International Journal of Security and Its Applications
Vol. 10, No. 3 (2016), pp.295-310
http://dx.doi.org/10.14257/ijsia.2016.10.3.26

Novel Digital Signature Schemes based on Factoring and Discrete Logarithms

Shin-Yan Chiou

Chang Gung University
ansel@mail.cgu.edu.tw

Abstract

In the paper, we propose a new digital signature scheme based on factoring and discrete logarithms. Specially, we prove that the security of the proposed signature scheme is based on both the security of the ElGamal signature scheme and the security of the modified OSS signature scheme. This is the first scheme which can be proved that its security is based on two hard problems. Like Meta-ElGamal signature schemes, the proposed signature scheme can be extended to many kinds of scheme. The corresponding computations for our proposed scheme are also discussed.

Keywords: *Digital Signature, ElGamal scheme, OSS scheme*

1. Introduction

A digital signature scheme is a protocol by which a signer can sign a signature for an electronic document by using his/her private key and a verifier can verify the signature of the electronic document by using the signer's public key. In 1976, Diffie and Hellman [3] proposed the concept of the digital signature. After that, Rivest [27], Rabin [26], Ong [24], ElGamal [5] and Schnorr [28] et al. proposed different kinds of digital signature schemes. The security of their digital signature schemes are based on either discrete logarithm problem or factoring problem.

The earliest digital signature scheme based on discrete logarithm is proposed by ElGamal [5]. Afterward, many signature schemes based on discrete logarithm such as the Schnorr Signature Scheme [28] and the Digital Signature Algorithm (DSA) [21] were then proposed. Many different schemes based on the ElGamal scheme are also appeared. In 1994, Horster et al. [10] integrated all these approaches in a Mega-ElGamal signature scheme. They classified the entire ElGamal-like signature schemes into seven generalizations. At the same time, He and Kiesler [9] proposed two digital signature schemes and one of them is based on discrete logarithm problem. In many countries, the security of the digital signatures in their standards including DSA [22], GOST 34.10 [19] and KCDSA [17] are based on discrete logarithm problem.

On the other hand, the earliest digital signature scheme based on factorization problem is proposed by three professors Rivest, Shamir and Adleman [27]. Afterward in 1979, Rabin proposed another signature scheme based on factorization problem [26]. In 1984, Ong, Schnorr and Shamir proposed an efficient digital signature scheme [24]. However in 1987, Pollard and Schnorr [25] indicated that their scheme is insecure. In 1994, Naccache [20] proposed a modified scheme to improve the original OSS scheme.

Up to now, the factoring problem and the discrete logarithm problem are still the security basis of many cryptographies and digital signature systems. Many countries in the world are doing their researches and writing programs to solve the problem of factoring and discrete logarithm. As we know for the factoring problem, we can factor 155 digits [2], while for the discrete logarithm problem we can solve 87 digits [23].

Therefore, the digital signature schemes based on discrete logarithm problem will become insecure if one day the discrete logarithm problem can be solved by a developed

ISSN: 1738-9976 IJSIA

efficient algorithm. On the other hand, the digital signature schemes based on factoring problem will become insecure if the factoring problem can be efficiently broken. Assume there is a scheme of which the security is based on both discrete logarithm problem and factoring problem. The scheme will be still secure if any one of the discrete logarithm problem and the factoring problem is solved. Basically, we have no idea that which problem will be firstly broken. Thus, considering the best security, we should use the digital signature whose security is based on two hard problems.

In 1988, McCurley [18] developed the first key distribution system based on both the discrete logarithm problem and the factoring problem. Instead of using a modulus number which is a large prime and used in [3], he used a modulus n which is the product of two large primes p and q. He adopted the ElGamal cryptosystem to achieve the same security level. As a result, we have to solve two problems if we want to break the system. One is the factoring problem to factor n into p and q. The other is the discrete logarithm problem in the subgroups of Zp* and Zq*. However, there are two disadvantages in the McCurley scheme. One is that the public-key size is much larger. The other is that the computing time is much longer.

In 1992, Brickell and MeCurley [1] constructed an interactive identification scheme in which the security is based on both discrete logarithm problem and factorization problem. Like the Schnorr identification scheme [28], they use a prime modulus p. Instead of only one large prime factor, p – 1 has two large prime factors p' and q'.

In 1994, Harn [6] proposed a digital signature scheme of which the security is based on both discrete logarithm problem and factorization problem. His algorithm combines the RSA [27] and ElGamal [5] signature schemes. Unfortunately in 1996, Lee and Hwang [15] indicated that there is a drawback on the security of Harn’s scheme. If the discrete logarithm problem can be broken, anybody can forge the signature for any chosen message. They also proposed an algorithm to improve Harn’s scheme.

At the same year in 1994, He and Kiesler [9] also proposed a digital signature scheme of which the security is based on both discrete logarithm problem and factorization problem. Their system constructs the basic structure of ElGamal digital signature scheme upon the exponential part. It increases one more hard problem, factorization problem, from the ElGamal signature scheme of which the security is based on discrete logarithm problem. This system then becomes two-hard-problem-based system. However in 1995, Lee and Hwang [14] indicated that their security is based on only discrete logarithm problem. If the discrete logarithm problem can be broken, an attacker can obtain the secret key of the system. At the same time, Harn [7] also indicated that their system is insecure and their security is based on only factorization problem. Similarly if the factorization problem can be broken, an attacker can obtain the secret key of the system. Even in 1996, Laih and Kuo [11] indicated that their system can be broken without solving either factorization problem or discrete logarithm problem.

In 1997, Laih and Kuo [12] proposed a new digital signature scheme based on two hard problems. Their scheme is still secure till now. However, the drawback is that their system is too complicated. Not only the public/private-key size is too large but also the computing time is too long.

In 1998, Shao [29] proposed two digital signature schemes based on the discrete logarithm and factorization problems. Specially, he used two equations to evaluate two parameters of the signature. The relationship between the public key and the private is also special. However in 1999, Lee [13] indicated that both schemes are insecure. The secret key can be evaluated under that situation that the factorization problem can be broken. Li and Xiao [16] also showed that the two schemes are insecure. If one valid signature is known, one can forge a valid signature of a randomly chosen message.

