A Formal Proof of Zhu's Signature Scheme

Huafei Zhu

Department of Information Science and Electronics Engineering, YuQuan Campus,
Zhejiang university, 310027, Hangzhou,PR. China
Email: zhuhf@zju.edu.cn

Abstract. Following from the remarkable works of Cramer and Shoup [5], three trapdoor hash signature variations have been presented in the literature: the first variation was presented in CJE'01 by Zhu [14], the second variation was presented in SCN'02 by Camenisch and Lysyanskaya [3] and the third variation was presented in PKC'03 by Fischlin [7]. All three mentioned trapdoor hash signature schemes have similar structure and the security of the last two modifications is rigorously proved. We point out that the distribution of variables derived from Zhu's signing oracle is different from that generated by Zhu's signing algorithm since the signing oracle in Zhu's simulator is defined over Z, instead of Z_n. Consequently the proof of security of Zhu's signature scheme should be studied more precisely. We also aware that the proof of Zhu's signature scheme is not a trivial work which is stated below:

- the technique presented by Cramer and Shoup [5] cannot be applied directly to prove the security of Zhu's signature scheme since the structure of Cramer-Shoup's trap-door hash scheme is double deck that is easy to simulate a signing query as the order of subgroup G is a public parameter;
- the technique presented by Camenisch and Lysyanskaya [3] cannot be applied directly since there are extra security parameters l and l_s guide the statistical closeness of the simulated distributions to the actual distribution;
- the technique presented by Fischlin cannot be applied directly to Zhu's signature scheme as the security proof of Fischlin's signature relies on a set of pairs $(\alpha_i, \alpha_i \oplus H(m_i))$ while the security proof of Zhu's signature should rely on a set of pairs $(\alpha_i, H(m_i))$.

In this report, we provide an interesting random argument technique to show that Zhu's signature scheme immune to adaptive chosen-message attack under the assumptions of the strong RSA problem as well as the existence of collision free hash functions.

Keywords: Adaptive chosen message attack, collision-free hash function, signature scheme, strong RSA assumption

1 Introduction

Digital signature schemes play central role in cryptology. Goldwasser, Micali and Rivest formally defined the strongest notion, called existential unforgeability

under adaptive chosen message attack for a digital signature protocol, together with a concrete example that attains this property (we call it GMR signature scheme, for short [10]). Intuitively, a signature scheme is said secure against existential unforgeability under adaptive chosen message attack if an adversary is able to forge a signature of a message m ($m \neq m_i$, $1 \leq i \leq k$) only with negligible probability after he/she has queried correspondent signature of each message $m_1, \cdots, m_k$, which is chosen adaptively by the adversary.

GMR signature scheme is based on a binary tree and involves a large number of authentication steps. Following the pioneer works of Goldwasser, Micali and Rivest [10], Bellare and Micali [1] presented a generic approach to construct a secure digital signature scheme based on the existence of any trapdoor permutation. Later Dwork and Naor improved GMR's signature scheme based on a flat tree [6], and finally Cramer and Damgard presented an improved scheme of [6] by eliminating the shared random string set [4]. The above mentioned signature schemes rely on the standard intractability of the factoring problem.

Recently, Gennaro, Halevi and Rabin present an efficient signature scheme based on the strong-RSA assumption as well as a chameleon hash function [9]. A similar signature scheme has been developed by Cramer and Shoup independently without chameleon hash assumption [5]. Cramer-Shoup's scheme is quite efficient and interesting both from the theoretical and practical views. Following from the remarkable works of Cramer and Shoup, three trapdoor hash signature variations have been presented in the literature: the first variation was presented in CJE'01 by Zhu [14], the second variation was presented in SCN'02 by Camenisch and Lysyanskaya [3] and the third variation was presented in PKC'03 by Fischlin [7]. All three mentioned trapdoor hash signature schemes have similar structure and the security of the last two modifications is rigorously proved. We point out that the distribution of variables derived from Zhu's signing oracle is different from that generated by Zhu's signing algorithm since the signing oracle in Zhu's simulator is defined over Z, instead of Z_n. Consequently the proof of security of Zhu's signature scheme should be studied more precisely. We also aware that the proof of Zhu's signature scheme is not a trivial work which is stated below:

- the technique presented by Cramer and Shoup [5] cannot be applied directly to prove the security of Zhu's signature scheme since the structure of Cramer-Shoup's trap-door hash scheme is double deck that is easy to simulate a signing query as the order of subgroup G is a public parameter;
- the technique presented by Camenisch and Lysyanskaya [3] cannot be applied directly since there are extra security parameters l and l_s guide the statistical closeness of the simulated distributions to the actual distribution;
- the technique presented by Fischlin cannot be applied directly to Zhu's signature scheme as the security proof of Fischlin's signature relies on a set of pairs $(\alpha_i, \alpha_i \oplus H(m_i))$ while the security proof of Zhu's signature should rely on a set of pairs $(\alpha_i, H(m_i))$.

