

A Secure Chameleon Hash Function without Key Exposure from Pairings

Jianhong Zhang¹, Hua Chen¹, and Qin Geng¹

¹ College of Sciences, North China University of Technology, Shijingshan District,
Beijing 100144, China
Email: jhzhang@ncut.edu.cn

Abstract—Chameleon signatures are based on well established hash-and-sign paradigm, where a chameleon hash function is used to compute the cryptographic message digest, and becomes an important building block. The chameleon hash function is a trapdoor one-way hash function with some special properties, and plays an important role in constructing chameleon signature. In the paper, we propose a new chameleon hash scheme which enjoys some advantages of the previous schemes: collision-resistant, semantic security, and key-exposure -freeness. At the same time, we show that the recipient's trapdoor information will never be compromised under the assumption of q -SDH+CDH problem which is a new security assumption

Index Terms—security analysis, chameleon hash function, key exposure free, the q -SDH+CDH problem

I. INTRODUCTION

A chameleon hash function is a trapdoor collision-resistant hash function: Without knowledge of the trapdoor information, a chameleon hash function has the same characteristics of any cryptographic hash function, such as pre-image and collision resistance; however, collisions and second pre-images can be easily computed once the trapdoor is known.

An interesting application of chameleon hashing is to obtain non-transferable signature algorithms known as chameleon signatures. Chameleon signatures, introduced in [5], are signature schemes based on the hash-and-sign paradigm. To authenticate a message m , a signer computes its digest value h using a chameleon hash function, and then signs h using an arbitrary signing algorithm of the signer's choice. Thus, chameleon hash function plays very important roles in constructing chameleon signature.

Hash function is an important building block in the construction of a secure signature scheme. When a chameleon hash function is used within a hash-and-sign signature scheme, it permits the party with knowledge of the trapdoor to re-use the signature value to authenticate other messages of choice. In particular, if the hash function is part of the recipients public key, then the signature is publicly verifiable by no one other than the intended recipient. On the other hand, if the recipient re-uses the hash value to obtain a signature on a second message, the signer can prove knowledge of a hash collision, since the original signed message and the claimed signed message have the same hash value. Because computing hash collisions is infeasible for the

signer, possession of such a collision is seen as proof of forgery by the signature recipient.

In [7], Chen *et al* provided a specific construction of a key-exposure free chameleon hash function, working in the setting of Gap groups with bilinear pairings. While that certainly constitutes the first full construction of a key-exposure free chameleon hash, it does not settle the question of whether constructions exist that are either based on other cryptographic assumptions, or of more efficient schemes, for instance of comparable performance to the original chameleon hash function [5]. In [1], Ateniese and Medeiros propose three schemes based on Stong RSA, RSA $[n,n]$ [10] and SDH (Strong Diffie-Hellman assumption) respectively. In fact, the ephemeral trapdoor recovered by a pair of collisions is a kind of signature of the label under the main trapdoor. So the property key exposure-freeness is due to the security of the signature applied to the label, such as the common RSA signature, the short signature based pairing [11]. Recently, Gao *et.al* proposed a novel chameleon hash scheme based on Schnorr signature in [3], but hash phase is interactive in their scheme. In this paper, we propose a novel chameleon hash function. The scheme enjoys some advantages of the previous schemes: collision-resistant, semantic security, and key-exposure-freeness. At the same time, we show that the recipient's trapdoor information will never be compromised under the assumption of q -SDH+CDH problem which is a new security assumption.

The rest of this paper is organized as follows. We describe the preliminaries of bilinear map and chameleon function in section 2. In section 3, a novel chameleon hash function scheme is given and the security of the corresponding scheme is analyzed in section 4. Finally, we conclude the paper in section 5.

II. PRELIMINARIES

We review some fundamental backgrounds required in this paper, namely bilinear pairing, complexity assumption and security model on which our scheme may be based.

A. Bilinear Maps

In the following, we recall the notions related to bilinear groups [11,12] as follows.

- G_1 and G_2 are two cyclic groups of prime order p ;
- g_1 and g_2 are two generators of groups G_1 and G_2 respectively.

