A study on the fast ElGamal encryption

Kim Gyu–Chol*, Li Su–Chol

a Kim Chaek University of Technology, Pyongyang, DPR of Korea

* Corresponding Author. Tel.: 0085023811811; Fax: 0085023814410;

E-mail address: kgc841110@star-co.net.kp; P.O. Box: 60 Kyogu Pyongyang

Abstract

ElGamal cryptosystem[1] is typically developed in the multiplicative group Z_p^* (p is a prime number), but it can be applied to the other groups in which discrete logarithm problem should be computationally infeasible. Practically, instead of ElGamal in Z_p^*, various variants such as EC–ElGamal (ElGamal in elliptic curve group), CRT–ElGamal (ElGamal in subgroup of Z_n^* where $n = pq$ and $p, q, \frac{p-1}{2}, \frac{q-1}{2}$ are primes) have already been used for the semantic security[2].

In this paper, for the fast decryption, we reduced the private CRT exponent $x_p (= x \, mod \, (p - 1))$ and $x_q (= x \, mod \, (q - 1))$ maintaining full sized private exponent x $(0 < x < n)$ in CRT–ElGamal as reducing $d_p (= d \, mod \, (p - 1))$ and $d_q (= d \, mod \, (q - 1))$ in RSA[3] for the fast decryption. (i.e. as in rebalanced RSA[4]).

In this case, unlike rebalanced RSA, decryption of CRT–ElGaml can be done faster without losing of encryption speed. As a result, it is possible to propose the fast public key cryptosystem that has fast encryption and fast decryption.

Keyword: RSA, ElGamal, public key, Rebalanced RSA, CRT

1. Introduction

CRT-ElGamal is a variant of ElGamal that is implemented in the subgroup of Z_n^* where $n = pq$ and $p, q, \frac{p-1}{2}, \frac{q-1}{2}$ are prime numbers and is believed to be semantically secure under the DDH assumption [2].

The key generation, encryption and decryption of CRT-ElGamal can be described as follows.

Algorithm 1.1: Key generation for the CRT-ElGamal.

Each user creates the public key and the corresponding private key.

1. Select a large composite number $n(= pq: p, q, \frac{p-1}{2}$ and $\frac{q-1}{2}$ are large primes) and a generator α of group G. G is the multiplicative subgroup of Z_n^* and order of G is $\lambda(= lcm(p-1, q-1))$.

   This can be described in details as follows.

   1.1 Select the large primes p, q, p' and q' such that $p = 2p' + 1$ and $q = 2q' + 1$ and calculate $n = pq$ and $\lambda = lcm(p-1, q-1) = 2p'q'$.

   1.2 Select a generator α_p of Z_p^* and generator α_q of Z_q^* and calculate α that satisfies $\alpha_p = \alpha \bmod p$ and $\alpha_q = \alpha \bmod q$ as follows.

$$\alpha = \Big(\big((\alpha_p - \alpha_q)(q^{-1} \bmod p)\big) \bmod p\Big) q + \alpha_q \qquad (1-1)$$

   In this case, α becomes the generator of subgroup G with order λ, which is the multiplicative subgroup of Z_n^*.

2. Select a random integer $x(1 \le x < n, gcd(x, \lambda) = 1)$ and compute $k = \alpha^{\lambda - x} \bmod n$.

   This can be described in details as follows.

   2.1. Select a random integer $x_p(1 < x_p < p-1)$ and $x_q(1 < x_q < q-1)$ such that $gcd(x_p, p-1) = 1$, $gcd(x_q, q-1) = 1$ and $x_p \equiv x_q \bmod 2$.

   2.2. Calculate $k_p = \alpha_p^{p-1-x_p} \bmod p, k_q = \alpha_q^{q-1-x_q} \bmod q$ and

$$k = \Big(\big((k_p - k_q)(q^{-1} \bmod p)\big) \bmod p\Big) q + k_q \qquad (1-2)$$

   In this case, $k^{-1} \bmod n = \alpha^x \bmod n, x_p = x \bmod (p-1)$ and $x_q = x \bmod (q-1)$ are satisfied.

3. Public key is (α, k, n) and private key is $x(or\ \lambda - x)$.

   This can be described in details as follows.

   3.1. Public key is (α, k, n) and private key is (x, x_p, x_q, p, q).

Algorithm 1.2: Encryption for the CRT-ElGamal.

User encrypts a message m.

