An Efficient Elliptic Curve Discrete Logarithm based Trapdoor Hash Scheme without Key Exposure

Yi Sun
Beijing Jiaotong University School of Computer&Information Technology
Zhengzhou Information Science and Technology Insitute
State Key Laboratory of mathematics Engineering and advanced computing
Zhengzhou, China
E-mail:11112072@ bjtu.edu.cn

Xingyuan Chen
Zhengzhou Information Science and Technology Insitute

Xuehui Du
Zhengzhou Information Science and Technology Insitute
State Key Laboratory of mathematics Engineering and advanced computing
Zhengzhou, China

***Abstract*—The trapdoor hash function plays essential role in constructing certain secure digital signature, and signature scheme that composed by trapdoor hash function is widely applied in different fields. However, the key exposure problem of trapdoor hash scheme has brought great distress. In this paper, an efficient trapdoor hash scheme without key exposure based on elliptic curve discrete logarithm is put forward and its security is analyzed, the scheme satisfies the five properties of trapdoor hash functions: effective calculation, trapdoor collision, collision resistance, key exposure resistance and semantic security. Through comparing and analyzing with the existing schemes, it shows that the proposed scheme, which has only multiplicative complexity and removes the operations of computing finite field element inverse, is more advantage in terms of safety and efficiency. Moreover, the scheme supports batch computation that it can greatly improve the efficiency of verification.**

***Index Terms*—Trapdoor hash function; Key-exposure; Elliptic curve discrete logarithm**

I. INTRODUCTION

The concept of trapdoor hash function concept is originally derived from the trapdoor commitment ideological proposed by Brassard et al [1]. A trapdoor hash function, also known as a chameleon hash function, was initially constructed by Krawczyk and Rabin [2]. A so-called chameleon hash function is a trapdoor one-way hash function with some special properties, which prevents everyone except the holder of the trapdoor information from computing the collisions for a randomly given input.

The trapdoor hash function plays essential role in constructing certain secure digital signature, and signature scheme that composed by trapdoor hash function is widely applied in different fields. Trapdoor hash function is originally used to design the chameleon signatures and undeniable signature [3], at the same time, it provides the non-repudiation signature information and shall not transfer, thus it has very extensive application in copyright protection and the anonymous credit certificate [6-8]. In 1990, Even et al [4] first time proposed online / offline signature scheme. Later Shamir and Tauman [5] employed trapdoor hash function to develop a new mechanism, called “hash-sign-switch”, that can be used to convert any kind of signature scheme into an online/offline signature scheme. In online/offline signature schemes, the signature process is divided into two stages offline and online. Offline phase refers to the signature of the message before sending, almost all the calculations are done in this stage, and the calculated results are stored. The phase after the signature of the message is given is the online stage, with news and offline phase calculated data as input, and generate signature after a small amount of computation. It can improve the response speed of signer after signature request arrives. After the message is given, with a small amount of calculation, it can quickly generate the

Manuscript received January 1, 2013; revised June 1, 2013; accepted July 1, 2013.
This paper is sponsored by “National Basic Research Program of China”(i.e. 973 Program 2011CB311801;863 Program 2012AA012704)

doi:10.4304/jcp.8.11.2851-2856

signature, sign and return the results to the requester. Such schemes can be used for signature schemes that require high response speed, or equipment calculation ability is limited. In offline stage, calculation can be implemented by powerful computing equipment in the equipment free time, and the result can be stored. Message is given after only a small amount of calculation with quick response. There is no requirement for high computing capacity equipment, and even in a weak processor (such as a smart card), signature operation can also be done very fast. At present, the smart card is widely used in devices such as mobile phone, PDA, and bank card [9-11, 26], so the online/offline signature has very important application value in reality. The difference between trapdoor hash function based on online/offline signature scheme and chameleon signature scheme is: a receiver has the trapdoor information in chameleon signature scheme; but the signer has the trapdoor information in online/offline signature scheme.

