack channel of adversaries, in which the secure problems of Public-key Cryptography is transformed into its capacity. According to this line of thought, we propose several attack channel models based on Shannon information theory in this paper. The average mutual information and conditional mutual information of information theory are used to describe plaintext-ciphertext metric, plaintext leakage metric, plaintext metric and leakage metric with background knowledge in adversary attack channel. The key point is to treat the attack system as a communication model. The security limitations of Public-key Cryptography encryption and signature under different types of attacks, that is, the security limitation of smart cards under different Public-key Cryptography algorithms are analyzed and described.

2 Public-key cryptography

The publication of Diffie and Hellman's New Directions in Cryptography was a landmark in computer cryptography. Based on this, the concept of a public key cryptography has emerged. It has two important principles: First, the encrypted ciphertext must be secure under the premise that both the encryption algorithm and the public key are public. Second, all cryptographers and decryptors with private secret keys are required to calculate or handle them in a relatively simple manner, but for others who do not have secret keys, deciphering them should be extremely difficult. In recent years, public key cryptography has been combined with technologies such as PKI, digital signature, and e-commerce to ensure the confidentiality, integrity, validity, and non-repudiation of online data transmission, and has played a huge role in network security and information security.

Figure 2 is a graph of asymmetric cryptography. In this asymmetric cipher model, both Alice and Bob have two keys, a public key which is exposed to anyone is used to encrypt

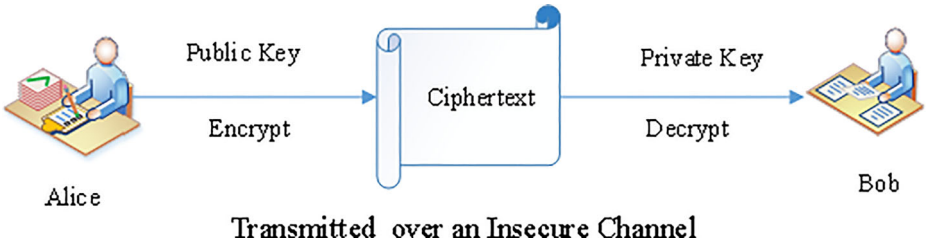

Figure 2 The basic model of public-key cryptography

messages to that person, and a private key which is kept secret is used to decrypt messages. So if Alice wants to send a message to Bob, she gets Bob's public key which can be published in a key directory, and encrypts her message by using Bob's public key. She then sends the message to Bob. When Bob receives the message, he uses his private key, which is known by himself, to decrypt Alice's message. Even if Eve intercepts Alice's message, she can not decrypt it. Because only the person with Bob's private key can decrypt a message encrypted with his public key and Bob keeps his private key secret from everyone.

The keys in the public key cryptography algorithm are classified according to their nature and can be divided into two types: public key and private key. The user or system generates a pair of keys, one of which is disclosed as a public key, and the other is reserved, called a private key. Anyone who knows the user's public key can encrypt the information with the user's public key and interact with the user to implement secure information. Due to the dependencies between the public key and the private key, only the user itself can decrypt the information, and any unauthorised user or even the sender of the information cannot decrypt the information. In the study of modern public key cryptography, their security is based on intractable computable problems. Such as large number decomposition problem, computation of finite field discrete logarithm problem, square residual problem and logarithm problem of elliptic curve.

Based on these problems, there are various public key cryptographys. There are numerous studies on public key cryptography, mainly focusing on Research on RSA public key system Research on elliptic curve cryptography, Research on various public key cryptographys and Research on digital signature.

2.1 The RSA algorithm

In 1978, Rivest, Shamir and Adleman proposed the RSA algorithm which is a well-recognized public key cryptographic algorithm. The RSA algorithm is the most effective security algorithm for secure communication and digital signature on the network. Its security is based on the difficulty of large prime decomposition in number theory. The more difficult the factorization, the harder it is to decrypt the ciphertext and the higher the encryption strength. Its public key and private key are functions of a pair of large prime numbers. The research status of factorization theory shows that the RSA key used requires at least 1024 bits to ensure sufficient long-term security.

The RSA algorithm is based on exponentiation in a finite field over integers (mod p) where p is a prime. And the security of the RSA algorithm lies in the big integer factor problem. It is easy to compute $n = p * q$, while it is very difficult to do the reverse. That is, it is extremely computationally expensive to find the prime factors of a large composite number.

2.2 The ElGamal algorithm

ElGamal proposed a double-key cryptography based on discrete logarithm problem in 1984, which can be used for both encryption and signature. It is a public key cryptography based on the difficulty of solving the discrete logarithm problem over finite multiplicative groups. The cryptography is still considered to be a public key cryptography with good security performance. There are ElGamal public key cryptography based on the multiplicative group $Z_p{}^*$ and the public key cryptography on any finite cyclic group.

The basic ElGamal encryption scheme is described as follows:

1. *Gen* algorithm: Public key p, g and y, where p is a large prime number, $g < p$, $y = g^d \bmod p$. Private key d, $2 \leq$ d $\leq$ p - 2.
2. *Encrypt* algorithm: Select random number r, where $2 \leq r \leq p - 2$. Ciphertext: $c = g^r \bmod p$, $c' = my^r \bmod p$.
3. *Decrypt* algorithm: Plaintext $m = \frac{c'}{c^d \bmod p}$.

ElGamal's security is based on DLP, and more strictly based on DHP. This algorithm can realize two-way identity authentication between the two parties, and effectively prevents the attacker from pretending to be a sender to forge a message. At the same time, the algorithm adds information that can track the source of the message during the communication process, so that the receiver can effectively verify the authenticity of the message. By double protection of the message, the system realizes secure communication on the public channel.