In this report, we provide an interesting random argument technique to show that Zhu's signature scheme immune to adaptive chosen-message attack under the assumptions of the strong RSA problem as well as the existence of collision free hash functions.

2 Related works

2.1 Notions and primitives

Definition of signature schemes [10]: Probabilistic polynomial time algorithms $(G, Sign, Verify)$ where G is the key generation algorithm, $Sign$ is the signature algorithm, and $Verify$ the verification algorithm, constitute a digital signature scheme for efficiently samplable (in the length of its index) message space M, if for all $m \in M$:

- Correctness: If a message m is in the message space for a given PK, and SK is the corresponding secret key, the output of $Sign_{SK}(m)$ will always be accepted by the verification algorithm $Verify_{PK}$. More formally, for all value m:

  $$\Pr[(PK, SK) \leftarrow G(1^k); \sigma \leftarrow Sign_{SK}(m) : m \in M \wedge Verify_{PK}(m, \sigma) = 0] = 0$$

- Security: Even if an adversary has oracle access to the signing algorithm which provides signatures on messages of the adversary's choice, the adversary cannot create a valid signature on a message not explicitly queried. More formally, for all families of probabilistic polynomial-time algorithm oracle Turing machine A_k, there exists a negligible function $\nu(k)$ such that $\Pr[(PK, SK) \leftarrow G(1^k); (Q, x, \sigma) \leftarrow A_k^{Sign_{SK}(1^k)} : Verify_{PK}(m, \sigma) = 1 \wedge \exists \sigma' Verify_{PK}(m', \sigma') = 1, m' \notin Q))] = \nu(k)$

Strong RSA assumption: Strong RSA assumption was introduced by Baric and Pfitzmann [2] and Fujisaki and Okamoto [8]: The strong RSA assumption is that it is hard, on input an RSA modulus n and an element $z \in Z_n^*$, to compute values $e > 1$ and y such that $y^e = z \bmod n$. More formally, we assume that for all polynomial time circuit families A_k, there exists a negligible function $\nu(k)$ such that:

$$\Pr[n \leftarrow G(1^k), z \leftarrow Z_n^*, (e, y) \leftarrow A_k(n, z) : e > 1 \wedge y^e = z \bmod n] = \nu(k)$$

The following lemma, due to Guillou-Quisquater [11], is useful to prove the security of Zhu's signature scheme.

Guillou-Quisquater lemma Suppose $w^e = z^b$ and $d = \gcd(e, b)$. Then there exists an efficient algorithm computing the (e/d)-th root of z.

Proof: Since $d = \gcd(e, b)$, by Euclidean algorithm, $d = ee' + bb'$. It yields the equation $z = (z^{e'} w^{b'})^{e/d}$.

2.2 Cramer-Shoup signature scheme and its variations

Cramer-Shoup's trapdoor hash scheme Cramer and Shoup presented an elegant signature scheme called trapdoor hash function defined below (see [5] for more details):

- Key generation algorithm: Let p, q be two large primes such that $p-1 = 2p'$ and $q-1 = 2q'$, where p', q' are two l'-bit strings. Let $n = pq$ and QR_n be the quadratic residue of Z_n^*. Let x, h be two generators of QR_n. Also chosen are a group G of order s, where s is $(l+1)$-bit prime, and two random generators g_1, g_2 of G. The public key is (n, h, x, g_1, g_2, H) along with an appropriate description of G including s. The private key is (p, q).
- Signature algorithm: To sign a message m, a $(l+1)$-bit prime e and a string $t \in Z_s$ is chosen. The are chosen at random. The equation $y^e = xh^{H(g_1^t g_2^{H(m)})} \mathrm{mod} n$ is solved for y. The corresponding signature of the message m is (e, t, y).
- Verification algorithm: Given a putative triple (e, t, y), the verifier first checks that e is an odd $(l+1)$-bit number. Second it checks the validation that $x = y^e h^{-H(g_1^t g_2^{H(m)})} \mathrm{mod} n$. If the equation is valid, then the verifier accepts, otherwise, it rejects.