More recently, D. Schroeder et al [13] and S. Chandrasekhar et al [12] further extend the application of trapdoor hash function to construct stream authentication scheme. In [13], the chameleon hash function is used to construct a data structure, and this data structure is called chameleon authentication tree (CAT). Based on the CAT, a very efficient verification algorithm is obtained. This scheme supports an exponential number of elements, efficient updates, and the items that in the database are publicly verifiable. As a second application of CAT, the paper constructed a new transformation from any one-time to many-time signature scheme that is more efficient than previously known solutions. In [12], reference to the ideas of the online/offline signature scheme, the trapdoor hash function is applied to the signature amortization mechanism and composes a stream authentication scheme. The scheme can better resist packet loss and reduce the overhead of computation, storage and communication, and achieve efficient and real-time authentication of data stream.

Overall, the application of trapdoor hash function is very important and wide. However, there is a limitation that the signatures for different messages must use different trapdoor hash values, since the trapdoor hash function is used to compute the message digest in some signature schemes. Otherwise, if the signer tries to use the same hash value twice to obtain two signatures on two different messages, the recipient will obtain a hash collision and use it to recover the signer's trapdoor information, which is the signer's secret key. This problem is known as the key exposure problem of trapdoor hashing. The key exposure problem results in the compromise of the (private) trapdoor key in the presence of a pair of messages with the same trapdoor hash value.

In order to solve the key exposure problem and further improve the efficiency and security strength of the scheme, this paper is put forward a new efficient multiple-collision trapdoor hash scheme without key exposure based on elliptic curve discrete logarithm, and analyses the security and performance of the scheme. The proposed trapdoor hash scheme is a little more efficient in both hashing computation and collision computation through comparing with the existing schemes. Moreover, the scheme supports batch computation, thus it can greatly improve the efficiency of verification.

The rest of this paper is organized as follows: We begin with a discussion of related work in Section 2, and provide a new trapdoor hash function without key exposure based on Elliptic Curve ($EDL-MCTH$) in Sections 3. We analyze the performance and security for the $EDL-MCTH$ scheme in Section 4. Finally, we conclude this paper in Section 5.

II. Related Work

Ateniese and de Medeiros [14] firstly addressed the key exposure problem of the trapdoor hash scheme in Financial Cryptography 2004, meanwhile, they proposed to use the identity-based chameleon hash function to solve the key exposure problem. The main idea of Ateniese and de Medeiros is based on the identity and a transaction to constructe one-time trapdoor information to solve the problem of key exposure, the trapdoor collision can only exposure one-time trapdoor information but cannot exposure long-term trapdoor information. The signature forgery can only let signature restore the trapdoor information related to the transactions in this scheme. So the signer will not be able to refuse the signature of any messages in other transactions, and will not exposure the key at the same time. But such theory only solves part of the problem of key compromise, because every transaction needs to change the recipient's public key. In the same year, Chen et al [15] used the bilinear that based on the Gap Diffie-Hellman groups to construct a chameleon hash function without key exposure for the first time. Later Ateniese and de Medeiros [16] improved the idea[14] and put forward three kinds of the chameleon hash functions without key exposure: one is based on bilinear pairings, the others two are based on the RSA assumption. In 2009, Gaoetal. [17] proposed a chameleon hash function of key exposure-free based on Schnorr signature. However, the program is an interactive protocol between the signer and the recipient, which is contrary to the originally defined chameleon hash function and signature schemes intended.

At present, to solve the problem of the key exposure of the trapdoor hash function it mainly has two methods: One method is through a short signature to construct the one-time key to solve the key exposure problems, such as literatures [14 -18, 27]. Another method is constructing different trapdoor element to solve the problem of key leak. Such as: in [19-21], the trapdoor hash schemes of key exposure-free is constructed base on integer factorization assumption; in [22, 23], a kind of special double trapdoor hash function is put forward, the key is divided into two parts: the key for a long time and the key for one-time; in [24], multiple-collision trapdoor hash families was constructed, respectively, based on the DL and factoring; In [26] , the message authentication code (with the key concepts of the Hash function) was introduced to construct a three trapdoor Hash function

