A New Public-Key Cryptosystem as Secure as Factoring

Tatsuaki Okamoto Shigenori Uchiyama

NTT Laboratories
1-1 Hikarinooka, Yokosuka-shi, 239-0847 Japan
Email: {okamoto, uchiyama}@sucaba.isl.ntt.co.jp

Abstract. This paper proposes a novel public-key cryptosystem, which is practical, provably secure and has some other interesting properties as follows:

1. Its trapdoor technique is essentially different from any other previous schemes including RSA-Rabin and Diffie-Hellman.
2. It is a probabilistic encryption scheme.
3. It can be proven to be as secure as the intractability of factoring $n = p^2q$ (in the sense of the security of the whole plaintext) against passive adversaries.
4. It is semantically secure under the p-subgroup assumption, which is comparable to the quadratic residue and higher degree residue assumptions.
5. Under the most practical environment, the encryption and decryption speeds of our scheme are comparable to (around twice slower than) those of elliptic curve cryptosystems.
6. It has a homomorphic property: $E(m_0, r_0)E(m_1, r_1) \bmod n = E(m_0 + m_1, r_2)$, where $E(m, r)$ means a ciphertext of plaintext m as randomized by r and $m_0 + m_1 < p$.
7. Anyone can change a ciphertext, $C = E(m, r)$, into another ciphertext, $C' = Ch^{r'} \bmod n$, while preserving plaintext of C (i.e., $C' = E(m, r'')$), and the relationship between C and C' can be concealed.

1 Introduction

1.1 Background and Previous Results

Diffie and Hellman proposed the concept of the public-key cryptosystem (or trapdoor one-way function) in 1976 [11]. Although extensive research has been made by numerous cryptographers and mathematicians to realize the concept of public-key cryptosystems for more than 20 years, very few concrete techniques that seem to be secure have been found.

A typical class of techniques is RSA-Rabin, which is the combination of the polynomial time algorithm of finding a root of a polynomial over a finite field and the intractability of the factoring problem. Another typical class of techniques is Diffie-Hellman, which is the combination of the commutative property of the logarithm in a finite Abelian group and the intractability of the discrete logarithm problem. The RSA-Rabin class includes RSA [35], Rabin [34], Williams [38, 39], LUC [36], Kurosawa-Itoh-Takeuchi [19], Cubic RSA [20] and the elliptic curve versions of RSA [18, 10]. The Diffie-Hellman class includes the Diffie-Hellman

K. Nyberg (Ed.): Advances in Cryptology - EUROCRYPT '98, LNCS 1403, pp. 308-318, 1998.

[11], ElGamal [12], and the elliptic/hyperelliptic curve versions of the Diffie-Hellman and ElGamal [25, 17, 6]. Several other techniques have been proposed such as the Goldwasser-Micali scheme [14] based on the quadratic residuosity, the Ajtai-Dwark scheme [2] based on the lattice problem, the McEliece scheme [22] based on the error correcting code, knapsack type cryptosystems including the Merkle-Hellman, Chor-Rivest and Naccache-Stern schemes [23, 7, 26], and multivariate polynomial type cryptosystems including the Matsumoto-Imai and Patarin-Goubin schemes [21, 28, 29], however they are not so efficient or not so secure[1]. Therefore, from the practical viewpoint, only two techniques, RSA-Rabin and Diffie-Hellman, have been used in many applications.

Among the RSA-Rabin and Diffie-Hellman type schemes, no scheme except the Rabin scheme and its variants such as its elliptic curve versions and Williams has been proven to be as secure as the primitive problems[2] (e.g., factoring and discrete logarithm problems) even against passive adversaries. Therefore, only one technique, Rabin's technique, is known to construct practical and provably secure public-key cryptosystems.

The Rabin scheme was proven to be secure in the sense that to decrypt a whole plaintext from a ciphertext is as hard as factoring. This, however, does not guarantee that no partial information (e.g., one bit) of the plaintext could be revealed from the ciphertext. Let k be the plaintext (or modulus) size of the Rabin scheme. As for the Rabin scheme, only the least $O(\log k)$ significant bits of the plaintext are proven to be as secure as factoring, but no security proof is given on the remaining $(k - O(\log k))$ bits of the plaintext. (Similarly, as for the RSA scheme, only the least $O(\log k)$ significant bits of the plaintext are proven to be as secure as RSA inversion.) [3]

In order to formalize the security level in which no partial information of a plaintext is revealed, Goldwasser and Micali introduced "semantical security" and gave a concrete scheme, the GM scheme, that realized this security [14, 24]. It is obvious from the definition that any semantically secure public-key cryptosystem should be probabilistic. Although the GM scheme was proven to be semantically secure under the quadratic residue assumption, it is not so efficient, since one bit of plaintext is encrypted to a modulus size (e.g., 1024 bits) ciphertext.