2.3 The SM2 algorithm

SM2 is the standard of public key cryptography in China, as well as it is a elliptic curve public key cryptography(ECC). Koblitz and Miller independently propose to apply elliptic curve to public key cryptography. The properties of the elliptic curve based on the ECC are as follows:

1. The elliptic curve in the finite domain constitutes a finite exchange group under the point addition operation, and its order is similar to the scale of the fundamental domain.
2. Similar to the power operation in the finite field multiplication group, the elliptic curve multi-point operation constitutes a one-way function.

SM2 algorithm includes digital signature algorithm, key exchange protocol, public key encryption algorithm and system parameters. The public key encryption algorithm requires the sender to encrypt the message with the receiver's public key, and the receiver uses its private key to decrypt the received message and restore it to the original message. SM2 public key encryption algorithm is designed based on the generalized ELGamal encryption algorithm, but the security level of the generalized ELGamal encryption algorithm is not high enough to reach the security of IND- CCA2. SM2 public key encryption algorithm for the security of the IND- CCA2.

3 Security limitation of encryption

The adversary Eve intercepts the ciphertext sent by the sender Alice to the receiver Bob, and assumes that the channel of disclosure of the plaintext is an adversary attack channel.

A random variable M is used to represent the message space composed of all plaintext, $M = \{m_1, m_2, \cdots, m_t\}$, where $i = 1, 2, \cdots, t$; The information set obtained by the adversary is represented by the random variable C, which is composed of all the messages obtained by the adversary, this is $\{c_1, c_2, \cdots, c_n\}$, where c_j $(j = 1, 2, \cdots, n)$ is a ciphertext message obtained for an adversary. Accordingly, a specific PKC encryption algorithm can be regarded as a way to transform and encode plaintext messages, which can protect information. The whole encryption algorithm constitutes a clear text protection mechanism space. The method of mining and analyzing plaintext information under certain background knowledge is called plaintext attack.

Based on this assumption, the communication framework based on Shannon information theory will be used to analyze the security limitation of the adversary in PKC under four

attack scenarios: Ciphertext-only Attack, Chosen Plaintext Attack (CPA), Chosen Ciphertext Attack (CCA) and Adaptive Chosen Ciphertext Attack (CCA2). We propose several attack channel models, including Ciphertext-only Attack Channel Model, Chosen Plaintext Attack Channel Model, Chosen Ciphertext Attack Channel Model and Adaptive Chosen Ciphertext Attack Channel Model.

3.1 Ciphertext-only attack (COA) channel model and security limitation

We first assume that the adversary has no attack ability and the adversary only observes the ciphertext information through the channel and only considers the discrete single plaintext source. The model definition is shown in Figure 3.

Assume the mathematical model of M be expressed as

$$\begin{pmatrix} M \\ P(M) \end{pmatrix} = \begin{pmatrix} m_1 & m_2 & \cdots & m_i & \cdots & m_t \\ p(m_1) & p(m_2) & \cdots & p(m_i) & \cdots & p(m_t) \end{pmatrix}$$

where $0 \leq p(m_i) \leq 1, \sum_{i=1}^{t} p(m_i) = 1$. Similarly, the mathematical model of C can be expressed as

$$\begin{pmatrix} C \\ P(C) \end{pmatrix} = \begin{pmatrix} c_1 & c_2 & \cdots & c_i & \cdots & c_t \\ p(c_1) & p(c_2) & \cdots & p\left(c_j\right) & \cdots & p(c_n) \end{pmatrix}$$

where $0 \leq p\left(c_j\right) \leq 1, \sum_{j=1}^{n} p\left(c_j\right) = 1$.

For this model, the plaintext entropy $H(M)$ is defined as

$$H(M) = -\sum_{i=1}^{t} p(m_i) \log_2 p(m_i)$$

$H(M)$ is used to describe the average mutual information of plaintext. The $H(M)$ is greater, the possibility of plaintext disclosure is less, thus the ability of hiding plaintext is stronger. This value is a definite value when no external conditions affect it.

When Eve acquires some ciphertext information, the conditional entropy $H(M/C)$ can be introduced to characterize the uncertainty of the plaintext source, which is defined as

$$H(M/C) = -\sum_{j=1}^{n} \sum_{i=1}^{t} p\left(m_i c_j\right) \log_2 p\left(m_i/c_j\right)$$

The conditional entropy denotes the uncertainty of the plaintext M after receiving C. The uncertainty is caused by the interference (plaintext protection) between the Alice ciphertext transmission channel and the Eve attack channel, that is, during the long term observation of

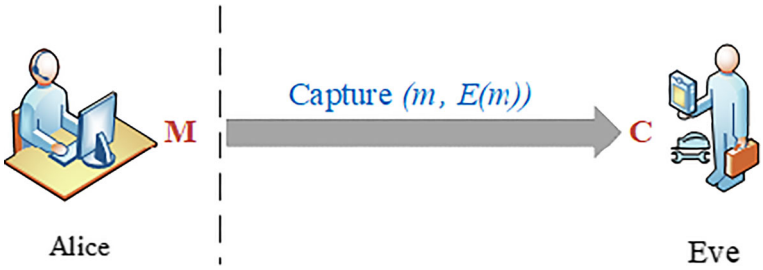

Figure 3 COA channel model

the plaintext source, because of some public key encryption protection mechanism of plaintext, there are still some unknown information sources. It is easy to prove that this plaintext information entropy satisfies the basic properties of Shannon source entropy. That is, it has non-negativity, symmetry, extensibility, certainty, additivity, extremum property, upper convexity, etc., and satisfies the maximum discrete entropy theorem. No more repetition.