base on the improved scheme[22]. Moreover, in [25], Identity-Based Chameleon Hash Scheme without key exposure is put forward, this scheme contains three trapdoors, two trapdoors for a long time that give priority to the private key, key and ID . A one-time trapdoor to use ID label private key signature, which only leaks the same collision trapdoor. Above the trapdoor hash functions scheme are mainly used to construct chameleon signatures and online/offline signature. As the development of trapdoor hash function in different applications, the new requirements are put forward for the existing trapdoor hash schemes. Apparently there will be further studies of trapdoor hash schemes and how to improve the scheme according to the new application requirements.

III. A NEW TRAPDOOR HASH FUNCTION WITHOUT KEY EXPOSURE BASED ON ELLIPTIC CURVE

First of all, in this section , the formal definition of the trapdoor hash function without key exposure is introduced, and then a new key-exposure-free trapdoor hash scheme is put forward based on the improvement of [22, 23].

A. Preliminaries

1) The assumptions of elliptic curve discrete logarithm

Let p be a prime power. $E(F_l)$ is elliptic curves over finite fields F_l . Let $\#E(F_l)$ of $E(F_l)$'s order, the order of element p in $E(F_l)$ is a prime number q and $q|\#E(F_l)$. Hutchison G is a q-order cyclic group P generates. Elliptic curve discrete logarithm problem (*ECDLP*) : given $(P,Q)\in E(F_l)$, find an integer $a\in Z_q$, so $Q=aP$ in G .

Definition 1 (elliptic curve discrete logarithmic assumption) If there is no probabilistic polynomial time algorithm (*PPT*) in T time to solve the elliptic curve discrete logarithm problem on the group G with ε probability , then the assumption $(T,\varepsilon)-ECDLP$ on the group G is established·

2) Trapdoor hash function

Definition 2 (Trapdoor *Hash* family) A trapdoor *Hash* family is composed by a tuple $(\mathcal{G},\mathcal{H})$:

· $\mathcal{G}$ is a probabilistic polynomial time key generation algorithm that on input 1^k , outputs a pair hash/trapdoor key (HK,TK) , such that the sizes of HK,TK are polynomially related to k .

· $\mathcal{H}$ is a family of randomized hash functions. Every hash function in $\mathcal{H}$ is associated with a hash key HK , and is applied to a message from a space M and a random element from a finite space R . The output of the *hash* function H_{HK} does not depend on TK .

A trapdoor *Hash* function family $(\mathcal{G},\mathcal{H})$ satisfies the following properties:

·Effective calculation: Given the *hash* key HK and a pair $(m,r)\in M\times R$, $H_{HK}(m,r)$ is computable in a polynomial time.

·Collision resistance: There is no polynomial time algorithm that given only HK ,can find two pairs $(m_1,r_1),(m_2,r_2)\in M\times R$ meet the $m_1\neq m_2$ and $H_{HK}(m_1,r_1)=H_{HK}(m_2,r_2)$ with a non-negligible probability (the probability is related with HK , here $(HK,TK)\leftarrow\mathcal{G}(1^k)$,and random algorithm throwing coins).

·Trapdoor collision: There exists a probabilistic polynomial time algorithm. Input $(HK,TK)\leftarrow\mathcal{G}(1^k)$, a pair $(m_1,r_1)\in M\times R$ and an additional message $m_2\in M$, the output $r_2\in R$ satisfies: $H_{HK}(m_1,r_1)=H_{HK}(m_2,r_2)$. If r_1 is uniformly distributed in R then the distribution of r_2 is computationally indistinguishable from uniform in R .

B. The Formal Definition of the Trapdoor Hash Function without Key Exposure

Definition 3 (The multiple-collision trapdoor *hash* function family) a multiple-collision trapdoor *hash* function family by a triple $(\mathcal{G},\mathcal{G}',\mathcal{H})$ consisting of:

· $\mathcal{G}$ is a probabilistic polynomial time in the key generation algorithm, input 1^k , outputs a long-term hash/trapdoor key pair (HK,TK) , such that the sizes of HK,TK are polynomially related to k .Note that (HK,TK) is associated with the all trapdoor hash functions in the family and can be used repeatedly during its life span.