The Blum-Goldwasser scheme [5] is almost as efficient as the Rabin and RSA "asymptotically", but it is not so efficient when the plaintext is short. Since a public-key cryptosystem is normally used only for distributing a secret key (112 bits, 128 bits etc long) of a secret-key cryptosystem such as triple-DES and IDEA, the Blum-Goldwasser scheme does not solve the efficiency problem of the GM scheme.

To the best of our knowledge, the most efficient semantically secure cryptosystem is EPE (Efficient Probabilistic Encryption) (page 78 in [13]). EPE can be implemented based on the RSA and Rabin schemes and its efficiency is almost as same as those of the RSA and Rabin schemes. When it is based on the Rabin (or RSA) scheme, it is proven to be semantically secure under the factoring (or RSA) assumption. In addition, semantical security of the ElGamal scheme is proven under the decision Diffie-Hellman assumption [37].

---

[1] The expression, "not so secure" includes the case where its security has not been sufficiently investigated by many researchers.

[2] We say a system is "provably secure" if it is proven to be as secure as the primitive problems.

1.2 Our Result

This paper proposes a novel public-key cryptosystem, which is practical, provably secure and has some other interesting properties as follows:

1. **New trick:** Its trapdoor technique is essentially different from any other previous scheme including RSA-Rabin and Diffie-Hellman. The proposed technique employs efficient (polynomial time) algorithms for solving the discrete logarithm over a specific finite subgroup.
2. **Probabilistic encryption:** It is a probabilistic encryption scheme. Let $E(m, r)$ be a ciphertext of plaintext m as randomized by r.
3. **One-wayness of the encryption function:** It can be proven to be as secure as the intractability of factoring $n = p^2q$ (in the sense of the security of the whole plaintext) against passive adversaries. The trick in proving its security differs from that used for Rabin type cryptosystems. For example, the proposed cryptosystem is probabilistic encryption, although the Rabin scheme and its variant are deterministic by nature. (i.e.., a plaintext can be encrypted to many ciphertexts with randomness and a ciphertext is uniquely decrypted to the plaintext in our cryptosystem, while plural plaintexts are encrypted to a ciphertext and a ciphertext is decrypted into plural plaintexts in the Rabin scheme.) The proof of the security of the proposed cryptosystem essentially utilizes this property: one plaintext can be encrypted to many ciphertexts with randomness while a ciphertext is uniquely decrypted.
4. **Semantical security:** It is semantically secure if the following assumption, p-subgroup assumption, is true: $E(0, r) = h^r \bmod n$ and $E(1, r') = gh^{r'} \bmod n$ is computationally indistinguishable, where r and r' are uniformly and independently selected from $\mathbf{Z}/n\mathbf{Z}$. This assumption is comparable to the quadratic residue and higher degree residue assumptions.
5. **Efficiency:** Under the most practical environment of using public-key cryptosystems, where a public-key cryptosystem is used only for distributing a secret key (e.g., 112 and 128 bits long) of a secret-key cryptosystem (e.g., triple-DES and IDEA), the encryption and decryption speeds of our scheme are comparable to (around twice slower than) those of elliptic curve cryptosystems.
   Compared with the RSA scheme with small e (e.g., 3 or $2^{16}+1$), although the encryption speed of our scheme is slower than that of RSA, the decryption speed of our scheme is faster than that of RSA.
   The size of a ciphertext of a k-bit (e.g., 340 bits) plaintext in our system is $3k$ bits, i.e., the size of modulus n (e.g., 1024 bits), which is almost the same as that of the RSA scheme. Note that the plaintext size of k bits (e.g., 340 bits) is sufficient in usual for the purpose of distributing a secret key (at most 256 bits in almost all block ciphers including AES).
6. **Homomorphic property:** It has a homomorphic property:
   $E(m_0, r_0)E(m_1, r_1) \bmod n = E(m_0 + m_1, r_3)$, if $m_0 + m_1 < p$.
   Such a property is used for electronic voting and other cryptographic protocols.
   Note that no other encryption scheme except the higher-degree residue encryption [8] has such a homomorphic property, and the higher-degree residue encryption is extremely inefficient in decryption.
7. **Randomizability of ciphertext:** Even someone who does not know the secret key can change a ciphertext, $C = E(m, r)$, into another ciphertext,

$C' = Ch^{r'} \bmod n$, while preserving plaintext m (i.e., $C' = E(m, r'')$), and the relationship between C and C' can be concealed (i.e., (C, C') and $(C, E(m', t))$ are indistinguishable from the semantical security).
Such a property is useful for privacy protecting protocols.