- $e: G_1 \times G_2 \rightarrow G_T$ is a bilinear map such that $|G_1| = |G_2| = |G_T|$.

Let G_1 and G_2 be two cyclic groups as above. Let G_1, G_2 be two bilinear group as follows. A bilinear map is a map $e: G_1 \times G_2 \rightarrow G_T$ with the following properties:

1. Bilinear: for all $u \in G_1$ and $v \in G_2$, and $a, b \in \mathbb{Z}_p$, $e(u^a, v^b) = e(u, v)^{ab}$
2. Non-degeneracy: for all $u \in G_1$ and $v \in G_2$, $e(u, v) \neq 1$.
3. Computable: pairing $e(u, v)$ can be efficiently computed for all $u \in G_1$ and $v \in G_2$

We note the modified Weil and Tate pairings associated with supersingular elliptic curves are examples of such admissible pairings. The security of the scheme discussed in this paper is based on the following security assumption..

B. Security Assumption

Here we first review the definition of the strong Diffie-Hellman (SDH) assumption introduced in [11], on which the security of our signature is based, and then extend it into a new security assumption, the extended strong Diffie-Hellman assumption, on which the security of a variant of our signature scheme is based on

Let G_1 and G_2 be two cyclic groups of prime order p . Let g_1 be a generator of G_1 and g_2 be a generator of G_2 such that $g_1 \notin \langle g_2 \rangle$. The q -SDH problem is defined as follows: given $(g_1, g_2, g_2^a, g_2^{a^2}, \dots, g_2^{a^q})$ as input, it outputs a pair $(c, g_1^{1/(a+c)})$ for any $c \in \mathbb{Z}_p$. An algorithm A has advantage ϵ in solving the q -SDH problem if

$$\Pr[A(g_1, g_2, g_2^a, \dots, g_2^{a^q}) = (c, g_1^{1/(a+c)})] \geq \epsilon$$

Where the probability is taken over the random oracle of $g_2 \in G_2$, $x \in \mathbb{Z}_p$, and the coin tosses of A .

Definition1: We say that the (q, t, ϵ) -SDH assumption holds in groups G_1 and G_2 if not t -time algorithm has advantage at least ϵ in solving the q -SDH problem.

[Computational Diffie-Hellman (CDH) Assumption]. Let G be a CDH parameter generator. We say an algorithm A has advantage $\epsilon(k)$ in solving the CDH problem for G_1 if for a sufficiently large k ,

$$Adv_{G,A}(t) = \Pr[A(p, G_1, g^x, g^y) = g^{xy} \mid (p, G_1) \leftarrow G^k, P \leftarrow G_1, x, y \leftarrow \mathbb{Z}_p]$$

We say that G_1 satisfies the CDH assumption if for any randomized polynomial time in t algorithm A we have the $Adv_{G,A}(t)$ is negligible function.

Definition2. Inverse Computational Diffie-Hellman Problem (Inv-CDHP): Let G be a CDH parameter generator. We say an algorithm A has advantage $\epsilon(k)$ in solving the Inv-CDH problem for G_1 if for a sufficiently large k ,

$$Adv_{G,A}(t) = \Pr[A(p, G_1, g, g^x) = g^{x^{-1}} \mid (p, G_1) \leftarrow G^k, g \leftarrow G_1, x \leftarrow \mathbb{Z}_p]$$

We say that G_1 satisfies the Inv-CDH assumption if for any randomized polynomial time in t algorithm A we have the $Adv_{G,A}(t)$ is negligible function.

Theorem The CDH problem and Inv-CDH problem are polynomial time equivalent.

