Available online at http://scik.org
Eng. Math. Lett. 2014, 2014:12
ISSN: 2049-9337

CERTIFICATELESS CHAMELEON HASH SCHEME BASED ON RSA ASSUMPTION

TEJESHWARI THAKUR*, BIRENDRA KUMAR SHARMA

School of Studies in Mathematics Pt. Ravishankar Shukla University, Raipur, India

Abstract. Certificateless public key cryptography (CL-PKC), does not require the use of the certificate to guarantee the authenticity of public keys. It does rely on the use of a trusted third party (TTP) who is in possession of a master key. CL-PKC does not suffer from the key escrow property. Thus, CL-PKC can be seen as a model for the use of public key cryptography.

Keywords: Chameleon hashing, certificateless cryptography, RSA.

2010 AMS Subject Classification: 94A60.

1. Introduction

Digital signature is a very important tool in cryptography. Digital signature provides signed message with the capabilities like integration, authentication and non-repudiation. Anyone can use the signers public key to verify the authenticity of the signature, but sometimes, the signer may need to protect certain interest, and therefore, do not wish their signature to be checked by anyone other than the specified message recipient. Chaum and Van Antwerpen [3] first proposed an undeniable signature to solve the above problem. Undeniable signature requires the collaboration of signers during its verification. Therefore, signer can control whether or not

*Corresponding author

Received April 15, 2013

the signed message is open to verification by a recipient, this is known as non-transferability property.

Krawczyk and Rabin [5] proposed a new type of signature scheme called chameleon signature. Chameleon signature is based on the well established hash-and-sign paradigm, where a chameleon hash function is used to calculate the message digest. A chameleon hash function is a trapdoor collision-resistant hash function. It has the same characteristics, such as pre-image and collision-resistance hash function. However, collisions and second pre-images can be easily computed once the trapdoor is known. Chameleon signature has the characteristics of an undeniable signature, that is, it is non-repudiable and non-transferable. It is, in fact, a variation of undeniable signature.

In traditional public key cryptography, a digital certificate generated by a trusted third party is needed to ensure the binding between the public key and the user's identity. Such system may face the certificate management problem. To solve this problem, Shamir [7] proposed the identity-based (ID-based) cryptosystem based on factoring problem, wherein, the user's public key could be computed from his identity and the user's secret key is generated by private key generater(PKG). However, the ID-based cryptosystem suffers from the key escrow problem, i.e. the PKG knows all the user's secret keys.

In 2003, Al-Riyami *et al.* [6] introduced the notion of the certificateless public key cryptography (CL-PKC). In the CL-PKC, a user's private key is a combination of a partial private key generated and a secret key chosen by the user. This may the key escrow problem in the ID-based cryptography can be solved. Moreover, in 2012, Hou [4] proposed certificateless chameleon hash scheme whose security is based on bilinear pairing in the random oracle model. Our proposed scheme based on RSA assumption, which is consumes less time as compute pairing having same security requirement. The paper is organized in the following way. We describe the preliminaries in Section 2. The algorithm of certificateless chameleon hashing is introduced in Section 3. Proposed scheme is introduced in Section 4. The security requirements are descried in Section 5. Finally, we conclude our opinion in Section 6.

2. Preliminaries

In this section, we describe the basic definition.

- **RSA Problem.** RSA public key (n, e) and a message M.

$$C = M^e (mod\ n), \text{ to compute M.}$$

- **RSA Assumption.** The RSA assumption was given in 1978 by Rivest, Shamir, Adleman. This assumption uses a generator algorithm to generate an instance of the problem, similar to factoring's. Let $n = pq$ be the product of two primes p,q is large prime and random prime integer $e > 2$ is prime to the order $\varphi(n) = (p-1)(q-1)$ of the multiplicative residues modulo n. The secret key d is computed such that $ed = 1\ mod\ \varphi\ (n)$. So that, the public key is (n, e).

3. Algorithm of Certificateless Chameleon Hashing

In this section, we describe the chameleon hashing and algorithm of certificateless chameleon hash scheme [4, 6] as below.

Chameleon Hashing. A chameleon hash 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. The hash key HK is just the identity information ID of the user. KGC computes the trapdoor key TK associated with HK for the user.

3.1. Certificateless Chameleon Hashing

A certificateless chameleon hash scheme [4, 6] consists of following phases.