Remarks:

- **On the security against active attacks:** The provable security of our scheme implies a weakness of our scheme against active attacks. This is similar to that of the Rabin scheme. However, our scheme can be easily modified to be secure against active attacks (namely, to be secure against chosen-ciphertext attacks) under the random oracle model [4]. The technique is similar to Bellare-Rogaway's OAEP [4] but our scheme is simpler than their modification since semantical security has been already guaranteed under the number theoretic assumption before applying the random oracle model in our scheme. (OAEP requires the random oracle technique even to satisfy the semantical security as well as the plaintext awareness.)
- **On non-malleability:** The last two properties of our scheme imply a kind of weakness in the sense of non-malleability [9]. However, if non-malleability is required for our cryptosystem, there are some practical (heuristic) ways to convert a malleable scheme to a non-malleable one.
- **On the intractability of factoring $n = p^2q$:** Although it is not known whether $n = p^2q$ is more tractable to factor than $n = pq$, some special algorithms to factor $n = p^2q$ have been studied [30, 31, 33, 1]. However, such techniques are specific on the elliptic curve factoring method, and the fastest algorithm for factoring both $n = pq$ and $n = p^2q$ is the number field sieve method, whose running time depends only on the composite size, $|n|$. Therefore, currently the size of $n = p^2q$ can be the same as $n = pq$ if n is sufficiently large (e.g., $|n|$ is at least 1024).

2 The Proposed Public-Key Cryptosystem

This section introduces our public-key cryptosystem, which is constructed on the multiplicative group over ring $\mathbf{Z}/n\mathbf{Z}$ ($n = p^2q$; p, q: primes). Our new technique is based on a logarithmic function, L, defined over the p-Sylow subgroup of $(\mathbf{Z}/p^2\mathbf{Z})^*$.

2.1 Logarithmic function

Definition 1. Let p be an odd prime, and Γ be the p-Sylow subgroup of $(\mathbf{Z}/p^2\mathbf{Z})^*$, i.e.,

$$\Gamma = \left\{ x \in (\mathbf{Z}/p^2\mathbf{Z})^* \mid x \equiv 1 \pmod{p} \right\}.$$

It is well-known that $(\mathbf{Z}/p^2\mathbf{Z})^*$ is a cyclic group with order $p(p-1)$, so $\#\Gamma = p$.

We now define a $\mathbf{F}_p$-valued function, L, on Γ as follows:
For $x \in \Gamma$,

$$L(x) = \frac{x-1}{p}.$$

Clearly, L is well-defined on Γ.

Function L has a homomorphic property from multiplication to addition, i.e., we can identify L as a "logarithmic function" on Γ.

Lemma 2. *For $a, b \in \Gamma$,*

$$L(ab) = L(a) + L(b) \bmod p,$$

Then, L is an isomorphism. (Here, ab means $(ab \bmod p^2) \in \Gamma$.)

Proof. It is easy to see that

$$\frac{ab-1}{p} = \frac{(a-1)(b-1)+(a-1)+(b-1)}{p} = \frac{(a-1)}{p}(b-1) + \frac{(a-1)}{p} + \frac{(b-1)}{p}$$
$$= L(a)(b-1) + L(a) + L(b).$$

Note that $(b-1) \equiv 0 \pmod p$. $L(ab) = \frac{ab-1 \bmod p^2}{p} = \frac{ab-1}{p} \bmod p$. Hence,

$$L(ab) = L(a) + L(b) \bmod p.$$

Clearly, L is an isomorphism. This completes the proof of this lemma.

□

Corollary 3. *Let $x \in \Gamma$ such that $L(x) \neq 0 \bmod p$, and $y = x^m \bmod p^2$ for $m \in \mathbf{Z}/p\mathbf{Z}$. Then,*

$$m = \frac{L(y)}{L(x)} = \frac{y-1}{x-1} \bmod p.$$

Remark Let g be a primitive root $\bmod p^2$, then there exists $r \in (\mathbf{Z}/p\mathbf{Z})^*$ such that $g^{p-1} = 1 + pr \bmod p^2$, i.e., $g^{p-1} \in \Gamma$.

$$L(g^{p-1}) = \frac{(1+pr)-1}{p} = r \bmod p.$$

So, we obtain $g^* = g^{p-1} \bmod p^2$ such that $L(g^*) \neq 0 \bmod p$.