In the following, we present a novel security assumption: q -SDH+CDH Assumption, by combining the strong Diffie-Hellman with the computational Diffie-Hellman.

q -SDH+CDH Assumption: The q -SDH+CDH problem in group G_1 is defined as follows: give $q + 1$ -tuple $(g_1, g_1^a, \dots, g_1^{a^q})$ random pair (g_1, g_1^r) of group G_1 as inputs, output $(\rho \leftarrow g_1^{r/(\alpha+c)}, c)$ where g_1 is a generator of group G_1 , $c, r \in \mathbb{Z}_p$. Note that α and r are unknown numbers. Algorithm A has advantage, $Adv_{SDH}(q)$, in solving q -SDH+CDH in G_1 if

$$Adv_{q\text{-SDH+CDH}}(q) \leftarrow \Pr[A(g_1, g_1^a, \dots, g_1^{a^q}, g_1^r) = (g_1^{r/(\alpha+c)}, c)]$$

Where the probability is taken over the random choices of $g_1 \in G_1$, $\alpha, r \in \mathbb{Z}_p$, and the coin tosses of A .

Definition4. Adversary $A(t, \epsilon)$ -breaks the q -SDH+CDH problem if A runs in time at most t and $Adv_{q\text{-SDH+CDH}}$ is at least ϵ . The (q, t, ϵ) -SDH+CDH assumption holds if no adversary $A(t, \epsilon)$ -breaks the q -SDH+CDH problem.

According to the above definition, we know that the novel security assumption: **q -SDH+CDH Assumption**, is not easier than either q -SDH assumption. Because if the q -SDH+CDH Assumption can be solved in polynomial time, then we set $r = 1$, the above q -SDH+CDH assumption is converted into q -SDH assumption. It denotes that the q -SDH assumption can also be solved in polynomial time. Thus, we can obtain the lemma.

Lemma1. If the q -SDH+CDH Assumption can be solved in the polynomial time with non-negligible probability, then the q -SDH assumption is solvable.

Proof. Suppose that q -SDH+CDH assumption is solved.

Given an instance of q -SDH problem $(g_1, g_1^a, \dots, g_1^{a^q})$, we randomly $r \in \mathbb{Z}_p$ to compute $B = g_1^r$. Take $(g_1, g_1^a, \dots, g_1^{a^q}, (g_1, g_1^r))$ as inputs of q -SDH+CDH problem, output $(g_1^{r/(\alpha+c)}, c)$. Then we can compute $g_1^{1/(\alpha+c)}$ by the known r . Thus the q -SDH problem can be solved. Because we know that original proposition is equivalent to converse-negative proposition.

lemma2. If the q -SDH assumption is hard to solve in polynomial time, then the q -SDH+CDH assumption is also hard to solve in the polynomial time.

lemma3. If the CDH problem is solvable in the polynomial time, then q -SDH+CDH problem is also solvable.

Proof. Assume that the CDH problem is solvable, given g_1, g_1^a, g_1^b , then g_1^{ab} is able to be obtained. Given a q -SDH+CDH problem instance $(g, g^a, g^{a^2}, \dots, g^{a^q}, g, g^r)$, randomly choose $c \in \mathbb{Z}_p$ to compute

$$(g, g^{\alpha+c}, \dots, g^{(\alpha+c)^q}, (g, g^r))$$

by the above q -SDH+CDH problem instance.

Let $g_0 = g^{(\alpha+c)^q}$, then the inverted sequence of

$(g, g^{\alpha+c}, \dots, g^{(\alpha+c)^q})$ can be expressed as

$$(g_0, g_{01}^{1/(\alpha+c)} = g^{(\alpha+c)^{q-1}}, \dots, g_{0q} = g^{1/(\alpha+c)^q} = g)$$

When q is an odd number, we set $\rho = (q-1)/2$, otherwise, q is an even number, we set $\rho = q/2$.

if q is an odd number, we obtain $g_{0,\rho} = g_0^{(1/(\alpha+c))^\rho}$ and $g_{0,\rho+2} = g_0^{(1/(\alpha+c))^{2\rho+2}}$. Because the CDH problem is solvable, then we can obtain

$$g_0^{(1/(\alpha+c))^{2\rho+2}} = g_0^{(1/(\alpha+c))^{q+1}}$$

by the values $(g_{0,\rho}, g_{0,\rho+2})$. Note that when q is an odd number, $2\rho+2=q+1$.

