Partially Opened Data and Its Security

Hidema TANAKA

***Abstract*—We discuss a method of disclosing data which includes secret information. In general, such method is called sanitizable signature and context extraction signature and many schemes are proposed. In the previous schemes, we can make an opened data (covered data) after signed the data which includes secret information. And maker of covered data and signer are another person. We assume that the person who knows the secret information is only signer and maker of covered data and signer are the same person. We analyze security requirements for such purpose and develop a proposal method. We show a security analysis of our proposal protocol and its applications. We also show that our proposal protocol is a method that can be used for not only the data concerning to national security and digital forensics but also the secure network construction.**

***Keywords* —Digital forensics, ElGamal encryption method, secure protocol, Partially opened data, Content Extraction Signature**

I. Introduction

A. Background

WE have demands for disclosing information partially while concealing the confidential information. For example, though all information can be opened at X-day, it is necessary to open it partially for one's innocence at the court before the day. Figure 1 shows the methods of disclosing printed data which includes secret information. There are two types of solution, TYPE-1 and TYPE-2. TYPE-1 is a method of painting out the secret information. This is a popular solution and they are founded in several place such as confidential documents of government which are allowed to be open under some condition, some indictment documents, X-Files and so on. TYPE-2 is a method of cutting off a secret information. It is well adopted to audio and video data than printed data. It is a technique for keeping the secret by removing an inconvenient part from the original data. In this paper, we discuss how such a method is applied to digital data. The necessity of this technology grows up greatly with an increase in the use of digital data. For instance, the Sarbanes - Oxley act [21] is enforced as for an economic activity, and management and disclosing digital data are the important problems for corporations. Moreover, it is necessary to treat as evidence of the criminal case. In the politics of Japan, assembly member Nagata's fake email in 2006 is famous [15]. He tried to open the main text without the informations of sender and he printed email and eliminated such information, then submitted as the evidence with his declare that all information is opened later. Fortunately his fake was solved by another matter, however, the case where digital data is treated as a legal evidence will increase.

H.Tanaka is with the National Institute of Information and Communications Technology, Japan, 4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan.

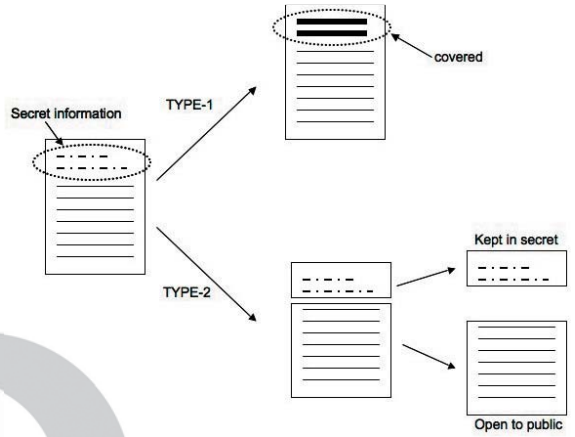

Fig. 1. Method of disclosing printed data including secret information

B. Previous works

If the data which includes secret information has already been signed, some methods have already been proposed [2], [10] and so on. They are applications of hash functions and aggregate signature scheme with pairing techniques [4]. The validity of the data (ciphertext) is guaranteed by the signature. So they do not consider the attack and injustice act of malicious signer by using unopened data which does not have been signed yet. The proposers assume the signer of the data and the maker of covered data (sanitized data) are another person. Therefore the maker can know the confident information. We assume that the person who know the secret information is only the signer, it is not suitable method for our purpose. Of course their methods can be improved to achieve our requirement, the weakness against attack using collision search of hash functions remains. An outline of previous proposal scheme is that it calculates the hash value at every the subblock of data, and calculates the signature of it. Then the signed subblock of data concatenated to another subblock of data and repeated above procedure. From such mechanism and procedure, they are categorized into TYPE-1 in Figure 1. From such a mechanism, estimating the secret information, we can determine the secret information using hash value and signature, so the essential security of the method depends on the difficulty of collision search of the hash function. The influence on the weakness of some concrete applications when the assumption of computational difficulty of collision search of hash function collapses is shown in [16] and [20]. The previous methods are not required to open the secret information later. In addition, it is needed for the maker of covered data to have anonymity and the method needs to prevent injustice act by them. These points are not

corresponding to our purpose. Especially, because we assume maker of covered data to be the same person with the signer, the discussion of anonymity of maker of covered data is omitted in this paper.

