Jan. 2007, Vol.22, No.1, pp.109–113 *J. Comput. Sci. & Technol.*

Chameleon Hashes Without Key Exposure Based on Factoring

Wei Gao[1] (高 伟), Xue-Li Wang[2] (王学理), and Dong-Qing Xie[3] (谢冬青)

[1] *School of Mathematics and Econometrics, Hunan University, Changsha 410082, China*

[2] *School of Mathematics Science, South China Normal University, Guangzhou 510631, China*

[3] *School of Computer and Communication, Hunan University, Changsha 410082, China*

E-mail: sdgaowei@yahoo.com.cn; wangxuyuyan@yahoo.com.cn; dqxie@hnu.cn

Received November 21, 2005; revised September 11, 2006.

Abstract Chameleon hash is the main primitive to construct a chameleon signature scheme which provides non-repudiation and non-transferability simultaneously. However, the initial chameleon hash schemes suffer from the key exposure problem: non-transferability is based on an unsound assumption that the designated receiver is willing to abuse his private key regardless of its exposure. Recently, several key-exposure-free chameleon hashes have been constructed based on RSA assumption and SDH (strong Diffie-Hellman) assumption. In this paper, we propose a factoring-based chameleon hash scheme which is proven to enjoy all advantages of the previous schemes. In order to support it, we propose a variant Rabin signature scheme which is proven secure against a new type of attack in the random oracle model.

Keywords chameleon signature, chameleon hash, key-exposure

1 Introduction

Chameleon signatures are introduced in [1]. A distinguishing feature of chameleon signature is that they are non-transferable, i.e., a signature issued to a designated recipient cannot be validated by other parties. While not universally verifiable, chameleon signatures provide the security for both the signer and the receiver: if presented with a forged signature claim, the signer can prove that the signature is forged (unforgeability), but is incapable of doing so for legitimate claims (non-repudiation).

Chameleon signatures are based on the well established hash-and-sign paradigm, where the cryptographic message digest is computed by using a chameleon hash function whose trapdoor is due to the designated verifier. Roughly speaking, non-repudiation and non-transferability result from the fact that for the signer who does not know the trapdoor information, a chameleon hash function has the same characteristics of any cryptographic hash function, such as pre-image resistance and collision resistance; however, for the designated verifier who knows the trapdoor information, collisions and second pre-images can be easily computed. For more details on the underlying idea, see [1].

Now, we sketch two properties of the chameleon hash scheme: key-exposure-freeness and message hiding. In the original chameleon signature scheme[1], a signature forgery results in the signer recovering the recipient's trapdoor information. Since this case is a highly undesirable outcome from the recipient's viewpoint, a third-party is therefore more likely to believe claims made by the recipient about presenting an original (non-forged) signature, knowing that a forgery would negatively affect the recipient. Hence, the deterrent effect of key exposure on forgeries threatens the claims of non-transferability provided by the scheme. In addition to the key-exposure-freeness, there is another attractive property called message hiding: given the forged message, the signer with the original one can compute a third message which is also a collision. This property of message hiding permits the signer to deny forged messages without the onus of confirming the original signature.

Some chameleon hash schemes with key-exposure-freeness and message hiding have been discussed in [2–4]. The problem of key exposure was partly addressed in [2], where it is shown how to build identity-based chameleon hash functions. In [3], Chen *et al.* provide the first full construction of a key-exposure-free chameleon hash function based on bilinear pairings. In [4], Ateniese and Medeiros propose another three schemes based on RSA, RSA$[n, n]$ and SDH (Strong Diffie-Hellman assumption) respectively. Additionally, there are some related cryptographic primitives, such as simulation-sound trapdoor commitments[5] and multi-trapdoor commitments[6], similar to but different from exposure-free chameleon hash.

The paradigm[2−4] to fix the key exposure problem is as follows. The public key is divided into two components, permanent and ephemeral. The ephemeral part will be called the label for some specific transaction of the chameleon hash. Such labels are specially formatted strings that describe the transaction, and which include the signer and recipient information as well as some nonce or time-stamp. Now when the signer finds a forged chameleon signature, he can only recover the ephemeral part of the secret key relating to the specific transaction while the main trapdoor of the designated receiver remains secure. In this setting, the intended

Short Paper

This work is partially supported by the National Natural Science Foundation of China under Grants No. 10271042 and No. 60373085.

receiver is willing to abuse his main trapdoor to forge signature without worrying its disclosure. So the key exposure problem is solved.

