

Short Paper

Improved Shao's Signature Scheme

H. F. LIN, JENSHIUH LIU AND C. Y. CHEN*

Department of Information Engineering and Computer Science

**Department of Communications*

Feng Chia University

Taichung, 407 Taiwan

In 1998, Shao proposed two digital signature schemes and claimed that the security of which is based on the difficulties of computing both integer factorization and discrete logarithm. However, in 1999, Lee demonstrated that Shao's signature schemes can be broken if the factorization problem can be solved. This paper presents an improvement of Shao's signature schemes and shows that it can resist Lee's attack. This makes our proposed scheme based on two hard problems. Some possible common attacks are considered. We show that the problem of recovering the signer's secret key from his/her public key is equivalent to solve both the discrete logarithm problem and the factorization problem; the problem of forging a valid signature for a message is at least equivalent to solve the discrete logarithm problem or the factorization problem. In addition, our proposed scheme is immune from substitution and homomorphism attacks.

Keywords: digital signature, factorization problem, discrete logarithm problem, double hard problem, quadratic residue

1. INTRODUCTION

The concept of public-key cryptography was invented by Diffie and Hellman [1] in 1976. Since then, several public-key cryptographic algorithms based on single computationally hard problem, such as factorization or discrete logarithm problem, have been proposed [2, 3]. Although, these algorithms appear secure today, it is very likely that a clever cryptanalyst will discover some efficient ways to solve one hard problem in the future. In 1988, McCurley [4] proposed a key distribution system based on double hard problems, *i.e.*, on both integer factorization and discrete logarithm problems. Since then, several cryptographic systems have been proposed that try to base their security on solving two or more hard problems simultaneously in order to enhance the security [5-11].

Laih and Kuo [9] presented two signature schemes that are based on two hard problems. However, their schemes suffer from both large computational complexity and memory requirement for keys. In 1998, Shao [10] proposed two digital signature schemes, the security of which were claimed to be based on the difficulties of computing integer factorization and discrete logarithm problems. Shao's work requires much less time and memory. However, Lee [12] demonstrated that Shao's schemes are not as secure

Received November 18, 2003; revised July 6 & September 19, 2005; accepted October 31, 2005.
Communicated by Tzong-Chen Wu.

as they have been claimed. In fact, Lee showed that if one can solve the factorization problem, one can recover the signer's secret key with a known signature. Accordingly, Shao's schemes are actually depended on a single hard problem. This paper presents an improvement of Shao's signature schemes and shows that our new scheme can resist Lee's attack. Hence, the security of our proposed scheme is based on two hard problems, *i.e.*, both the difficulties of computing integer factorization and discrete logarithm. Security analysis shows that our scheme can resist substitution and homomorphism attacks.

The rest of this paper is organized as follows. In section 2, we briefly review Shao's scheme and give some properties employed in our scheme. We present our improved scheme in section 3. Security analysis of our proposed scheme is given in section 4. Finally, concluding remarks are given in section 5.

2. PRELIMINARIES

Our proposed scheme is based on quadratic residues. In this section, we briefly review Shao's signature scheme. Then, we give some number theory properties related to quadratic residues.

2.1 Review of Shao's Signature Schemes

Shao has proposed two digital signature schemes. Both schemes can be divided into *key generation*, *signature generation* and *signature verification* phases. Shao's first scheme is as follows.

2.1.1 Key generation

Shao's signature scheme requires each entity, who wants to sign messages, to generate the following system parameters:

1. a prime number p , where $p = 4p_1q_1 + 1$, $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$, and p_1, p_2, q_1, q_2 are all large primes;
2. an integer $g \in Z_p^*$ (the multiplicative group of integer modulo p) of order p_1q_1 .

The parameters p, g and product p_1q_1 are published publicly while p_1, q_1, p_2 and q_2 must be kept secretly from all users and they can be discarded once p and g are produced.

Any user A chooses her/his *secret key* x ($1 < x < p_1q_1/2$) and publishes her/his corresponding *public key* $y = g^{x^2+x^2} \pmod{p}$.