2.2 Our Scheme

This subsection shows how to construct our cryptosystem based on the logarithmic function, L.

Choose two large primes p, q ($|p| = |q| = k$), and let $n = p^2q$. Choose $g \in (\mathbf{Z}/n\mathbf{Z})^*$ randomly such that the order of $g_p = g^{p-1} \bmod p^2$ is p. (Note that $\gcd(p, q-1) = 1$ and $\gcd(q, p-1) = 1$.) Let $h = g^n \bmod n$.

Our cryptosystem, based on the exponentiation $\bmod n$, is constructed as follows:

[Public-Key] (n, g, h, k)
[Secret-Key] (p, q)

Note: h is a supplementary parameter for improving the efficiency of encryption, since h can be easily calculated from g and n.

[Encryption] Let m $(0 < m < 2^{k-1})$ be a plaintext. Select $r \in \mathbf{Z}/n\mathbf{Z}$ uniformly.

$$C = g^m h^r \bmod n.$$

[Decryption] $C_p = C^{p-1} \bmod p^2$,

$$m = \frac{L(C_p)}{L(g_p)} \bmod p$$

3 Encryption Function is One-Way

This section proves that inverting the encryption function (i.e., calculating a plaintext, m, from the ciphertext, $E(m,r)$) of our scheme is as hard as factoring $n = p^2q$.

Definition 4. Let $\mathcal{G}_1$ be an instance generator such that $\mathcal{G}_1(1^k) \rightarrow n$, $n = p^2q$, $|p| = |q| = k$, $(p, q$: primes). Here, the distribution of n is the same as that of n with our scheme. The *factoring* problem is, given (n, k), to find (p, q).

The factoring problem is *intractable*, if for any (uniform/non-uniform) probabilistic polynomial time machine A, for any constant c, for sufficiently large k,

$$\Pr[A(1^k, n) = (p, q)] < 1/k^c.$$

The probability is taken over the coin flips of $\mathcal{G}_1$ and A.

Definition 5. Let $\mathcal{G}_2$ be a generator in our scheme such that $\mathcal{G}_2(1^k) \rightarrow (n, g, C)$, (n, g, k) is a public-key and C is a ciphertext of our scheme (with the same distribution of the scheme).

Inverting the encryption function of our scheme is *intractable* if for any (uniform/non-uniform) probabilistic polynomial time machine Adv, for any constant c, for sufficiently large k,

$$\Pr[Adv(1^k, n, g, C) = m] < 1/k^c.$$

The probability is taken over the coin flips of $\mathcal{G}_2$ and Adv.

Theorem 6. *Inverting the encryption function of our scheme is intractable if and only if the factoring problem is intractable.*

Proof. (Only if:)

Assume that the factoring problem is not intractable. A polynomial time machine, then, can factor n with non-negligible probability, and break our scheme with non-negligible probability.

(If:) Let assume that our scheme is not secure (i.e., there exists an adversary, Adv, who can compute m from C with non-negligible probability). We will then construct a probabilistic polynomial time algorithm A, with help of Adv as an oracle, which, given (n, k), can factor n with non-negligible probability.

First, given (n, k), A should generate g by itself in order to input (n, g, k) to Adv. When A randomly selects $g \in (\mathbf{Z}/n\mathbf{Z})^*$, $g^{p-1} \bmod p^2$ has the order of p with probability $(p-1)/p$ (overwhelming probability).

A then chooses $z' \in \mathbf{Z}/n\mathbf{Z}$ uniformly, and computes $C' = g^{z'} \bmod n$. A provides (n, g, k) and C' to Adv as a public-key and ciphertext. Adv can output a correct plaintext for a non-negligible fraction of the correct public-key set $\{(n, g, k)\}$ and correct ciphertext set $\{C\}$ with non-negligible probability (taken over the coin flips of Adv).

The distribution of n given by $\mathcal{G}_1$ is exactly same as that given by $\mathcal{G}_2$ in our cryptosystem, and the distribution of g given by A is statistically close to that given by our system. Therefore, we have to check whether the distribution of C' given by A is close to the distribution of C given by $\mathcal{G}_2$ in our cryptosystem.