Although the assumption of integer factoring is weaker than the above mentioned ones, no exposure-free chameleon hash scheme based on factoring has been proposed before. To close this gap, we propose a new chameleon hash scheme based factoring and prove its security by introducing a variant Rabin signature scheme which is just customized for our chameleon hash based on factoring. It seems that the construction of the factoring-based chameleon hash scheme is very different from the previous ones based on other assumptions and needs more detailed requirements such as the customized hash functions. It is obvious that our scheme is based on a much weaker assumption and can be more efficiently implemented than that based on bilinear pairings whose computation is time-consuming[7].

The rest of the paper is organized as follows. Some preliminary work is given in Section 2. A new version of Rabin signature is constructed and proven to satisfy a stronger security definition in the random oracle model in Section 3. In Section 4, based on this Rabin signature scheme, we construct and analyze a new chameleon hash scheme with the properties of key-exposure-freeness and message hiding in addition to collision-resistance and semantic security. Section 5 sketches its application to chameleon signature. At last, we conclude this paper in Section 6.

2 Preliminary

This part follows the description of [2, 4].

Definition 1 (Key-Exposure-Free Chameleon Hashing Scheme). *A key-exposure-free chameleon hashing scheme* $\mathcal{EFCH} = (\mathsf{GenKey}, \mathsf{Hash}, \mathsf{UForge}, \mathsf{SForge})$ *is specified by four probabilistic polynomial-time algorithms and the functionality is as follows*:

• GenKey. *On input a security parameter* 1^k, *output a pair* (pk, sk) *of a public key and a secret key.*

• Hash. *On inputs the public key* pk, *a label* L, *a message* m, *choose an auxiliary random parameter* r, *and output a hash value* $h = Hash(pk, L, m, r)$.

• UForge *(universal forge). On input the private key* sk *associated to the public key* pk, *the label* L, *a message* m *and its random parameter* r, *output a second message* m' *and its random string* r' *such that* $Hash(pk, L, m', r') = Hash(pk, L, m, r)$

• SForge *(instance forge). On input a tuple* (pk, L, m, r, m', r') *of a public key, a label, and two pairs of a message and random parameter, where* $Hash(pk, L, m, r) = Hash(pk, L, m', r') = h$, *compute another collision pair* (m'', r'') *that also satisfies* $Hash(pk, L, m'', r'') = h$.

The security requirements of a chameleon hash include:

Collision-Resistance. There is no efficient algorithm that given only pk, L, m, r, can find a second pair (m', r') such that $Hash(pk, L, m, r) = Hash(pk, L, m', r')$ with non-negligible probability over the choices of pk, L, m, r.

Semantic Security. Informally speaking, the chameleon hash value $h = Hash(pk, L, m, r)$ reveals no information about the possible message m that is hashed. In formal terms, let $E[X]$ denote the entropy of a random variable X, and $E[X|Y]$ 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 $E[m|h]$ of the message given its chameleon hash value h equals the total entropy $E[m]$ of the message space.

Message Hiding. Given (m, r) and (m', r') which form a pair of collisions, i.e., $Hash(pk, L, m, r) = Hash(pk, L, m', r')$, the sender can successfully contest this invalid claim by releasing a third pair (m'', r'') s.t., $Hash(pk, L, m'', r'') = Hash(pk, L, m', r')$, without having to reveal any information of the original hashed message m. 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: $E[(m, r)|C, (m', r'), (m'', r'')] = E[(m, r)|C]$.

Key Exposure Freeness. Given $h = Hash(pk, L, m, r), pk, L, m, r$ and oracle access to the function $UForge(sk, \cdot, \cdot, \cdot)$ with triples $(L_i(\neq L), m_i, r_i)$ of the label, message and its random string, no efficient algorithm can find a collision, a second pair (m', r') such that $Hash(pk, L, m, r) = Hash(pk, L, m', r')$.

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[1]. In [3], the counterpart of the label is called "Customized Identities".

3 Signature Scheme Based on Factoring

In the following, we present a signature scheme which can be seen as a variant of well-known Rabin signature[8] just customized for the construction in the next section. (a) The provable security is customized: in the random oracle model[9], such variant scheme can be easily proven existentially unforgeable under an attack slightly stronger than the well-known adaptive chosen message attack[10]. And such slightly extended security will be enough to easily reduce the property of key-exposure-freeness of the following chameleon hash scheme. (b) The hash function H (in our case of full domain hash) is customized: it can be computed by both the signer and the receiver without the private key. Our variant of Rabin signature scheme consists of 3 efficient algorithms as follows.