2.1.2 Signature generation

The digital signature of a message m is (k, r, s) , which is signed by user A as follows:

1. Randomly chooses an integer t such that $1 < t < p_1q_1/2$.
2. Compute

$$r = g^{t^2+t^2} \pmod{p}.$$

3. Find s and k such that

$$\begin{aligned} xs + x^{-1}r &= mt + kt^{-1} \pmod{p_1q_1}, \\ x^{-1}s + xr &= mt^{-1} + kt \pmod{p_1q_1}. \end{aligned}$$

If k is even, then to choose a new value for t and repeat steps 1, 2 and 3 until k is odd.

2.1.3 Signature verification

The signature (k, r, s) of a message m can be verified by the use of signer's A 's public key y as follows.

1. Compute and check whether the following equation holds

$$y^{(s^2+r^2)} = r^{(m^2+k^2)} g^{A(mk-sr)} \pmod{p}. \quad (1)$$

2. Accept the validity of (k, r, s) if Eq. (1) holds.

Shao claimed that both his schemes were unbreakable if one cannot simultaneously solve both factorization and discrete logarithm problems. However, Lee [12] showed that both Shao's signature schemes are, in fact, based only on the factorization problem.

2.2 Quadratic Residues

Our work is based on quadratic residues.

Definition 1 (Quadratic Residue) If n is a positive integer, we say that the integer a is a *quadratic residue* (denoted by $a \in QR_n$) of n if $\gcd(a, n) = 1$ and the congruence $x^2 \equiv a \pmod{n}$ has a solution. If the congruence $x^2 \equiv a \pmod{n}$ has no solution, we say that a is a *quadratic non-residue* of n (denoted by $a \in QNR_n$).

Propositions 1 to 3 are some basic properties related to residue numbers. Proofs of these can be found in many places (e.g., [13, 14]). Given an integer a and an odd prime p , Proposition 1 enables us to quickly decide if a is a quadratic residue of p or not.

Proposition 1 (Euler's Criterion) Let p be an odd prime and a be any positive integer such that $\gcd(a, p) = 1$. Then

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p}, & \text{if } a \in QR_p \\ -1 \pmod{p}, & \text{if } a \in QNR_p \end{cases}.$$

It is known that not all the numbers are quadratic residues. The following properties lead us to convert any integer into a quadratic residue.

Proposition 2 Let p be an odd prime and a, b be integers.

1. If $a, b \in QR_p$, then $a * b \in QR_p$.
2. If $a, b \in QNR_p$, then $a * b \in QR_p$.

Proposition 2 shows that the product of two quadratic residues is still a quadratic residue. On the other hand, we may convert a quadratic non-residue to a quadratic residue by multiplying a quadratic non-residue. We next focus on square root modulo n , where n is a product of two distinct odd primes p and q . It can be shown that any integer can be classified into one of the following four classes.

Proposition 3 Let p and q be two distinct primes. Any integer falls in exactly one of the following four classes:

1. $Z_{(1,1)} = QR_p \cap QR_q$,
2. $Z_{(1,-1)} = QR_p \cap QNR_q$,
3. $Z_{(-1,1)} = QNR_p \cap QR_q$, and
4. $Z_{(-1,-1)} = QNR_p \cap QNR_q$.

Definition 2 Let p and q be two distinct odd primes and $n = pq$. We say that an integer a is a quadratic residue of $n(QR_n)$ if $a \in Z_{(1,1)}$ and a is a quadratic non-residue of $n(QNR_n)$ if $a \in Z_{(1,-1)} \cup Z_{(-1,1)} \cup Z_{(-1,-1)}$.

The next proposition identifies four special integers, one for each class, which can be used to convert an integer in any of the four classes to a quadratic residue.

Proposition 4 Let p and q be two distinct odd primes and $n = pq$. Let c_1, c_2, c_3 and c_4 be four parameters such that $c_1 \in Z_{(1,1)}$, $c_2 \in Z_{(1,-1)}$, $c_3 \in Z_{(-1,1)}$ and $c_4 \in Z_{(-1,-1)}$. Then, for any integer a , we may choose a proper c_i ($i = 1, 2, 3, 4$) such that $c_i a \in QR_n$. In particular, let $p \equiv 7 \pmod{8}$ and $q \equiv 3 \pmod{8}$. Then, we may choose $c_1 = 1$, $c_2 = 2$, $c_3 = -2$ and $c_4 = -1$.