In this paper, we introduce ciphertext average mutual information $I(M;C)$ to describe the degree of plaintext leakage on the channel, which is defined as

$$I(M;C) = \sum_{j=1}^{n}\sum_{i=1}^{t} p(m_i c_j)\log_2 \frac{p(m_i/c_j)}{p(m_i)}$$

$I(M;C)$ represents the average mutual information between the plaintext M and the ciphertext C, that is, the amount of plaintext information on the attack channel. It can describe the degree to which the adversary acquires the plaintext information from the ciphertext as a whole, so it can be used as a security measure for the disclosure of plaintext. Therefore, the maximum extent of plaintext leakage is the maximum value of the average mutual information between M and C, that is $I_{MAX}(M;C)$. In this case, the security limitation of PKE under ciphertext-only attack model is the lowest.

3.2 Chosen plaintext attack (CPA) channel model and security limitation

The information entropy model of ciphertext attack proposed in the previous section objectively describes the problem of ciphertext measurement in the absence of the adversary's ability to attack. In the actual system, there is often a ciphertext attack analysis. The adversary can analyze the attack under certain background knowledge. For example, in the Chosen Plaintext Attack, the adversary not only has known 'plaintext-ciphertext pairs', but also can choose the encrypted plaintext and obtain the corresponding ciphertext. In this case, the adversary can choose a specific block of plaintext data to encrypt, and compare the plaintext with the corresponding ciphertext to analyze and find more information related to the key. The model definition is shown in Figure 4.

In this model, Z represents the knowledge space of the plaintext-ciphertexts pair known to the adversary, and its mathematical model can also be defined as

$$\begin{pmatrix} Z \\ P(Z) \end{pmatrix} = \begin{pmatrix} z_1 & z_2 & \cdots & z_k & \cdots & z_l \\ p(z_1) & p(z_2) & \cdots & p(z_k) & \cdots & p(z_l) \end{pmatrix}, 0 \le p \le 1, \sum_{k=1}^{l} p(z_k) = 1$$

The adversary can use the plaintext-ciphertext pairs Z to enhance the attack on the plaintext. For the attacker, he can combine the ciphertext message $C'(C' \in C)$ through the selected

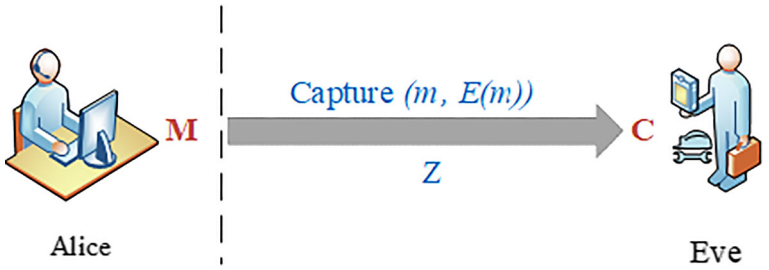

Figure 4 CPA channel model

plaintext and the plaintext-ciphertext pairs Z to attack, introducing the attack conditional entropy:

$$H(M/CZ) = -\sum_{j=1}^{n}\sum_{i=1}^{t}\sum_{k=1}^{l} p(m_i c_j z_k)\log_2 p(m_i/c_j z_k)$$

The $H(M/CZ)$ reflects the uncertainty about M that still exists after the adversary selects the ciphertext message C and the plaintext-ciphertext pairs Z, which can actually be used as the uncertainty of the plaintext under a certain attack method. Similarly, the attack average mutual information is further defined as:

$$I(M; C/Z) = -\sum_{j=1}^{n}\sum_{i=1}^{t}\sum_{k=1}^{l} p(m_i c_j z_k)\log_2 \frac{p(m_i z_k/c_j)}{p(m_i/z_k)p(c_j/z_k)}$$

$I(M; C/Z)$ reflects the average mutual information between C and M under the condition of Z, that is, the adversary obtains the amount of plaintext information, and also describes the degree of plaintext leakage under the attack with plaintext-ciphertext pairs. Therefore, the maximum extent of plaintext leakage is the maximum value of the average mutual information between the M and the C, that is $I_{\max}(M; C/Z)$. In this case, the security limitation of PKE system under CPA model is the lowest.

3.3 Chosen ciphertext attack (CCA) channel model and security limitation

To consider IND-CCA security, there is such a game, the participants in the game include attacker and challenger. The rule of the game includes attacker selecting two plaintext M and N, and then challenger randomly selecting one to encrypt the ciphertext. Attacker can do some querying with challenger at any time before the game is over, including the Hash function query and decryption of some ciphertext queries, of course, the attacker can't be queried on C. When attcker thinks it's time to end the game, he has to report an answer to challenger, which plaintext he thinks C corresponds to (one of M and N), and attacker wins the game if the answer he gives is exactly the same as that chosen by challenger.

The attacker selects the ciphertext and obtains the decryption service to produce the corresponding plaintext. After the target ciphertext is obtained the decryption service stops immediately. If the attacker can obtain the message of the secret plaintext from the target ciphertext, the attack is said to have been successful, the attacker expects a plaintext-ciphertext to reduce the security of the PKC.

Obviously, CCA is a more powerful attack model than CPA. The model definition is shown in Figure 5.