$$g_0^{(1/(\alpha+c))^{2\rho+2}} = g_0^{(1/(\alpha+c))^{q+1}} = (g^{(\alpha+c)^q})^{(1/(\alpha+c))^{q+1}} = g^{1/(\alpha+c)}$$

2) if q is an even number, we obtain $g_{0,\rho}$ and $g_{0,\rho+1}$. Because the CDH problem is solvable, then we can obtain $g_{0,\rho+2} = g_0^{(1/(\alpha+c))^{2\rho+2}}$ by $(g_{0,\rho}, g_{0,\rho+1})$. Note that when q is an even number, $2\rho+1 = q+1$.

$$g_0^{(1/(\alpha+c))^{2\rho+2}} = g_0^{(1/(\alpha+c))^{q+1}} = (g^{(\alpha+c)^q})^{(1/(\alpha+c))^{q+1}} = g^{1/(\alpha+c)}$$

Given (g, g^r) , since the CDH problem is solvable, then we can obtain $g^{(\alpha+c)^r}$. This denotes that q -SDH+CDH problem is also solvable. \square

By the above discussion, we can obtain

Theorem4. the q -SDH problem \leq q -SDH+CDH problem \leq the CDH problem.

where symbol \leq denotes that the problem A is easier than the problem B to be solved.

C. Chameleon Hashing

A chameleon hashing function is a trapdoor collision resistant hash function, which is associated with a key pair (sk, pk) . Anyone who knows the public key pk can efficiently compute the hash value for each input. However, there exists no efficient algorithm for anyone except the holder of the secret key sk , called a trapdoor, to find collisions for every given input. Formally, a chameleon hashing scheme consists of the following efficient algorithms:

- System Parameters Generation PG : An efficient probabilistic algorithm that, on input a security parameter k , outputs the system parameters SP .
 - Key Generation KG : An efficient algorithm that, on input the system parameters SP , outputs a secret/public key pair (sk, pk) for each user.
 - Hashing Computation H : An efficient probabilistic algorithm that, on input the public key pair pk of a certain user, a label L a message m , and an auxiliary random integer $r \in \mathbb{Z}_p$, outputs the hash value $h = \text{Hash}(m, r, pk, L)$
 - Collision Computation UF : An efficient algorithm that, on input the secret key sk of the user which associate to public pk , a message m , a label L and auxiliary random integer r , and computes a second message m^f and random parameter $r^f \in \mathbb{Z}_p$ such that $\text{Hash}(pk, L, m, r) = \text{Hash}(pk, L, m^f, r^f) = C$. Namely, $UF(sk, L, m, r) \rightarrow (m^f, r^f)$, such that $\text{Hash}(pk, L, m, r) = C = \text{Hash}(pk, L, m^f, r^f)$
- A secure chameleon hashing scheme satisfies the following properties:

- Collision resistance: Without the knowledge of trapdoor information sk , there exists no efficient algorithm that, on input a message m , a random integer r , and another message m , outputs a random integer that satisfy $\text{Hash}(m^f, r^f) = \text{Hash}(m, r)$, with non-negligible probability.

- Semantic security: The chameleon hash value C does not reveal anything about the possible message m that was hash. For all pairs of message m and m' , the probability distribution of the random value $\text{Hash}(m^f, r)$ and $\text{Hash}(m, r)$ are computationally indistinguishable.

- Message hiding: Assume the recipient has computed a collision using the universal forgery algorithm, i.e., a second pair (m', r') s.t. $\text{Hash}(pk, L, m, r) = C = \text{Hash}(pk, L, m', r')$, where (m, r) was the original value signed. Then the signer, upon seeing the claimed values (m', r') , can successfully contest this invalid claim by releasing a third pair (m'', r'') , without having to reveal the original signed message. Moreover, the entropy of the original value (m, r) is unchanged by the revelation of the pairs (m', r') , (m'', r'') , and any further collisions: $H[(m, r)/C, (m', r'), (m'', r'')] = H[(m, r)/C]$.