C. Our purpose

First of all, we assume that the secret information should be open to public later and the person who knows the secret is only the signer before the day. The signer and the maker of covered data are the same person. Therefore, we develop the method which can be applied to the data which has not been signed yet. We assume that the secret information is concerning to national security and digital forensics such as legal evidences. So the security and consistency of data are higher level than previous proposal schemes are required. Since the signer and the maker of covered data are the same person, the injustice act and attack of signer is needed to be prevented. Similarly, the signer should show that any injustice act is not done before X-day. The differences of purpose and condition between previous methods and our method are summarized as Table 1. In Section 2 we discuss the security requirements for our purpose. In the section, we summarize the property of security and analyze their purpose in details. In Section 3, we show our proposal method. It is based on ElGamal encryption method. Our proposal method is categorized into TYPE-2. In Section 4, we show a security analysis of our proposal method according to the security requirements in Section 2. In Section 5, we propose another application of our method. We assume that the secret data is concerning to high secret important data such as national security. However, when the small size data is used, some applications are considered.

II. Security requirements

Suppose that Alice has a digital data M which contains secret information. After X-day, she can open all of M, however, she wants to open a part of M which contains no secret information before the day. Let M' be a part of M which can be open to Public. We call M' "partially opened data". Authority who does not know M, authenticates that M' is a part of M and guarantees that M can not be changed after M' is open. We assume that Authority is a trusted person and we can believe that he does not do any injustice acts. Table 2 shows the variables and their roles in the protocol.

Then we faces the following security requirements.

[R1] It is impossible to calculate M using open data in the protocol.

First of all, it is necessary to prevent to re-caliculation of the secret part of M using partially opened data M'. In addition, the protocol opens some data for verification and authentication which are generated from M and Alice's secret information. As the results, the attacker can use many open information (For examples, see Table 4). This is the fundamental requirement for the protocol. Therefore if the term when M is kept secret long, it is necessary to choose the parameters of cryptographic primitives considering the evolution of computer and cryptanalysis techniques. This is a requirement concerning Alice's secrecy.

[R2] It is possible to verify that M' is a part of M without opening M.

It is necessary to verify that the partially opened data M' is a part of M. We assumed that M is kept secret, the verification are done without opening M. Blind signature scheme [3] and partially signature scheme [10] seems to have same purpose. Both of them can verify the ciphertext without opening plaintext to verifier. However they can not decrypt a part of ciphertext. And they can not prove the relation between partially opened data and its ciphertext. For the methods using hash functions, the calculation of hash value of a part of data is done at the same time as the data creation. Therefore it is not secure to apply such method to the data which was made in the past. It is because the change in the content by attack using collision search of hash function. The attacks of X.509 certificates [20] and pdf files [16] are well known as the advanced attack using collision search of hash function. Such attack method can be applied to previous methods for unsigned data. To solve these problem, we show a proposal protocol in Section 3. We should show that the partially opened data can not be generated by another data. Or when forgery data M is open, It is necessary for us to find out the injustice act. This is a requirement concerning authentication of data M and M'.

[R3] It is impossible to change M after M' is opened.

To hold this requirement, it is necessary to show that it is secure against following two types of attack; one is an injustice attack of Alice and another is forgery attack of malicious people who can get open data. This is a requirement concerning consistency of data M and M'. Though these attack techniques are essentially the same, Alice has advantageous condition because she can prepare forgery data beforehand. Thus it is necessary for us to find out her injustice. Detailed security analysis for our proposal protocol is shown in Section 4.

[R4] It is possible to verify that Alice *did no injustice act before X-day.*

When Alice opens the all of data M, it is necessary to be proven that she did no injustice act for M and M'. This is a requirement concerning integrity of data M and M'. It is considered that this requirement is held if the R1, R2 and R3 are held.