• GenKey. Here we use a setting similar to that in [11]. On input a security parameter 1^k, choose randomly two distinct odd primes p, q of the same length such that $p \equiv q \equiv 3 \mod 4$ and $2^{k-1} < N = pq < 2^k$ (such an integer N is called a Blum integer). The public key is N and the secret key is (p, q). And

the scheme is parameterized by the following cryptographic hash function: $H : \{0,1\}^* \to \mathbb{Z}_N^*[+1]$ where $\mathbb{Z}_N^*[+1] = \{x \in \mathbb{Z}_N^* | \mathrm{Jac}_N(x) = +1\}$ is the set of elements of $\mathbb{Z}_N^*$ with Jacobi symbol $+1$.

• Sign. On input the message $m \in \{0,1\}^*$, set the signature as:

$$\sigma \stackrel{R}{\leftarrow} |H(m)|^{\frac{1}{2}} \mod N$$

where if $H(m) \in QR_N$, $|H(m)| = H(m)$, else $|H(m)| = -H(m)$.

• Ver. On input σ, m, verify the following equality $\sigma^2 \equiv \pm H(m) \mod N$. In other words, if $\sigma^2 \equiv H(m) \mod N$ or $\sigma^2 \equiv -H(m) \mod N$, the signature is valid.

Now we present some interpretation for the scheme:

Facts of Number Theory. Let $QR_N = \{x^2 \mod N | x \in \mathbb{Z}_N^*\}$ be the set of all quadratic residues modulo N. If N is a Blum integer, then we have the following facts: 1) the function of 2^l-th ($l \in \mathbb{Z}^+$) power is a permutation over QR_N; 2) every quadratic residue modulo N has four 2^l-th ($l \in \mathbb{Z}^+$) roots modulo N; 3) $-1 \in \mathbb{Z}_N^*[+1] \setminus QR_N$; 4) either $H(m)$ or $-H(m)$ is in QR_N; 5) without known p, q, we can determine whether $x \in \mathbb{Z}_N^*[+1]$ but cannot determine whether $x \in QR_N$.

Constructing Hash Function. As for the hash function H, we require that the party only with N but not p, q can also compute it. So by the above fact 5), if let the range of the function of H be $\mathbb{Z}_N^*[+1]$ but not QR_N then H can be easily instantiated. Assuming that there is a cryptographic hash function $H' : \{0,1\}^* \to \mathbb{Z}_N^*$, we first fix an $S \in \mathbb{Z}_N^*[-1]$, i.e., Jacobi symbol of S is -1. To get the hash value of H on input x, we compute $H'(x) \in \mathbb{Z}_N^*$, and let $H(x) = H'(x)$ if $H'(x) \in \mathbb{Z}_N^*[+1]$, else $H(x) = H'(x)S \mod N$. So we get a hash function mapping to $\mathbb{Z}_N^*[+1]$ by fixing the hash function H' and S as the description of H. Thus, with the public description of H (description of H' and S), every party can compute the hash function without p, q.

Provable Security. It is well known that Rabin signature can be proven existentially unforgeable against chosen message attack in the random oracle model under the factoring intractable assumption[9,12]. Now we first review the standard definition of signature scheme[10]:

Definition 2. *A signature scheme* $\mathcal{S} = \langle \mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Ver} \rangle$ *is existentially unforgeable under an adaptive chosen message attack if it is infeasible for a forger who only knows the public key to produce a valid message-signature pair after obtaining polynomially many signatures on messages of its choice from the signer. Formally, S is called* (t, ϵ)*-secure, if for every probabilistic polynomial* $t(k)$*-time forger algorithm* $\mathcal{F}$ *there does not exist a non-negligible probability* $\epsilon(k)$ *such that* $Adv(\mathcal{F}) =$

$$Pr\left[\begin{array}{l} \langle pk, sk\rangle \stackrel{R}{\leftarrow} \mathsf{KeyGen}(1^k); \\ \text{for } i = 1, 2, \ldots, j: \\ \quad m_i \leftarrow \mathcal{F}(pk, m_1, \sigma_1, \ldots, m_{i-1}, \sigma_{i-1}); \\ \quad \sigma_i \leftarrow \mathsf{Sign}(sk, m_i); \\ \langle m, \sigma\rangle \leftarrow \mathcal{F}(pk, m_1, \sigma_1, \ldots, m_j, \sigma_j); \\ m \notin \{m_1, \ldots, m_j\} \\ \quad \textit{and } \mathsf{Ver}(pk, m, \sigma) = \textit{accept} \end{array}\right] \geqslant \epsilon.$$