In 2001, He [8] proposed a digital signature scheme based on the discrete logarithm problem and the factorization problem. However, Sun [29] indicated that the scheme is based on only discrete logarithm problem. If the discrete logarithm problem can be solved and one valid signature is known, we can then forge a signature for any chosen message by using the known signature. At the same time, Ding and Laih [4] also mentioned that He's scheme is insecure if the discrete logarithm problem can be solved. They used another algorithm that can also forge a signature for a chosen message with one known signature to break He's scheme.

In the paper, we propose a new digital signature scheme based on factoring and discrete logarithms. Specially, we can prove that the security of the proposed signature scheme is based on both the security of the ElGamal signature scheme and the security of the modified OSS signature scheme [20]. Like Meta-ElGamal signature schemes [10], the proposed signature scheme can be extended to many kinds of schemes. The corresponding computations for our proposed scheme are also discussed.

2. The ElGamal and the Modified OSS Digital Signature Schemes

Since the security of our schemes is on the basis of ElGamal digital signature scheme and the modified OSS signature scheme, we introduce these two schemes in this section. Notice that each digital signature scheme has its name, such as The ElGamal Signature Scheme, and three phases that are Parameters and Key Generation phase, Signature Generation phase and Signature Verification phase. The Parameters and Key Generation phase is for the system or the signer. The Signature Generation phase is for the signer, and the Signature Verification phase is for the verifier. In the parameters and key generation phase, the private key is chosen by the signer and the public key is computed from the private key. In the signature generation phase, the signer uses her/his private key at least once to sign the signature for the message. In the signature verification phase, there is at least one congruence equation to check whether the signature for the corresponding message is valid or not.

2.1 ElGamal Digital Signature Scheme

In 1985, ElGamal [5] proposed a well-known digital signature scheme based on discrete logarithm problem. The detailed scheme is described as follows.

Algorithm 1. The ElGamal Signature Scheme

1. Parameters and Key Generation Phase
   (1) A signer or a system firstly chooses a large prime p and a number g such that g is a primitive element of $GF(p)$. Then she or he publishes the two numbers p and g.
   (2) Signer's Keys
      (A) Private Keys: $x \in Z_p^*$
      (B) Public Keys: $y \equiv g^x \bmod p$
2. Signature Generation Phase
   Assume m is the message to be signed.
   (1) The signer chooses a random integer k with $\gcd(k, p - 1) = 1$.
   (2) Compute $r \equiv g^k \bmod p$.
   (3) Compute s such that $m \equiv xr + ks \bmod p - 1$ (or $s \equiv k^{-1}(m - xr) \bmod p - 1$).
   Then, (r, s) is the signature for the message m signed by the signer.
3. Signature Verification Phase
   Anyone can verify whether (r, s) is a valid signature of the message m by checking the congruence
   $$g^m \equiv y^r \cdot r^s \bmod p.$$
   If it holds, (r, s) is a valid signature of the message m.
   Notice that
   $$g^m \equiv g^{xr+ks} \equiv g^{xr} \cdot g^{ks} \equiv (g^x)^r \cdot (g^k)^s \equiv y^r \cdot r^s \bmod p.$$

The ElGamal signature scheme is claimed that its security is based on the discrete logarithm problem. If the discrete logarithm problem can be solved, the ElGamal signature scheme is then broken. However, it is just believed that the security is based on the discrete logarithm problem. We can just describe that it seems to be secure if the discrete logarithm problem cannot be broken. We cannot prove that it is really based on the discrete logarithm problem. If we can prove that "if the ElGamal signature scheme can be broken, the discrete logarithm problem can then be solved", we can completely prove that the security of the ElGamal signature scheme is based on the discrete logarithm problem. However, the ElGamal signature scheme is well known and used for many years. Thus, we can trust it.

2.2 The Modified OSS Signature Scheme

In 1984, Ong, Schnorr and Shamir proposed an efficient digital signature scheme [24]. The scheme is called "OSS digital signature scheme." They used the congruence $x^2 + ky^2 \equiv m \bmod n$ to evaluate the signature (x, y) for the message m, where k is the public key and n is a product of two large prime numbers p and q. It was claimed that its security is based on factoring problem. If we can factor n into p and q, their scheme can then be broken. Unfortunately, the original OSS was proven to be insecure by Pollard and Schnorr [25]. They used a recursive algorithm to evaluate the values x and y for a message m.

In 1994, Naccache [20] proposed a modified scheme to improve the original OSS scheme. He used $k(x)$ to substitute the value k, where $k(x)$ is a non-polynomial function of x. Thus, the checking congruence of the verification phase becomes $x^2 + k(x)y^2 \equiv m \bmod n$. His scheme is secure under the Pollard-Schnorr attack. In general, we believe that the security of the modified scheme is based on factoring problem. The detailed algorithm of the modified scheme is described as follows.

Algorithm 2. The Modified OSS Signature Scheme

1. Parameters and Key Generation Phase
   (1) A signer firstly chooses two large primes p and q. She or he then computes $n = pq$ and publishes the value n.
   (2) Let f be a one way hash function with c-bits length output.
   (3) Signer's Keys:
      (A) Private Keys: $u_1, u_2, \dots, u_c \in Z_n$.
      (B) Public Keys: $k_1, k_2, \dots, k_c$, such that $k_i u_i^2 \equiv 1 \bmod n$, $i = 1, 2, \dots, c$.
2. Signature Generation Phase
   Assume m is the message to be signed.
   (1) The signer randomly chooses integers $r_1, r_2, \dots, r_t$ with $\gcd(r_i, n) = 1$, $i = 1, 2, \dots, t$.
   (2) Compute $x_i \equiv (r_i + \frac{m}{r_i}) \bmod n$, $i = 1, 2, \dots, t$.
   (3) Calculate $\{e_i\}$ $(= (e_{i1}, e_{i2}, \dots, e_{ic})) = f(x_i)$, where $\in \{0, 1\}$, $i = 1, 2, \dots, t$.
   (4) Compute $y_i \equiv (\prod_{e_{ij}=1} u_j)(r_i - \frac{m}{r_i}) \bmod n$, $i = 1, 2, \dots, t$.
   Then, $(\{x\}, \{y\})$ is the signature of the message m.
3. Signature Verification Phase
   Anyone can verify whether $(\{x\}, \{y\})$ is a valid signature of the message m by the following steps.
   (1) Evaluate $\{e_i\}$ $(= (e_{i1}, e_{i2}, \dots, e_{ic})) = f(x_i)$, $i = 1, 2, \dots, t$.