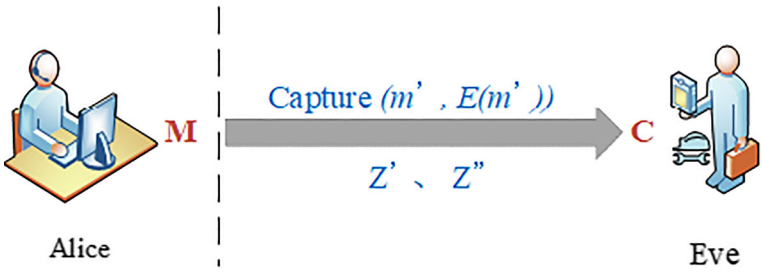

Figure 5 CCA channel model

In this model, the adversary obtained the decryption result asked by the decryption oracle and represented the knowledge space of the plaintext-ciphertext pairs after first and second interrogations oracle in training stage. The mathematical model can also be defined as

$$\begin{pmatrix} Z' \\ P(Z') \end{pmatrix} = \begin{pmatrix} z'_1 & z'_2 & \cdots & z'_{k'} & \cdots & z'_{l'} \\ p(z'_1) & p(z'_2) & \cdots & p(z'_{k'}) & \cdots & p(z'_{l'}) \end{pmatrix}$$

where $0 \le p(z'_{k'}) \le 1, \sum_{k'=1}^{l'} p(z'_{k'}) = 1$.

$$\begin{pmatrix} Z'' \\ P(Z'') \end{pmatrix} = \begin{pmatrix} z''_1 & z''_2 & \cdots & z''_{k''} & \cdots & z''_{l''} \\ p(z''_1) & p(z''_2) & \cdots & p(z''_{k''}) & \cdots & p(z''_{l''}) \end{pmatrix}$$

where $0 \le p(z''_{k''}) \le 1, \sum_{k''=1}^{l''} p(z''_{k''}) = 1$.

The adversary can use the plaintext-ciphertext pairs Z' and Z'' to enhance the attack on the plaintext. For the attacker, he can combine the selected ciphertext message $C'(C' \in C)$ and the plaintext-ciphertext pairs Z' and Z'' to attack , introducing the attack conditional entropy:

$$H(M \,/\, CZ'Z'') = -\sum_{i=1}^{t}\sum_{j=1}^{n}\sum_{k'=1}^{l'}\sum_{k''=1}^{l''} p(m_i c_j z'_{k'} z''_{k''}) \log_2 p(m_i \,/\, c_j z'_{k'} z''_{k''})$$

$H(M \,/\, CZ'Z'')$ reflects the uncertainty about M that still exists after the adversary selects the ciphertext message C' and the plaintext-ciphertext pairs Z' and Z'', which can actually be used as the uncertainty of the plaintext under a certain attack method. Similarly, the attack average mutual information is further defined as:

$$H(M; C \,/\, Z'Z'') = \sum_{i=1}^{t}\sum_{j=1}^{n}\sum_{k'=1}^{l'}\sum_{k''=1}^{l''} p(m_i c_j z'_{k'} z''_{k''}) \log_2 \frac{p(m_i z'_{k'} z''_{k''} \,/\, c_j)}{p(m_i \,/\, z'_{k'} z''_{k''}) P(c_j \,/\, z'_{k'} z''_{k''})}$$

$I(M; C \,/\, Z'Z'')$ reflects the average mutual information between C and M under the condition of Z' and Z'', that is, the amount of plaintext information obtained by the adversary, and also describes the degree of plaintext leakage under the attack with plaintext-ciphertext pairs. Therefore, the maximum extent of plaintext leakage is the maximum value of the average mutual information between the M and the C, that is, $I_{\max}(M; C \,/\, Z'Z'')$.

As the number of interrogations increases(polynomial time inquiry), the average mutual information between M and C can be expressed as

$$I\left(M; C \,/\, Z'Z''\cdots Z^{(n)}\right) = \sum_{i=1}^{t}\sum_{j=1}^{n}\sum_{k'=1}^{l'}\sum_{k''=1}^{l''}\cdots\sum_{k^{(n)}=1}^{l^{(n)}} p\left(m_i c_j z'_{k'} z''_{k''}\cdots z^{(n)}_{k^{(n)}}\right) \times \log_2 \frac{p\left(m_i z'_{k'} z''_{k''}\cdots z^{(n)}_{k^{(n)}} \,/\, c_j\right)}{p\left(m_i / z'_{k'} z''_{k''}\cdots z^{(n)}_{k^{(n)}}\right) P\left(c_j / z'_{k'} z''_{k''}\cdots z^{(n)}_{k^{(n)}}\right)}$$

That is, the maximum amount of plaintext information obtained by the adversary, $I_{\max}(M; C/Z'Z''\cdots Z^{(n)}) > I_{\max}(M; C \,/\, Z'Z'')$, and the adversary has increased the amount of plaintext information but not the whole amount of plaintext information, that is $M'M'' < M'M''\cdots M^{(n)} < M$.

3.4 Adaptive Chosen ciphertext attack (CCA2) channel model and security limitation

In CCA2, an attacker can always get decryption service except decrypting the target ciphertext. The rules of the IND-CCA2 game are as follows: the adversary first asks the challenger for decryption (can be repeated), that is, take the ciphertext c to the challenger, after the challenger decrypts, challenger give the plaintext to the adversary; Then the adversary chooses two plaintext m_0 and m_1, the challenger chooses one at random to encrypt to get the ciphertext c_b, where the random value $b \in \{0, 1\}$. Next the adversary can make decryption query to the challenger (multiple times), that is, get the ciphertext c ($c \neq c_b$) to the challenger and the challenger decrypts the text to the adversary. The adversary guessed b', if the answer he gave was the same as the original text chosen by the challenger, the adversary would succeed.

Obviously, CCA2 is a more powerful attack model than CCA. The model definition is shown in Figure 6.