Proposition 5 Let $n = pq$, where p and q are two distinct odd primes such that $p \equiv 7 \pmod{8}$ and $q \equiv 3 \pmod{8}$. Then, for any integer $a \in QR_n$, the congruence equation

$$x^{2^t} \equiv a \pmod{n}$$

has at least one solution for every $t \geq 1$.

3. AN IMPROVEMENT OF SHAO'S SIGNATURE SCHEMES

We now present our proposed scheme and give some comparison to the Shao's scheme.

3.1 An Improved Scheme

3.1.1 Key generation

Similar to Shao's schemes, each entity is responsible for generating the following

system parameters:

1. a prime number p , where $p = 4p_1q_1 + 1$, $p_1 \equiv 7 \pmod{8}$, $q_1 \equiv 3 \pmod{8}$, $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$, and p_1, p_2, q_1, q_2 are all large primes;
2. an integer $g \in Z_p^*$ of order p_1q_1 .

The parameters p , g and product p_1q_1 are published publicly while p_1, q_1, p_2 and q_2 must be kept secretly from all other users.

Any user A chooses her/his *secret key* x ($1 < x < p_1q_1/2$) and publishes her/his *public key*

$$y = g^{x^2} \pmod{p}.$$

3.1.2 Signature generation

To create a signature for a message m , signer A proceeds as follows:

1. Randomly choose an integers a between 1 and p_1q_1 with $\gcd(a, p_1q_1) = 1$.
2. Choose, by Proposition 4, a proper integer c such that $c \in \{1, 2, -1, -2\}$ and $c(1 - a^2) \in QR_{p_1q_1}$.
3. Compute, according to the method given in [13, 15, 16], an integer b such that $b^2 = c(1 - a^2) \pmod{p_1q_1}$ or equivalently $b^2 + ca^2 = c \pmod{p_1q_1}$.
4. Randomly choose an integer t_1 between 1 and p_1q_1 with $\gcd(t_1, p_1q_1) = 1$ and $t_1^2 ab \neq 1 \pmod{p_1q_1}$. Compute $t = at_1 \pmod{p_1q_1}$.
5. Compute $r = g^{ct^2 + t^2} \pmod{p}$.
6. Find s_1 and k_1 such that

$$a^{-1}t_1^{-1}r + ca^2t_1k_1 = bxm^2 + ca^2xs_1 \pmod{p_1q_1}, \quad (2)$$

$$a^{-1}t_1^{-1}k_1 - t_1r = bxs_1 - xm^2 \pmod{p_1q_1}. \quad (3)$$

7. Let $s_2 = cas_1, k_2 = ak_1$.
8. The signer derives, by Proposition 5, two integers $s, k \in Z_{p_1q_1}^*$ such that $s^4 = s_2^2 \pmod{p_1q_1}$ and $k^4 = k_2^2 \pmod{p_1q_1}$.
9. Let (r, s, k, c) be the signature for the message m .

3.1.3 Signature verification

The validity of a signature (r, s, k, c) for message m can be verified by using signer A 's public key y as follows:

1. Compute and check whether the following equation holds

$$r^{r^2 + ck^4} = y^{cm^4 + s^4} \pmod{p}. \quad (4)$$

2. Accept the validity of (r, s, k, c) if the above equation holds.

The signature verification process, *i.e.*, Eq. (4), is proved by the following theorem.

Theorem 1 If the signer follows the signing protocol, the verifier always accepts the signature.

Proof: Eqs. (2) and (3) can be rewritten as

$$t^{-1}r + ct_k = bxm^2 + axs_2 \pmod{p_1q_1}, \quad (5)$$

$$a^{-1}t^{-1}k_2 - a^{-1}tr = a^{-1}c^{-1}s_2bx - xm^2 \pmod{p_1q_1}. \quad (6)$$

By taking square of Eqs. (5) and (6), respectively, we have

$$t^{-2}r^2 + 2rck_2 + c^2t^2k_2^2 = b^2x^2m^4 + 2abx^2m^2s_2 + a^2x^2s_2^2 \pmod{p_1q_1}, \quad (7)$$

and

$$\begin{aligned} & a^{-2}t^{-2}k_2^2 + a^{-2}t^2r^2 - 2a^{-2}k_2r \\ &= a^{-2}c^{-2}b^2x^2s_2^2 + x^2m^4 - 2a^{-1}c^{-1}x^2s_2bx^2m^2 \pmod{p_1q_1}. \end{aligned} \quad (8)$$