III. Proposal scheme

A. Protocol flow

Our proposal scheme is as follows. Table 3 shows variables used in the protocol. The protocol is based on ElGamal encryption method [7]. Figure 2 shows the diagram of the protocol.

<**Proposal protocol for secure partially opened data**>

Step 1 Alice sends the size of data M to Authority.

TABLE I
DIFFERENCE OF PURPOSE AND CONDITION

	maker of covered data	secret information	category in Figure 1
Previous method	another person of signer	not required to be open	TYPE-1
Our method	same person of signer	required to open after X-day	TYPE-2

TABLE II
VARIABLES AND THEIR ROLES

Alice	A holder of data M. She wants to open a part of M.
Authority	Trusted party such as organizations of government or court.
M	Secret data of Alice.
M'	Partially opened data. Disclosable part of M.
X-day	The day when Alice can open all of M.
Public	People who want to know M. Before X-day, they want to get information as much as possible .

TABLE III
VARIABLES

G	A multi-plicate cyclic group of order q	K	A public key of Alice, $K = g^{k_s}$
q	A prime number	M	A secret data of Alice, $M \in G$
g	A generator of G	M'	Partially opened data of Alice, $M \in G$
r	A random number chosen from $\{0, \ldots, q-1\}$	$\|X\|$	The size of X
k_s	A secret key of Alice chosen from $\{0, \ldots, q-1\}$		

Step 2 According the size, Authority chooses G, g and q whose size is larger than M. Then he open to public G, q and g. Authority chooses a random number r from $\{0, \ldots, q-1\}$ then he sends g^r to Alice.
Step 3 Alice converts her data into elements of G. Next she chooses a secret key k_s from $\{0, \ldots, q-1\}$ and calculate her public key $K = g^{k_s}$ and K^{-1} which is an inverse of K. She calculates $M \cdot g^{Kr}$, g^M and $g^{g^{K^{-1}+1}}$ and then sends them to Authority. Note that public key K is kept secret before X-day.
Step 4 Authority calculates $\alpha = (g^M)^{g^r} \times (g)^{M \cdot g^{Kr}}$ and $\beta = (g^{g^{K^{-1}+1}})^{M \cdot g^{Kr}}$. If $\alpha = \beta$, he can fix the message M without opening it. He guarantees g^M.
Step 5 Alice makes a partial open data M' from M. Then she opens M' and $g^{M-M'}$ to Public.
Step 6 Public can know M' and verify $g^{M'} \times g^{M-M'} = g^M$.
Step 7 After X-day, Alice opens M and k_s and Authority opens r.

B. Characteristic of our protocol

Our proposal protocol is an application of ElGamal encryption method. Therefore the security of protocol depends on the security of ElGamal. The main feature of this protocol is that the validity of M' is guaranteed by ciphertext $M \cdot g^{Kr}$, g^M and $g^{M-M'}$. To keep secret M and K, we uses the data $g^{g^{-K}+1}$. By using it, Authority and Public can verify M'. The detailed security analysis is shown in Section 4.

There is difficulty in implementation. Our proposal protocol uses many times of multi-plicate calculation. We assume M is the data concerning to the very important data such as national security or digital forensics, so it is not a disadvantageous problem the necessity of a large computing time. However in the case of huge size of M, it becomes impossible to calculate. For such a case, it is necessary to reduce M beforehand. Let $M = (m_1||m_2||m_3)$ be a huge size data and we assume that Alice want to open a part of m_2 which includes secret information. Alice makes a shrunken data $\tilde{M} = (hash(m_1)||m_2||hash(m_3))$ and opens $hash(M)$ (where $hash(\cdot)$ denotes a secure hash function). Then Alice starts the protocol with $\tilde{M}$. Alice also open m_1 and m_2.

IV. SECURITY ANALYSIS

We analyze the security of our proposal protocol according to the security requirements shown in section 2. Table 4 shows the variables which appear in the protocol. From the purpose of the protocol, all variables are opened after X-day. Adding the analysis for security requirements, we analyze the security against malicious Public in "[RX] Attack of malicious Public".

[R1] It is impossible to calculate M using open data in the protocol.

In Step 3 and Step 4, the attacker can get some information which generated from M, that is $M \cdot g^{Kr}$, g^M and pair of $(M', g^{M-M'})$. The attack scenarios are follows (in the following (given information)→target).