Let the order of $g \bmod p^2$ is pp' and the order of $g \bmod q$ is q' such that $p'|p-1$ and $q'|q-1$. The distribution of C can be represented by the distribution of

$z = [z_1, z_2]$ ($z \equiv z_1 \bmod p, z \equiv z_2 \bmod \mathrm{lcm}(p', q')$) such that $C = g^z = g^{m+nr} = g^m h^r \bmod n$. (Here note that $\gcd(p, \mathrm{lcm}(p', q')) = 1$ and $\gcd(q, \mathrm{lcm}(p', q')) = 1$, i.e., $\gcd(n, \mathrm{lcm}(p', q')) = 1$.) We define similarly $z' = [z'_1, z'_2]$ ($z' \equiv z'_1 \bmod p, z' \equiv z'_2 \bmod \mathrm{lcm}(p', q')$) such that $C' = g^{z'} \bmod n$. When z_1 and z'_1 are fixed, the distributions of z_2 and z'_2 are statistically close. Note that z_1 is uniformly distributed over $\mathbf{Z}/2^{k-1}\mathbf{Z}$, while z'_1 is uniformly distributed over $\mathbf{Z}/p\mathbf{Z}$. Therefore, although they are not statistically close, the probability of each value of z_1 is at most twice of that of z'_1. Hence, a non-negligible fraction of z_1 is also non-negligible in z'_1.

Therefore, if Adv can output a correct plaintext for a non-negligible fraction of our scheme's public-key set $\{(n, g, k)\}$ and correctly generated ciphertext set $\{C\}$, then Adv can output a correct plaintext for a non-negligible fraction of $\{(n, g, k)\}$ and ciphertext set $\{C'\}$ given by A.

When Adv outputs a correct answer, m, for $C' = g^{z'} \bmod n$, m should satisfy: $m < 2^{k-1}$ and $z' \equiv m \pmod p$. Since z' is uniformly chosen over $\mathbf{Z}/n\mathbf{Z}$, $z' \geq 2^{k-1}$ (i.e., $z' \not\equiv m \pmod n$) with overwhelming probability. We then have $\gcd(z' - m, n)$ which is either p, p^2, or pq, since $(z' - m)$ is a multiple of p, $(z' - m) < n$ and $n = p^2 q$. Thus, A can factor n with the help of Adv with non-negligible probability.

□

4 Semantical Security

This section proves that our cryptosystem is semantically secure if and only if the p-subgroup problem is intractable (i.e., the p-subgroup assumption is true). Here the p-subgroup assumption is stronger than the factoring assumption but still reasonable since it is comparable to the quadratic residue and higher degree residue assumptions.

Definition 7. Let $\mathcal{G}_3$ be a generator regarding our scheme such that $\mathcal{G}_3(1^k) \rightarrow (n, g, m_0, m_1, C)$, (n, g, k) is a public-key and C is a ciphertext of (randomly selected) either one of m_0 and m_1 (say m). That is, $C = E(m, r)$, where E is the encryption function with random value r.

Our scheme is *semantically secure* (against passive adversaries), if for any (uniform/non-uniform) probabilistic polynomial time machine Adv, for any constant c, for sufficiently large k,

$$\Pr[Adv(1^k, n, g, m_0, m_1, C) = m] < 1/2 + 1/k^c.$$

The probability is taken over the coin flips of $\mathcal{G}_3$ and Adv.

Definition 8. Let $\mathcal{G}_4$ be a generator regarding our scheme such that $\mathcal{G}_4(1^k) \rightarrow (n, g, C)$, (n, g, k) is a public-key and C is a ciphertext of (randomly selected) either one of 0 and 1 (say b). That is, $C = E(b, r)$.

The *p-subgroup problem* is *intractable* if for any (uniform/non-uniform) probabilistic polynomial time machine Adv, for any constant c, for sufficiently large k,

$$\Pr[Adv(1^k, n, g, C) = b] < 1/2 + 1/k^c.$$

The probability is taken over the coin flips of $\mathcal{G}_4$ and Adv.

The assumption that the *p-subgroup problem* is *intractable* is called the *p-subgroup assumption*.

Theorem 9. *Our scheme is semantically secure (against passive adversaries) if and only if the p-subgroup problem is intractable.*

Proof. In this proof, we will simply write $E(m)$ in place of $E(m, r)$.
(Only if:)

Assume that the p-subgroup problem is not intractable. A polynomial time machine, A, then, can distinguish $E(0)$ and $E(1)$ with non-negligible probability.

Given $(m_0, m_1, C = E(m \in \{m_0, m_1\}))$, $(m_0 < m_1)$, we will construct a polynomial time machine, B, with help of A as a blackbox, which can distinguish $E(m_0)$ and $E(m_1)$ with non-negligible probability.

