Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080408

A Provably Secure Signature Scheme based on Factoring and Discrete Logarithms

Zuhua Shao[1,*] *and Yipeng Gao*[2]

[1] No. 210, Wulin Road, Hangzhou, Zhejiang, 310006, P. R. China
[2] Department of Materials Science and Engineering, The Ohio State University, USA

Received: 9 Jul. 2013, Revised: 11 Oct. 2013, Accepted: 12 Oct. 2013
Published online: 1 Jul. 2014

Abstract: To make users put much confidence in digital signatures, this paper proposes the first provably secure signature scheme based on both factoring and discrete logarithms. The new scheme incorporates both the Schnorr signature scheme and the PSS-Rabin signature scheme. Unless both the two cryptographic assumptions could be become solved simultaneously, anyone would not forge any signature. The proposed scheme is efficient since the computation requirement and the storage requirement are slightly larger than those for the Schnorr signature scheme and the PSS-Rabin signature scheme.

Keywords: Digital signature, factoring, discrete logarithm, random oracle model.

1 Introduction

Since Diffie and Hellman invented the concept of public key cryptography [1], two families of public key cryptosystems have been proposed. Diffie-Hellman, and later ElGamal, DSA, and Elliptic Curve, Pairings are all in Discrete Logarithm (DL) family, whereas RSA, Rabin and related systems make up Factoring (FAC) family. It means that the security of these public key cryptographic cryptosystems is based the assumption of one mathematic hard problem, DL or FAC. If the hard problem becomes easy to be solved, the corresponding cryptosystem will no longer be secure. DL and FAC are seemingly hard but not NP-complete, it is possible that the two problems could be become solved some days later. Some signatures must be kept in the archives for dozens of years. However, it is very unlikely that multiple hard problems would simultaneously become easy to be solved. Although shor [2] showed that both factoring and discrete logarithm can be solved by quantum algorithms in polynomial time, but it will take a long time to put quantum computers into practice.

Thus several signature schemes tried to base their security on the two well-known assumptions so as to enhance security [3,4,5,6,7,8]. Unless both the two cryptographic assumptions could be become solved simultaneously, anyone would not forge any signature. But several literatures have shown these schemes to be flawed [9,10,11,12,13,14]. Only the Laih-Kuos signature scheme [15] and the Ismail et al.s signature scheme [16] have not been broken so far though they have not provided formal security proofs.

Recently, Zhang et al. [17] proposed an improved scheme of [8] and claimed that the scheme is provably secure in the radon oracle model. But their proof has not showed that a forgery can be used to solve any given FAC problem and any given DL problem simultaneously. In fact, the Pollard-Schnorr algorithm [18] can easily forge the signature for any message if the DL problem is solved.

Hence it is attractive to design provably secure and efficient signature schemes based on multiple hard problem assumptions simultaneously.

The trivial way to enhance security is to sign messages twice; one adopts a FAC-based signature scheme and one uses a DL-based signature scheme. However, more computation and more storage are required. Furthermore, the two signatures would be separated. In contrast with the trivial way, the Laih-Kuos signature scheme is less efficient in terms of computation, storage and key pairs.

By far, the Schnorr signature scheme and the RSA signature scheme are most commonly used in the real

* Corresponding author e-mail: zhshao_98@yahoo.com

world. They are provably secure under FAC assumption and DL assumption respectively in the random oracle model.

In this paper, we will propose the first provably secure signature scheme based on factoring and discrete logarithms simultaneously by combining the Schnorr signature scheme and the PSS-Rabin signature scheme. We will show that the new scheme is strong existentially unforgeabable under adaptive chosen-message attacks in the random oracle model, making better security confidence than those offered by existing signatures based on either discrete-log assumption or factoring assumption. In our security proof, the challenger can solve both FAC and DL simultaneously with one simulation.

The rest of this paper is organized as follows. In section 2, we review briefly a precise definition of generic signature schemes [19], and present the new signature scheme. Then, we provide a formal security proof in section 3. Finally, in section 4, we discuss the performance of the scheme.