[Case1] $(g, g^M) \rightarrow M$
[Case2] $(g, g^r, M \cdot g^{Kr}) \rightarrow M$
[Case3] $(g, M', g^M, g^{M-M'}) \rightarrow M$

It is easy to see that the attack condition of [Case1] and [Case3] are equivalent to the discrete logarithm problem. Therefore the attacker can not get no information on M in the cases. In the same way, it is easy to see that the condition of [Case2] is equivalent to the attack of ElGamal encryption method. Therefore the security of M depends on the security of ElGamal encryption method. As a result, it can be concluded that requirement [R1] has been achieved.

It is well known that ElGamal encryption method is unconditionally malleable and therefore it is not secure against chosen ciphertext attack. So the attacker can easily construct a valid ciphertext $2M \cdot g^{Kr}$ and g^{2M} for the data $2M$. However,

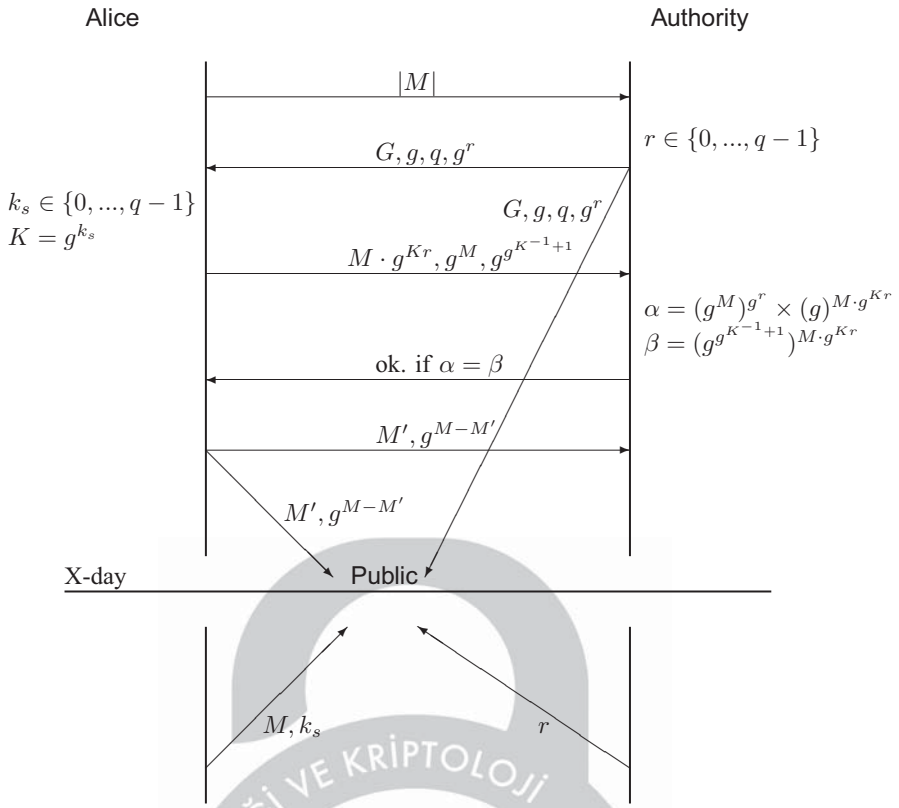

Fig. 2. Diagram of proposal protocol

TABLE IV
VARIABLES IN PROTOCOL

Public information	G, q, g	setup of procol
	g^r	opened by Authority
	$M \cdot g^{Kr}$,g^M, $g^{g^{-K}+1}$, $g^{M-M'}$	contains secret information M and secret key K
	M'	Alice's open information
Secret Information	M,k_s, K	Alice's secret information
	r	Authority's secret information

in Step 5, Alice opens $(M', g^{M-M'})$ then we can find out that such attack is done. In this attack scenario, there are no benefit for Alice and Authority and such attack is easy to find.

[R2] It is possible to verify that M' is a part of M without opening M.

