Available online at http://scik.org
J. Math. Comput. Sci. 6 (2016), No. 3, 281-289
ISSN: 1927-5307

AN ID-BASED KEY-EXPOSURE FREE CHAMELEON HASHING UNDER SCHNORR SIGNATURE

TEJESHWARI THAKUR*, BIRENDRA KUMAR SHARMA

School of Studies in Mathematics, Pt.Ravishankar Shukla University, Raipur(C.G.)-492010, India

Abstract. An ID-based key exposure free chameleon hashing scheme under the Schnorr signature system is proposed in this paper. Gao et al [5] first proposed chameleon hashing based on schnorr signature. This scheme inherited the qualities of Schnorr scheme [7], but our proposed scheme used in schnorr scheme quality and our design based on ID-based system in chameleon hashing, because the owner of a public key does not necessarily need to retrieve the associated secret key. And I have been implementing the algorithm in Mathematica 7.0 and here are provided the steps of the algorithm and discusses the security and efficiency.

Keywords: Schnorr signature; Chameleon hashing; Chameleon signature; ID-based cryptography; Key exposure scheme.

2010 AMS Subject Classification: 94A60.

1. Introduction

The concept of chameleon hashing first introduced by Krawczyk and Rabin [6], which was based on well established hash-and-sign paradigm, where a chameleon hash function is used to compute the cryptographic message digest. A chameleon hash function is a trapdoor one-way hash function, which prevents everyone except the holder of the trapdoor information from

*Corresponding author.

Received July 27, 2015

computing the collisions for a randomly given input.

ID-based cryptosystem was first introduced by Shamir [8]. The main idea of such cryptosystem is that the identity information of each user works as his public key, in other words, the users public key can be calculated directly from his identity rather than being extracted from a certificate issued by a certificate authority (CA). The ID-based public key setting can be a good alternative to a certificate-based public key setting, especially when efficient key management and moderate security are required.

Ateniese and Medeiros [1] first introduced the concept of ID-based chameleon hash function. ID-based cryptography in general, has the advantage of easier key distribution as compare to the conventional public key cryptography. In the case of chameleon hashing these advantages are multiplied by the fact that the owner of a public key does not necessarily need to retrieve the associated secret key. Therefore, ID-based chameleon hashing can support single use public keys very efficiently. The next ID-based chameleon hashing using bilinear pairing is designed by Zhang Naini and Susilo [9]. Further Chen et al.[3] proposed the first full construction of a key-exposure free chameleon hash function in the gap Diffie-Hellman groups with bilinear pairings.

Ateniese and De Mederious [2] presented three key-exposure free chameleon signature schemes. Out of these three, only two are key exposure free. Next Gao et al. [5] have also addressed chameleon hash which was key exposure free on the Schnorr signature. Obviously it inherited the qualities of Schnorr [7] scheme. On the other hand, Ateniese and de Mederious [1] proposed an interesting open problem in 2004: Is possible for construction an efficient identity-based chameleon hash function without key exposure? next Chen et al. [4] first introduce the identity-based chameleon hash scheme without key exposure, which gave a positive answer for the open problem. However, the scheme is constructed in the setting of gap Diffie-Hellman group with pairings and thus less efficient.

In this paper, we propose the ID-based key-exposure free chameleon hashing under the Schnorr Signature scheme. Our construction is also a little different from the traditional ID-based systems since the recipient of a public key does not necessarily need to retrieve the associated secret key. The advantage of our implementing check the algorithm in mathematica 7.0.

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. The definitions associated with ID-based chameleon hashing is introduced in Section 3. The proposed scheme define in section 4. Proposed security analysis given in section 5. Implementation and efficiency define in section 6. Finally, conclusions will be made in Section 7.

2. Preliminaries

First, We review some notations used in this paper.

Chameleon hashing: A chameleon hashing scheme is a trapdoor collision resistant hash function 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.