(2) Check whether all the t equations

$$x_i^{\,2} - (\prod_{e_{ij}=1} k_j) y_i^{\,2} \equiv 4m \bmod n,\ i = 1, 2, \ldots, t$$

hold. If they hold, ({x}, {y}) is a valid signature of the message m.
Notice that

$$\begin{aligned} x_i^{\,2} - (\prod_{e_{ij}=1} k_j) y_i^{\,2} &\equiv (r_i + \frac{m}{r_i})^2 - (\prod_{e_{ij}=1} k_j)(\prod_{e_{ij}=1} u_j)^2 (r_i - \frac{m}{r_i})^2 \bmod n \\ &\equiv (r_i + \frac{m}{r_i})^2 - (\prod_{e_{ij}=1} k_j u_j^{\,2})(r_i - \frac{m}{r_i})^2 \bmod n \\ &\equiv (r_i + \frac{m}{r_i})^2 - (r_i - \frac{m}{r_i})^2 \bmod n \equiv 4m \bmod n. \end{aligned}$$

3. The Proposed Scheme

In this session, we propose a digital signature scheme of which the security is based on two assumptions. The difference, compared with other schemes, is that the security of the proposed scheme can be proved. Moreover, we will also extend our scheme to many different digital signature schemes.

In section 3.1, we will introduce our first scheme, basic scheme, and prove that it is based on both the discrete logarithm problem and the factorization problem. In section 3.2, we show the extended schemes that are extended from our basic scheme. In section 3.3, we will have a discussion on the security of the basic and extended schemes.

3.1 Basic Scheme

As we described, the basic scheme is our first scheme. It is also the “normal-mode” scheme. Truly speaking, we cannot directly show that our proposed scheme is based on both the discrete logarithm problem and the factorization problem. However, we can prove that the security of the basic scheme is based on both the security of the ElGamal signature scheme and the security of the modified OSS signature scheme.

We know that the security of the ElGamal digital signature scheme is believed being based on the discrete logarithm problem and the security of the modified OSS signature is believed being based on the factorization problem. For many years, they are still secure and well used. Many experts have been trying to break them but unfortunately they are fail. Thus we can believe that both the ElGamal digital signature scheme and the modified OSS scheme are secure. Therefore, we can believe that our basic scheme is secure and its security is based on two hard problems.

Algorithm 3. The Basic Scheme

1. Parameters and Key Generation Phase
   (1) Let p be a large prime such that $p = 4\rho p_1 q_1 + 1$, where ρ is a randomly chosen number, $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$ and p_1, p_2, q_1, q_2 are distinguished large primes.
   (2) Let $n = p_1 q_1$ and $g \in Z_p^{\,*}$ such that $g^n \equiv 1 \bmod p$, $g^{p_1} \neq 1 \bmod p$ and $g^{q_1} \neq 1 \bmod p$.
   (3) Randomly choose a value x such that $1 < x < n$ and $\gcd(x, p - 1) = 1$.
   (4) Compute $y \equiv g^{x^2} \bmod p$.
   (5) Signer’s Keys:
   (A) Private Keys: x, p_1, q_1.

(B) Public Keys: y, p.

2. Signature Generation Phase

Assume $m \in Z_n^*$ is the message to be signed.

(1) The signer randomly chooses an integer k such that $1 < k < n$ and $\gcd(k, n) = 1$.

(2) Compute $r \equiv g^k \bmod p$.

(3) Find s' such that

$$m^2 \equiv x^2r^2 + ks' \bmod n. \qquad (1)$$

(4) If $s' \in QR_n$, evaluate s that such $s^2 \equiv s' \bmod n$.

(5) If $s' \in QNR_n$, go to step 1.

Then, (r, s) is the signature of the message m.

3. Signature Verification Phase

To verify that (r, s) is a valid signature of message m, one can simply check the following congruence.

$$g^{m^2} \equiv y^{r^2} r^{s^2} \bmod p\,.$$

If it holds, (r, s) is a valid signature of the message m.

Note: From Eq. (1), we know that $m^2 \equiv x^2r^2 + ks^2 \bmod n$. Therefore, the verification congruence is

$$g^{m^2} \equiv y^{r^2} r^{s^2} \bmod p\,.$$

As to the bit length of the designed parameters, we recommend that $|p| = 1024$, $|\rho| = 1\sim 32$ and $|n| = 990 \sim 1022$, where $|i|$ denotes the bit length of i.

In the signature generation phase, the evaluated s' in Eq. (1) must be QR_n so that we can compute its root s to be one parameter of the signature. If the evaluated s' is not QR_n, we have to choose another integer k. It takes time to determine whether s' is QR_n and evaluate its root s if s' is QR_n. To solve these problems, we will especially give a discussion in section 4.

As we described, the security of our basic scheme is based on both the ElGamal digital signature scheme and the modified OSS scheme. If one day the discrete logarithm problem is broken, our basic scheme can be transformed into the modified OSS scheme of which the security is based on factorization problem. On the other hand, if one day the factorization problem is broken, our basic scheme can be mapped into the ElGamal digital signature scheme of which the security is based on discrete logarithm problem. In the following two lemmas, we show that our basic scheme is based on both the ElGamal digital signature scheme and the modified OSS scheme.

Lemma 1. If the discrete logarithm problem can be solved, the security of the basic scheme is equivalent to the security of the modified OSS scheme.

Proof.

(1) Assume the discrete logarithm problem can be solved. We can then get the value x^2 from the public key $y \equiv g^{x^2} \bmod p$. (Note that we can get the value b from $a = g^b \bmod p$ if a is known and the discrete logarithm problem can be solved.)