2 The proposed signature scheme

In this section, we first review a precise definition of generic signature schemes [19], and then present the new signature scheme under the setting as the Schnorr signature scheme [20] and the Rabin signature scheme [21].

2.1 Definition

Definition 1 (Signature Scheme)

A signature scheme (Gen, sign, Verify) is a triple of algorithms:

-The key generation algorithm Gen that when given a security parameter 1^k as input, outputs a pair (sk, pk) of matching private key and public key. It is clear that Gen must be a probabilistic algorithm.
-The signing algorithm Sign that when given the pair (sk, pk) of the matching private key and public key and a message m as input, produces a signature σ. The signing algorithm might be probabilistic, and in some schemes it might receive other input as well.
-The verification algorithm Verify that on input (pk, m, σ), obtains either *invalid* or *valid*, with property that if $(sk, pk) \leftarrow \text{Gen}(1^k)$ and $\sigma \leftarrow (sk, pk, m)$, then $\text{Verify}(pk, m, \sigma) = valid$. In general, the verification algorithm need not be probabilistic.

2.2 The proposed signature scheme

(1)The key generation algorithm:

The authority chooses the public parameters:
p is a large prime number.
q is a prime divisor of $p-1$.
g is an element of order q in the group Z_p^*.

Each signer chooses an element x in Z_q^*, two larger prime numbers, p_1 and q_1, and computes $n = p_1 q_1$, $y = g^x \pmod p$, where $p_1 = q_1 = 3 \pmod 4$. And then he chooses a random a satisfying Jacobi symbol $\left(\frac{a}{n}\right) = -1$.

$H : \{0,1\}^* \times Z_p^* \to Z_n^*$ is a one-way hash function.

The private key of the signer is (x, p_1, q_1), and the public key is (p, q, g, y, n, a, H).

The subgroup of the group Z_p^* generated by g can be replayed by other groups, such as those built on elliptic curves $G_{g,p} = \{g^0, g^1, \cdots, g^{q-1}\}$.

(2)The signing algorithm:

For a message $m \in \{0,1\}^*$ to be signed, the signer chooses a new random integer k, $1 < k < q$, computes $r = g^k \pmod p$, $s = k - H(m,r)x \pmod q$, and computes c_1 and c_2, respectively.

$$c_1 = \begin{cases} 0, \text{ if Jacobi symbol } \left(\frac{H(m,r)}{n}\right) = 1, \\ 1, \text{ if Jacobi symbol } \left(\frac{H(m,r)}{n}\right) = -1. \end{cases}$$

$l = a^{c_1} H(m,r)$.

$$c_2 = \begin{cases} 0, \text{ if Legendra symbol } \left(\frac{l}{p_1}\right) = \left(\frac{l}{q_1}\right) = 1, \\ 1, \text{ if Legendra symbol } \left(\frac{l}{p_1}\right) = \left(\frac{l}{q_1}\right) = -1. \end{cases}$$

computes e such that $e^2 = (-1)^{c_2} a^{c_1} H(m,r) \pmod n$ by using his private key (x, p_1, q_1).

The signature of the message m is (s, e, c_1, c_2).

Notice that the length of the signature is len(q) + len(n) + 2bit.

(3)The verification algorithm:
Any verifier can verify the signature by checking

$$\frac{e^2}{(-1)^{c_2} a^{c_1}} (\bmod n) = H\left(m, g^s y^{\left(\frac{e^2}{(-1)^{c_2} a^{c_1}} (\bmod n)\right) (\bmod q)} (\bmod p)\right).$$

The verification equation can be regarded as the variants of either the Schnorr signature [20] or the Rabin signature [21].

3 Security model and security proof

In this section, we first review the security model of signature schemes. Then we show that the proposed signature scheme is strong existentially unforgeable against chosen message attacks in the random oracle model assuming that any of the factoring or discrete log problems is hard.