1. Obtain authentic public key (α, k, n).
2. Represent the message as an integer m in the interval $[0,\ n-1]$.
3. Select a random integer y $(1 < y < n)$.
4. Compute $c_1 = \alpha^y \ mod\ n$ and $c_2 = k^y m \ mod\ n$.
5. Send the cipher text $c = (c_1,\ c_2)$.

Algorithm 1.3: Decryption for the CRT-ElGamal.

User recovers plaintext m from $c = (c_1,\ c_2)$.

Recover

$$m = c_1^x \ c_2 mod\ n \qquad (1-3)$$

by using private key x.

This can be described in details as follows.

1. Calculate $c_{1p} = c_1 mod\ p, c_{1q} = c_1 mod\ q, c_{2p} = c_2 mod\ p$ and $c_{2q} = c_2 mod\ q$.
2. Calculate

$$m_p = c_{1p}^{x_p} c_{2p} mod\ p \qquad (1-4)$$

and

$$m_q = c_{1q}^{x_q} c_{2q} mod\ q \qquad (1-5)$$

3. Calculate m as follows.

$$m = \Big(\big((m_p - m_q)(q^{-1} mod\ p)\big) mod\ p\Big) q + m_q \qquad (1-6)$$

CRT-ElGamal has a possibility to increase the decryption speed four times faster than ElGamal by using CRT. In this paper, we reduced the CRT private exponents in the CRT-ElGamal key generation for the fast decryption just as in rebalanced RSA. Unlike rebalanced RSA, in this case, encryption speed is not affected. (Practically, encryption of ElGamal can be done fast[5] by using the pre-calculated table that contains the main exponentiations of generator and public key and

random exponents with low Hamming weights). That is, it is possible to make both encryption and decryption fast.

Based on such an idea, we described the possibility of fast decryption in CRT-ElGamal and the efficiency comparing to RSA, CRT-RSA, rebalanced RSA, ElGamal and CRT-ElGamal.

This paper is organized as follows. In Section 2, we reviewed the rebalanced RSA briefly. In Section 3, we described the possibility of reducing CRT exponents in CRT-ElGamal encryption system. Finally we concluded this paper in Section 4.

2. Rebalanced RSA

Rebalanced RSA[4] is a variant that changes the key generation in typical RSA for the fast decryption (or signature generation).

The main issue of rebalanced RSA is to reduce the private CRT exponents $d_p(= d \ mod \ (p - 1))$ and $d_q(= d \ mod \ (q - 1))$ while maintaining private exponent d of the same bit size as modulus n.

For the security proof of proposed scheme, we modified the key generation algorithm of rebalanced RSA as follows by adding a little restriction except for $gcd(p-1, q-1) = 2$ in prime generation. Of course, such a modification does not compromise the security of rebalanced RSA.

Algorithm 2.1: Key generation for the rebalanced RSA (modified version).

1. Select a large composite number $n(= pq: p, q, \frac{p-1}{2}$ and $\frac{q-1}{2}$ are large primes) and compute $\lambda = lcm(p-1, q-1)$.
2. Pick two random $w(w < 1/2log_2 n)$–bit values d_p and d_q such that $gcd(d_p, p-1) = 1$, $gcd(d_q, q-1) = 1$ and $d_p \equiv d_q mod\ 2$.
3. Find d such that $d = d_p mod(p-1)$ and $d = d_q mod(q-1)$.
4. Compute $e = d^{-1} mod\ \lambda$.
5. Public key is (n, e) and private key is (p, q, d, d_p, d_q).

Encryption and decryption are identical to CRT-RSA[6]. The only issue is that d_p and d_q are small, so decryption can be done faster than CRT-RSA.

However, e will increase to be of the same bit size as modulus n and it will cause encryption (or signature verification) speed to be further slowed down[4] compared to standard CRT-RSA that uses 3 or 65537 as public exponent e.

Attacks to rebalanced RSA (Small private CRT exponent attacks to RSA)

When the CRT exponents are sufficiently small, there are several small CRT exponent attacks to rebalanced RSA. Among them, we introduce the typical three attacks[7][8] as follows. For the other attacks, see [9],[10],[11] and so on.