(2) Let f be a function to solve discrete logarithm problem (i.e. $a = g^{f(a)} \bmod p$). Thus, $x^2 = f(y)$ and $k = f(r)$.

(3) From Eq. (1), we know that

$$m^2 \equiv x^2r^2 + ks' \bmod n.$$

Since $s' = s^2$, we can rewrite the equation as

$$x^2r^2 + ks^2 = m^2 \bmod n.$$

By using the function f, we can get k from $f(r)$ and it becomes

$$x^2r^2 + f(r)s^2 = m^2 \bmod n.$$

From dividing by x^2, we can get

$$r^2 + (f(r)/x^2)s^2 = m^2/x^2 \bmod n.$$

Let $m' = m^2/x^2$ and g be a function such that $g(r) = f(r)/x^2$. The equation then becomes

$$r^2 + g(r)s^2 = m' \bmod n,$$

where (r, s) is the signature of the message m and m' can be obtained by m if the discrete logarithm problem can be solved. Therefore, the security of the basic scheme is equivalent to the security of the modified OSS scheme if the discrete logarithm problem can be solved. (Note that in the modified OSS scheme, the verification function is $x^2 + k(x)y^2 = m \bmod n$, where (x, y) is the signature of the message m.) □

Lemma 2. If the factorization problem can be solved, the security of the basic scheme is equivalent to the security of the ElGamal digital signature scheme.*Proof.*

(1) Assume the factorization problem can be solved. We can then get the value p_1, q_1, p_2, q_2 from $n = p_1q_1$ and $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$, where $n = (p - 1)/4\rho$. (Note that we can obtain the value b from $b^2 = a \bmod n$ if $a \in QR_n$ is known and the factorization problem can be solved.)

(2) Let $X = x^2 \bmod n$, $M = m^2 \bmod n$, $R = r^2 \bmod n$ and $R' = r^2$. (Note that $|R'| = 2|r|$, where $|R'|$ and $|r|$ represent the bit length of R and r.) Thus we rewrite our basic scheme as follows.

Algorithm. The Basic Scheme (Rewritten)

1. Parameters and Key Generation Phase

   (1) Let p be a large prime such that $p = 4\rho p_1q_1 + 1$, where ρ is a randomly chosen number, $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$ and p_1, p_2, q_1, q_2 are distinguished large primes.

   (2) Let $n = p_1q_1$ and $g \in Z_p^*$ such that $g^n \equiv 1 \bmod p$, $g^{p_1} \neq 1 \bmod p$ and $g^{q_1} \neq 1 \bmod p$.

   (3) Randomly choose a value X such that $1 < X < n$ and $\gcd(X, p - 1) = 1$.

   (4) Compute $y \equiv g^X \bmod p$. (Note: $y \equiv g^{x^2} \bmod p$)

   (5) Signer's Keys:
   (A) Private Keys: X.
   (B) Public Keys: y, p.

2. Signature Generation Phase

   Assume $m \in Z_n^*$ is the message to be signed.

   (1) The signer randomly chooses an integer k such that $1 < k < n$ and $\gcd(k, n) = 1$.

   (2) Compute $r \equiv g^k \bmod p$.

   (3) Find s' such that

   $$M \equiv XR + ks' \bmod p - 1. \qquad (2)$$

   (4) If $s' \in QNR_n$, go to step (1).

   Then, (r, s') is the signature of the message m.

3. Signature Verification Phase

   To verify that (r, s) is a valid signature of message m, one can simply check whether the following congruence holds.

   $$g^M \equiv y^{R'} R'^{\sigma} \bmod p,$$

   where $\sigma = 2^{-1}s^2 \bmod n$. If it holds, (r, s) is a valid signature of the message m.

   Note:

   (A) In the original basic scheme, the verification equation is

   $$g^{m^2} \equiv y^{r^2} r^{s^2} \bmod p.$$

(B) Since n is odd, we know gcd(2, n) = 1. Thus 2^{-1} mod n is existence.

(3) Since the basic scheme can be written as an ElGamal scheme if the factorization problem can be solved, we can induce that the security of basic scheme is equivalent to the security of the ElGamal scheme if the factorization problem can be solved. □

3.2 Extended Schemes

Like Meta-ElGamal, we extend our basic scheme to many kinds of digital signature schemes of which the security is based on two assumptions. The security of our basic scheme is based on both the ElGamal digital signature scheme and the modified OSS scheme. It can be regarded as the combination of the ElGamal scheme and the modified OSS scheme. Thus, some extended schemes can be regarded as the combination of the Meta-ElGamal schemes and the “Meta-modified OSS” schemes. Like what we described, if the discrete logarithm problem is broken, these schemes can be transformed into the “Meta-modified OSS” schemes. If the factorization problem is broken, these schemes can be transformed into the Meta-ElGamal digital signature scheme. Thus these schemes can be taken apart. However, some extended schemes cannot be taken apart. These schemes will be regarded as insecure and the security of these schemes will be not based on two assumptions.

Here, we will discuss what kinds of extended schemes can be regarded as secure schemes. Like the second generalization (i.e. number of variant) of Meta-ElGamal scheme [10], we can let the extended signature schemes be $A \equiv x^2B+kC$ mod n and the values of A, B, C be the permutation of (M', R', S'), where $M' = m^2$, $R' = r^2$ and $S' = s^2$. In Table 1, all the permutations are shown. At the same time, the corresponding equations

$$Dr^2+Es^2 \equiv Fm' \bmod n$$

Table 1. Permutation of Three Parameters

No	signature	A	B	C	D	E	F	verification
1	$m^2 \equiv x^2r^2+ks^2$	M'	R'	S'	1	$g(r)$	1	$g^{m^2} = y^{r^2} r^{s^2}$ mod p
2	$m^2 \equiv x^2s^2+kr^2$	M'	S'	R'	$g(r)$	1	1	$g^{m^2} = y^{s^2} r^{r^2}$ mod p
3	$s^2 \equiv x^2r^2+km^2$	S'	R'	M'	1	$-X^{-1}$	$-g(r)X$	$g^{s^2} = y^{r^2} r^{m^2}$ mod p
4	$s^2 \equiv x^2m^2+kr^2$	S'	M'	R'	$g(r)$	$-X^{-1}$	$-X$	$g^{s^2} = y^{m^2} r^{r^2}$ mod p
5	$r^2 \equiv x^2s^2+km^2$	R'	S'	M'	X^{-1}	-1	$g(r)X$	$g^{r^2} = y^{s^2} r^{m^2}$ mod p
6	$r^2 \equiv x^2m^2+ks^2$	R'	M'	S'	X^{-1}	$-g(r)$	X	$g^{r^2} = y^{m^2} r^{s^2}$ mod p

on Meta-modified OSS schemes are also shown in table 1, where

$$m' = m^2/x^2,\ X' = x^2,\ g(r) = f(r)/x^2$$

and f is a function to solve discrete logarithm problem (i.e. $a = g^{f(a)}$ mod p).