B calculates $X = C/g^{m_0} \bmod n$, and set $g' = g^{(m_1 - m_0) + rn} \bmod n$ and $h' = g'^n \bmod n$, where $r \in \mathbf{Z}/n\mathbf{Z}$ is randomly selected. Let E' denote the encryption function with g', and $L = \mathrm{lcm}(p-1, q-1)$. When $C = E(m_1) = g^{m_1} h^{r_1} \bmod n$, $X = E'(1) = g' h'^{t_1} \bmod n$, if $t_1 = (r_1 - r)/(m_1 - m_0 + rn) \bmod L$ is defined. When $C = E(m_0) = g^{m_0} h^{r_0} \bmod n$, $X = E'(0) = h'^{t_0} \bmod n$, if $t_0 = r_0/(m_1 - m_0 + rn) \bmod L$ is defined. t_0 and t_1 are defined with non-negligible probability (over the distribution of r, r_0 and r_1).

For any $(m_1 - m_0)$, the order of $g'_p = g'^{p-1} \bmod p^2$ is p, since $(m_1 - m_0) < p$. For any $(m_1 - m_0)$, $(m_1 - m_0 + rn) \bmod L$ is distributed statistically uniformly over $\mathbf{Z}/L\mathbf{Z}$, since $\gcd(p, q-1) = 1$ and $\gcd(q, p-1) = 1$.

Therefore, a non-negligible fraction of g' has the distribution statistically close to that of g, for any $(m_1 - m_0)$.

B then gives X to A, and gets an answer from A whether X is $E(0)$ or $E(1)$. This answer is correct with non-negligible probability, and the correct answer immediately implies whether C is $E(m_0)$ or $E(m_1)$.
(If:)

Assume that our scheme is not semantically secure: i.e., there exists an adversary, A, who, given $(m_0, m_1, C = E(m \in \{m_0, m_1\}))$, $(m_0 < m_1)$, can distinguish $E(m_0)$ and $E(m_1)$ with non-negligible probability.

We will then construct a polynomial time machine, B, with help of A as a blackbox, which can distinguish $E(0)$ and $E(1)$ with non-negligible probability.

Given C which is either $E(0)$ or $E(1)$, B calculates $X = C^{m_1 - m_0} \bmod n$, and $\hat{C} = X g^{m_0} \bmod n$. If $C = E(0)$, $\hat{C} = E(m_0)$ $(X = E(0))$, and if $C = E(1)$, $\hat{C} = E(m_1)$ $(X = E(m_1 - m_0))$. B also randomizes $\hat{C}$ and obtains $\hat{C}' = \hat{C} g^{nr} \bmod n$, $r \in_R \mathbf{Z}/n\mathbf{Z}$. B then gives $\hat{C}'$ to A, and gets an answer from A whether $\hat{C}'$ is $E(m_0)$ or $E(m_1)$. This answer is correct with non-negligible probability, and the correct answer immediately implies whether C is $E(0)$ or $E(1)$.

□

5 A Practical Modification

In most applications, a public-key cryptosystem is used only for distributing a secret key (e.g., 112 and 128 bits long) of a secret-key cryptosystem (e.g., triple-DES and IDEA), hence the plaintext size is fairly small (e.g., 128 bits). Then the encryption speed of our scheme will be much faster if the size of r in the encryption procedure is limited to the same as that of message m. We call this modification (limitation) the *limited random size version*.

We can prove the semantical security of the limited random size version under a specified assumption, the limited random size version of the p-subgroup assumption. Due to space limitation in this paper, we omit the formal description on the security of the limited random size version, and will show it in our full paper.

Here, we only describe a slightly modified version of our scheme, which is introduced to prove the security of the limited random size version.

[Modified version of our scheme] The only difference of the modified version is h: $h = h_0^n \bmod n$, where h_0 is selected from $(\mathbf{Z}/n\mathbf{Z})^*$ randomly and independently from g. We also assume that $p-1 = p'u$ and $q-1 = q'v$, where p' and q' are primes, and $|u|$ and $|v|$ are $O(\log k)$. (We can consider that the basic version of our scheme is a special case of this modified version such as $h_0 = g$.)

6 Performance

In this section, we compare the computation amount of our scheme with those of the representative practical public-key cryptosystems, RSA, ElGamal, ECC (elliptic curve cryptosystems) and EPE, using the required number of modular multiplications mod$n$, where n is 1024 bits.

We assume that modulus n for our scheme, RSA and EPE, and modulus p for ElGamal are 1024 bits and modulus p for ECC is 160 bits, where ECC is based on an elliptic curve over the finite field with p-elements. (See Introduction for the reason why n for our scheme is assumed to have the same size as that of n for RSA.)