- **Setup.** This algorithm, run by the PKG, takes a security parameter as an input, and then returns the master secret key, and system parameter.
- **Partial-Private-Key-Extract.** This algorithm, run by the PKG, takes parameter, and a users identity ID as inputs. It generates a partial-private-key D_{ID}, and sends it to the user via a secure channel.
- **Set-Secret-Value.** This algorithm, run by a user, returns a secret value,x_{ID}.

- **Set-Secret-Key.** This algorithm, run by a user, takes the users partial private- key D_{ID} and the secret value x_{ID} as inputs, then returns the users full secret key, sk_{ID}.
- **Set-Public-Key.** This algorithm, run by a user, takes parameter and the users full secret key as inputs, and returns a public key PK_{ID} for the user.
- **Hash.** A probabilistic polynomial algorithm which, on input an identity string ID, message m and random string r, outputs the hashed value

$$H = Hash(ID, PK_{ID}, m, r)$$

Note that H does not depend on TK.

- **Forge.** A deterministic polynomial algorithm F is that, on input the trapdoor key TK associated to the identity string ID, a hash value H of a message m, a random string r, and another message $m' \neq m$, outputs a string r' that satisfies $H = Hash(ID, PK_{ID}, m, r) = Hash(ID, PK_{ID}, m', r')$. Moreover, if r is uniformly distributed in a finite space R, then the distribution of r' is computationally indistinguishable from uniform in R.

3.2. Security Requirements of Chameleon Hash Scheme

A secure chameleon hashing scheme [4] satisfies the following properties.

- **Collision Resistance.** Without the knowledge of trapdoor key TK, there exists no efficient algorithm which on input, a message m, a random string r, and another message m', outputs a string r' that satisfy $Hash(ID, m', r', PK_{ID}) = Hash(ID, m, r, PK_{ID})$, with non-negligible probability.
- **Semantic Security.** For all pairs of messages m and m', the probability distributions of the random values $Hash(ID, m', r)$ and $Hash(ID, m, r)$ are computationally indistinguishable.
- **Key Exposure Freeness.** If a recipient has never computed a collision under ID, then there is no efficient algorithm for an adversary to find a collision for a given chameleon hash value$Hash(ID, m, r)$. This must remain true even if the adversary has oracle access to F and is allowed polynomially many queries on triples (ID_j, m_j, r_j) of his choice, except that ID_j is not allowed to equal the challenge ID.

- **Message Hiding.** For all identity strings ID, assume that the recipient has computed a collision (m', r') such that

$$H = Hash(ID, PK_{ID}, m', r') = Hash(ID, PK_{ID}, m, r)$$

, where m is the original message that was hashed. Then the signer, upon seeing the claimed values (m', r'),can successfully compute another collision $(m", r")$ such that $H = Hash(ID, PK_{ID}, m", r")$, without revealing the message m.

4. The Proposed Certificateless Chameleon Hash Scheme based on RSA Assumption

We propose a certificateless chameleon hash scheme consists of following phases.

(1) **Setup.** Let the security parameter 1^k as input, the PKG generates a RSA group as follows: PKG generates two large prime numbers p and q i.e $n = pq$ as a RSA modular number, $e < \varphi(n)$ is the public key of PKG, and satisfy $gcd(e, \varphi(n)) = 1$, where $\varphi(\cdot)$ is the Euler totient function and choose two cryptographic hash functions $H_0 : \{0,1\}^* \longrightarrow Z_n^*$ and $H_1 : Z_n^4 \times \{0,1\}^* \longrightarrow \{0,1\}^l$, where l is SHA 160 bit. PKG computes d such that $ed = 1 \ mod \varphi(n)$ with the master key d and publish the system parameter $= \{n, e, H_0, H_1\}$.

(2) **Extract.** Given an identity string ID as input, PKG computes partial key $ID_{ID} = J$, where $J = H_1(ID)^d$ mod n. The user chooses a random integer x_{ID} as it's secret value. The trapdoor key is $SK_{ID} = \{x_{ID}, D_{ID}\}$ and public key is $PK_{ID} = H_1(ID)^{x_{ID}} \ mod \ n$.

(3) **Hash.** Taking message m, the input identifier ID, and the hash key PK_{ID}, the random integer x_{ID}, computes r. Our proposed chameleon hash function is defined as below:

$$H = Hash(ID, m, r, PK_{ID}) = r^e H_1(ID)^{x_{ID} H_0(m)}.$$

Note: H does not depend on trapdoor key SK_{ID}.

(4) **Forge.** For any hash value H, the algorithm F can be used to compute a string with the trapdoor key $SK_{ID} = (x_{ID}, D_{ID})$ as follows:

$$r' = forge(J, r, m, m', H, x_{ID}) = rJ^{x_{ID}(H_0(m) - H_0(m'))}$$

Note that if $Hash(ID,m,r,PK_{ID}) = Hash(ID,m',r',PK_{ID})$ then forgery is successful.