In this model, the adversary has obtained the decryption result that asks the decryption prophecy or challenger, Z and R respectively represent the knowledge space of plaintext-ciphertext pairs obtained from the first and second stages of training, in which $Z = \{f(C'), C'\}$, $R = \{f(C''), C''\}$, $C' \in C$ represents chosen ciphertext for the first stage training selection and the corresponding plaintext is $m' = f(C')$, $C'' \in C$ represents chosen ciphertext for the first stage training selection and the corresponding plaintext is $m'' = f(C'')$. The mathematical model can also be defined as

$$\begin{pmatrix} Z \\ P(Z) \end{pmatrix} = \begin{pmatrix} z_1 & z_2 & \cdots & z_{k_1} & \cdots & z_{l_1} \\ p(z_1) & p(z_2) & \cdots & p(z_{k_1}) & \cdots & p(z_{l_1}) \end{pmatrix}$$

where $0 \leq p(z_{k_1}) \leq 1$, $\sum_{k_1=1}^{l_1} p(z_{k_1}) = 1$.

$$\begin{pmatrix} R \\ P(R) \end{pmatrix} = \begin{pmatrix} r_1 & r_2 & \cdots & r_{k_2} & \cdots & r_{l_2} \\ p(r_1) & p(r_2) & \cdots & p(r_{k_2}) & \cdots & p(r_{l_2}) \end{pmatrix}$$

where $0 \leq p(r_{k_2}) \leq 1$, $\sum_{k_2=1}^{l_2} p(r_{k_2}) = 1$.

The adversary can use the plaintext-ciphertext pairs Z and R to enhance the attack on the plaintext. For the attacker, he can combine the selected ciphertext message C' and C'' and the plaintext-ciphertext pairs Z and R to attack , introducing the attack conditional entropy:

$$H(M; C/ZR) = \sum_{i=1}^{t} \sum_{j=1}^{n} \sum_{k_1=1}^{l_1} \sum_{k_2=1}^{l_2} p\left(m_i c_j z_{k_1} r_{k_2}\right) \log_2 p\left(m_i / c_j z_{k_1} r_{k_2}\right)$$

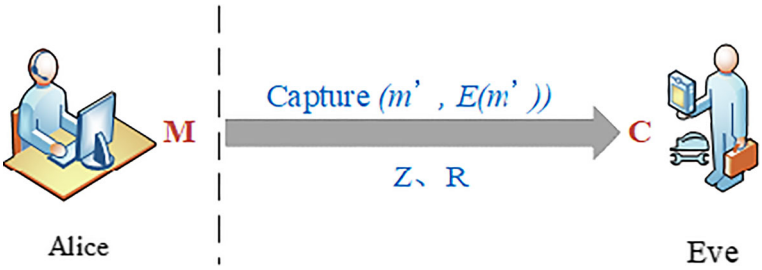

Figure 6 CCA2 channel model

The $H(M/CZR)$ reflects the uncertainty about M that still exists after the adversary selects the ciphertext message C and the plaintext-ciphertext pairs Z and R, which can actually be used as the uncertainty of the plaintext under a certain attack method. Similarly, the attack average mutual information is further defined as:

$$I(M; C/ZR) = \sum_{i=1}^{t} \sum_{j=1}^{n} \sum_{k_1=1}^{l_1} \sum_{k_2=1}^{l_2} p\left(m_i c_j z_{k_1} r_{k_2}\right) \log_2 \frac{p(m_i z_{k_1} r_{k_2}/c_j)}{p\left(m_i/z_{k_1} r_{k_2}\right) p\left(c_j/z_{k_1} r_{k_2}\right)}$$

$I(M; C/ZR)$ eflects the average mutual information between C and M under the condition of Z and R, that is, the amount of plaintext information obtained by the adversary, and also describes the degree of plaintext leakage under the attack with plaintext-ciphertext pairs. Therefore, the maximum extent of plaintext leakage is the maximum value of the average mutual information between the M and the C, that is $I_{\max}(M; C/ZR)$. In this case, the *security limitation* of PKE system is the lowest after two inquiries in CCA2 model. With the increase of the number of interrogations in the two training stages, the amount of plaintext information obtained by the enemy increases gradually, and the PKE security limitation decreases gradually.

Theorem 1 *If PKC satisfies COA, CPA, CCA, and CCA2-security separately, there is the security factors of the four models are sorted as follows:*

$$Secure_{COA} < Secure_{CPA} < Secure_{CCA} < Secure_{CCA2}$$

Proof In the COA, CPA, CCA, CCA2 security model, the knowledge background of the adversary increases in turn, that is

$$\text{Know}_{COA} < \text{Know}_{CPA} < \text{Know}_{CCA} < \text{Know}_{CCA2}$$

There is

$$I_{\max}(M; C) < I_{\max}(M; C/Z) < I_{\max}\left(M; C/Z'Z'' \cdots Z^{(n)}\right) < I_{\max}(M; C/ZR)$$

Therefore, the ability of the adversary to successfully break through PKE increases exponentially under these four models, but if the adversary does not break PKC, the security factor of CCA2 is the highest, and that of COA is the lowest and the security factors of the four models are sorted as follows:

$$\text{Secure}_{COA} < \text{Secure}_{CPA} < \text{Secure}_{CCA} < \text{Secure}_{CCA2}$$

□

4 Security limitation of signature

According to the PKC model, we consider the man-in-the-middle attack of digital signature, and define two types of adversary:

Type I adversary attack. The adversary has obtained the private key of Alice through intermediate attack and can forge the signature message.

Type II adversary attack. The adversary has the public key of Alice, intercepts the signature of Alice and forges a signature message, which is different from the true signature of the sender.

4.1 Direct forgery attack channel model and security limitation

The process of type I adversary attack is as follows: The adversary forges a signature as Alice, and sends the signed message to Bob, Bob does not know the message is forged. We describe the definition of the attack channel model as shown in Figure 7, where M represents the signature and its message, S represents the message which Bob receives signed by the adversary.