Multiplying Eq. (8) by a factor of ca^2 and adding to Eq. (7), we obtain

$$(t^{-2} + ct^2)(r^2 + ck_2^2) = (b^2 + ca^2)x^2(m^4 + c^{-1}s_2^2) \pmod{p_1q_1}.$$

By definitions of integers s , k and b , we have

$$(t^{-2} + ct^2)(r^2 + ck^4) = cx^2(m^4 + c^{-1}s^4) \pmod{p_1q_1}, \quad (9)$$

which is equivalent to

$$g^{(t^{-2}+ct^2)(r^2+ck^4)} = g^{cx^2(m^4+c^{-1}s^4)} \pmod{p}. \quad (10)$$

By definition of integer r and the public key y , we have

$$r^{r^2+ck^4} = y^{cm^4+s^4} \pmod{p}. \quad \square$$

3.2 Computation Comparison

We next compare computation complexity between our proposed and Shao's second signature schemes. It is known (see *e.g.*, [13]) that modular addition or subtraction takes $O(\log n)$ time; modular multiplication, inverse, or determination if a certain number is quadratic residue takes $O(\log^2 n)$ time; modular exponentiation or square root computation takes $O(\log^3 n)$ time, where n is the modulus of the congruence operations.

Similar to Shao's scheme, our proposed scheme requires one modular exponentiation for computing a signature, and two exponentiations for verifying a signature. Major extra cost in our proposed scheme is five square root computations: one in step 3 and four in step 8. There is, however, some minor extra cost as follows. Two determinations of quadratic residue are required in step 2. Moreover, our scheme needs 13 more multiplications

and one more addition compared to Shao's. These are not significant, since they are of less computation complexity ($O(\log^2 n)$) compared to square root computation ($O(\log^3 n)$).

4. SECURITY ANALYSIS

In this section, we shall examine some possible attacks on our proposed scheme. The following theorem is proved by Shao [10], which will be needed later in our analysis.

Theorem 2 The problem of recovering x from the equation $y = g^{x^2+x^2} \pmod{p}$ or from $y = g^{x^2+d} \pmod{p}$ (where d is a constant) is polynomial equivalent to compute both the factorization of p and the discrete logarithm of $y = g^u \pmod{p}$.

Proof: This is an immediate result from Theorem 2 in [10] and its corollary. \square

We now consider the following different attacks.

4.1 Recover the Secret Key

Attack 1 An attacker attempts to recover the signer's secret key x from his/her public key $y = g^{x^2} \pmod{p}$.

Analysis: By Theorem 2, this task is equivalent to solve the factorization and the discrete logarithm problems, both of which are believed to be intractable.

4.2 Forge a Signature

We consider a general forgery attack, where an attacker attempts to forge a signature without any key information.

Attack 2 An attacker attempts to forge a valid signature (r, s, k, c) for a message m .

Analysis: There are four possible values for parameter c . Without loss of generality, we assume that $c = 1$. An attacker may try to find a set of parameters (r, s, k) that satisfies Eq. (4). We distinguish between the following three cases:

Case 1: The attacker first picks two of them arbitrarily, and then computes the third one;

Case 2: The attacker first picks one of them arbitrarily, and then computes the other two;

Case 3: The attacker computes all three (r, s, k) simultaneously.

Let's consider case 1. Assume that the attacker arbitrarily picks r and k and then solves (computes) s by Eq. (4). He/she has to solve s by the following equation

$$C_1 = y^{s^4+c^2} \pmod{p}, \quad (11)$$

where C_1 and C_2 are some fixed values. Solving s from Eq. (11) by Theorem 2, is equivalent to compute both the factorization (factoring $(p-1)/4$ to obtain p_1, q_1) and the discrete logarithm problems (computing discrete logarithm of y to obtain s^4), which is intractable. Similarly, it can be shown that it is mathematically intractable if the attacker picks both r, s and then tries to compute k from Eq. (4). The task is even more difficult if the attacker picks both s, k and then tries to compute r , since he/she has to solve the following equation

$$C_1 = C_2 r^{r^2} \pmod{p},$$

where C_1 and C_2 are some fixed values. Therefore, it is computationally intractable to pick two parameters arbitrarily then compute the third one.