- Key Exposure Freeness: If a recipient with public key pk has never computed a collision under label L , then given $C = \text{Hash}(pk, L, m, r)$ there is no efficient algorithm that can find a collision (a second pair m^f, r^f , mapping to the same digest C). This must remain true even if the adversary has oracle access to $\text{UForge}(sk, \dots)$ and is allowed polynomial many queries on triples (L_i, m_i, r_i) of his choice, except that L_i is not allowed to equal the challenge label L .

Remark: Notice that when a chameleon hash with key exposure freeness is employed within a chameleon signature then any label L must be explicitly committed to the signature along with the identity of the recipient and a description of the hashes (see [5]).

III. OUR CHAMELEON HASH FUNCTION WITHOUT KEY EXPOSURE

In the following, we describe our chameleon hash function. The scheme consists of the following four algorithms:

[System Parameters Generation PG]: Let G_1, G_2, G_T be three cyclic bilinear groups, where $|G_1|=|G_2|=|G_T|=q$, $g_2 \in G_2$ is a random generator of group G_2 . ψ is an isomorphism from G_2 to G_1 , with $\psi(g_2) = g_1$. $e : G_1 \times G_2 \rightarrow G_T$ is the bilinear pairing. The system parameters are $SP = \{G_1, G_2, G_T, \psi(), g_2, e, q\}$

[Key Generation KG]: Each user randomly chooses an integer $\beta \in \mathbb{Z}_p$ as his private key, and publishes his public key $z = g_1^\beta$. The validity of public key z can be ensured by a certificate issued by a trusted third party.

[Hashing Computation H]: On input the public key z of a certain user. Randomly choose an integer $\delta_1 \in G_1$ to compute $e(\delta_1, g_2^{\beta-m})$. we define hash function as follows:

$$h = \text{Hash}(m, \delta_1, z) = e(\delta_1, g_2^{\beta-m}) = e(\delta_1, z/g_1^m)$$

[Collision Computation F]: For any valid hash function h , the algorithm F can be used to compute a hash collision

$$F(\beta, h, \delta_1, m, m') = \pm \delta_1^{\frac{z-m}{z-m'}}$$

where $\pm \delta_1' = \delta_1^{\frac{z-m}{z-m'}}$

Note that

$$\begin{aligned} \text{Hash}(m', \delta_1', z) &= e(\delta_1', z / g_2^{m'}) \\ &= e(\delta_1^{\frac{z-m}{z-m'}}, z / g_2^{m'}) = e(\delta_1^{\frac{z-m}{z-m'}}, g_2^{\beta-m'}) = e(\delta_1, z / g_2^m) \\ &= \text{Hash}(m, \delta_1, z) \end{aligned}$$

Thus, the forgery is valid.

Remark: According to the statement above, we find that our chameleon hash doesn't satisfy message hiding.

IV. SECURITY ANALYSIS

Theorem5. Our proposed chameleon hashing scheme is resistant to forgery under the assumption of q -SDH+CDHP in G_1 is intractable.

Proof. Given $(g_1 = \psi(g_2), \hat{z} = \psi(g_2^\beta) = g_1^\beta, \delta_1 = g_1^\alpha \in G_1)$, where $\alpha, \beta \in \mathbb{Z}_p$ are unknown, let us define the chameleon hash function $h = \text{Hash}(m, \delta_1, z) = e(\delta_1, z/g^m)$. Given a pair collisions (m, δ_1) and (m', δ_1') that satisfy $\text{Hash}(m, \delta_1, z) = \text{Hash}(m', \delta_1', z)$, namely, $e(\delta_1, z/g^m) = e(\delta_1', z/g^{m'})$. Then we can deduce the following relation

$$\begin{aligned} \delta_1' &= \delta_1^{\frac{z-m}{z-m'}} = \delta_1^{1 + \frac{m-m'}{z-m'}} \\ \delta_1' / \delta_1 &= \delta_1^{\frac{m-m'}{z-m'}} \\ (\delta_1' / \delta_1)^{1/(m-m')} &= \delta_1^{(m-m')/(z-m')} = g^{a/(z-m')} \end{aligned}$$

Thus, we can obtain a pair $(m', (\delta_1' / \delta_1)^{1/(m-m')})$. Obviously, it is contradiction to q -SDH+CDH assumption.