Zhu's signature scheme In their scheme, another extra group G is defined. From the point views of computational complexity it is non-trivial work therefore if one can reduce the computational and communication complexity while its provability and efficiency can be maintained. Based on this observation, Zhu provides a variation scheme below [14]:

- Key generation algorithm: Let p, q be two large primes such that $p-1 = 2p'$ and $q-1 = 2q'$, where p', q' are two $(l'+1)$-bit strings. Let $n = pq$ and QR_n be the quadratic residue of Z_n^*. Let g, h be two generators of QR_n. The public key is (n, g, h, X, H), where $X \in QR_n$ and H is a collision free hash function with output length l. The private key is (p, q).
- Signature algorithm: To sign a message m, a $(l+1)$-bit prime e and a string $t \in \{0,1\}^l$ are chosen at random. The equation $y^e = Xg^t h^{H(m)} \mathrm{mod} n$ is solved for y. The corresponding signature of the message m is (e, t, y).
- Verification algorithm: Given a putative triple (e, t, y), the verifier first checks that e is an odd $(l+1)$-bit number. Second it checks the validation that $X = y^e g^{-t} h^{-H(m)} \mathrm{mod} n$. If the equation is valid, then the verifier accepts, otherwise, it rejects.

Camenisch-Lysyanskaya's signature scheme In SCN'02, Camenisch and Lysyanskaya [3] presented alternative signature scheme. The Camenisch and Lysyanskaya signature is described as follows (see [3] for more details).

- Key generation algorithm: On input 1^k, choose a special RSA modulus $n = pq$, $p = 2p' + 1$, $q = 2q' + 1$ of length $l_n = 2k$. Choose, uniformly at random, $a, b, c \in QR_n$. Output $PK = (n, a, b, c)$, and $SK = p$.

– Message space. Let l_m be a parameter. The message space consist of all binary string of length l_m. Equivalently, it can be thought of as consisting of integers in the range $[0, 2^{l_m})$.
– Signing algorithm: On input m, choose a random prime number $e > 2^{l_m+1}$ of length $l_e = l_m + 2$, and a random number s of length $l_s = l_n + l_m + l$, where l is a security parameter. Compute the value v such that

$$v = ca^m b^s \mathrm{mod} n$$

– Verification algorithm: To verify that the tuple (e, s, v) is a signature on message m in the message space, check that $v = ca^m b^s \mathrm{mod} n$ and check that $2^{l_e} > e > 2^{l_2-1}$.

Fischlin's signature scheme Later a similar modification is presented in PKC'03 by Marc Fischlin. Fischlin's signature scheme is defined as follows [7]:

– Key generation: Generating $n = pq$, where $p = 2p' + 1$ and $q = 2q' + 1$ for primes p, q, p', q'. Also pick three quadratic residue $h_1, h_2, x \in QR_n$. The public key verification key is (n, h_1, h_2, x) and the private key is (p, q).
– Signing: To sign a message m calculate the l-bit hash value $H(m)$ with a collision-intractable hash function $H(\cdot)$. Pick a random $(l + 1)$-bit prime e, and a random l-bit string α and compute a representation $(-\alpha, -(\alpha \oplus H(m)), y)$ of x with respect to h_1, h_2, e, n, i.e.,

$$y^e = x{h_1}^{\alpha}{h_2}^{\alpha \oplus H(m)} \mathrm{mod} n.$$

Computing this e-th root y from $x{h_1}^{\alpha}{h_2}^{\alpha \oplus H(m)}$ is easy given the factorization of n. The signature is (e, α, y).
– Check that e is an odd $(l + 1)$-bit integer, that α is l bits long, and that $y^e = x{h_1}^{\alpha}{h_2}^{\alpha \oplus H(m)} \mathrm{mod} n$.

The relationship between Zhu's signature and Camenisch-Lysyanskaya's signature scheme is obvious. Here we remark the relationship between Zhu's signature schemes and Fischlins's scheme therefore.