Assume the mathematical model of M be expressed as

$$\begin{pmatrix} M \\ P(M) \end{pmatrix} = \begin{pmatrix} m_1 & m_2 & \cdots & m_i & \cdots & m_t \\ p(m_1) & p(m_2) & \cdots & p(m_i) & \cdots & p(m_t) \end{pmatrix}$$

where $0 \leq p(m_i) \leq 1$, $\sum_{i=1}^{t} p(m_i) = 1$. Similarly, the mathematical model of S can be expressed as

$$\begin{pmatrix} S \\ P(S) \end{pmatrix} = \begin{pmatrix} s_1 & s_2 & \cdots & s_j & \cdots & s_n \\ p(s_1) & p(s_2) & \cdots & p(s_j) & \cdots & p(s_n) \end{pmatrix}$$

where $0 \leq p(s_j) \leq 1$, $\sum_{j=1}^{n} p(s_j) = 1$.

For this model, the source entropy $H(M)$ is defined as

$$H(M) = -\sum_{i=1}^{t} p(m_i) \log_2 p(m_i)$$

$H(M)$ is used to describe the average mutual information of M, which is also the uncertainty of the source.

When Bob acquires a signature message, the conditional entropy $H(M/S)$ is introduced to characterize the uncertainty of the source, which is defined as

$$H(M/S) = -\sum_{j=1}^{n} \sum_{i=1}^{t} p(m_i s_j) \log_2 p(m_i/s_j)$$

The conditional entropy indicates that after Bob receives S, the uncertainty of source M still exists. The uncertainty is due to the Bob's trust in the signature of the message. It can actually be regarded as the uncertainty of M in some attack.

A forgery attack average mutual information $I(M; S)$ is introduced below to describe the forgery information metric transmitted on the channel, which is defined as

$$I(M; S) = \sum_{j=1}^{n} \sum_{i=1}^{t} p(m_i s_j) \log_2 \frac{p(m_i/s_j)}{p(m_i)}$$

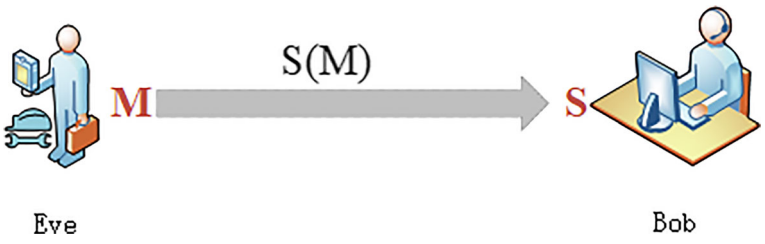

Figure 7 Type I attack channel model

$I = (M; S)$ reflects the average mutual information exchanged between M and S, that is, the amount of fake information on the attack channel. It can precisely describe the degree to which Bob acquires forged information from the whole receiving signature message, thus it can be used as an insecure measure by an adversary to successfully attack Bob. Therefore, the maximum degree of successful attack is the maximum of the average mutual information between M and C, that is $I_{\max} = (M; S)$. In this case, the PKE digital signature security limitation reaches the minimum.

4.2 Tampering attack channel model and security limitation

The process of type II adversary attack is as follows: the adversary intercepts the message sent by Alice with signature, tampers with the message and forges a signature S', and sends the signed message to Bob, at which time Bob does not know whether the message has been tampered with or not. Next, we define the attack channel model of the adversary as shown in Figure 8. We define the interaction between Alice and Bob as a series channel, the interaction between Alice and Eve as class I channel, and the interaction between Eve and Bob as class II channel, where M represents the signature of Alice and its message, S indicates the signature and message intercepted by the adversary, and S' denotes that Bob receives the adversary's signature and message.

Assume the mathematical model of M be expressed as

$$\begin{pmatrix} M \\ P(M) \end{pmatrix} = \begin{pmatrix} m_1 & m_2 & \cdots & m_i & \cdots & m_t \\ p(m_1) & p(m_2) & \cdots & p(m_i) & \cdots & p(m_t) \end{pmatrix}$$

where $0 \le p(m_i) \le 1$, $\sum_{i=1}^{t} p(m_i) = 1$. Similarly, the mathematical model of Ss can be expressed as

$$\begin{pmatrix} S \\ P(S) \end{pmatrix} = \begin{pmatrix} s_1 & s_2 & \cdots & s_j & \cdots & s_n \\ p(s_1) & p(s_2) & \cdots & p(s_j) & \cdots & p(s_n) \end{pmatrix}$$

where $0 \le p(s_j) \le 1$, $\sum_{j=1}^{n} p(s_j) = 1$. Similarly, the mathematical model of S' can be expressed as

$$\begin{pmatrix} S' \\ P(S'') \end{pmatrix} = \begin{pmatrix} s'_1 & s'_2 & \cdots & s'_k & \cdots & s'_l \\ p(s'_1) & p(s'_2) & \cdots & p(s'_k) & \cdots & p(s'_l) \end{pmatrix}$$

where $0 \le p(s'_k) \le 1$, $\sum_{k=1}^{l} p(s'_k) = 1$.

Figure 8 Type II attack channel model

For series channel, similar to Section 4.1, average mutual information $I\left(M; S'\right)$ is introduced to describe the amount of information transmitted over the series channel, which is defined as

$$I\left(M; S'\right) = \sum_{k=1}^{l} \sum_{i=1}^{t} p\left(m_i s'_k\right) \log_2 \frac{p\left(m_i / s'_k\right)}{p\left(m_i\right)}$$

$I\left(M; S'\right)$ represents the average mutual information that M and S' interact with, that is, the amount of information on the series channel. It can describe the degree to which the Bob obtains M from the received signature message, thus it can represent the security of the series channel. So its security limitation is the maximum of the average mutual information between M and S', that is $I_{\max}\left(M; S'\right)$. In this case, the security limitation of PKE digital signature reaches the maximum.