For our variant Rabin signature, we consider a seemingly more powerful attacker denoted by *uf-ecma* which slightly extends the above attacker denoted by *uf-cma*. The only difference between *uf-ecma* and *uf-cma* is that the attacker of the former type has access to an oracle of function $\mathsf{Sign}'(m) = |H(m)|^{1/2^{f(k)}} \mod N$ with some parameter $f(k)$ being super-logarithmic in k (i.e., $f(k) = \omega(\log k)$) instead of the signing oracle $\mathsf{Sign}(m) = |H(m)|^{1/2} \mod N$.

Theorem 1. *In the random oracle model, i.e., the hash function is modeled as an oracle of ideal random function, the above variant signature is existentially unforgeable against the extended attacker uf-ecma under the factoring assumption.*

Proof. The security of the above variant Rabin signature is just a very similar result falling in the field of the provable security of the FDH signature except that the simulated hash value for some m is $r^{2^{f(k)}}$ instead of r^2 where $r \stackrel{R}{\leftarrow} \mathbb{Z}_N$. Since the provable security of the full domain hash signature is so popular, we omitted the complete proof here. And we refer readers to [12] for more details. □

4 Chameleon Hash Based on Factoring

Now with the customized Rabin signature scheme, we can present the four probabilistic polynomial time algorithms which consist our chameleon hash scheme as follows. Especially note that in Remark 2, we present the slightly generalized notion of collisions as well as the meaning of the notation "$= \pm$".

• GenKey. Same to that of the above signature scheme. Additionally, we restrict the considered message space of the chameleon hash is $\{0,1\}^{f(k)}$ where $f(k)$ is super-logarithmic in k (i.e., $f(k) = \omega(\log k)$). The case of the message space of $\{0,1\}^*$ can be easily extended by using a resistant hash function from $\{0,1\}^*$ to $\{0,1\}^{f(k)}$.

• Hash. Given the public key N, the label L and the message $m \in \{0,1\}^{f(k)}$, first choose a random string $r \in \mathbb{Z}_N$ and compute the hash value:

$$h = Hash(pk, L, m, r) = bJ^m r^{2^{f(k)}} \mod N$$

where $J = H(L), b \stackrel{R}{\leftarrow} \{+1, -1\}$.

Remark 1. In the common Rabin signature scheme, for example that in [12], the signer first applies a secure hash-and-encode scheme, mapping arbitrary bit-strings (the message) to integers in QR_N. Since the party without (p, q) cannot determine whether a given integer is a quadratic residue, he cannot do such a procedure to hash-and-encode the message. However, the hash-and-encode scheme in our scheme is just H whose computation is independent on the knowledge of (p, q). And we are afraid that this is just one of the reasons why there is no chameleon hash scheme based factoring proposed before by just using the similar method for the construction of RSA-based chameleon hash scheme.

Remark 2. Given the fixed label L, h is a random variable dependent on the random bit b. In the following, when $X = \pm Y \mod N$ is mentioned, we mean that either $X = Y \mod N$ or $X = -Y \mod N$. And we slightly extend the usual notion of a collision as follows. If $Hash(pk, L, m, r) = \pm Hash(pk, L, m', r')$, we say that (m, r) and (m', r') are a pair of collisions.

• UForge. Given the secret key p, q, the original hashed value (m, r) and the message m' to be forged, first compute the ephemeral trapdoor for the label L: $B \xleftarrow{R} |H(L)|^{\frac{1}{2^{f(k)}}} \mod N$ using the factor p, q. Then for m', set the corresponding simulated random string $r' = rB^{m-m'} \mod N$. Note that

$$\begin{aligned} Hash(N, L, m', r') &= \pm H(L)^{m'} r'^{2^{f(k)}} \\ &= \pm H(L)^{m'} (rB^{m-m'})^{2^{f(k)}} \\ &= \pm H(L)^{m'} |H(L)|^{m-m'} r^{2^{f(k)}} \\ &= \pm H(L)^{m} r^{2^{f(k)}} \\ &= \pm Hash(N, L, m, r). \end{aligned}$$

Therefore, the forgery is successful. In other words, since the the only difference between $Hash(N, L, m, r)$ and $Hash(N, L, m', r')$ is $\pm$, (m, r) and (m', r') are collisions as in Remark 2.