3.1 Security model of signature scheme

Definition 2 (Security of a signature scheme)

A probabilistic algorithm F is said to $(t, q_H, q_S, \varepsilon)$-breaks a signature scheme if after running for at most t steps, making at most q_H adaptive queries to the hash function oracles, and requesting signature oracles on at most q_S adaptively chosen messages, F outputs a new forged signature pair (m, σ) on some message m with probability at least ε, where the probability is taken over the coins of F, the Gen algorithm and the Sign algorithm and the hash function oracle.

We say that a signature scheme is $(t, q_H, q_S, \varepsilon)$-security if no forger can $(t, q_H, q_S, \varepsilon)$-break it.

Definition 3 (DL assumption)

A probabilistic algorithm D is said to (t, ε)-break a DL problem in a group $G_{g,p}$, if D runs in at most t steps and computes the discrete logarithm $DL_{g,p}(g^a) = a$ on input (g, p, q, g^a) with probability at least ε, where the probability is taken over the coins of D and a chosen uniformly from Z_q^*.

We say that the DL problem is (t, ε)-security if no algorithm can (t, ε)-break it.

Definition 4 (FAC assumption)

A probabilistic algorithm F is said to (t, ε)-break a FAC problem, if F runs in at most t steps and computes two primes p and q on input $n, (n = pq)$, with probability at least ε, where the probability is taken over the coins of F, and p and q chosen uniformly.
We say that the FAC problem is (t, ε)-security if no algorithm can (t, ε)-break it.

Goldwasser et al. [22] proposed the standard definition of the security of signature schemes, as well as the first construction that satisfies it.

However, the underlying signatures of our new scheme, the Schnorr signature and the PSS-Rabin signature, are not deterministic. The signer may generate several signatures corresponding to a given message. We adopt a stronger security model, strong existential unforgeability [23], where the adversary is allowed to ask for signatures of the same message many times, and he would obtain useful information from each new answer. The adversary is required to forge a new signature on a previously signed message or a new message. This model gives the adversary more powers and more chances for success in the following attack game:

Gen: The challenger takes a security parameter 1^k and runs a key-generation algorithm. It gives the adversary the resulting system parameters and a random public key of the signer.
Queries: The adversary A issues queries $q_1, \ldots, q_m$ adaptively:
- Sign query $< M_i >$.
Response: Finally, the adversary outputs a new signature σ for a message M.
The adversary A wins the game if the outputted signature (M, σ) is nontrivial, i.e. it is not an answer of any sign query for the message M.

The probability is over the random bits used by the challenger and the adversary.

Notice that the adversary is allowed to ask for signatures of the same message M_i many times, even of the message M.

3.2 Formal security proof

Theorem: Let the hash function H be random oracle. Then the proposed signature scheme is Strong Existentially UnForgeable against adaptive Chosen Message Attacks (SEUF-CMA) under both the FAC assumption and the DL assumption. Concretely, suppose that there is an adversary A that has advantage ε against the scheme and A runs in step at most t. Suppose that A makes at most q_H queries to the hash functions H, at most q_S queries to the signature oracle. Then there is an algorithm D that has advantage ε' with running step t to solve the FAC problem and the DL problem simultaneously, where

$$t \approx t'/2 - 2q_S C_{exp}(G_{g,p}),$$

$$\varepsilon \leq (4q_H)(2\varepsilon')^{1/3} + 1/n + q_S(q_H + q_S)/p.$$

Here $C_{exp}(G_{g,p})$ denotes the computation step of a long exponentiation in the group $G_{g,p}$.

Proof. Suppose that we are given a DL problem $(p, q, g, y = g^x)$ and a FAC problem $(n = p_1 q_1)$. We also choose a at random. The probability of a satisfying Jacobi symbol $\left(\frac{a}{n}\right) = -1$ is $1/2$.