Similarly, for class I channel and class II channel, separate definition

$$I\left(M; S\right) = \sum_{j=1}^{n} \sum_{i=1}^{t} p\left(m_i s_j\right) \log_2 \frac{p\left(m_i / s_j\right)}{p\left(m_i\right)}$$

$$I\left(S; S'\right) = \sum_{k=1}^{l} \sum_{j=1}^{n} p\left(s_j s'_k\right) \log_2 \frac{p\left(s_j / s'_k\right)}{p\left(s_j\right)}$$

$I = (M; S)$ means the average amount of information between M and S, which shows the degree to which the adversary acquired M. $I\left(S; S'\right)$ means the average amount of information between S and S', which shows that Bob acquires the amount of information tampered with by the adversary, that is, the measure of successful attack by the adversary. Therefore, it can be used to express the degree of insecurity of the class II channel, the limitation of which is the $I_{\max}\left(S; S'\right)$.

Lemma 1 ***(Data processing theorem)*** *As the number of processors increases, the average mutual information between the input message and the output message tends to become smaller.*

$$I\left(X; Z\right) \leq I\left(X; Y\right)$$
$$I\left(X; Z\right) \leq I\left(Y; Z\right)$$

It is assumed that X and Z are independent of each other under Y condition.

In this model, the data processing system of the adversary Eve is regarded as the class II channel, and the series channel is formed with the class I channel and class II channel, so the input and output messages of the sender and receiver can be quantified compared by the data processing theorem. Theorem 2 can be obtained from Lemma 1.

Theorem 2 *When the signature message of Alice is tampered with by the adversary Eve, the average mutual information between the input and output messages of the series channel does not exceed the average mutual information between the input and output messages of the class I channel, and it does not exceed the average mutual information between the input and output messages of the class II channel. So the following inequality holds:*

$$I\left(M; S'\right) \leq I\left(M; S\right)$$
$$I\left(M; S'\right) \leq I\left(S; S'\right)$$

From the above inequalities we have

$$I_{\max}\left(M; S'\right) \leq I_{\max}\left(S; S'\right)$$

That is, the security limitation of series channel is less than or equal to that of the class II channel, where $I_{\max}\left(S; S'\right)$ represents insecurity limitation of the class II channel and $I_{\max}\left(M; S'\right)$ represents security limitation of the series channel.

5 Discussion of secure limitation

This paper analyses the security of Public-key Cryptography in smart card environment. We establish mathematical models of public key encryption and public key signature respectively and simulate adversary's attack on Public-key Cryptography as a communication process, then describe the attack ability of the attacker and analyze the security limitation of the Public-key Cryptography by using the information theory, such as the the average mutual information and conditional mutual information.

This work only considers an insecure limitation in the perspective of the adversary, although the value of insecure limitation may be also equal to the value of secure limitation in the view of communication parties. The Insecure limitation is the bound of attack ability to an adversity, which is a point that communication parties need to defense the cryptosystem. Thus, The value of Secure Limitation, denoted by D, to communication parties and Insecure limitation, denoted by C, to adversaries are the key factors, which show the security of whole cryptosystem. If $C < D$, then this cryptosystem is insecure; However, if $C \geq D$,then this cryptosystem is secure. Therefore, We can also convert the secure problems of Public-key Cryptography into the defense channels capacity of communication parties that the maximum value of the average mutual information is the *secure limitations* of a Public-key Cryptography scheme, which will be an important research issue.

The proposed method of secure limitation provides a naive solution to the secure bound problem of a Public-key Cryptography system, which is also applicable to other secure Attack and defense systems.

6 Conclusion

Aiming at the security problem of Public-key Cryptography of smart card, we introduced a naive notion of security for Public-key Encryption called *insecure limitation* which is a bound with respect to a adversary attacking the Public-key Cryptography system, as well as the value of *insecure limitation* also is a bound with respect to the communication parties secure guarding their cryptosystems. Based on the relevant knowledge of information theory, the key point of this paper is to treat the process of the adversary's attack on Public-key Cryptography as a communication model. We give the quantification method of Public-key Cryptography under different attack models by defining the source, the sink and the channel, and introduce the concepts of information entropy, conditional entropy, the average mutual information and conditional mutual information. Although the work of this paper only gives a more basic Public-key Cryptography security limitation model, but in order to solve the quantification problem of Public-key Cryptography security limitation, a feasible system foundation is established. And it is believed that under the support of the information theory related achievements, the relevant research can be further developed. Including the Public-key Cryptography security limitation under more complex multi-adversary attacks and the

study of Public-key Cryptography security limitation by generalized information theory and fuzzy information theory have the feasibility of further research.

Acknowledgements We would like to thank the anonymous reviewers for their valuable suggestions. This work is supported by National Natural Science Foundation of China under Grant Nos.61662009 and 61772008; Guizhou Provincial Department of Education Science and Technology Top Talent Support Project under Grant No.[2016]060; Science and Technology Major Support Program of Guizhou Province under Grant No.20183001; Science and Technology Program of Guizhou Province under Grant No.[2017]5788; Ministry of Education-China Mobile Research Fund Project under Grant No.MCM20170401; Guizhou University Cultivation Project under Grant No.[2017]5788; Key Projects Supported by The Joint Fund of The National Natural Science Foundation of China under Grant No.U1836205; Science and Technology Program of Guizhou Province under Grant No.[2019]1098.