• SForge. Let (m, r) and (m', r') be a pair of collision. So we have $\pm H(L)^m r^{2^{f(k)}} = H(L)^{m'} r'^{2^{f(k)}} \mod N$. Then we have $|H(L)|^{(m-m')} = (r'/r)^{2^{f(k)}}$. First, compute one square root of $J' = |H(L)|$:

$$b = ((r'/r)^u J^v)^{2^{f(k)-s-1}} \mod N$$

where $2^s = \gcd(m - m', 2^{f(k)})$, $0 \leqslant s < f(k)$, $J = H(L)$.

Indeed, we can use the similar technique in [13] as follows. We have

$$J'^{m-m'} = (r'/r)^{2^{f(k)}} \mod N.$$

Compute $u, v \in \mathbb{Z}$ such that $u(m - m') + v2^{f(k)} = 2^s$, and then compute

$$\begin{aligned} J'^{2^s} &= J'^{u(m-m')+v2^{f(k)}} \\ &= (J'^{m-m'})^u \cdot (J'^v)^{2^{f(k)}} \\ &= ((r'/r)^u J'^v)^{2^{f(k)}} \mod N. \end{aligned}$$

Let $b = ((r'/r)^u J^v)^{2^{f(k)-s-1}}$, then

$$J'^{2^s} = (b^2)^{2^s}.$$

Since $J', b^2 \in QR_N$ and squaring permutes QR_N where N is a Blum integer, so we have $J' = b^2 \mod N$. So we get a square root b of J'.

Now if $m' > 2^{f(k)-1}$, let $m'' = m' - 2^{f(k)-1}$ and $r'' = r'b \mod N$; if $m' \leqslant 2^{f(k)-1}$, $m'' = 2^{f(k)-1} + m'$ and $r'' = r'/b \mod N$.

Indeed, if $m' > 2^{f(k)-1}$, we can see that

$$\begin{aligned} Hash(N, L, m'', r'') &= \pm H(L)^{m''} r''^{2^{f(k)}} \\ &= \pm H(L)^{m'-2^{f(k)-1}} (r'b)^{2^{f(k)}} \\ &= \pm H(L)^{m'-2^{f(k)-1}} (b^2)^{2^{f(k)-1}} r'^{2^{f(k)}} \\ &= \pm H(L)^{m'} r'^{2^{f(k)}} \\ &= \pm Hash(N, L, m', r') \mod N. \end{aligned}$$

If $m' \leqslant 2^{f(k)-1}$, we can show $Hash(N, L, m', r') = \pm Hash(N, L, m'', r'')$ using the similar technique to the above.

Below, we discuss the security of the above chameleon hash scheme.

Theorem 2. *The above chameleon hash scheme enjoys all advantages of the previous schemes: collision-resistance, message-hiding, semantic security, and key-exposure-freeness.*

Proof. Collision Resistance. Given two collisions (m, r) and (m', r') with the same hash value for some label L, as in $SForge()$ we can compute $|H(L)|^{1/2} \mod N$ which is just a variant Rabin signature on L. So by the security of the variant Rabin signature scheme, the chameleon hash scheme is collision resistant.

Message Hiding. Given (m', r') and (m, r) with the same chameleon hash value, by the algorithm $SForge()$ we can get another collision pair (m'', r'').

Semantic Security. For each message m, the value $h = \pm Hash(N, L, m, r)$ is uniquely determined by the value $r^{2^{f(k)}} (\in QR_N)$ with ignoring $\pm$, and vice-versa. So, the conditional probability taken over the message space $\mu(m|h) = \mu(m|r^{2^{f(k)}})$. And $\mu(m|r^{2^{f(k)}}) = \mu(m)$ since m and r are independent variables. So $\mu(m|h) = \mu(m)$, i.e., the chameleon hash value h discloses no information about the message m.

Key Exposure Freeness. If an attacker $\mathcal{A}_1$ against the above chameleon hash scheme can be successful with respect to the property of key-exposure-freeness, then we can use it to construct an attacker $\mathcal{A}_2$ of type *uf-ecma* against the above variant Rabin signature as follows. First $\mathcal{A}_2$ is given the public parameters of the variant Rabin signature, i.e., the public key N and the description of the hash function H including $f(k)$, and $\mathcal{A}_2$ pass them to $\mathcal{A}_1$. Then when $\mathcal{A}_1$ makes a query (L_i, m_i, r_i) of oracle access to $UForge(sk, \cdot, \cdot, \cdot)$, $\mathcal{A}_2$ can get the ephemeral trapdoor $H(L_i)^{1/2^{f(k)}} \mod N$ from

its own oracle access and further compute a collision (m'_i, r'_i) as in *UForge* and return it. At last, when $\mathcal{A}_1$ returns $(m, r), (m', r')$ and a never queried label L such that $Hash(N, L, m, r) = Hash(N, L, m', r')$, $\mathcal{A}_2$ can compute $|H(L)|^{1/2} \mod N$ as in *SForge*. Now $\mathcal{A}_2$ is secure against the above variant Rabin signature in the model of the attack *uf-ecma*. □