We use the random oracle model to show the security of the proposed signature scheme. Assume that we are given a SEUF-CMA forger A that $(t, q_H, q_S, \varepsilon)$-breaks the signature scheme. That is, A is a probabilistic polynomial time computer program which is supplied with a long public sequence of random bits, and is allowed to ask a polynomial number of questions to the random oracles H, S. We want to construct a simulator algorithm D, which takes (p, q, g, y, n, a) as input. Algorithm D tries to use A to find the discrete logarithm $log_g y$ and the factoring of the composite n simultaneously.

Algorithm D uses oracle replay technique of Pointcheval and Stern [19] and simulates two runs of the signature scheme to the forger A. Algorithm D answers A's hash function queries H, signature queries S, and tries to translate A's possible forgeries into the solutions to the discrete logarithm $log_g y$ and the factoring of the composite n simultaneously. Algorithm D starts the simulations by providing the same (p, q, g, y, n, a) and the same long sequence of random bits for A. Then Algorithm D answers As queries as follows:

Answering H-oracle queries: If A issues a random oracle query (m_i, r_i) where $1 \leq i \leq q_H$, D looks up the H-list (a query-answer list, where entry consists of $((m_i, r_i), h_i, e_i, c_{1i}, c_{2i})$) to get the corresponding answer.

If there is a tuple $((m_i,r_i),h_i,e_i,c_{1i},c_{2i})$ in the H-list, D answers with h_i. Otherwise D generates e_i from Z_n^* uniformly at random and (c_{1i},c_{2i}) from $\{0,1\}$ uniformly at random, computes $h_i = e_i^2/((-1)^{c_{2i}}a^{c_{1i}}) \pmod n$, answers with h_i, and adds $((m_i,r_i),h_i,e_i,c_{1i},c_{2i})$ to the H-list.

Answering S-oracle queries: If A issues a signature query (m_i) where $1 \le i \le q_S$, D first picks s_i uniformly at random from Z_q^*, e_i from Z_n^* uniformly at random and (c_{1i},c_{2i}) from $\{0,1\}$ uniformly at random, computes $h_i = e_i^2/((-1)^{c_{2i}}a^{c_{1i}}) \pmod n$. Then D computes $r_i = g^{s_i}y^{h_i(\mathrm{mod}q)} \pmod p$ and answers with (s_i,e_i,c_{1i},c_{2i}), and adds $((m_i,r_i),h_i,e_i,c_{1i},c_{2i})$ to the H-list. If there is a tuple $((m_i,r_i),h_i',e_i',c_{1i}',c_{2i}')$ in the H-list with $h_i \ne h_i'$, D aborts and restarts simulation. The probability of this unfortunate coincidence occurring is at most $(q_H+q_S)/p$.

Obviously, the outputs of the simulated oracles are computationally indistinguishable from those in the real attacks.

By assumption, with the probability ε, the forger A returns a new valid message and signature pair (m,s,e,c_1,c_2). If A has not queried $H(m,r)$, the probability

$$Pr\Big\{\tfrac{e^2}{(-1)^{c_2}a^{c_1}} (\mathrm{mod}\ n) = H\big(m, g^s y^{\frac{e^2}{(-1)^{c_2}a^{c_1}}(\mathrm{mod}\ n)(\mathrm{mod}\ q)} (\mathrm{mod}\ p)\big)\Big\} \le 1/n.$$

since $H(m,r)$ is generated randomly.

Hence, with the probability $\varepsilon - 1/n - q_S(q_H+q_S)/p$, the forger A returns a new signature (m,s,e,c_1,c_2) such that

$$\tfrac{e^2}{(-1)^{c_2}a^{c_1}} (\mathrm{mod}\ n) = H\big(m, g^s y^{\frac{e^2}{(-1)^{c_2}a^{c_1}}(\mathrm{mod}\ n)(\mathrm{mod}\ q)} (\mathrm{mod}\ p)\big)$$

and $H(m,r) \in H$-list.