ID-based chameleon hashing: Definition are same chameleon hashing but this is use PKG (Private Key Generator). The hash key PK is just the identity information ID of the user. A trusted third party called (PKG) computes the trapdoor key SK associated with PK for the user.

3. Algorithm for ID-Based Chameleon Hashing Scheme

(1) *Setup*: The PKG runs this probabilistic polynomial-time algorithm to generate a pair of keys (SK, PK) defining the scheme. PKG publishes the system parameters SP including PK, and keeps the master key SK secret. The input to this algorithm is a security parameter 1^k.

(2) *Extract*: A deterministic polynomial-time algorithm that, on input the master key SK and an identity string ID, outputs the trapdoor information associated to the hash key ID.

(3) *Hash*: A probabilistic polynomial-time algorithm that, on input the master public key PK, an identity string ID, a customized identity L, a message m, and a random string r, outputs the hash value $h = Hash(ID, L, m, r)$. Note that h does not depend on TK.

(4) *Forge*: A deterministic polynomial-time algorithm F that, on input the trap- door key TK associated to the identity string ID, a customized identity L, a hash value h of a

message m, a random string r, and another message $m' \neq m$, outputs a string r' that satisfies $h = Hash(ID, L, m, r) = Hash(ID, L, m', r')$.

3.1. Security Requirements

Ateniese and B.de Medeiros [2] have identified for an ID-based chameleon hashing scheme as below:

- *Collision resistance:* Let ID be a target identity string and m be a target message. Let k be the security parameter. The chameleon hash scheme is collision resistance against active attackers if for all non-constant polynomials $f_1()$ and $f_2()$ Without the knowledge of trapdoor key TK, there exists no efficient algorithm that, on input a message m, a random string r, and another message m', outputs a string r' that satisfy $Hash(ID, L, m', r') = Hash(ID, L, m, r)$, with non-negligible probability.
- *Semantic security:* For all pairs of messages m and m', the probability distributions of the random values $Hash(ID, L, m', r')$ and $Hash(ID, L, m, r)$ are computationally indistinguishable. In formal terms, let $H[X]$ denote the entropy of a random variable X, and $H[X_jY]$ the entropy of the variable X given the value of a random function Y of X. Semantic security is the statement that the conditional entropy $H[m_jh]$ of the message given its chameleon hash value h equals the total entropy $H[m]$ of the message space.
- *Message hiding:* For all identity string ID and all customized identity L and given a collision (m', r') and (m, r) of the chameleon hash scheme, i.e. $h = Hash(ID, L, m', r') = Hash(ID, L, m, r)$. Then the sender can successfully contest this invalid claim by releasing a third pair $(m", r")$ such that $h = Hash(ID, L, m", r")$ without having to reveal the original signed message m.
- *Key exposure freeness:* If a recipient with identity ID has never computed a collision under a customized identity L, then there is no efficient algorithm for an adversary to find a collision for a given chameleon hash value $Hash(ID, L, m, r)$. This remains true even if the adversary has oracle access to F and is allowed make polynomially many queries on triples (L_j, m_j, r_j) of his choice, except when L_j is not allowed to equal the challenge L.

4. The Proposed our Scheme

The proposed scheme consists of four phase's, namely Setup, Extract, signature generation, verification.

Set of System parameter Phase: The PKG performs the following case.

Let $H : \{0,1\}^* \to Z_q^*$ be cryptography hash function. Given an identity information ID.

(1) Select p and q with the property that q divides $(p-1)$

(2) Select a random integer x s.t. $1 \leq x \leq q-1$

(3) Suppose the signer's identity is ID. The secret key x of the identity is then given by $H(ID)$. A's public key is (p,q,y).

(4) Compute A's public key is (p,q,y) and A's secret master private key x and the master public key $y = g^x \; mod \; p$.

Signature Generation Phase:

To create a signature of the message $m \in \{0,1\}^*$, Alice follows.