5 Chameleon Hash Signature

Using the general paradigm[1,2] of chameleon-hash-and-sign to construct chameleon signature, we can use the above chameleon hash and the RSA signature or Rabin signature with the same public setting to construct a chameleon signature with message hiding and key-exposure-freeness. Because of the simplicity of the modular construction of a chameleon signature scheme with the framework and the chameleon hash scheme, we omit the details here.

6 Conclusion

In this paper, we first propose a variant of Rabin signature and prove that it is existentially unforgeable against a stronger adaptive chosen message attack (*uf-ecma*) in the random oracle model. Then based on such Rabin signature, we propose a new chameleon hash scheme which is based on a weaker assumption of factoring than RSA assumption and remains the similar computational efficiency. And we prove that it enjoys all advantages of the previous schemes: collision-resistant, message hiding, semantic security, and key-exposure-free. And in order to support it, we first propose a variant Rabin signature scheme and prove such signature scheme is secure against a new type of attack in random oracle model.

References

[1] Krawczyk H, Rabin T. Chameleon signatures. In *Proc. Symposium on Network and Distributed System Security Symposium* (*NDSS 2000*), San Diego, CA, February, 2000, pp.143–154.

[2] Ateniese G, de Medeiros B. Identity-based chameleon hash and applications. In *Proc. Financial Cryptography* (*FC'04*), Key West, Florida, USA, February 9–12, 2004, Springer-Verlag, *LNCS 3110*, pp.164–180.

[3] Chen X, Zhang F, Kim K. Chameleon hashing without key exposure. In *Proc. the 7th Information Security Conference* (*ISC'04*), Palo Alto, USA, September 27–29, 2004, Springer-Verlag, *LNCS 3225*, pp.87–98.

[4] Ateniese G, de Medeiros B. On the key exposure problem in chameleon hashes. In *Proc. the 4th Conference on Security in Communication Networks* (*SCN'04*), Amalfi, Italy, September 8–10, 2004, Springer-Verlag, *LNCS 3352*, pp.165–179.

[5] MacKenzie P, Yang K. On simulation-sound trapdoor commitments. In *Proc. EUROCRYPT'04*, Interlaken, Switzerland, May 2–6, 2004, Springer-Verlag, *LNCS 3027*, pp.382–400.

[6] Gennaro R. Multi-trapdoor commitments and their applications to proofs of knowledge secure under concurrent man-in-the-middle attacks. In *CRYPTO'04*, Santa Barbara, California, USA, August 15–19, 2004, Springer-Verlag, *LNCS 3152*, pp.220–236.

[7] Hu L, Dong J, Pei D. Implementation of cryptosystems based on Tate pairing. *J. Comput. Sci. & Technol.*, 2005, 20(2): 264–269.

[8] Rabin M. Digital signatures. Foundations of Secure Computation. Dobkin D, Jones A, Lipton R (eds.), New York: Academic Press, 1978, pp.155–168.

[9] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. the 1st ACM Conf. Computer and Communications Security*, Fairfax, VA, November 3–5, 1993, pp.62–73.

[10] Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal of Computing*, 1998, 17(2): pp. 281–308.

[11] Bellare M, Namprempre C, Neven G. Security proofs for identity-based identification and signature schemes. In *Proc. Eurocrypt'2004*, Interlaken, Switzerland, May 2–6, 2004, Springer-Verlag, *LNCS 3027*, pp. 268–286.

[12] Bellare M, Rogaway P. The exact security of digital signatures: How to sign with RSA and Rabin. In *Proc. Eurocrypt 96*, Zaragoza, Spain, May 12–16, 1996, Springer-Verlag, *LNCS 1070*, pp.399–416.

[13] Fischlin M, Fischlin R. The representation problem based on factoring. In *Proc. the Cryptographer's Track at the RSA Conference on Topics in Cryptology 2002* (*Topics in Cryptology—CT-RSA 2002*), San Jose, CA, USA, February 18–22, 2002, Springer-Verlag, *LNCS 2271*, pp.96–113.