For example, the no. 2 of the extended scheme in table 1 can be written as follows.

Algorithm 4. The Extended Scheme (no. 2)

1. Parameters and Key Generation Phase
   (1) Let p be a large prime such that $p = 4\rho p_1q_1 + 1$, where ρ is a randomly chosen number, $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$ and p_1, p_2, q_1, q_2 are distinguished large primes.
   (2) Let $n = p_1q_1$ and $g \in Z_p^*$ such that $g^n \equiv 1 \bmod p$, $g^{p_1} \neq 1 \bmod p$ and $g^{q_1} \neq 1 \bmod p$.
   (3) Randomly choose a value x such that $1 < x < n$ and $\gcd(x, p-1) = 1$.
   (4) Compute $y \equiv g^{x^2} \bmod p$.
   (5) Signer's Keys:
   (A) Private Keys: x, p_1, q_1.
   (B) Public Keys: y, p.
2. Signature Generation Phase
   Assume $m \in Z_n^*$ is the message to be signed.
   (1) The signer randomly choose an integer k such that $1 < k < n$ and $\gcd(k, p-1) = 1$.
   (2) Compute $r \equiv g^k \bmod p$.
   (3) Find s' such that

$$m^2 \equiv x^2s' + kr^2 \bmod n. \tag{3}$$

   (4) If $s' \in QR_n$, evaluate s that such $s^2 \equiv s' \bmod n$.
   (5) If $s' \in QNR_n$, go to step 1.
   Then, (r, s) is the signature of the message m.
3. Signature Verification Phase
   To verify that (r, s) is a valid signature of message m, one can simply check the following congruence.

$$g^{m^2} \equiv y^{s^2} r^{r^2} \bmod p.$$

   If it holds, (r, s) is a valid signature of the message m.
   Note: From Eq. (3), we know that $m^2 \equiv x^2s^2 + kr^2 \bmod n$. Therefore, the verification congruence is

$$g^{m^2} \equiv y^{s^2} r^{r^2} \bmod p$$

In addition to the second generalization, the forth generalization of the Meta-ElGamal can be also applied to our extended schemes. Except that, other generalizations cannot be put on our extended schemes.

3.3 The Security of the Proposed Schemes

As we described, the security of our proposed scheme is based on two hard problems. The main point is that we sign the signature by two keys in two different places. In the first place, we use the private key x to compute the value s' by the equation $m^2 \equiv x^2r^2 + ks' \bmod n$ in our basic scheme. To get the value s' by the above equation, the value x^2 must be obtained. The difficulty in obtaining the value x^2 form the public key $y \equiv g^{x^2} \bmod p$ or other public parameters is equivalent to the difficulty in solving the discrete logarithm problem. In the second place, we use the private key p_1 and q_1 to find the square root s of value s'. The difficulty in obtaining the private key p_1 and q_1 from the public value $n = p_1q_1$ is equivalent to the difficulty in solving the factorization problem. The difficulty in evaluating s that such $s^2 \equiv s' \bmod n$ is also equivalent to the difficulty in solving the factorization problem.

To reach the security based on two hard problems, it is important to use two different keys to sign a signature. Compared with others, many insecure schemes use only one key to sign a signature in the signature generation phase. In this case, the designed schemes may be insecure.

4. Discussion for Computations

In this section, we discuss the computation for our proposed signature schemes. In our proposed schemes, we have to determine whether $s' \in QR_n$ or $s' \in QNR_n$. It costs us much computation time. After determining that $s' \in QR_n$, we have to evaluate s that such $s^2 \equiv s' \bmod n$. This also takes computation time. If we can find an algorithm depending on the special parameter on our proposed scheme to compute the value s efficiently, this will speed up our signature signing.

We have found an algorithm to compute the value s specially. This algorithm depends on the designed parameter in our proposed scheme. However, it is not truly efficient. Even in such case, we still describe the algorithm as follows and hope one day an efficient algorithm can be found.

Algorithm 5. Computing square root for special parameters.

Assumption**:** $n = p_1q_1$ such that $p_1 \leq q_1$, where $p_1 = 2p_2 + 1$, $q_1 = 2q_2 + 1$ and p_1, p_2, q_1, q_2 are distinguished large primes.

Goal: (1) Randomly choose $y \in Z_n^*$ and determine whether $y \in QR_n$.

(2) Computer x such that $x^2 \equiv y \bmod n$ if $y \in QR_n$.

Steps:

(1) Let $p' \equiv \dfrac{p_2q_2+1}{2} \bmod 2p_2$ and $q' \equiv \dfrac{p_2q_2+1}{2} \bmod 2q_2$.

(2) Randomly choose $y \in Z_n$*.

(3) Determine whether the congruence

$$y^{p_2} \equiv 1 \bmod p_1 \tag{4}$$

holds. If it does not hold, go to step 2.

(4) Determine whether the congruence

$$y^{q_2} \equiv 1 \bmod q_1 \tag{5}$$

holds. If it does not hold, go to step 2.

(5) $y \in QR_n$ and $x = \mathrm{CRT}(x_p, x_q; p_1, q_1)$, where

$$x_p \equiv y^{p'} \bmod p_1$$

and

$$x_q \equiv y^{q'} \bmod q_1.$$

Therefore we can obtain the value x and y such that $y \in QR_n$ and $x^2 \equiv y \bmod n$.