Because A has queried $H(m,r)$, D guesses a fixed index $1 \le k_H \le q_H$ and the query $H(m,r)$ is the k_Hth *H-oracle queries*. Suppose that D makes good guesses by chance, denoted by the event GoodGuess. The probability of the event GoodGuess is

$$Pr[GoodGuess] = 1/q_H.$$

Algorithm D uses two copies of the signature forger A. D gives two copies of the forger A the same system parameters (p,q,g,y,n,a) and same sequence of random bits, and the same random answers to their oracle queries until at the same time they ask for $H(m,r)$. This is the forking point. At this point, D gives two independent random answers $h_1 = (e_1')^2/((-1)^{c_{21}'}a^{c_{11}'}) \pmod n$, and $h_2 = (e_2')^2/((-1)^{c_{22}'}a^{c_{12}'}) \pmod n$ to the hash queries $H(m,r)$ in the two runs. Thus, D obtains two signatures $(m,s_1,e_1,c_{11},c_{21})$ and $(m,s_2,e_2,c_{12},c_{22})$ such that

$$\frac{e_1^2}{(-1)^{c_{21}}a^{c_{11}}} (\mathrm{mod} n) = H\big(m, g^s y^{h_1(\mathrm{mod}q)} (\mathrm{mod} p)\big)$$

and $H(m,r) \in H$-list.

$$\frac{e_2^2}{(-1)^{c_{22}}a^{c_{12}}} (\mathrm{mod} n) = H\big(m, g^s y^{h_2(\mathrm{mod}q)} (\mathrm{mod} p)\big)$$

and $H(m,r) \in H$-list.

Hence, $r = g^{s_1}y^{h_1(\mathrm{mod}q)} = g^{s_2}y^{h_2(\mathrm{mod}q)} \pmod p$
implies $x = (s_1-s_2)/(h_2-h_1) \pmod q$.
Meanwhile, $H(m,r) = e_1^2/((-1)^{c_{21}}a^{c_{11}}) \pmod n$

$$= (e_1')^2/((-1)^{c_{21}'}a^{c_{11}'}) \pmod n$$

implies $(e_1/e_1')^2 = ((-1)^{c_{21}-c_{21}'}a^{c_{11}-c_{11}'}) \pmod n$.

Notice that $(e_1/e_1')^2$ is a quadratic residue of Z_n^*. However, neither (-1) nor (a) is a quadratic residue of Z_n^*. Thus $(e_1/e_1')^2 = 1, -a$ or $(-a)^{-1} \pmod n$. But the probability of $(e_1/e_1')^2 = 1$ is about $1/2$. So is that of $e_2^2 = (e_2')^2 \pmod n$.

The equation $z^2 = \alpha \pmod{p_1q_1}$ has four roots $\beta, \gamma, n-\beta, n-\gamma$, where $\beta \notin \{\gamma, n-\gamma\}$. Hence, $\Pr\{e_1' \notin \{e_1, n-e_1\}\} = \Pr\{e_2' \notin \{e_2, n-e_2\}\} = 1/2$.

If $e_1' \notin \{e_1, n-e_1\}$, $e_1^2 = (e_1')^2 \pmod n$ implies $e_1^2 - (e_1')^2 = (e_1-e_1')(e_1+e_1') = 0 \pmod n$. So $gcd(e_1-e_1', n) = p_1$ or q_1. The probability that D can factor n from either $e_1^2 = (e_1')^2 \pmod n$ or $e_2^2 = (e_2')^2 \pmod n$ is about $1/2$.

Therefore, the probability that D can obtain the solutions to the discrete logarithm $log_g y$ and the factoring of the composite n simultaneously is $\varepsilon'' = (\varepsilon - 1/n - q_S(q_H+q_S)/p)/(2q_H)$.

We use the "splitting lemma" [19] to compute the probability that D works as hoped. Let X be the set of possible sequences of random bits and random function values that take the forger A up to the point where A asks for $H(m,r)$; let Y be the set of possible sequences of random bits and random function values after that. By assumption, for any $x \in X, y \in Y$, the probability that A is supplied the sequences of random bits and random values $(x||y)$, D obtains the solutions of the two hard problems is ε''. By "splitting lemma", there exists a "good" subset $\Omega \in X$ such that

1. $\Pr\{x \in \Omega\} \ge \varepsilon''/2$.
2. Whenever $d \in \Omega, y \in Y$, the probability that A is supplied the sequences of random bits and random values $(d||y)$, D obtains the solutions is at least $\varepsilon''/2$.