– It is clear that the algebraic structures of Zhu's and Fischlin's signature are same;
– If there is no collision hash function involved in the above two schemes, then it is not hard to show that the above two signature schemes are equivalent in the same security level. More precisely, if Zhu's scheme can be broken by an adversary A with non-negligible probability then there exists an adversary B^A so that Fischlin's signature scheme can be broken with the same probability. The statement is also true by means of vis-a-vis argument.
– In case of a collision free hash function involved in both schemes, suppose Zhu's signature scheme can be broken with non-negligible probability, i.e., there is an adversary A is able to forge a faking message m in Zhu's signature scheme, denoted by $\sigma(m) = (e, y, t)$ with non-negligible probability. Then

there exists an adversary B^A in Fischlin's signature scheme so that it is able to produce a valid signature $\sigma(m') = (e, y, t)$ for any message in the set $S := \{m' | H(m) \oplus H(m') = t\}$, where t is a component of faking signature $\sigma(m)$ correspondent to Zhu's signature scheme. The statement is also true by means of vis-a-vis argument.

3 The proof of security

Main result: Zhu's signature scheme is immune to adaptive chosen-message attack under joint assumptions of the strong RSA problem as well as the existence of collision free hash function.

Proof: Assume that the signature scheme is NOT secure against adaptive chosen message attack. That is, there is an adversary, who is able to forge the signature (e, t, y) of a message $m(m \neq m_i,\ 1 \leq i \leq f)$ with non-negligible probability after it has queried correspondent signature of each message $m_1, \cdots, m_f$, which is chosen adaptively by the adversary. Let $(e_1, t_1, y_1), \cdots, (e_f, t_f, y_f)$ be signatures provided by the signing oracle corresponding to a set of messages $m_1, \cdots, m_f$. We consider three types of forgeries: 1) for some $1 \leq j \leq f$, $e = e_j$ and $t = t_j$; 2) for some $1 \leq j \leq f$, $e = e_j$ and $t \neq t_j$; 3) for all $1 \leq j \leq f$, $e \neq e_j$. We should show that any forgery scheme of the two types will lead to a contradiction to the assumptions of the theorem. This renders any forgery impossible.

Type 1-Forger

We consider an adversary who chooses a forgery signature such that $e = e_j$ for a fixed j: $1 \leq j \leq f$, where f is the total number of the queries to the signing oracle. If the adversary succeeds in a signature forgery as type1 with non-negligible probability then given n, we are able to compute $z^{1/r}$ with non-negligible probability, where r is a $(l+1)$-bit prime. This contradicts to the assumed hardness of the standard RSA problem. We state the attack in details as follows: given $z \in Z_n^*$ and r, we choose a set of total $f-1$ primes with length $(l+1)$-bit $e_1, ...e_{j-1}, e_{j+1}, ..., e_f$ uniformly at random. We then create the correspondent public key (X, g, h) of the simulator as follows: given $z \in Z_n^*$ and r, we choose a set of total $f-1$ primes with length $(l+1)$-bit $e_1, ...e_{j-1}, e_{j+1}, ..., e_f$ uniformly at random. We choose $w, v \in Z_n$ uniformly at random, and compute $h = z^{2e_1 \cdots e_{j-1} e_{j+1} \cdots e_f}$, $g = v^{2e_1 \cdots e_f} z^{2e_1 \ldots e_{j-1} e_{j+1} \ldots e_f}$ and $X = w^{2\beta e_1 \cdots e_f} z^{2e_1 \ldots e_{j-1} e_{j+1} \ldots e_f(-\alpha)}$, where $\alpha \in \{0,1\}^l$ and $\beta \in Z_n$ are chosen uniformly at random.

Since the simulator knows each e_i, therefore it is easy to compute the i-th signing query. What we need to show is how to simulate the j-th signing query. This can be done as follows:

$$y_j^{e_j} = X g^{t_j} h^{H(m_j)} = (w^{\beta} v^{t_j})^{2e_1 \cdots e_f} z^{2e_1 \ldots e_{i-1} e_{i+1} \ldots e_f(-\alpha + t_j + H(m_j))}$$

Now we set $-\alpha + t_j + H(m_j) = 0$, i.e, $t_j = \alpha - H(m_j)$. To show the simulation above is non-trivial, we should show $Pr\{\alpha \geq H(m_j)\}$ is an non-negligible amount.

For the fixed collision-free hash function H, denote p_i the probability that a message $m \in \{0,1\}^{poly(k)}$ is mapped to an element $i \in \{0,1\}^l$, where k is a security parameter (here we view the j-th message chosen by the adversary adaptively as a random variant). Since X is a public key, the information (α, β) is the random from the point views of the adversary up to the j-th query. Hence, the choice of the j-th query $H(m_j)$ to the signing oracle is independent to α. Now, suppose $H(m_j) = j'$ for the j-th query message m_j, then the probability that the event $\{\alpha \geq H(m_j)\}$ occurs can be evaluated as follows:

$$\Pr(\alpha \geq H(m_j)) = \Pr(\alpha \geq j') = \sum_{j',\cdots,2^l} \frac{1}{2^l} = 1 - \frac{j'}{2^l}$$

Suppose the probability $\Pr(\alpha \geq H(m_j))$ is an negligible amount. Equivalently, the range of hash function H is restricted to the fix point 2^l except for an negligible amount. This contradicts the collision-free assumption.