Furthermore, we also assume that the group addition on ECC costs 10 times as much as the modular multiplication mod$p$ does. A modular exponentiation with exponent e (k bits) requires $3k/2$ modular multiplications in the standard binary method, and the extended binary method (4.6.3 ex.27 in [16]) takes $7k/4$ modular multiplications, if the size of both exponents m, r are k bits. (For example, the extended binary method is used in the encryption of our scheme, $g^m h^r \bmod n$.)

Since public-key encryption schemes are normally utilized for distributing a secret key (e.g., 128 bits long) of a block-cipher, we assume that the size of a plaintext is 128 bits.

First, we will evaluate the efficiency of "encryption" procedures of these schemes. Note that the efficiency of encryption process in RSA, ElGamal and ECC, does not depend on the size of a plaintext, while that of EPE and our scheme depends on the size of a plaintext.

The encryption procedure of our scheme requires about 230 ($= 7/4 \times 130$) modular multiplications, where we assume that the size of a parameter r is around 130 bits (see Section 5).

The encryption procedures of RSA, ElGamal, ECC, and EPE takes about 2 through 1500 (with e is 3 thorough 1000 bit long), 3000, 120 and 13 modular multiplications, respectively. Here, we assume that the least 10 ($= \log 1024$) significant bits are used in one modular squaring step of EPE.

Next we will evaluate the efficiency of "decryption" procedures of these schemes.

The almost all processing time for the decryption process of our scheme is consumed by computing $C_p = C^{p-1} \bmod p^2$. Since $|p| = |n|/3$ and $p^2 = 2|n|/3$, the required number of the modular exponentiation (with 1024 bits) is around

230 ($\approx 340 \times (3/2) \times (4/9)$). In addition, we can reduce this amount into around 140 by employing a sophisticated arithmetic over modular multiplication mod p.

The decryption procedures of RSA, ElGamal, ECC and EPE require about 400, 1500, 60 and 400, respectively. Here we assume the Chinese remainder technique for RSA and EPE.

7 Conclusion

This paper has proposed a novel public-key cryptosystem, which is practical, provably secure and has several interesting properties.

By using techniques similar to those shown in [15], we can prove that any bit of a plaintext in our scheme is individually secure (i.e., hard core bit) assuming the intractability of factoring $n = p^2q$ [27].

References

1. Adleman, L.M. and McCurley, K.S.: Open Problems in Number Theoretic Complexity,II (open problems: C7, O7a and O7b), Proc. of ANTS-I, LNCS 877, Springer-Verlag, pp.291-322 (1995).
2. Ajtai, M. and Dwork, C.: A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence, Proc. of STOC'97, pp. 284-293 (1997).
3. Alexi, W., Chor, B.Z., Goldreich, O. and Schnorr, C.P.: RSA and Rabin Functions: Certain Parts Are as Hard as the Whole, SIAM Journal of Computing, 17, 2, pp.449–457(1988).
4. Bellare, M. and Rogaway, P. : Optimal Asymmetric Encryption, Proc. of Eurocrypt'94, LNCS 950, Springer-Verlag pp.92-111 (1995).
5. Blum, M. and Goldwasser, S.: An efficient probabilistic public-key encryption scheme which hides all partial information, Proc. of Crypto'84, LNCS 196, Springer-Verlag, pp.289-299 (1985).
6. Chao, J., Matsuda, N. and Tsujii, S.: Efficient construction of secure hyperelliptic discrete logarithm problems, Proc. of ICICS'97, LNCS 1334, Springer-Verlag, pp.292-301 (1997).
7. Chor, B. and Rivest, R.L.: A knapsack type public key cryptosystem based on arithmetic in finite fields, Proc. of Crypto'84, LNCS 196, Springer-Verlag, pp.54-65 (1985).
8. Cohen, J. and Fischer.: A Robust and Verifiable Cryptographically Secure Election Scheme, FOCS, pp.372-382 (1985).
9. Dolev, D., Dwork, C. and Naor, M.: Non-Malleable Cryptography, Proc. of STOC, pp.542–552 (1991).
10. Demytko, N.: A New Elliptic Curve Based Analogue of RSA, Proc. of Eurocrypt'93, LNCS 765, Springer-Verlag, pp.40-49 (1994).
11. Diffie, W. and Hellman, M.: New Directions in Cryptography, IEEE Trans. on Information Theory, IT-22, 6, pp.644–654 (1976).
12. ElGamal, T.: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. on Information Theory, IT-31, 4, pp.469–472 (1985).
13. Goldwasser, S. and Bellare, M: Lecture Notes on Cryptography, http://www-cse.ucsd.edu/users/mihir/ (1997).
14. Goldwasser, S. and Micali, S.: Probabilistic Encryption, JCSS, 28, 2, pp.270-299 (1984).
15. Hastad, J., Schrift, A.W. and Shamir, A.: The Discrete Logarithm Modulo a Composite Hides $O(n)$ Bits, J. of Computer and System Sciences, 47, pp.376-404 (1993).