References

1. Bellare, M., Boldyreva, A., Desai, A., Pointcheval, D.: Key-privacy in public-key encryption. In: Proceedings of the 7th international conference on the theory and application of cryptology and information security: Advances in cryptology. pp. 566–582. ASIACRYPT '01. Springer-Verlag, Berlin (2001). http://dl.acm.org/citation.cfm?id=647097.717024
2. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: Proceedings of the 1st ACM conference on computer and communications security. pp. 62–73. CCS '93. ACM, New York (1993). https://doi.org/10.1145/168588.168596
3. Boyen, X., Mei, Q., Waters, B.: Direct chosen ciphertext security from identity-based techniques. In: Proceedings of the 12th ACM conference on computer and communications security. pp. 320–329. CCS '05. ACM, New York (2005). https://doi.org/10.1145/1102120.1102162
4. Camenisch, J., Shoup, V.: Practical verifiable encryption and decryption of discrete logarithms. In: Boneh, D. (ed.) Advances in cryptology - CRYPTO 2003, pp. 126-144. Springer Berlin Heidelberg, Berlin (2003)
5. Chang, C.C., Wu, T.C.: Remote password authentication with smart cards. IEEE Proc.-E **138**(3), 165–168 (1991)
6. Chien, H.Y., Jan, J.K., Tseng, Y.M.: An efficient and practical solution to remote authentication: Smart card. Comput. Secur. **21**(4), 372–375 (2002)
7. Coron, J.: Resistance against differential power analysis for elliptic curve cryptosystems. In: International workshop on cryptographic hardware and embedded systems (1999)
8. Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.) Advances in Cryptology — CRYPTO '98, pp. 13-25. Springer, Berlin (1998)
9. Cramer, R., Hanaoka, G., Hofheinz, D., Imai, H., Kiltz, E., Pass, R., Shelat, A., Vaikuntanathan, V.: Bounded cca2-secure encryption. In: Proceedings of the advances in crypotology 13th international conference on theory and application of cryptology and information security. pp. 502–518. ASIACRYPT'07. Springer-Verlag, Berlin (2007). http://dl.acm.org/citation.cfm?id=1781454.1781497
10. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976). https://doi.org/10.1109/TIT.1976.1055638
11. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic analysis: Concrete results. Ches May **2162**, 251–261 (2001)
12. Hsiang, H.C., Shih, W.K.: Improvement of the secure dynamic id based remote user authentication scheme for multi-server environment. Computer Standards and Interfaces **31**(6), 1118–1123 (2009)
13. Izu, T., Takagi T.: A fast parallel elliptic curve multiplication resistant against side channel attacks (2002)
14. Jiang, Q., Ni, J., Ma, J., Yang, L., Shen, X.: Integrated authentication and key agreement framework for vehicular cloud computing. IEEE Netw. **32**(3), 28–35 (2018). https://doi.org/10.1109/MNET.2018.1700347
15. Joye, M., Yen, S.M.: The montgomery powering ladder. In: International workshop on cryptographic hardware and embedded systems (2002)
16. Kocher, P.C.: Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In: International cryptology conference on advances in cryptology (1996)
17. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. Proc. Crypto. **1666**, 388–397 (1999)
18. Mamiya, H., Miyaji, A., Morimoto, H.: Efficient Countermeasures against RPA, DPA and SPA (2004)

19. Messerges, T.S.: Using second-order power analysis to attack dpa resistant software. In: International workshop on cryptographic hardware and embedded systems (2000)
20. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Investigations of power analysis attacks on smartcards. In: Usenix workshop on smartcard technology on usenix workshop on smartcard technology (1999)
21. Micali, S., Reyzin, L.: Physically observable cryptography (2004)
22. Moebius, N., Stenzel, K., Borek, M., Reif, W.: Incremental development of large, secure smart card applications. In: Workshop on model-driven security (2012)
23. Nojima, R., Imai, H., Kobara, K., Morozov, K.: Semantic security for the mceliece cryptosystem without random oracles. Des. Codes Cryptogr. **49**(1-3), 289–305 (2008). https://doi.org/10.1007/s10623-008-9175-9
24. Park, J.W., Sherman, M., Colombo, M., Roberts, L.R., Schwartz, M.E., Degos, F., Chen, P.J., Chen, M., Kudo, M., Johnson, P.J., Huang, B., Orsini, L.S.: Observations of hepatocellular carcinoma (hcc) management patterns from the global hcc bridge study: First characterization of the full study population. J. Clin. Oncol. **30**(15), 4033–4033 (2012)
25. Qi, J., Ma, J., Wei, F.: On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE Syst. J. **PP**(99), 1–4 (2016)
26. Quisquater, J.J., Samyde, D.: Electromagnetic analysis (ema): Measures and counter-measures for smart cards. In: International conference on research in smart cards: Smart card programming and security (2001)
27. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978). https://doi.org/10.1145/359340.359342
28. Schneier, B. Applied cryptography: Protocols, Algorithms, and Source Code in C, 2nd edn. John Wiley & Sons, Inc., New York (1995)
29. Tian, Y., Guo, J., Wu, Y., Lin, H.: Towards attack and defense views of rational delegation of computation. IEEE Access **7**, 44037–44049 (2019). https://doi.org/10.1109/ACCESS.2019.2908858
30. Tunstall, M.: Smart card security. Smart Cards Tokens Security and Applications **3**, 195–228 (2014)
31. Wang, B., Lei, H., Hu, Y.: D-ntru: More efficient and average-case ind-cpa secure ntru variant. Inf. Sci. **438**, 15–31 (2018). https://doi.org/10.1016/j.ins.2018.01.037. http://www.sciencedirect.com/science/article/pii/S0020025518300513
32. Waters, B.: Efficient identity-based encryption without random oracles. In: Proceedings of the 24th annual international conference on theory and applications of cryptographic techniques. pp. 114–127. EUROCRYPT'05. Springer-Verlag, Berlin (2005)