We now consider case 2 (Pollard-Schnorr Attack [11]). Assume that the attacker arbitrarily picks an integer v , sets $r = y^v \pmod{p}$ and then computes s and k by solving Eq. (4), which becomes

$$(y^v)^{r^2 + ck^4} = y^{cm^4 + s^4} \pmod{p}.$$

This is equivalent to solve s and k in the following equation

$$vr^2 + vck^4 = cm^4 + s^4 \pmod{p_1q_1}. \quad (12)$$

Let $w = s^2 \pmod{p_1q_1}$ and $z = k^2 \pmod{p_1q_1}$, then the Eq. (12) can be written as

$$w^2 - vcz^2 = (vr^2 - cm^4) \pmod{p_1q_1}. \quad (13)$$

Variables w and z in Eq. (13) can be solved efficiently by an algorithm presented by Pollard and Schnorr [16]. To compute s and k , we need to solve both

$$s^2 = w \pmod{p_1q_1}$$

and

$$k^2 = z \pmod{p_1q_1}.$$

Both of above equations are intractable, since the factorization of p is not known. Therefore, it is computational intractable to forge a signature by picking r and then computing s and k . The task is even more difficult if the attacker picks s (respectively k) and then tries to compute r and k (respectively s). In case 3, the attacker has to solve for the three (r, s, k) simultaneously. To our best knowledge, we are not able to find an efficient algorithm to accomplish this.

We then consider that the attacker randomly selects r, s, k and tries to compute (discover) a proper value of c in order to forge a signature of message m . Recall that there are four possible values for parameter c . In the following, we will show that the probability to get a proper value of c by randomly selecting r, s, k is $O(1/p)$, which is equivalent to a random guess. Eq. (4) can be rewritten as

$$r^{r^2} (y^{s^4})^{-1} = [(r^{k^4})^{-1} y^{m^4}]^c \pmod{p}. \tag{14}$$

Let $U_1 = \{A \in Z_p^* \mid A = r^{r^2} (y^{s^4})^{-1} \pmod{p}\}$, where $r, s \in Z_p^*$, $U_2 = \{B \in Z_p^* \mid B = (r^{k^4})^{-1} y^{m^4} \pmod{p} \mid k \in Z_p^*\}$ and $U = \{(A, B) \in Z_p^* \times Z_p^* \mid A \in U_1, B \in U_2\}$, where Z_p^* is the multiplicative group of Z_p . Then, Eq. (14) can be further rewritten as

$$A = B^c \pmod{p}, \tag{15}$$

where $(A, B) \in U$. We now show that the size of set U is no less than $\frac{1}{16}(p-1)^2$. It is known that Z_p^* is a cyclic group of order $p-1 = 4p_1q_1$. Let g be a generator of Z_p^* . Then, both $\{k^4 \in Z_p^* \mid k \in Z_p^*\}$ and $\{s^4 \in Z_p^* \mid s \in Z_p^*\}$ are subgroup of Z_p^* , and they are of order p_1q_1 . This implies that the sizes of sets $\bar{U}_1 = \{(g^{s^2} (y^{s^4})^{-1} \pmod{p}) \mid s \in Z_p^*\}$, $\bar{U}_2 = \{(g^{k^4})^{-1} y^{m^4} \pmod{p} \mid k \in Z_p^*\}$ and $\bar{U} = \{(g^{s^2} (y^{s^4})^{-1} \pmod{p}), (g^{k^4})^{-1} y^{m^4} \pmod{p}\} \in Z_p^* \times Z_p^* \mid s, k \in Z_p^*\}$ are p_1q_1, p_1q_1 and $p_1^2q_1^2$, respectively. Since U_1, U_2 and U contains \bar{U}_1, \bar{U}_2 and \bar{U} , respectively, we have $|U_1| \geq p_1q_1, |U_2| \geq p_1q_1$ and

$$|U| \geq p_1^2q_1^2 = \frac{1}{16}(p-1)^2. \tag{16}$$

Let $E = \{(A, B) \mid A = B^c, (A, B) \in U, c \in \{1, 2, -1, -2\}\}$. It is known that

$$E \subseteq \{(B, B) \mid B \in U_2, c = 1\} \cup \{(B^2, B) \mid B \in U_2, c = 2\} \cup \{(B^{-1}, B) \mid B \in U_2, c = -1\} \cup \{(B^{-2}, B) \mid B \in U_2, c = -2\}.$$