To analyze this security requirement, it is necessary to show that g^M is generated from M without opening M. In Step 4, Authority and Public can check $\alpha = (g^M)^{g^r} \times (g)^{M \cdot g^{Kr}}$ and $\beta = (g^{g^{-K}+1})^{M \cdot g^{Kr}}$. We should check that α and β can be calculated from M and K uniquely. Therefore the attack scenario is summarized as follows. Note that the size of $\hat{M}$ equals to M.

[Case4] $(g, M, \hat{M}(\neq M), g^r, K) \rightarrow (g^M)^{g^r} \times (g)^{M \cdot g^{Kr}} = (g^{\hat{M}})^{g^r} \times (g)^{\hat{M} \cdot g^{Kr}}$

As mentioned above, we can easily make $\hat{M}$ which holds $M \cdot g^{Kr} = \hat{M} \cdot g^{Kr}$. However, for malicious Public who does not know M, it is impossible to find $\hat{M}$ which can hold $g^M = g^{\hat{M}}$ at the same time because this problem is based on the discrete logarithm problem. And for malicious Alice who knows M, it is impossible to find out $\hat{M}$ whose size is equals to q. On the other hand, if $|\hat{M}| > |M|$, malicious Alice can make $\hat{M}$ as $M+nq$ where $n = 1, 2, ...$ because of $g^q = 1$. But in this case, the size of $\hat{M}$ becomes larger than the size of q, Authority and Public can easy to find out the malicious Alice's injustice after X-day. Considering the purpose of this protocol, we can conclude that there are no benefit for Alice in such attack.

Under the assumption that we can verify that g^M is generated from M without opening M by the method in Step 4, we analyze the requirement by the following attack scenario.

[Case5] $(g, M', g^M, g^{M-M'}) \rightarrow \hat{M}$ which holds $g^{\hat{M}} \times g^{M'} = g^M$

A malicious Alice can find out such $\hat{M}$ but there are no benefit for Alice because M has been already fixed. As the result, we

can verify that M' is a part of M without opening M by the method in Step 5 and Step 6.

[R3] It is impossible to change M after M' is opened.

From the analysis of security requirement [R2], under the assumption of using same key K, it is obvious that it is impossible to rewrite M after M' is opened.

There is another attack scenario.

[Case6] (M_1, K_1, M_2, K_2) where $M_1 \neq M_2$ and $K_1 \neq K_2 \rightarrow M_1 \cdot g^{K_1 r} = M_2 \cdot g^{K_2 r}$, $g^{M_1} = g^{M_2}$ and $g^{g^{K_1^{-1}+1}} = g^{g^{K_2^{-1}+1}}$

Under the condition of $|M_1| = |M_2|$, from the result of analysis of [R2], it is impossible to do the attack according to this scenario. Under the condition of $|K_1| \neq |K_2|$, we can find pair of (K_1, K_2) which holds $g^{K_1^{-1}+1} = g^{K_2^{-1}+1}$. So the attacker can execute the above scenario for $|M_1| \neq |M_2|$. Therefore if malicious Alice prepared such pairs of (M_1, K_1) and (M_2, K_2), she can success the attack in this scenario. Of course, after X-day, the unnatural setting of size of G is found in this scheme. Therefore Public will have a doubt in the validity of M and Alice. However, the countermeasure against this attack is easy by using hash functions or time stamp protocol. For example, in Step 3, Alice opens the hash value of M with the time stamp protocol. In that case, the validity of M depends on the security of hash function and time stamp protocol. We assume that our proposal protocol is used for long term validity of partial opened data M'. In this case, the security requirement of hash function becomes high performance. Such discussion is found in [9].

[R4] It is possible to verify that Alice *did no injustice act before X-day.*

In Step 7, Alice opens M and her secret key k_s and Authority opens his random number r. So Public can calculate $K = g^{k_s}$ and decrypt $M \cdot g^{Kr}$. In Step 3, Alice opens $g^{g^{K^{-1}}+1}$. Public can not verify that it is generated by k_s without knowing its value. This is an open problem of our protocol. However, as mentioned above, some attack and injustice activity are discovered as an unnatural setting of G.

[RX] Attack of malicious Public

We analyze the attack of malicious Public who want to ruin Alice's confidence. In this section, we assume an active attack to the protocol.