· $\mathcal{G}'$ is a probabilistic polynomial time in the key generation algorithm, input 1^k , outputs a one-time hash/trapdoor key pair (HK',TK') , such that the sizes of HK',TK' are polynomially related to k . Note that (HK',TK') can be used only once during its life span.

· $\mathcal{H}$ is a random *hash* function family. Input 1^k , a pair hash/trapdoor key (HK,TK) , a pair $(m,r)\in M\times R$ and a message $m'\neq m$, outputs a collision parameters r' and HK' such that $H_{HK}(m,r)=H_{HK'}(m',r')$. When $HK\neq HK'$, the hash key HK' along with the corresponding trapdoor key TK' is called a one-time key pair and can be used only once.

Definition 4 A multiple-collision trapdoor *hash* function family $(\mathcal{G},\mathcal{G}',\mathcal{H})$ should meet the following properties:

Property 1: Effective calculation. Given *hash* key HK and a pair $(m,r)\in M\times R$, $H_{HK}(m,r)$ is computable in polynomial time.

Property 2: Trapdoor collision. There exists a probabilistic polynomial time algorithm that given only HK , can find two pairs $(m_1,r_1),(m_2,r_2)\in M\times R$ meet the $m_1\neq m_2$ and $H_{HK}(m_1,r_1)=H_{HK}(m_2,r_2)$ in a non-negligible probability. If r_1 is uniformly distributed in R then the distribution of r_2 is computationally indistinguishable from uniform in R .

Property 3: Collision resistance. There is no polynomial time algorithm A , the only input HK , can

obtain two pairs of $(m,r),(m',r') \in M \times R$ satisfies: $[m \neq m'] \wedge [TH_{HK}(m,r) = H_{HK'}(m',r')]$, with non-negligible probability.

Properties 4: Key exposure resistance. There is no polynomial time algorithm A , the input of a long-term *hash* key HK , the two one-time *hash* keys HK' and HK'' , two pairs of $(m,r),(m',r') \in M \times R$ and satisfies $[m \neq m'] \wedge [TH_{HK}(m,r) = H_{HK'}(m',r')]$, then can find the long-term trapdoor key TK , with non-negligible probability.

Property 5: Semantic security. Let $H[X]$ denote the entropy of a random variable X , and $H[X|Y]$ the entropy of the variable X given the value of a random function Y of X . Semantic security means that the conditional entropy H[m|C] of the message given its trapdoor hash value C equals the total entropy H[m] of the message sapce.

C. An Efficient Multiple-collision Trapdoor Hash Scheme without Key Exposure

This section provides a new key-exposure trapdoor hash scheme based on the elliptic curve .

Definition 5 ($EDL-MCTH$) An efficient multiple-collision trapdoor hash scheme ($EDL-MCTH$) without key exposure based on elliptic curve discrete logarithm is a four-tuple $TH = (SysParGen, KeyGen, THGen, TrapColGen)$.

· *SysParGen* :Let l be a prime power, and $E(F_l)$ an elliptic curve over finite field F_l . Let $\# E(F_l)$ be the number of points of $E(F_l)$,and P be a point of $E(F_l)$ with prime order q where $q | \# E(F_l)$. Denote by G the subgroup generated by P . Define a collision resistant hash function $f : Z_q \times G \to Z_q$ .The system public parameters is $params = \{G, q, P, f\}$, where p and q are 1024-bit and 160-bit primes.

· *KeyGen* :An entity uses the system public parameters *params* , to generate trapdoor/hash key pair $(TK, HK) = (\alpha, Y)$, where $\alpha \in_R Z_q^*$ and $Y = \alpha P$.

· *THGen* :An Entity selects element $r \in Z_q$ and uses the *hash* key Y to generate a trapdoor hash function for message $m \in Z_q$, the trapdoor *hash* function is defined as: $TH_Y(m,r) = f(m,Y)Y + rP$.