Verification.

(1) Let $z \equiv y^{p_2q_2} \bmod n$. By using CRT, we can evaluate $z \equiv \mathrm{CRT}(z_p, z_q; p_1, q_1)$, where $z_p \equiv y^{p_2q_2} \bmod p_1$ and $z_q \equiv y^{p_2q_2} \bmod q_1$. Since the order in p_1 is $\phi(p_1) = 2p_2$, we have

$$z_p \equiv y^{p_2q_2 \bmod 2p_2} \bmod p_1.$$

Because q_2 is an odd number, thus

$$z_p \equiv y^{p_2} \bmod p_1.$$

In the same way, we can conclude that

$$z_q \equiv y^{q_2} \bmod q_1.$$

(2) If $y \in QR_n$, there must exist a value x such that $x^2 \equiv y \bmod n$. Thus we know that

$$y^{p_2} \equiv y^{\frac{p_1-1}{2}} \bmod p_1.$$

Since $y \equiv x^2 \bmod n$, we can conclude that

$$y^{p_2} \equiv (x^2)^{\frac{p_1-1}{2}} \bmod p_1 \equiv (x)^{p_1-1} \bmod p_1 \equiv 1 \bmod p_1.$$

In the similar way, we can conclude that $y^{q_2} \equiv 1 \bmod q_1$. Therefore

$$z \equiv \mathrm{CRT}(z_p, z_q; p_1, q_1) \equiv \mathrm{CRT}(1, 1; p_1, q_1) \equiv 1 \bmod n.$$

(i.e. $y \in QR_n \Rightarrow y^{p_2} \equiv 1 \bmod p_1$ and $y^{q_2} \equiv 1 \bmod q_1 \Rightarrow y^{p_2q_2} \equiv 1 \bmod n$)

(3) If $z \equiv 1 \bmod n$, then

$$z_p \equiv y^{p_2q_2} \bmod p_1 \equiv 1 \bmod p_1$$

and

$$z_q \equiv y^{p_2q_2} \bmod q_1 \equiv 1 \bmod q_1.$$

Thus, we know that

$$z_p \equiv y^{p_2} \bmod p_1 \equiv 1 \bmod p_1$$

and

$$z_q \equiv y^{q_2} \bmod q_1 \equiv 1 \bmod q_1.$$

(i.e. $y^{p_2q_2} \equiv 1 \bmod n \Rightarrow y^{p_2} \equiv 1 \bmod p_1$ and $y^{q_2} \equiv 1 \bmod q_1$)

Therefore, we can conclude that $y^{p_2q_2} \equiv 1 \bmod n$ iff $y^{p_2} \equiv 1 \bmod p_1$ and $y^{q_2} \equiv 1 \bmod q_1$.

(4) If $z \equiv 1 \bmod n$, then

$$y^{p_2q_2+1} \equiv y \bmod n.$$

Since $p_2q_2 + 1$ is an even number, there exist a value

$$x \equiv y^{\frac{p_2q_2+1}{2}} \bmod n \tag{6}$$

such that $x^2 \equiv y \bmod n$. Hence, $y \in QR_n$ (i.e. $y^{p_2q_2} \equiv 1 \bmod n \Rightarrow y \in QR_n$)

Therefore, we can conclude that $y^{p_2q_2} \equiv 1 \bmod n$ iff $y \in QR_n$.

Consequently, we can summarize that

(A) $y \in QR_n$ iff $y^{p_2} \equiv 1 \bmod p_1$ and $y^{q_2} \equiv 1 \bmod q_1$,

(B) $y \in QR_n$ iff $y^{p_2q_2} \equiv 1 \bmod n$.

(i.e. $y^{p_2q_2} \equiv 1 \bmod n \Leftrightarrow y^{p_2} \equiv 1 \bmod p_1$ and $y^{q_2} \equiv 1 \bmod q_1 \Leftrightarrow y \in QR_n$.)

(5) If $y \in QR_n$, from Eq. (6) we know that $x \equiv y^{\frac{p_2q_2+1}{2}} \bmod n$ such that $x^2 \equiv y \bmod n$. By using CRT, we can evaluate $x \equiv \mathrm{CRT}(x_p, x_q; p_1, q_1)$, where

$$x_p \equiv y^{\frac{p_2q_2+1}{2}} \bmod p_1$$

and

$$x_q \equiv y^{\frac{p_2q_2+1}{2}} \bmod q_1.$$

Since the order in p_1 is $\phi(p_1) = 2p_2$ and the order in p_1 is $\phi(q_1) = 2q_2$,we have $x_p \equiv y^{p'} \bmod p_1$ and $x_q \equiv y^{q'} \bmod q_1$, where

$$p' \equiv \frac{p_2q_2+1}{2} \bmod 2p_2$$

and

$$q' \equiv \frac{p_2q_2+1}{2} \bmod 2q_2.$$ □

Notice that:

(1) In step 1, the values *p*' and *q*' can be pre-computed.

(2) The step 3 and step 4 is to determine whether $y^{p_2q_2} \equiv 1 \bmod n$. The congruence $y^{p_2q_2} \equiv 1 \bmod n$ holds if and only if both the following two congruence hold.

$$y^{p_2} \equiv 1 \bmod p_1,$$
$$y^{q_2} \equiv 1 \bmod q_1.$$

(3) Eq. (4) is to determine whether $y \in QR_{p_1}$ and eq. (5) is to determine whether $y \in QR_{q_1}$.

(4) The probability that $y^{p_2} \equiv 1 \bmod p_1$ hold is 1/2 and the probability that $y^{q_2} \equiv 1 \bmod q_1$ hold is also 1/2. Thus the probability that both $y^{p_2} \equiv 1 \bmod p_1$ and $y^{q_2} \equiv 1 \bmod q_1$ hold is 1/4. Therefore, the probability that the chosen *y* belongs to QR_n is 1/4. (i.e. Prob($y \in QR_n$) = 1/4.)