Man-in-the-middle-attack : In place of Alice, malicious Public opens another M' or M. In Step 3 and Step 5, malicious Public can changes Alice's data. So, if there are no authentication protocol between Alice and Authority, the attack successes. Before Step 1, Alice and Authority must make a secure channel by using PKI and so on.

Forgery attack : At X-day, malicious Public opens forgery data $\hat{M}$. As mentioned above, if $|M| = |\hat{M}|$, it is impossible to do such attack. If $|M| \neq |\hat{M}|$, the attack is discovered by another Public and Authority.

Basically, the attack which Alice can not execute, can not be done by malicious Public. Therefore the protocol which holds security requirements shown in Section 2, is secure against malicious Public.

We confirmed the security of our proposal protocol for the requirements shown in Section 2. As a results, we conclude that our protocol holds the security requirements.

V. Applications

A. Incident analysis

CERT and IRT analyze the incident which caused by malicious software (Malware), illegal access, DoS attack and so on . They collect data concerning attacks or incidents from user who are in trouble. Such data has often includes privacy information which should be kept secret. On the other hand, CERT and IRT need to confirm the report of attacks is the true. The difference exists in information that the user can show and information that CERT and IRT need. Today they solve this problem by making NDA each other. Because it is such a situation, the information from general user is difficult to collect. Additionally, if it can, there will be a possibility that information from general user contains lies and mistakes. By using proposal protocol, CERT and IRT get more information from general users. As mentioned above, user's privacy is protected and CERT and IRT know the details of attacks and incidents. And CERT and IRT can check the information is true or false. It is expected that our proposal can be applied effectively to such use.

B. Encryption Email

Some email servers such as in the corporation, the encryption email to the address that has not been permitted is prohibited. Though it is because of prevention of information leakage, it limits the activity of staff. Such a problem can be solved by submitting the partially opened data which is generated by our protocol. Our protocol can verify the ciphertext and partially opened data, so if the information is leaked by encryption email, we can find the malicious user.

C. Traceable network and incident detection

It is well known that the attack to the network using encrypted IP packet. Since the router, the server, and the administrator can not analyze the content, encrypted IP packet is an effective attack method. As the countermeasure against such problem, our proposed protocol can be used. For example, the router issues ID to the sender. The sender writes ID in his IP packet, then he encrypts it. (Of course, plaintext IP packet should be written ID, too.) Next he make partially opened data which open only ID and sends encrypted IP packet, ID, g^M and $g^{M-\mathsf{ID}}$. The router checks ID and stores ID, g^M and $g^{M-\mathsf{ID}}$. In the same way as the case of Section 5.2, the administrator can find the packet which makes incident or troubles and the sender. In this system, the router, the server and client PCs need to do the large number of calculation for huge number of IP packets. It is a problem of implementation of our protocol and it is hard to solve at once.

VI. Conclusion

In this paper, we propose a protocol which generates partially opened data. The security requirements are shown in Section 2 and proposal protocol is shown in Section 3.

In Section 4, we analyze the security of our proposal protocol. Note that we did not discuss whether forgery data $\hat{M}$ was possible to have semantic meaning which is effective for attack. Suppose text data M, it is very hard to find some meaning in $\hat{M} = M + nq$. Therefore we conclude that the successful attack in Section 4 has no sense for real data. In addition, even if most successful attack, since the evidence was left Alice gets disadvantageous. As a result, we conclude that our proposal protocol is secure enough for semantic data.

In Section 5, we show an application of our protocol whose purpose is other than national security and digital forensics. For the usage for national security and digital forensics, necessity of huge computational cost does not become a fatal problem. For the general usage, it becomes important problem to be solved.

Analysis of security concerning $g^{g^{-K}+1}$ and improvement of protocol is our next research topics. It is a disadvantageous not to be able to verify $g^{g^{-K}+1}$ until X-day. Our proposal protocol uses transmission of a huge amount of data and it has some redundant steps. The optimization of the data transfer is our next theme.