· *TrapColGen* :Given the trapdoor key and hash key pair $(TK, HK) = (\alpha, Y)$, $(m \times r) \in Z_q \times Z_q$, and a additional message $m' \in Z_q$, compute collisions $r' \in Z_q$ fellow the steps :

(1) choose a one-time trapdoor $\beta \in_R Z_q^*$ compute $K = \beta P$.

(2) use trapdoor key α and β compute r' , such that $TH_Y(m,r) = TH_K(m',r')$, compute: $r' = \alpha f(m,Y) - \beta f(m',K) + r \bmod q$.

IV. Security and Performance Analysis

In this session, the detailed security analysis of the proposed scheme in Section 3 is provided and its performance is compared with some classic shemes.

A. EDL – MCTH Scheme Security Analysis

Proving the security of $EDL-MCTH$ scheme: it is to prove that $EDL-MCTH$ scheme satisfies five properties of the definition 4, under the discrete logarithm problem assumption on the group G .

Theorem 1 $EDL-MCTH$ scheme under the assumption of $(T,\varepsilon)-ECDLP$, elliptic curve discrete logarithm problem is intractable on the Group G .

Proof:

(1)Effective calculation

Given *hash* key HK and a pair $(m,r) \in M \times R$, $H_{HK}(m,r)$ can be computed in polynomial time.

(2)Trapdoor collision

Assuming given *hash* key (HK, HK') , trapdoor key (TK, TK') , and a pair $(m,r) \in M \times R$ and a message $m' \in M$, find r' such that $f(m,Y)Y + rP = f(m',K)K + r'P$, the value r' can be calculated as follows: $r' = \alpha f(m,Y) - \beta f(m',K) + r$ .If r is uniformly distributed in R then the distribution of r' is computationally indistinguishable from uniform in R .

(3)Collision resistance

According to definition 4, we need to consider two cases: (a) $HK = HK'$ (for resistance to simple collision forgery) (b) $HK \neq HK'$ (for resistance to one-time collision forgery).

(a) $HK = HK'$. collision forgery resisitance means assume that the input parameters *params* and *hash* key HK does not exist a PPT collision forger $\mathcal{F}$ can successfully output $[m \neq m'] \wedge [TH_{HK}(m,r) = H_{HK}(m',r')]$ in non-negligible probability ε .

Reduction to Absurdity, suppose that exists a PPT collision forger $\mathcal{F}$ can successfully output $[m \neq m'] \wedge [TH_{HK}(m,r) = H_{HK}(m',r')]$ in non-negligible probability ε . Given a discrete logarithm instance $< G, q, P, Y >$, which trapdoor/hash key is $(y, Y = yP)$, we can get equation: $yf(m,Y) + r = yf(m',Y) + r' \bmod q$, which can find $y = ((f(m,Y) - f(m',Y))^{-1} + r' - r) \bmod q$ .So y contrary $(T,\varepsilon)-ECDLP$,then the problem is proved.

In fact, the simple problem of collisions of the situations described in (a), is the famous key compromise problem mentioned in the introduction, by the above analysis that if given two pairs of messages to meet $(m,r),(m',r') \in M \times R$, third party can successfully use $(m,r),(m',r') \in M \times R$ to calculated trapdoor key TK , thereby producing the problem of key exposure.

(b) $HK \neq HK'$. Suppose there is a *PPT* collisions forged $\mathcal{F}$ resistance to a non-negligible probability ε definition 5 trapdoor *hash* scheme. Given the *hash* key $HK, HK' (HK' \neq HK)$ and the system parameter *params* , $\mathcal{F}$ runs in polynomial time and outputs $< m, r, m', r' >$,here $m \neq m', r \neq r'$, and