Suppose the adversary is able to forge a faking signature of message m, denoted by (e, y, t), such that $e_j = e(= r)$, $t_j = t$. Notice that one can not assume that $e_j = e$, $t_j = t$ and $y_j = y$, since H is a collision free hash function. Now we have two equations: $y_j^e = Xg^t h^{H(m_j)}$ and $y^e = Xg^t h^{H(m)}$. Consequently, we obtain the equation:

$$(\frac{y_j}{y})^e = h^{H(m_j)-H(m)} = z^{2e_1,\ldots e_{j-1},e_{j+1},\ldots,e_f(H(m_j)-H(m))}$$

It follows that one can extract the e-th root of z with non-negligible probability. Therefore, we arrive at the contradiction of the standard hardness of RSA assumption.

Remark on Type 1- Forger: The idea behind of our proof is that we view the j-th message m_j chosen by an adversary as a random variable from the point views of simulator. Therefore, our proof does not rely on the randomness of hash function H as that in the random oracle paradigm.

Type 2-Forger

We consider an adversary who succeed in forging a valid signature such that $e = e_j$, $t \neq e_j$ for a fixed j: $1 \leq j \leq f$, where f is the total number of the queries to the signing oracle. If the adversary succeeds in a signature forgery as type1 with non-negligible probability then given n, we are able to compute $z^{1/r}$ with non-negligible probability for a given z and r, where r is a $(l+1)$-bit prime. This contradicts to the assumed hardness of the standard RSA problem. We state the attack in details as follows: given $z \in Z_n^*$ and r, we choose a set of total $f-1$ primes with length $(l+1)$-bit $e_1, \ldots e_{j-1}, e_{j+1}, \ldots, e_f$ at random. We then create the correspondent public key (X, g, h) of the simulated signature

scheme as follows: $g = z^{2e_1 \ldots e_{j-1} e_{j+1} \ldots e_f}$, $h = v^{2e_1 \ldots e_f}$ and $X = g^{-\alpha} w^{2e_1 \ldots e_f}$, where $w, v \in Z_n$ and α is a l-bit random string. Since QR_n is a cyclic group, we can assume that g, h are generators of QR_n with overwhelming probability. To sign the i-th message $m_i (i \neq j)$, the signing oracle selects a random string $t_i \in \{0,1\}^l$, and computes:

$$y_i{}^{e_i} = ((wv^{H(m_i)})^{2e_1 \ldots e_{i-1} e_{i+1} \ldots e_f} z^{2(t_i - \alpha) \Pi_{s \neq i, s \neq j} e_s})^{e_i}$$

The output of the signing oracle is a signature of message m_i, denoted by $\sigma(m_i) = (e_i, y_i, t_i)$.

To sign the j-th message m_j, the signing oracle, sets $t_j \leftarrow \alpha$ and computes:

$$y_j{}^{e_j} = ((wv^{H(m_j)})^{2\Pi_{s \neq j} e_s})^{e_j}$$

The output of the signing oracle is a signature of message m_j, denoted by $\sigma(m_j) = (e_j, y_j, t_j)$.

Let $\sigma(m) = (e, y, t)$ be a valid signature forged by the adversary of message m. By assumption, we know that $y^e = X g^t h^{H(m)}$. Consequently, we have the following equation:

$$g^{t_j} h^{H(m_j)} y_j{}^{e_j} = g^t h^{H(m)} y^e$$

Equivalently

$$z^{2(\alpha - t) \Pi_{i \neq j} e_i} = (v^{2(H(m) - H(m_j)) \Pi_{i \neq j} e_i} \frac{y}{y_j})^{e_j}$$

Since $t_j = \alpha$ and $t \neq t_i$ by assumption, it follows that $t \neq \alpha$. We then apply Guillou-Quisquater lemma to extract the r-th root of z, where $r = e_j$.