(1) Select a random secret integer k, $1 \leq k \leq q-1$

(2) Compute $r_1 = g^k \; mod \; p$;

(3) Encrypts $e = H(ID \parallel m \parallel r_1)$;

(4) compute $S_1 = r_1 y^e \; mod \; q$;

A's compute hash value as follows:

Hashing Phase:

(1) An input the hash key ID;

(2) choose a random integer $r_2 \in Z_q$;

(3) chameleon hash scheme $h = Hash(ID, m, r_2) = g^m S_1^{r_2} \; mod \; q$. And trapdoor extract is $S_1 = g^{\sigma_1} \; mod \; q$.

Note that for $\sigma_1 = xe + k$, (e, σ_1) forms a Schnorr signature on the identity ID.

Forge Phase: For any valid hash value h, and string r_2' with the trapdoor key S_{ID} as follows:

$$r_2' = \sigma_1^{-1}(m - m') + r_2 \; mod \; q$$

Verification Phase:

(1) Given the message-signature pair $(e, \sigma_1))$;

(2) Bob does the signature verification as follows by using user As identity ID.

(3) Compute $v = g^{\sigma_1} y^{-e} \; mod \; p$ user and $e' = H(h \parallel m \parallel v)$. Accept the signature if and only if $e = e'$ otherwise reject.

5. Security Analysis

Theorem 1. In the random oracle model in the proposed identity-based chameleon hash scheme is collision resistance against active attackers under the Schnorr signature problem is intractable.

Proof. Let ID be the target identity string and m be the target message. Suppose that adversary $\mathscr{A}$ makes at most $f_1(k)$ quires to the Extract oracle where f_1 is non-constant polynomial and recipient $\mathscr{B}$ is run the setup algorithm and responds to the H query and Extract query of $\mathscr{A}$ as follows.

If $\mathscr{A}$ can output a message $m' \neq m$ and the string r_2 and r_2' , such that $Hash(ID,m,r_2) = Hash(ID,m',r_2')$, we have that

$$g^m S_1^{r_2} = g^{m'} S_1^{r_2'} \Rightarrow g^{(m-m')} = S_1^{r_2'-r_2} \Rightarrow = g^{-\sigma_1(r_2'-r_2)} \Rightarrow g^{(m-m')} = g^{\sigma_1(r_2-r_2')} \Rightarrow \sigma_1^{-1}(m-m') = (r_2-r_2') \Rightarrow r_2' = -\sigma_1^{-1}(m-m') + r_2 \text{ and } \sigma_1 = (m-m')(r_2-r_2')^{-1} \; mod \; q$$

which is the non-negligible probability ε,then $\mathscr{B}$ can compute.

Theorem 2. The proposed chameleon hashing scheme is semantically secure.

Proof. The given an identity ID, for message m and fixed r_1 , the given one-to-one correspondence between the hash value $h = Hash(ID,m,r_2)$ is uniquely determine by the r_2, and vice-versa, therefor the conditional probabilistic. Therefore, the conditional probability $\mu(m|h) = \mu(m|r_2)$ and note that m and r are independent variables, the equation $\mu(m|r_2) = \mu(m)$ holds. Then, we can prove that the conditional entropy $H[m|h]$ equals the entropy $H[m]$ as follows:

$$\mu(m \mid h) = \sum_m \sum_H \mu(m,h) log(m|h)$$

$$= \sum_m \sum_H \mu(m,h) log(\mu(m)) = \sum_m \mu(m) log(\mu(m))$$

$$= H[m]$$

Theorem 3. The given by ID-based chameleon hash scheme satisfies the property of message hiding.

Proof. Give a collision (m, r_2) and (m', r'_2) we can compute the trapdoor S_1 similar to theorem 1. Then for any message m'' a string r''_2 can be computed with the trapdoor key S_1 as below : $r''_2 = r'_2 + \sigma_1^{-1}(m - m')$.

Theorem 4. In the random oracle model, the proposed identity-based chameleon hash scheme is key-exposure free under the schnorr signature under the is intractable.