Suppose that the sequences of random bits and random function values supplied up to the point in the first simulation are d. Hence for any $y \in Y$, the probability that A is supplied $(d||y)$, D obtains the solutions in the two simulations is $(\varepsilon''/2)^3$.

Additionally, the probability of a satisfying Jacobi symbol $(\frac{a}{n}) = -1$ is $1/2$.

Hence, algorithm D solves the discrete logarithm problem and the factoring problem simultaneously with probability (approximately) at least

$$((\varepsilon - 1/n - q_S(q_H+q_S)/p)/(4q_H))^3/2.$$

The computation steps in one simulation is $t + 2q_S C_{exp}(G_{g,p})$. Hence

$$t \approx 2(t + 2q_S C_{exp}(G_{g,p})),$$

$$\varepsilon' \geq ((\varepsilon - 1/n - q_S(q_H + q_S)/p)/(4q_H))^3,$$

here $C_{exp}(G_{g,p})$ denotes the computation step of a long exponentiation in the group $G_{g,p}$. Q.E.D.

4 Conclusions

We have proposed a signature scheme based on factoring and discrete logarithms. We have showed that if there is a forgery algorithm against this scheme, we can construct an attack algorithm to solve the two hard mathematics problems simultaneously. Because, it is very unlikely that multiple cryptographic problems would simultaneously become easy to be solved, this signature scheme would give more confidence to the users in digital signatures.

Finally, we compare the performance of the proposed with the related scheme as the following table:

	Schnorr scheme	PSS-Rabin signature	trivial scheme	proposed scheme
sign	1E+1H	1E+1H	2E+2H	2E+1H
verify	2E+1H	1H	2E+2H	2E+1H
Signature size	$2\|q\|$	$\|n\|+0.5\|q\|$	$\|n\|+2.5\|q\|$	$\|n\|+\|q\|$

where E denotes exponentiation, H denotes Hash function and $|n|$ denotes the bit size of n.

Compared with the Schnorr signature scheme, the proposed scheme needs only one more multiplication to verify a signature and one more exponentiation to generate a signature.

Compared with the PSS-Rabin signature scheme, the proposed scheme needs only one more exponentiation to generate a signature and to verify a signature respectively. Moreover, the storage requirement of the proposed scheme is the same as that of the PSS-Rabin signature scheme.

Compared with the trivial scheme (one Schnorr signature + one PSS-Rabin signature), the proposed scheme needs one hash function less to generate, as well as verify, a signature. Moreover, the signature size reduces by $1.5|q|$. Hence the proposed signature scheme is efficient.

Because the settings of the Schnorr signature and the PSS-Rabin signature are widely in the existing PKI, the new signature scheme is of more practical interest.

References

[1] W. Diffie, M. E. Hellman, New directions in cryptography, *IEEE Trans.*, **IT-22**, 644-654 (1976).

[2] P. W. Shor, Polynomial-time algorithm for prime factorization and discrete logarithm on quantum computer, *SIAM Journal on Computing*, **26**, 1484-1509 (1997).

[3] L. Harn, Public-Key cryptosystem design based on factoring and discrete logarithms, *IEE Proc. Comput. Digit. Tech.*, **141**, 193-195 (1994).

[4] J. He, T. Kiesler, Enhancing the security of original ElGamals signature scheme, *IEE Proc. Comput. Digit. Tech*, **141**, 249-252 (1994).

[5] N. Y. Lee, T. Hwang, Modified Harn signature scheme based on factoring and discrete logarithms, *IEE Proc. Comput. Digit. Tech.*, **143**, 193-195 (1994).