(5) If $\mathrm{Ord}_n(y) \mid p_2q_2$, we can conclude that

(A) the value *y* must be QR_n (because $y^{p_2q_2} \equiv 1 \bmod n$) and

(B) $y^{\frac{p_2q_2+1}{2}} \bmod n$ must be QR_n (because $(y^{\frac{p_2q_2+1}{2}})^{p_2q_2} \equiv 1 \bmod n$).

(6) If $\mathrm{Ord}_n(y)$ can not divide p_2q_2, then there must be no solution for *x*.

(7) This algorithm can be used in the situation that $\mathrm{Ord}_n(y)$ is an odd value.

(8) This algorithm can be used in the situation that both p_1 and q_1 are odd primes.

5. Comparison

In this session, we make some comparisons between RSA scheme, the ElGamal scheme and the basic one of the proposed schemes. In Table 2, the compared items are the security basis, the complexity of signature generation phase and the complexity of signature verification phase.

RSA scheme is the simplest one in the three schemes. Its security basis is the factoring problem (FAC). Assume the modular composite number used in the signature generation phase and in the signature verification phase is *n*''. It needs only one exponentiation computation under the modular *n*'' in the signature generation phase. It needs also only one exponentiation computation under the modular *n*'' in the signature verification phase.

The security basis of the ElGamal scheme is the discrete logarithm problem (DLP). Assume the modular prime number used in the signature verification phase is *p*'. In the signature verification phase, it needs one exponentiation computation under the modular *p*', one inverse computation under the modular *p*'-1, two multiplication computations under the modular *p*'-1 and one addition computation under the modular *p*'-1. In the signature verification phase, it needs three exponentiation computations under the modular *p*' and one multiplication computation under the modular *p*'.

Table 2 Complexity Comparison

Schemes Items	RSA Scheme	ElGamal Scheme	Proposed Scheme
Security Basis	FAC	DLP	FAC and DLP
Signature Generation	$\text{Exp}_{n''} \times 1$	$\text{Exp}_{p'} \times 1$ $\text{Inv}_{p'\text{-}1} \times 1$ $\text{Mul}_{p'\text{-}1} \times 2$ $\text{Add}_{p'\text{-}1} \times 1$	$\text{Exp}_{p} \times 1 \times 4$ $\text{Inv}_{n} \times 1 \times 4$ $\text{Mul}_{n} \times 2 \times 4$ $\text{Sqr}_{n} \times (1 + 1 \times 4)$ $\text{Add}_{n} \times 1 \times 4$ $\text{Exp}_{p_1} \times 5$ $\text{Exp}_{q_1} \times 3$ $\text{CRT}_{p_1 \times q_1} \times 1$
Signature Verification	$\text{Exp}_{n''} \times 1$	$\text{Exp}_{p'} \times 3$ $\text{Mul}_{p'} \times 1$	$\text{Exp}_{p} \times 3$ $\text{Mul}_{p} \times 1$ $\text{Sqr}_{p\text{-}1} \times 3$

Exp_n: Exponentiation computation under the modular n.
Inv_n: Inverse computation under the modular n.
Mul_n: Multiplication computation under the modular n.
Sqr_n: Square computation under the modular n.
Add_n: Addition computation under the modular n.
$\text{CRT}_{p_1 \times q_1}$: Chinese remainder theorem computation under the modular $p_1 \times q_1$.

The security bases of the proposed scheme are both the factoring problem and the discrete logarithm problem. Assume we can find s' such $s' \in QR_n$ directly in the signature generation phase of our basic scheme. It needs one exponentiation computation under the modular p to compute the value r. It needs one square computation under the modular n to compute the value m^2. It also needs one inverse computation under the modular n, two multiplication computations under the modular n, one square computation under the modular n (assume x^2 can be pre-computed) and one addition computation under the modular n to compute the value $s' \equiv k^{-1}(m^2 - x^2r^2) \bmod n$.

However in average, we need four times to get s' such that $s' \in QR_n$. Thus, except the requirement for computing the value m^2 is still one square computation under the modular n, we need four exponentiation computations under the modular p to compute the value r. We also need four inverse computations under the modular n, eight multiplication computations under the modular n, four square computations under the modular n and four addition computations under the modular n to compute the value $s' \equiv k^{-1}(m^2 - x^2r^2) \bmod n$. Besides this, we have to determine whether $s' \in QR_n$ and compute the value s which is the square root of s'. By using our algorithm in session 4, it needs (assume $\frac{p_2q_2+1}{2} \bmod 2p_2$ and $\frac{p_2q_2+1}{2} \bmod 2q_2$ can be pre-computed) four exponentiation computations under the modular p_1 to test whether $s'^{p_2} \equiv 1 \bmod p_1$ and two exponentiation computations under the modular q_1 to test whether $s'^{q_2} \equiv 1 \bmod q_1$ in average since Prob($s'^{p_2} \equiv 1 \bmod p_1$) = Prob($s'^{q_2} \equiv 1 \bmod q_1$) = 1/2. After finding s' such that $s'^{p_2} \equiv 1 \bmod p_1$ and $s'^{q_2} \equiv 1 \bmod q_1$, we still need one exponentiation computation under the modular p_1 to compute $s_p \equiv s'^{\frac{p_2q_2+1}{2}} \bmod p_1$, one exponentiation computation under the modular

q_1 to compute $s_p \equiv s'^{\frac{p_2 q_2 + 1}{2}} \bmod q_1$ and one computation by using Chinese remainder theorem under the modular $p_1 \times q_1$ to compute s = CRT(s_p, s_q; p_1, q_1).

In the signature verification phase, it needs three exponentiation computations under the modular p, one multiplication computation under the modular p and three square computations under the modular p – 1 to check whether $g^{m^2} \equiv y^{r^2} r^{s^2} \bmod p$.

6. Conclusion

In this paper, we proposed a digital signature scheme and proved that it is based on factoring and discrete logarithm problems. This is the first scheme which can be proved that its security is based on two hard problems. We also extended our basic signature scheme to many extended schemes. The drawback of our proposed schemes is that (1) we have to determine whether a number belongs to the Quadratic Residue of a composite number and (2) we have to evaluate the square root in the signature-generation phase. Aiming to this, we discuss and propose an algorithm on it. Compared with Harn's scheme [6], our proposed schemes combine the ElGamal and the modified OSS schemes together while Harn's scheme string up the ElGamal and the RSA scheme. Compared with Laih and Kuo's scheme [12], our schemes are much easier while their schemes are more complicated.