Proof. Even if the adversary has oracle access to F and is allowed to make polynomially many queries on triple $(ID_j, m_j, g^{\sigma_j}, y^{x_j})$ of his choice, there is no efficient algorithm for him to find a collision for the theorem 1., collision of the hash value $h = Hash(ID, m, g^{\sigma_1}, y^x)$ where $ID \neq ID_j$. Note that finding collision is hard without knowledge of the ephemeral trapdoor σ_1. So finally schnorr signature scheme is secure from key exposure scheme.

6. Implementation and Efficiency of Proposed Scheme

Proposed algorithm check in mathematica 7.0.

```
q = Take[7];
p = Take[29];
Print[”q is : ”, q];
g = PrimitiveRoot[q];
Print[”g is : ”, g];
x = RandomInteger[3, q − 1];
Print[”x is : ”, x];
y = PowerMod[g, x, p];
Print[”Y is : ”, y];
k = RandomInteger[4, q − 1];
Print[”k is : ”, k];
r1 = PowerMod[g, k, p];
Print[”r1 is : ”, r1];
ID := ImportString[”ID”, ”Bit”];
m := RandomInteger[5, q − 1];
e = H[ID, m, r1];
a1 := PowerMod[y, e, q];
s1 := r1 ∗ a1
```

$r2 = RandomInteger[7, q-1];$

$h = PowerMod[Power[g, m], Power[s1, r2], q];$

$a2 := x * e + k$

$s1 := PowerMod[g, a2, q];$

$m1 := RandomInteger[9, q-1];$

$r3 := Power[a2, -1] * (m - m1) + r2;$

$h1 := PowerMod[Power[g, m1], Power[s1, r3], q];$

The output is rhs and lhs is equal and time is 0.063 second.

Efficiency of proposed scheme

Computational cost of our proposed scheme is given below: E: Exponent,M: multiplication, A: Addition.

Phases	Setup	Extract	Hash	Forge
Our Scheme	$1E$	$3E+1M$	$2E+1M$	$1A+1M$

Table 1: Computational cost of proposed scheme.

7. Conclusion

In this paper, we propose the Id-based chameleon hashing under schnorr signature which is key exposure free and more efficiency and low computational cost. This algorithm is suitable for low computation time.

Conflict of Interests

The authors declare that there is no conflict of interests.

REFERENCES

[1] G. Ateniese and B. de Medeiros. Identity-based chameleon hash and applications, FC 2004, Lecture Notes in Computer Science 3110, Springer-Verlag,(2004), 164-180.

[2] G. Ateniese and B. de Medeiros. On the key-exposure problem in chameleon hashes, SCN 2004, Lecture Notes in Computer Science 3352, Springer-Verlag,(2005), 165-179.

[3] X. Chen, F. Zhang, and K. Kim. Chameleon hashing without key exposure, ISC 2004, Lecture Notes in Computer Science 3225, Springer-Verlag,(2004), 87-98.

[4] X. Chen, F. Zhang, H. Tian, and K. Kim. Identity-based chameleon hash scheme without key exposure, ACISP 2010, Lecture Notes in Computer Science 6168, Springer-Verlag,(2010), 200-215.

[5] W. Gao, Fei Li, Xueli Wang. Chameleon hash without key exposure based on schnorr signature, Computer Standards and Interfaces 31,(2009),282-285.

[6] H. Krawczyk and T. Rabin. Chameleon hashing and signatures, Proc. of NDSS 2000,(2000), 143-154.

[7] C.Schnorr ,Efficient identification and signatures for smartcards, CRYPTO 1989, LNCS 435,Springer-Verlag,(1990), 239-252.

[8] A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology- Crypto, Springer-Verlag,LNCS 196,(1984), 47-53.

[9] F. Zhang, R. Safavi-Naini, and W. Susilo. ID-based chameleon hashes from bilinear pairings, available at Cryptology ePrint Archive: Report 2003/208, (2003).