Type 3-Forger

We consider the second type of the attack: the adversary forgery is that for all $1 \leq j \leq f$, $e \neq e_j$. If the adversary succeeds in forgery with non-negligible probability, then given n, a random $z \in Z_n^*$, we are able to compute $z^{1/d}$ $(d > 1$) with non-negligible probability, which contradicts to the assumed hardness of strong RSA assumption. We state our attack in details as follows: we generate g and h with the help of z. We define $g = z^{2e_1 \ldots e_f}$ and $h = g^a$, where $a \in (1, n^2)$, is a random element. We can assume that g is a generator of QR_n with overwhelming probability. Finally, we define $X = g^b$, where $b \in (1, n^2)$. Since the simulator knows the all e_j, the signature oracle can be perfectly simulated. Let (e, t, y) be a forgery signature of message m. It yields the equation $y^e = X g^t h^{H(m)} = z^E$, where $E = (b + t + aH(m)) 2e_1 \ldots e_f$.

Since we are able to compute (e/E)-th root of z provided e is a not a divisor of E according to the lemma of Guillou and Qusiquater, it is sufficient to show that e is not a divisor of E with non-negligible probability. Due to the the fact that $\gcd(e, e_1 e_2 \cdots e_f) = 1$, it is sufficient to show that e is not a divisor of $b+t+aH(m)$ with non-negligible probability. Since $b \in (1, n^2)$, it follows that one can write $b = b' p' q' + b''$. Therefore, the probability that $b + t + aH(m) \equiv 0 \mathrm{mod} e$ is about $1/e$.

Remark on Type 3- Forger: We remark that to show that $e|(b+t+aH(m)$ with negligible probability, one may make use of randomness of $a \in (1, n^2)$. That is one can write a as $a = a'p'q' + a''$. It follows a' is a random element from the adversary's view. Hence the probability that $b + t + aH(m) \equiv 0 \mathrm{mod} e$ is about $1/e$. Thus, with non-negligible probability, e is not a divisor of $b+t+aH(m)$. We point out that since the adversary may find $H(m) = 0$, the term $aH(m)$ may be cancelled in the formula in the equation. Thus the random argument must be done in term b instead of $aH(m)$ since collision-resistance does not imply zero-finder intractability in general. This remark also suitable for Cramer-Shoup's argument.

4 Conclusion

In this report, we provide a rigorous proof of security of Zhu's signature scheme and we have shown that Zhu's signature scheme is immune to adaptive chosen-message attack under joint assumptions of the strong RSA problem as well as the existence of collision free hash function.

References

1. M. Bellare and S. Micali. How to sign given any trapdoor permutation. Journal of the ACM, Vol. 39, No. 1, January 1992, pp. 214–233.
2. N. Braic and B. Pfitzmann. Collision free accumulators and fail-stop signature scheme without trees. Eurocrypt'97, 480-494, 1997.
3. J.Camenisch, A. Lysyanskaya. A Signature Scheme with Efficient Protocols. SCN 2002: 268-289
4. R. Cramer and I. Damgard. New generation of secure and practical RSA-based signature. Crypto'96. 173-185, 1996.
5. R. Cramer and V. Shoup. Signature scheme based on the Strong RAS assumption. 6th ACM Conference on Computer and Communication Security, Singapore, ACM Press, November 1999.
6. Cynthia Dwork, Moni Naor: An Efficient Existentially Unforgeable Signature Scheme and its Applications. *CRYPTO* 1994: 234-246.
7. Marc Fischlin: The Cramer-Shoup Strong-RSASignature Scheme Revisited. Public Key Cryptography, 2003: 116-129
8. E. Fujisaki, T. Okamoto. Statistical zero-knowledge protocols to prove modular polynomial relations. Crypto'97, LNCS 1294, Springer-verlag, 1997.
9. R. Gennarou, S. Halevi and T. Rabin. Secure hash-and-sign signatures without random oracle. Eurocrypto'99. 123-139, 1999.
10. S. Goldwasser, S. Micali, R. Rivest: A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. SIAM J. Comput. 17(2): 281-308, 1988.
11. L. Guillou, J. Quisquater. A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory. Eurocrypto'88, 123-128, 1988.

12. H.Krawczyk, T. Rabin. Chameleon hashing and signatures. Theory of Cryptography Library. March 1998.
13. V. Shoup and R. Gennaro. Securing threshold cryptosystems against chosen cipher-text attack. Crypto'98, 1-16, 1998.
14. Huafei Zhu. New Digital Signature Scheme Attaining Immunity to Adaptive Chosen-message attack. Chinese Journal of Electronics, Vol.10, No.4, Page 484-486, Oct, 2001.