Acknowledgments

This work is partially supported by the Ministry of Science and Technology under Grant MOST 104-2221-E-182-012. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] E. F. Brickell and K. S. McCurley, "An interactive identification scheme based on discrete logarithms and factoring", Journal of Cryptology, vol. 5, no. 1, **(1992)**, pp. 29-40.
[2] J.-S. Coron, M. Joye, D. Naccache, and P. Paillier, "New Attacks on PKCS#1 v1.5 Encryption", Eurocrypt, **(2000)**.
[3] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Trans., vol. IT-22, **(1976)**, pp. 644-654.
[4] L. Ding and C. S. Laih, "Comment: Digital signature scheme based on factoring and discrete logarithms", **(2002)**.
[5] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on the Discrete Logarithm", IEEE Trans. on Information Theory, vol. IT-31, **(1985)**, pp. 469-472.
[6] L. Harn, "Public-key Cryptosystem Design Based on Factoring and Discrete Logarithms", IEE Proc.-Computers and Digital Techniques, **(1994)**.
[7] L. Harn, "Comment: Enhancing of the Security of ElGamal's Signature scheme, IEE Proc.-E, **(1995)**.
[8] W. H. He, "Digital Signature Scheme Based on Factoring and Discrete Logarithms", Electronics Letters vol. 37, no. 4, **(2001)**, pp. 220 –222.
[9] J. He and T. Kiesler, "Enhancing the Security of ElGamal's Signature Scheme", IEE Proc.-E, **(1994)**.
[10] P. Horster, M. Michels and H. Petersen, "Meta-ElGamal Signature Schemes Using a Composite Module", Technical Report TR-94-16-E, University of Technology Chemnitz-Zwickau, **(1994)**.
[11] C. S. Laih and W. C. Kuo, "Cryptanalysis of Enhancing the Security of ElGamal's Signature Scheme", Proc. Cryptography: Policy and Algorithms. Lecture Notes in Computer Science, Springer-Verlag, Berlin Heidelberg, **(1996)**.
[12] C. S. Laih and W. C. Kuo, "New Signature Schemes Based on Factoring and Discrete Logarithms", IEICE Trans. Fundamentals, vol. E80-A, no. 1, **(1997)**, pp. 46-53.
[13] N. Y. Lee "Security of Shao's Signature Schemes Based on Factoring and Discrete Logarithms", IEE Proc., **(1999)**.
[14] N. Y. Lee and T. Hwang, "The Security of He and Kiesler's Signature Schemes", IEE Proc.-E, **(1995)**.
[15] N. Y. Lee and T. Hwang, "Modified Harn signature scheme based on factoring and discrete logarithms", IEE Proc. Computers And Digital Techniques, **(1996)**.
[16] J. Li and G. Xiao, "Remarks on new signature scheme based on two hard problems", Electronics Letters vol. 34, no. 25, **(1998)**, p. 2401.

[17] C.-H. Lim and P.-J. Lee, “A study on the proposed Korean digital signature algorithm”, Advances in Cryptology - Asiacrypt, LNCS 1514, Springer-Verlag, **(1998)**, pp. 175-186.

[18] K. C. McCurley, “A key distribution system equivalent to factoring”, Journal Cryptology, vol. 1, no. 2, **(1988)**, pp. 95-106.

[19] M. Michels, D. Naccache, and H. Petersen, “GOST 34.10-A brief overview of Russia’s DSA”, Computers and Security, vol. 15, no. 8, **(1996)**, pp. 725-732.

[20] D. Naccache, "Can O.S.S. be Repaired? Proposal for a New Practical Signature Scheme", Advances in Cryptology: Proceedings of Eurocrypt (Lecture Notes in Computer Science), Springer-Verlag, **(1994)**; New York.

[21] National Institute of Standards and Technology, “The Digital Signature Standard”, Comm. ACM, vol. 35, no. 7, **(1992)**, pp. 36-40.

[22] NIST, Digital signature standard, FIPS PUB 186, **(1994)**.

[23] A. M. Odlyzko, "Discrete logarithms: The past and the future", Designs, Codes, and Cryptography, vol. 19, **(2000)**, pp. 129-145.

[24] H. Ong, C. Schnorr and A. Shamir, "An Efficient Signature Scheme Based On Quadratic Equations", Proceedings of the 16th Symposium on the Theory of Computing, **(1984)**; Washington.

[25] J. Pollard and C. Schnorr, "An Efficient Solution of the Congruence x2 + ky2 = m mod n", IEEE Trans. on Information Theory, vol. IT-33, **(1987)**, pp. 17-28.

[26] M. O. Rabin, "Digitalized Signatures and Public-Key Functions as Intractable as Factorization", MIT/LCS/TR-212, MIT Lab. for Computer Science, Cambridge, Mass, **(1979)**.

[27] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystem", Communications of the ACM, vol. 21, **(1978)**, pp. 120-126.

[28] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards", Advances in Cryptology: Proceedings of Eurocrypt (Lecture Notes in Computer Science), Springer-Verlag, **(1990)**; New York.

[29] Z. Shao, “Signature schemes based on factoring and discrete logarithms”, Computers and Digital Techniques, IEE Proceedings, **(1998)**.

[30] H. M. Sun, “Cryptanalysis of a digital signature scheme based on factoring and discrete logarithms”, NCS, **(2002)**.

Authors

Shin-Yan Chiou, He received the PhD degree in Electrical Engineering from National Cheng Kung University, Taiwan, in 2004. From 2004 to 2009, he worked at Industrial Technology Research Institute as a RD Engineer. Since 2009, he joined the faculty of the Department of Electrical Engineering, Chang Gung University, Taoyuan, Taiwan, where he is currently an Associate Professor. He has published a number of journal and conference papers in the areas of information security, social network security and mobile security. His research interests include information security, cryptography, social network security, and secure applications between mobile devices.