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.
[2] G. Ateniese, D. Chou, B. Medeiros, G. Tsudik, "Sanitizable Signatures", ESORICS 2005, LNCS 3679, pp.159-177, Springer, 2005.
[3] M.Bellare and P.Rogaway, " The Exact Security of Digital Signatures - How to Sign with RSA and Rabin, " Proc.of EUROCRYPT1996,LNCS 1070,pp.399-416, Springer,1996.
[4] D. Boneh, C. Gentry, B. Lynn, H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps", EUROCRYPT 2003, LNCS 2656, pp.416-432, Springer, 2003.
[5] R.Cramer and V.Shoup, " Signature Schemes Based on the Strong RSA Assumption" Proceedings of the 6th ACM conference on Computer and communications security ,pp.46-51,1999
[6] D.Chaum, " Blind signature for untraceable payments", Advances in Cryptology: Proceedings of Crypto 82, pp.199–203, Plemum, New York, 1983
[7] T. El Gamal,"A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", Advances in Cryptology, Proceedings of CRYPTO '84, LNCS 196, pp.10-18, Springer, 1984
[8] S.Goldwasser,S.Micali.and R.L.Rivest, " A digital signature scheme secure against adaptive chosen message attacks, " SIAM Journal on Computing,pp.236- 238,1988.
[9] Y.Hirai, T.Kurokawa, S.Matsuo, H.Tanaka and A.Yamamura," Classification of Hash Functions Suitable for Real-Life Systems" IEICE Transactions 91-A(1): pp.64–73 (2008)
[10] T. Izu, N. Kanaya, M. Takenaka, T. Yoshioka, "PIATS: A Partially Sanitizable Signature Scheme", ICICS 2005, LNCS 3783, pp.72-83, Springer, 2005.
[11] H. Kuwakado, M. Morii, "Restrictively Sanitizable Signature Scheme", SCIS 2006, 4A1-3, pp.274, 2006.
[12] K. Miyazaki, G. Hanaoka, H. Imai, "Digitally Signed Document Sanitizing Scheme from Bilinear Maps", SCIS 2005, 3E3-5, pp.1471-1476, 2005.
[13] K. Miyazaki, M. Iwamura, T. Matsumoto, R. Sasaki, H. Yoshiura, S. Tezuka, H. Imai, "Digitally Signed Document Sanitizing Scheme with Disclosure Condition Control", IEICE Transactions on Fundamentals, Vol E88-A, pp.239-246, No. 1, 2005.
[14] K. Miyazaki, S. Susaki, M. Iwamura, T. Matsumoto, R. Sasaki, H. Yoshiura, "Digital Documents Sanitizing Problem", IEICE Technical Report, ISEC 2003-20, pp.61-67, 2003.
[15] H.Nakata,"Nagata now admits e-mail was fake, faces Diet discipline", The Japan Times Online, 3rd Mar, 2006, http://search.japantimes.co.jp/cgi-bin/nn20060303a1.html
[16] M. Gebhardt, G. Illies and W. Schindler, "A Note on Practical Value of Single Hash Collisions for Special File", Proc. of NIST 1st Cryptographic Hash Workshop, 2005
[17] S.Lu,R.Ostrovsky,A.Sahai,H.Shacham and B.Waters, " Sequential Aggregate Signatures and Multisignatures without Random Oracles, " Cryptology ePrint Archive,Report 2006/141,2006.
[18] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards, " Advances in Cryptology - CRYPTO '89, LNCS 435, pp.239-252, 1990.
[19] R. Steinfeld, L. Bull, Y. Zheng, "Content Extraction Signatures", ICICS 2001, LNCS 2288, pp.285-304, Springer, 2001.
[20] M.Stevens, A.Lenstra and B.Weger, "Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities", Proc.of EUROCRYPT2007, LNCS 4515, pp.1-22, Spring, 2007.
[21] P.Sarbanes and M.G.Oxley, "Public Company Accounting Reform and Investor Protection Act of 2002", PL 107-204, 2002
[22] M. Suzuki, T. Isshiki, K. Tanaka, "Sanitizable Signature with Secret Information", SCIS 2006, 4A1-2, pp.273, 2006.
[23] B.Waters, "Efficient identity based encryption without random oracles", Proc.of EUROCRYPT2005, LNCS 3494, pp.114-127, Spring, 2005.