16. Knuth, D.E.: The Art of Computer Programming, Addison-Wesley Publishing Co.,(1981).
17. Koblitz, N.: Elliptic Curve Cryptosystems, Math. Comp., 48, 177, pp.203–209 (1987).
18. Koyama, K. , Maurer, U. M. , Okamoto, T. and Vanstone, S. A.,: New Public-key Schemes based on Elliptic Curves over the Ring Zn, Proc. of Crypto'91, LNCS 576, Springer-Verlag, pp.252-266 (1992).
19. Kurosawa, K., Ito, T. and Takeuchi, M.: Public Key Cryptosystem using a Reciprocal Number with the same Intractability as Factoring a Large Number, Cryptologia, 12, 4, pp.225-233 (1988).
20. Loxton, J.H., Khoo, D.S.P., Bird, G.J. and Seberry, J.: A Cubic RSA Code Equivalent to Factorization, Journal of Cryptology, 5, 2, pp.139-150 (1992).
21. Matsumoto, T. and Imai, H.: Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption, Proc. of Eurocrypt'88, LNCS 330, Springer-Verlag, pp.419-453 (1988).
22. McEliece, R.J.: A Public-Key Cryptosystem Based on Algebraic Coding Theory, DSN progress report 42-44, Jet Propulsion Laboratories, Pasadena (1978).
23. Merkle, R.C. and Hellman, M.E.: Hiding Information and Signatures in Trapdoor Knapsacks, IEEE Trans. on Inform. Theory, 24, pp.525-530 (1978).
24. Micali, S., Rackoff, C. and Sloan, B.: The notion of security for probabilistic cryptosystems, SIAM Journal on Computing, 17, 2, pp.412-426 (1988).
25. Miller, V.S.: Use of Elliptic Curves in Cryptography, Proc. of Crypto'85, LNCS 218, Springer-Verlag, pp.417-426 (1985).
26. Naccache, D. and Stern, J.: A New Public-Key Cryptosystem, Proc. of Eurocrypt'97, LNCS 1233, Springer-Verlag, pp.27-436 (1997).
27. Okamoto, T. and Uchiyama, S.: Individual Bit Security of a New Public-Key Cryptosystem, Manuscript (1998).
28. Patarin, J. and Goubin, L.: Trapdoor one-way permutations and multivariate polynomials, Proc. of ICICS'97, LNCS 1334, Springer-Verlag, pp.356-368 (1997).
29. Patarin, J. and Goubin, L.: Asymmetric cryptography with S-Boxes, Proc. of ICICS'97, LNCS 1334, Springer-Verlag, pp.369-380 (1997).
30. Peralta, R.: Bleichenbacher's improvement for factoring numbers of the form $N = PQ^2$ (private communication) (1997).
31. Peralta, R. and Okamoto, E.: Faster Factoring of Integers of a Special Form, IEICE Trans. Fundamentals, E79-A, 4, pp.489-493 (1996).
32. Pointcheval, D. and Stern, J.: Security Proofs for Signature Schemes, Proc. of Eurocrypt'96, LNCS 1070, Springer-Verlag, pp.387-398 (1996).
33. Pollard, J.L.: Manuscript (1997).
34. Rabin, M.O.: Digital Signatures and Public-Key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCS/TR-212 (1979).
35. Rivest, R., Shamir, A. and Adleman,L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Vol.21, No.2, pp.120-126 (1978).
36. Smith, P. and Lennon, M.: LUC: A New Public Key System, Proc. of IFIP/SEC'93, pp. 103-117, North-Holland (1993).
37. Tsiounis, Y. and Yung, M.: On the Security of ElGamal-based encryption, to appear in Proc. of PKC'98, LNCS, Springer-Verlag.
38. Williams, H.C.: A Modification of the RSA Public Key Encryption Procedure, IEEE Trans. on Inform. Theory, IT-26, 6, pp.726-729 (1980).
39. Williams, H.C.: Some Public-Key Crypto-Functions as Intractable as Factorization, Proc. of Crypto'84, LNCS 196, Springer-Verlag, pp.66-70 (1985).