Since $|U_2|$ is less than $4p_1q_1$, we obtain that

$$|E| \leq 16p_1q_1 = 4(p-1). \tag{17}$$

The upper bound of the probability to get a proper value of c by randomly selecting r, s, k is $|E|/|U|$. Therefore, by Eqs. (16) and (17), we have the probability to get a proper value of c by randomly selecting r, s, k is less than $64/(p-1)$, which is $O(1/p)$.

4.3 Substitution Attack

With a valid signature for a message, an attacker may try a substitution attack to forge a signature for another message. In the following, we first show that Shao's signature schemes are subject to ElGamal's substitution attack [2]. Then, we consider the substitution attack on our improved scheme.

Given a valid signature (r, s, k) for a message m , then the verification equation can be rewritten [10] as:

$$g^{(x^2+x^{-2})(s^2+r^2)} = g^{(t^2+t^{-2})(m^2+k^2)} g^{4(mk-sr)} \pmod{p}. \tag{18}$$

Define integers $u = m^2 + k^2$, $v = a^2 - (s^2 + r^2)$, and $w = 4(mk - sr)$, where $a^2 = 1$ (all calculations mod p_1q_1). Set

$$\begin{aligned} r' &= r^u y^v g^w \pmod{p}, \\ s' &= am' \pmod{p_1 q_1}, \\ k' &= a^{-1} r' \pmod{p_1 q_1}. \end{aligned}$$

We claim that (r', s', k') signs an arbitrary message m' . To see this, we calculate the left hand side of Eq. (1):

$$\begin{aligned} y^{(s'^2+r'^2)} &= g^{(x^2+x^{-2})(s'^2+r'^2)} \pmod{p} \\ &= g^{a^2(x^2+x^{-2})(m'^2+k'^2)} \pmod{p} \\ &= g^{(x^2+x^{-2})(m'^2+k'^2)} \pmod{p}. \end{aligned} \tag{19}$$

The right hand side of Eq. (1) is calculated as follows

$$\begin{aligned} r'^{(m'^2+k'^2)} g^{4(m'k'-s'r')} \\ &= g^{[(t^2+t^{-2})u+(x^2+x^{-2})v+w](m'^2+k'^2)} g^{4(m'k'-s'r')} \pmod{p} \\ &= g^{[(t^2+t^{-2})(m'^2+k'^2)+(x^2+x^{-2})(a^2-(s^2+r^2))+4(mk-sr)](m'^2+k'^2)} g^{4(m'k'-s'r')} \pmod{p}. \end{aligned}$$

With Eq. (18), the right hand side can be rewritten as

$$\begin{aligned} r'^{(m'^2+k'^2)} g^{4(m'k'-s'r')} &= g^{a^2(x^2+x^{-2})(m'^2+k'^2)} g^{4m'k'(a^2-1)} \pmod{p} \\ &= g^{(x^2+x^{-2})(m'^2+k'^2)} \pmod{p}. \end{aligned} \tag{20}$$

Therefore, by Eqs. (19) and (20), we have proved that m' and (r', s', k') satisfies Eq. (1), *i.e.*, (r', s', k') is a valid signature for an arbitrary message m' .

Similarly, it can be shown that Shao's second scheme is also subject to Substitution attack. We now consider substitution attack on our improved scheme.

Attack 3 (ElGamal's Substitution Attack) Given a valid signature (r, s, k, c) of a message m , the attacker tries to generate another valid signature (r', s', k', c') for another message m' without knowing the secret key x .