$TH_{HK}(m,r)=TH_{HK'}(m',r')$ has a non-negligible probability. Assume that $\mathscr{T}$ can be constructed a PPT algorithm h able to crack the discrete logarithm problem. Given a discrete logarithm problem instance $<G,q,P,X>$, h need to find $x\in Z_q^*$ to satisfie $X=xP$. h selects $y\in_R Z_q^*$ and calculates $Y=yP$, $X=xP$. h independently in parallel runs two instances of the forger $\mathscr{T}$, $\mathscr{T}$ each instance input $<G,q,P,X>$ is randomly selected. Until $\mathscr{T}$ of each instance of $<m_1,r_1,m_1',r_1'>$ and $<m_2,r_2,m_2',r_2'>$ respectively generate a collision forgery, $m_1=m_2$ or $r_1=r_2$ or $m_1'=m_2'$ or $r_1'=r_2'$, $\mathscr{T}$ is repeatedly executed. Given $TH_{HK}(m_1,r_1)=TH_{HK'}(m_1',r_1')$ and $TH_{HK}(m_2,r_2)=TH_{HK'}(m_2',r_2')$, we get the following two linear equations:

$$xf(m_1,X)+r_1=yf(m_1',Y)+r_1'\bmod q$$
$$xf(m_2,X)+r_2=yf(m_2',Y)+r_2'\bmod q$$

Apparently the above two linear equations is solvable, it can find x and y, contrary to $(T,\varepsilon)-ECDLP$ assumptions. Then the problem is proved.

(4)Key exposure resistance

According to $EDL-MCTH$ scheme, the so-called key exposure resistance means that a given two tuples $<m,r,HK>$ and $<m',r',HK'>$, here $m\neq m'$, $r\neq r'$ and $TH_{HK}(m,r)=TH_{HK'}(m',r')$, the probability that a PPT algorithm outputs TK is negligible.

To the contrary, suppose there is a PPT algorithm can output TK with non-negligible probability. Then it can be computed the discrete logarithm TK' of the hash key HK'.

$$TK'=f(m',HK')^{-1}(f(m,HK)TK+r-r')\bmod q$$

Clearly contrary to the $(T,\varepsilon)-ECDLP$ assumption, so the problem is proved. Therefore, the proposed trapdoor $hash$ scheme is against key exposure.

(5)Semantic security

Since m,r is the independent variable, so the conditional probability $\mu(\mathrm{m}|\mathrm{C})=\mu(\mathrm{m}|\mathrm{r})$ is established, then we will be able to prove that the conditional entropy $H[\mathrm{m}|\mathrm{C}]=H[\mathrm{m}]$.

$$H[\mathrm{m}|\mathrm{C}]=-\sum_m\sum_c\mu(m,c)\log(\mu(m\mid c))=-\sum_m\sum_c\mu(m,c)\log(\mu(m))$$
$$=-\sum_m\mu(m)\log(\mu(m))=H[\mathrm{m}]$$

In summary, the $EDL-MCTH$ scheme satisfies the five properties: effective calculation , trapdoor collision, collision resistance, key exposure resistance and semantic security, under $(T,\varepsilon)-ECDLP$ assumption.

B. Performance Analysis

For fairness of comparison, Tables 1 present performance numbers for the discrete log-based version of the key-exposure-free trapdoor hash scheme. The proposed trapdoor hash scheme is a little more efficient in both hashing computation and collision computation.

Moreover, during computation of the trapdoor hash value of $m_i,...m_{i+n}$ we observe the following:

$$\sum_{i=0}^{m}f(m_{n+i},Y_{n+i})Y_{n+i}+P\sum_{i=0}^{m}r_{n+i}=\sum_{i=0}^{m}[f(m_0,Y_0)Y_0+r_0P]=\sum_{i=0}^{m}TH_{Y_0}(m_0,Y_0)$$

Thus, the scheme supports batch computation and this performance can greatly improve the efficiency of verification.