The theorem denotes that our chameleon hashing scheme is key-exposure-freeness.

Theorem6. Our proposed chameleon hashing scheme is semantically secure

Proof. Given a hash function h , a public key pk and any message m , there exists exactly one value δ_1 such that $h = \text{Hash}(m, \delta_1, z)$.

V. CONCLUSION

Chameleon signatures are based on well established hand-sign paradigm, where a chameleon hash function is used to compute the cryptographic message digest. Chameleon signatures simultaneously provide non-repudiation and non-transferability for the signed message, thus can be used to solve the conflict between authenticity and privacy in the digital signatures. One limitation of the initial chameleon signature scheme is that signature forgery results in the signer recovering the recipient's trapdoor information, i.e. private key. Therefore, the signer can use this information to deny other signatures given to the recipient. This creates a strong disincentive for the recipient to forge signatures, partially undermining the concept of non-transferability. In the paper, we propose a new chameleon hash scheme which enjoys some advantages of the previous schemes:

collision-resistant, semantic security, and key-exposure-freeness. At the same time, we show that the recipient's trapdoor information will never be compromised under the assumption of q -SDH+CDH problem which is a new security assumption.

ACKNOWLEDGMENT

I thank the anonymous referees for their very valuable comments on this paper. This work is supported by the National Natural Science Foundation of China (No: 60703044), the Nova Programma (No:2007B-001), the PHR fund and Program for New Century Excellent Talents in University (NCET-06-188).

REFERENCES

- [1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," *Phil. Trans. Roy. Soc. London*, vol. A247, pp. 529–551, April 1955.
- [2] M. Young, *The Technical Writer's Handbook*. Mill Valley, CA: University Science, 1989.
- [3] G. Ateniese, Medeiros B. de, "On the key exposure problem in chameleon hashes", the Fourth Conference on Security in Communication Networks (SCNT04), LNCS, Springer-Verlag, Amalfi, 2004.
- [4] Gentry, C. "Certificate-based encryption and the certificate revocation problem". Eurocrypt 2003, LNCS 2656, pp 272-293, Springer-verlag, 2003.
- [5] W.Gao, F.Li and X.Wang, "Chameleon hash without key exposure based on Schnorr signature", Computer Standards & Interfaces, Vol.31(2009), pp 282-285.
- [6] S. Goldwasser, S. Micali and R. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks", *SIAM Journal of computing*, 17(2), pp. 281-308, April 1988.
- [7] Krawczyk, H., Rabin, T., "Chameleon signatures in: Proceedings of NDSS 2000". (2000) pp.143- 154
- [8] B.G.Kang, J.H.Park and S.G.Hahn, "A certificate-based signature scheme", CT-RSA2004, LNCS 2964, pp99-111, springer-verlag, 2004.
- [9] Chen, X., Zhang, F., and Kim, K., "Chameleon hashing without key exposure". To appear in the proceedings of the 7th Information Security Conference (ISC 04), Palo Alto, California. Available online at <http://eprint.iacr.org/2004/038/>.
- [10] K.Nyberg and R.A.Rueppel, "Message recovery for signature schemes based on the discrete logarithm", EUROCRYPT'94, LNCS 1, pp 175-190, springer-verlag, 1994.
- [11] Pointcheval, D and Stern, I., "Security proof for signature scheme", Eurocrypt'96 in Lect. Notes comput. Sci. 1996.1070. pp 387-398.
- [12] P. Paillier, "Public key cryptosystems based on composite degree residuosity classes", Advances in Cryptology-EUROCRYPT99. LNCS 1592, Springer-Verlag, pp. 223-238.
- [13] D. Boneh, X. Boyen, "Short signatures without random oracles", Advances in Cryptology CEUROCRYPT 04, LNCS3027, Springer-Verlag, 2004, pp. 56-73.
- [14] Waters, B. "Efficient identity-based encryption without random oracles". In: Cramer, R. (ed.) EUROCRYPT 2005, LNCS 3494, pp 114-127, Springer, 2005.