[6] Zuhua Shao, Signature Schemes Based on Factoring and Discrete Logarithms, *IEE Proc. Comput. Digit. Tech.*, **145**, 33-36 (1998).

[7] Wei-Hua He, Digital signature schemes based on factoring and discrete logarithms, *Electronics Letters*, **37**, 220-222 (2001).

[8] L.-H. Li, S.-F. Tzeng, M.-S. Hwang, Improvement of signature scheme based on factoring and discrete logarithms, *Applied Mathematics and Computation*, **161**, 49-54 (2005).

[9] K. Tu, Comment "Public-Key cryptosystem design based on factoring and discrete logarithms", *IEE Proc. Comput. Digit. Tech.*, **143**, 96 (1996).

[10] N. Y. Lee, The security of Shaos signature schemes based on factoring and discrete logarithms, *IEE Proc. Comput. Digit. Tech.*, **146**, 119-121 (1999).

[11] J. Li, G. Xiao, Remarks on a new signature scheme based on two hard problems, *Electronics Letters*, **34**, 2401 (1998).

[12] Zuhua Shao, Comment on signature schemes based on factoring and discrete logarithms, *Electronics Letters*, **38**, 1518-1519 (2002).

[13] H. Qian, Z. Cao, H. Bao. Cryptanalysis of Li-Tzeng-Hwangs of improved signature scheme based on factoring and discrete logarithms, *Applied Mathematics and Computation*, **166**, 501-505 (2005).

[14] Zuhua Shao, Security of a new digital signature scheme based on factoring and discrete logarithms, *Computer Mathematics*, **82**, 1215-1219 (2005).

[15] C.-S. Laih and W.-C. Kuo, New signature scheme based on factoring and discrete logarithms, *IEICE Transaction on Fundamentals on Cryptography and Information Security*, **E80-A 1**, 46-53 (1997).

[16] E. S. Ismail, N. M. F. Tahat and R. R. Ahmad. A new digital signature schemes based on factoring and discrete logarithms, *Journal of mathematics and statistics*, **4**, 223-226 (2008).

[17] J. Zhang, Q. Geng and S. Gao, Cryptanalysis of a digital signature scheme based on factoring and discrete logarithms, *Journal of computational information systems*, **5**, 1193-1200 (2009).

[18] J. M. Pollard and C. Schnorr, An efficient solution of the congruence $x^2 + ky^2 = m \pmod{n}$, *IEEE Trans.*, **IT-33**, 702-709 (1987).

[19] D. Pointcheval, J. Stern, Security arguments for digital signatures and blind signatures, *Journal of Cryptology*, **13**, 361-396 (2000).

[20] C. P. Schnorr, Efficient signature generation by smart cards, *Journal of Cryptology*, **3**, 161-174 (1991).

[21] M. O. Rabin, Digitalized signatures, *Foundations of Secure Communication*, Academic Press, 155-168 (1978).

[22] S. Goldwasser, S. Micali, R. Rivest, A digital signature scheme secure against adaptive chosen-message attacks, *SIAM Journal on Computing*, **17**, 281-308 (1988).

[23] J. An, Y. Dodis, and T. Rabin, On the security of joint signature and encryption, *Advances in Cryptology - Eurocrypt02*, LNCS 2332, Springer-Verlag, Berlin, 83-107 (2002).

Zuhua Shao received B.S. degree in mathematics and M.S. in algebra from the Northeastern Normal University, Peoples Republic of China in 1976 and 1981 respectively. From 1990 to 2000 he taught computer science as an associated professor in the Hangzhou Institute of Financial Managers, The Industrial and Commerce Bank of China. Then he became a professor at the Zhejiang University of Science and Technology. He was retired in 2011. His current research interests are cryptography and financial data security.

Yipeng Gao is a PhD student in Department of Materials Science and Engineering at The Ohio State University. His primary research interests are in the field of applied mathematics and applied physics including theoretical modeling of structural phase transitions, which includes the crystallographic study of phase transitions through group theory and graph theory. He is also interested in information security and mathematical applications in cryptography.