TABLE 1
PERFORMANCE COMPARISON OF PROPOSED TRAPDOOR HASHING SCHEME EDL- MCTH WITH EXISTING SCHEMES

Scheme	Hash computation	Collision computation	Batch computation	Mathematical assumption
NRTH [16]	$2T_{\exp}+T_m$	$2T_{\exp}+T_a+T_m$	NO	DL
MCDLTH [24]	$3T_{\exp}+2T_a$	$T_I+3T_a+2T_s+2T_m$	Yes	DL
DL_MTH [12]	$2T_{\exp}+T_a$	$T_I+2T_a+T_s+T_m$	Yes	DL
ECCH [22]	$2T_{\exp}+T_s$	$T_I+2T_a+T_m$	NO	ECDL
TECCH [23]	$3T_{\exp}+T_s$	$2T_a+T_s$	NO	ECDL
EDL-MCTH	$2T_{\exp}+T_s$	$2T_a+T_s+T_m$	Yes	ECDL

Note: $T_a,T_s,T_m,T_{\exp},T_I$ respecting the operating time of a module multiplication, a module addition, a module subtraction, a module exponentiation, a module inverse.

V. CONCLUSION

Trapdoor hash scheme plays a very important role in practical application due to its unique characters. But the traditional trapdoor hash scheme usually has key exposure problem [14], which significantly limits its further application in practice. Therefore the key-exposure-free trapdoor hash scheme is critical for the study of the trapdoor hash scheme. In this paper, we propose an efficient key-exposure-free trapdoor hash scheme which is based on elliptic curve discrete logarithm. We prove that the proposed scheme satisfies the five properties of the trapdoor hash function. We also compare the key-exposure-free trapdoor hash scheme performance with the existing scheme. The analysis shows that the key-exposure-free trapdoor hash scheme is more efficient and applicable, since the scheme has only multiplicative complexity, removes the operations of computing finite field element inverse and supports batch validation.

ACKNOWLEDGMENT

The authors gratefully acknowledge the sponsorship of “National Basic Research Program of China”(i.e. 973 Program2011CB311801, 863 Program 2012AA012704)

And gratitude should go to all the people, who help to make this paper finished, and ZhengZhou Information Science and Technology Institude for its support in making this work possible. We are also thankful for the provious work that has done in this research area.

REFERENCES

[1] G. Brassard, D. Chaum, and C. Cre´ peau, "Minimum Disclosure Proofs of Knowledge," J. Computer and System Sciences, vol. 37, no. 2, pp. 156-189, 1988.

[2] H. Krawczyk, T. Rabin, Chameleon hashing and signatures, in: Proceeding of the 7th Annual Network and Distributed System Security Symposium,2000, pp. 143–154.

[3] D. Chaum, H. van Antwerpen, Undeniable Signatures, Advances in Cryptology-Crypto 1989, LNCS, vol. 435, Springer-Verlag, 1989, pp. 212–216.

[4] Even, S., Goldreich, O. and Micali, S. (1990) On-line/Off-line Digital Signatures. Proc. Crypto'89, Santa Barbara, CA, USA, August 20–24, Lecture Notes in Computer Science, Vol. 435,pp. 263–277. Springer, Berlin.

[5] Shamir, A. and Tauman, Y. (2001) Improved On-line/Off-line Signature Schemes. Proc. Crypto'01, Santa Barbara, CA, USA, August 19–23, Lecture Notes in Computer Science, Vol. 2139, pp. 355–367. Springer, Berlin.

[6] D.Chaum.Security without Identification:Transacation Systems to Make Big Brother Obsolete.Communication soft he ACM,28(10).ACM Press,1985,1030-1044

[7] E.Bangerter,J.Camenisch,A.Lysyanskaya.A Cryptographc Frameworkfor the Controlled Release of Certified Data.Proc.of the 12th International Workshop Oil Security Protocols.LNCS 3957,Springer-Verlag,2006,20-42

[8] J.Camenisch,A.Lysyanskaya.Asignature Scheme with Efficient Protocols.Security in Communication Networks(SCN2002).LNCS2576,Springer-Verlag,2003,268-289

[9] C.-L. Hsu and C.-F. Lu, "A Security and Privacy Preserving E-Prescription System Based on Smart Cards", J. Med. Syst., vol 36, no 6, pp 3637–3647, Dec 2012.