5. Security analysis

The above certificateless chameleon hash scheme satisfies security properties such as Collision-resistance, key-exposure-freeness, Semantic security and Message hiding as given below.

(1) **Collision-resistance and key-exposure-freeness**. If the attacker A can produce as output a message $m \neq m'$, and two strings r and r' such that

$$Hash(ID,m',r',PK_{ID}) = Hash(ID,m,r,PK_{ID}),$$

and we have $r'^{e} H_1(ID)^{x_{ID} H_0(m')} = r^{e} H_1(ID)^{x_{ID} H_0(m)} \Rightarrow$

$$r'^{e} = r^{e} H_1(ID)^{x_{ID}(H_0(m) - H_0(m'))}$$

$\Rightarrow r' = rJ^{x_{ID}(H_0(m) - H_0(m'))}$. Let $\Delta = x_{ID}(H_0(m) - H_0(m'))$, we can see that these values are relatively prime, i.e. $gcd(e,\Delta)) = 1$, then there exists two numbers a, b satisfying $a\Delta + be = 1$. Thus, J can now be extracted: $(\frac{r'}{r})^{a} H_1^{b}(ID) = J^{a\Delta + be} = J$. As J is secure RSA signature on identity string, private key generater can't compute collision (m',r') without knowledge of the trapdoor. Finally, notice that since revealing collision is equivalent to computing signature, the scheme is safe from key exposure.

(2) **Semantically secure**. For the given identity ID, there is a one-to-one correspondence between the hash value H and the string r for each message m. Therefore, the conditional probability $\mu(m|H) = \mu(m|(r))$. Note that m and r are independent variables, the equation $\mu(m|H) = \mu(m)$ holds. Then the conditional entropy $H[m|H]$ equals the entropy H[m] as follows:

$$\begin{aligned} \mu(m \mid H) &= \sum_{m}\sum_{H} \mu(m,H) log(m|H) \\ &= \sum_{m}\sum_{H} \mu(m,H) log(\mu(m)) = \sum_{m} \mu(m) log(\mu(m)) \\ &= H[m] \end{aligned}$$

(3) **Message Hiding**. Let H be the hash value as given in [1], it is sufficient to show that, once a collision is revealed, a person who does not know even the trapdoor can compute a de-commitment to H under any message m'' of his/her user choice. In fact, as in Forge phase, given (m', r') and (m, r) with the same chameleon hash value, one can get another collision (m'', r'') for any message m".

5.1. Efficiency

The performance analysis of Certificateless chameleon hash function based on RSA Assumption is executed as per following table: In the above table, Exp-Exponential, Mul-Multiplication

Phase	Exponent	Multiplication Modulo	Hash Function
Setup	*1 Exp*	*1 Mul*	*2 H*
Extract	*1 Exp*	*0 Mul*	*1 H*
Hash generation	*2 Exp*	*1 Mul*	*1 H*
Forge	*1 Exp*	*1 Mul*	*2 H*

TABLE 1. Computational cost in our scheme.

modulo and H-Hash Function. The setup phase having 1E+1M+2H, the extract phase is 1E+0M+1H, hash generation is 2E+1M+1H and forge is 1E+1M+2H in computational aspect.

6. Conclusion

In this paper, we have proposed a new certificateless chameleon hash scheme based RSA assumption without the key escrow problems. Moreover, the proposed scheme can achieve all the desired security requirements with more efficiency.

Conflict of Interests

The authors declare that there is no conflict of interests.

REFERENCES

[1] G. Ateniese, B.de Medeiros, On the key-exposure problem in chameleon hashes, Springer-Verlag 2005.

[2] G. Ateniese, B. de Medeiros, Identity-based chameleon hash and applications, Springer-Verlag 2004.

[3] D. Chaum, H. van Antwerpen, Undeniable signatures, Advances in Cryptology-Crypto, Springer-Verlag. 1989.

[4] H. Hongxia, Certificateless based chameleon hash scheme, IEEE Computer Soiceity (2012), 1126-1129.

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

[6] S. A. Riyami, K. Paterson, Certificateless public key cryptography, Springer Heidelberg 2003.

[7] A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology- Crypto, Springer-Verlag 1984.

[8] J. Zhang, J. Mao, An efficient RSA-based certificateless signature scheme, J. Sys, Software. 85 (2012), 638-642.