Analysis: There are four possible values for parameter c' . Without loss of generality, we assume that $c' = 1$. Eq. (10) for signature verification becomes

$$g^{(t^2+t^{-2})(r'^2+k'^4)} = g^{x^2(m^4+s^4)} \pmod{p}. \tag{21}$$

To make a substitution attack, the attacker sets

$$r' = r^u y^v g^w \pmod{p}.$$

Then, the left hand side of the verification equation (Eq. (4)) becomes

$$r'^{(r'^2+k'^4)} = g^{[(t^2+t^{-2})u+x^2v+w](r'^2+k'^4)} \pmod{p}. \tag{22}$$

To eliminate the private key x in the above equation, the attacker further chooses

$$\begin{aligned} u &= r^2 + k^4, \\ v &= a - (m^4 + s^4), \text{ and} \\ w &= 0, \end{aligned}$$

where a is an arbitrary integer and all calculations mod p_1q_1 . With the known signature for message m (Eq. (21)), Eq. (22) can be rewritten as

$$\begin{aligned} r^{a(r^2+k^4)} &= g^{x^2a(r^2+k^4)} \pmod{p} \\ &= y^{a(r^2+k^4)} \pmod{p}. \end{aligned}$$

To make (r', s', k', c') be an valid signature for message m' , the attacker must solve s' and k' for the verification equation (Eq. (4)), which now becomes

$$y^{a(r'^2+k'^4)} = y^{m'^4+s'^4} \pmod{p}. \quad (23)$$

To our best knowledge, we are not able to find an efficient algorithm to accomplish this.

4.4 Homomorphism Attack

Attack 4 (Homomorphism Attack [7]) Suppose that an attacker has three signatures (r_1, s_1, k_1, c_1) , (r_2, s_2, k_2, c_2) and (r_3, s_3, k_3, c_3) for messages m_1, m_2 and m_3 , respectively, such that $r_3 = r_1r_2 \pmod{p}$. The attacker tries to use the three signatures to recover the signer's secret key x .

Analysis: Recall that $r = g^{ct^2+t^2} \pmod{p}$. Since $r_3 = r_1r_2 \pmod{p}$, we have

$$c_3t_3^2 + t_3^{-2} = c_1t_1^2 + t_1^{-2} + c_2t_2^2 + t_2^{-2} \pmod{p_1q_1}.$$

By Eq. (9), the three signatures satisfy

$$(t_1^{-2} + c_1t_1^2)(r_1^2 + c_1k_1^4) = x^2(c_1m_1^4 + s_1^4) \pmod{p_1q_1}, \quad (24)$$

$$(t_2^{-2} + c_2t_2^2)(r_2^2 + c_2k_2^4) = x^2(c_2m_2^4 + s_2^4) \pmod{p_1q_1}, \quad (25)$$

$$(t_3^{-2} + c_3t_3^2)(r_3^2 + c_3k_3^4) = x^2(c_3m_3^4 + s_3^4) \pmod{p_1q_1}. \quad (26)$$

By adding Eq. (24) $\times (r_2^2 + c_2k_2^4)(r_3^2 + c_3k_3^4)$ with Eq. (25) $\times (r_3^2 + c_3k_3^4)(r_1^2 + c_1k_1^4)$ and then subtracting Eq. (26) $\times (r_1^2 + c_1k_1^4)(r_2^2 + c_2k_2^4)$, what the attacker can obtain is that

$$0 = 0 \cdot x^2 \pmod{p_1q_1}.$$

Hence, the attacker cannot recover the secret key x from three known signatures (r_1, s_1, k_1, c_1) , (r_2, s_2, k_2, c_2) and (r_3, s_3, k_3, c_3) such that $r_3 = r_1 r_2 \pmod{p}$.

4.5 Lee's Attack

Attack 5 Given a valid signature (r, s, k, c) of a message m , an attacker can recover the signer's secret key if he/she can only solve the factorization problem.

Analysis: Suppose a signature (r, s, k, c) of a message m is known to the attacker. There are at least three unknowns a , t and x in Eqs. (5) and (6). However, the attacker can eliminate at most one unknown by applying Lee's attack. Hence, the attacker cannot recover signer's secret key x .