[10] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures: Implementation and Evaluation", IEICE Trans. Inf. Syst., vol E95D, no 1, pp 126–133, Jan 2012.

[11] Wang J S, Yang F Y, Paik I. A novel E-cash payment protocol using trapdoor hash function on smart mobile devices[J]. International Journal of Computer Science and Network Security, 2011, 11(6): 12-19.

[12] S. Chandrasekhar, S. Chakrabarti, and M. Singhal, "A Trapdoor Hash-Based Mechanism for Stream Authentication", IEEE Transactions on Dependable and Secure Computing, vol 9, no 5, pp 699 –713, Oct 2012.

[13] D. Schroeder and H. Schroeder, "Verifiable data streaming", in Proceedings of the 2012 ACM conference on Computer and communications security(CCS), New York, NY, USA, 2012, pp 953–964.

[14] G.Ateniese and B. deMedeiros, Identity-based chameleon hash and applications, FC2004, NCS3110,pp.164-180,Springer-Verlag,2004.

[15] X. Chen, F. Zhang, and K. Kim, "Chameleon Hashing without Key Exposure," Proc. Seventh Int'l Conf. Information Security (ISC), K. Zhang and Y. Zheng, eds., pp. 87-98, 2004.

[16] G.Ateniese and B. de Medeiros, On the key exposure problem in chameleon hashes, SCN 2004,LNCS3352,pp.165-179,Springer-Verlag,2005

[17] W.Gao,F.Li,and X.Wang, Chameleon hash without key exposure based on Schnorr signature, Computer Standards and Interfaces31(2009)282-285.

[18] X. Chen, F. Zhang, H. Tian, B. Wei, and K. Kim, "Discrete logarithm based chameleon hashing and signatures without key exposure", Computers & Electrical Engineering, vol 37, no 4, pp 614–623, 2011.

[19] K.Kurosawa,K.Schmidt—Samoa.New Online/Offine Signature Schemes without Random Oracles.PKC2006.LNCS 3958,Springer—Verlag,2006,330-346

[20] W.Gao,X.Wang,D.Xie.Chameleon Hashes without Key Exposure based on Factoring.Journal of Computer Science and Technology.2007,22(1):109-113

[21] X.Chen,H.Tian,F.Zhang.Comments and Improvements on Chameleon Hashing Without Key Exposure Based on Factoring.Cryptology ePrint Archive,2009,http://eprint.iacr.org/2009/319

[22] Chen, X., Zhang, F., Susilo, W. and Mu, Y. (2007) Efficient Generic On-Line/Off-Line Signatures Without Key Exposure.Proc. ACNS'07, Zhuhai, China, June 5–8, Lecture Notes inComputer Science, Vol. 4521, pp. 18–30. Springer, Berlin.

[23] Chen, X., Zhang, F., Tian, H., Wei, B., Susilo, W., Mu, Y.,Lee, H. and Kim, K. (2008) Efficient generic on-line/off-line(threshold) signatures without key exposure. Inform. Sci. 178, 4192–4203.

[24] L. Harn, W.-J. Hsin, and C. Lin, "Efficient On-line/Off-line Signature Schemes Based on Multiple-Collision Trapdoor Hash Families", Comput. J., vol 53, no 9, pp 1478–1484, 2010.

[25] X. Chen, F. Zhang, W. Susilo, H. Tian, J. Li, and K. Kim, "Identity-Based Chameleon Hash Scheme without Key Exposure", in Information Security and Privacy, R. Steinfeld and P. Hawkes, Eds Springer Berlin Heidelberg, 2010, pp 200–215.

[26] D.-R. Lin, C.-I. Wang, and D. J. Guan, "Efficient vehicle ownership identification scheme based on triple-trapdoor chameleon hash function", J. Netw. Comput. Appl., vol 34, no 1, pp 12–19, Jan 2011.

[27] X. Chen, F. Zhang, H. Tian, B. Wei, and K. Kim, "Discrete logarithm based chameleon hashing and signatures without key exposure", Computers & Electrical Engineering, vol 37, no 4, pp 614–623, 2011.