5. CONCLUSIONS

In this paper, we present an improvement of Shao's signature schemes and show that our new scheme can resist Lee's attack. Therefore, the security of our proposed scheme is based on the difficulties of computing integer factorization and discrete logarithm. We have demonstrated that our proposed scheme can resist the following attacks: (1) the task for an attacker to try to recover the signer's secret key from his public key is equivalent to solve both the discrete logarithm problem and the factorization problem; (2) the task of forging a valid signature for a message is at least equivalent to solve the discrete logarithm problem or the factorization problem; (3) the proposed scheme can resist substitution attack if the factorization problem is unsolvable; and (4) the proposed scheme is immune from homomorphism attacks. One disadvantage of our proposed scheme is that our signature needs some more computational effort and one more integer field compared to Shao's.

REFERENCES

1. W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, 1976, pp. 644-654.
2. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, Vol. IT-31, 1985, pp. 469-472.
3. R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Vol. 21, 1978, pp. 120-126.
4. K. McCurley, "A key distribution system equivalent to factoring," *Journal of Cryptology*, Vol. 1, 1988, pp. 95-106.
5. E. F. Brickell and K. S. McCurley, "An interactive identification scheme based on discrete logarithms and factoring," *Journal of Cryptology*, Vol. 5, 1992, pp. 29-39.
6. L. Harn, "Public-key cryptosystems design based on factoring and discrete logarithms," *IEE Proceedings of Computer Digital Techniques*, Vol. 141, 1994, pp. 193-195.

7. J. He and T. Kiesler, "Enhancing the security of Elgamal's signature scheme," in *IEE Proceedings of Digital Techniques*, Vol. 141, 1994, pp. 249-252.
8. N. Lee and T. Hwang, "Modified Harn signature scheme based on factorizing and discrete logarithms," in *IEE Proceedings of Computer Digital Techniques*, Vol. 143, 1996, pp. 196-198.
9. C. Laih and W. C. Kuo, "New signature schemes based on factoring and discrete logarithms," *IEICE Transactions on Fundamentals*, Vol. E80-A, 1997, pp. 46-53.
10. Z. Shao, "Signature schemes based on factoring and discrete logarithms," in *IEE Proceedings on Digital Techniques*, Vol. 149, 1998, pp. 33-36.
11. S. Y. Chiou, "The design and analysis of digital signatures based on factoring and discrete logarithm problems," Ph.D. Thesis, Dept. of Electrical Engineering, National Cheng Kung University, Taiwan, 2004.
12. N. Lee, "Security of Shao's signature schemes based on factoring and discrete logarithms," in *IEE Proceedings on Computer Digital Techniques*, Vol. 146, 1999, pp. 119-121.
13. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press series on discrete mathematics and its applications, CRC Press, 1997.
14. K. H. Rosen, *Elementary Number Theory and its Applications*, 4th ed., Addison Wesley, 1999.
15. R. Peralta, "A simple and fast probabilistic algorithm for computing square roots modulo a prime number," *IEEE Transactions on Information Theory*, Vol. 32, 1986, pp. 846-847.
16. J. M. Pollard and C. P. Schnorr, "An efficient solution of the congruence $x^2 + ky^2 = m \pmod{n}$," *IEEE Transactions on Information Theory*, Vol. 33, 1987, pp. 702-709.

H. F. Lin (林秀峰) was born in Taipei, Taiwan. He received his B.S. degree in Mathematics from Fu Jen Catholic University in 1970 and M.S. degree in Mathematics from the National Tsing Hua University in 1974. Currently, he is an Associate Professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His major areas of interest are computer cryptography, computer arithmetic, and algorithms.

Jenshiuh Liu (劉振緒) received his B.S. and M.S. degrees in Nuclear Engineering from National Tsing Hua University, also M.S. and Ph.D. degrees in Computer Science from Michigan State University in 1979, 1981, 1987 and 1992, respectively. Since 1992, he has been an Associate Professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taiwan. His research interests include parallel and distributed processing, computer system security, and computer algorithms.

C. Y. Chen (陳志澂) was born in Taiwan in 1951. He received the B.S. degree and the M.S. degree in Mathematics from Tamkang University in 1974 and National Central University in 1976, respectively, and the Ph.D. degree in Computer Sciences from Na-

tional Tsing Hua University in 1995. He is currently a Professor in the Department of Communications, Feng Chia University, Taichung, Taiwan. His main research interests include database design, algorithm design and analysis, coding theory, and computer cryptography.