Attack 1 is to find b that satisfies $gcd((c^b - m)\ mod\ n\ , n) \neq 1$ when c is $m^e mod\ n$ and attack 2 is finding small roots of the polynomial $f(x_1, x_2, x_3, x_4) = 0$ given by

$$f = e^2 x_1 x_2 + ex_1 x_4 - ex_1 + ex_2 x_3 - ex_2 - (n - 1)x_3 x_4 - x_3 - x_4 + 1 \qquad (2-1)$$

Attack 3 is finding small roots x and y of the polynomial $f_e(x, y) = 0$ given by

$$f = (n - 1)x\ y + x + y - 1\ (mod\ e) \qquad (2-2)$$

CRT exponents d_p and d_q cannot be reduced to below the certain limit to be secure from small CRT exponent attacks. In other words, rebalanced RSA becomes to be insecure when $d_p(d_q) < n^\delta$ is satisfied for the proper δ because of small CRT exponent attacks including attack 1, 2, 3, etc.

In several attacks such as attack2 and 3, δ is changed along to the $\beta(= log_n e)$. On the other hand, δ is not related to β in attacks such as attack1. The discussions on the lowest limit of d_p and d_q have been mentioned in many references so, skipped here. See [7][8][9][10][11] for more details.

3. Possibility of fast decryption in CRT-ElGamal

It is not possible to reduce the private key d for the security problem [12][13][14] in RSA and so, rebalanced RSA that reduces the CRT exponents d_p and d_q instead of d has been proposed for the fast decryption. It is not possible to reduce the private key x for the security problem in CRT-

ElGamal, too. However it would be possible to reduce the CRT exponents x_p and x_q in CRT-ElGamal as in rebalanced RSA.

In this section, we described the possibility of reducing CRT exponents in CRT-ElGamal and set the limit of small x_p and x_q.

3.1 Reducing the CRT exponents in CRT-ElGamal key generation.

Key generation algorithm of proposed scheme can be described similarly to Algorithm 1.1 (mentioned in Section1).

Compared to key generation of CRT-ElGamal(Algorithm1.1), the selection range of $x_p(x_q)$ is only reduced to 2^w from $p-1(q-1)$ in step 2.1. In this case, $w < 1/2log_2 n$

That is, the key generation algorithm of proposed scheme is same as the one of the CRT-ElGamal except for the step2.1, which can be described as follows.

2.1. Select a random integer $x_p(1 < x_p < 2^w)$ and $x_q(1 < x_q < 2^w)$ such that $gcd(x_p, p-1) = 1$, $gcd(x_q, q-1) = 1$ and $x_p \equiv x_q mod\ 2$. In this case, $w < 1/2log_2 n$.

And key generation algorithm of proposed scheme can also be described similarly to Algorithm 2.1 (mentioned in Section2) as follows.

Algorithm 3.1: Key generation for the proposed scheme.

1. Select a large composite number $n(= pq: p, q, \frac{p-1}{2}$and $\frac{q-1}{2}$ are large primes) and calculate $\lambda = lcm(p-1, q-1)$.
2. Pick two random $w(w < 1/2log_2 n)$–bit values x_p and x_q such that $gcd(x_p, p-1) = 1$, $gcd(x_q, q-1) = 1$ and $x_p \equiv x_q mod\ 2$.
3. Find a x such that $x = x_p mod(p-1)$ and $x = x_q mod(q-1)$.
4. Select a generator α of group G and compute $k = \alpha^{\lambda - x} mod\ n$. G is a multiplicative subgroup of Z_n^* and order of G is λ.
5. Public key is (α, k, n) and private key is (p, q, x, x_p, x_q).

Compared to the key generation of rebalanced RSA(Algorithm2.1), only step4 and 5 are different in Algorithm3.1.

Unlike rebalanced RSA, in proposed scheme, modular inverse of private key (i.e. $x^{-1} mod\ \lambda$) is not published and instead, generator α of group G and $k(= \alpha^x mod\ n)$ are published.

3.2 Security.

Rebalanced RSA is a kind of RSA, and so all attacks to RSA can also be applied to this scheme.

However, among them, only the small CRT exponent attacks have been considered in security analysis because other attacks except for small CRT exponent attacks are not effective to rebalanced RSA.

Similarly, we considered only the small CRT exponents attacks to CRT–ElGamal in the security analysis of proposed scheme.

The following proposition shows the discussion of the lowest limit of w for the security from the small CRT exponent attacks in proposed scheme.

Proposition 1: Let $\boldsymbol{n = pq}$ where $\boldsymbol{p, q, \frac{p-1}{2}}$ and $\boldsymbol{\frac{q-1}{2}}$ are primes. If there is a polynomial time algorithm to find the private key $(\boldsymbol{x, x_p, x_q, p, q})$ from the public key $(\boldsymbol{\alpha, k, n})$ in proposed scheme when $\boldsymbol{log_2 x_p \approx log_2 x_q \leq w}$ for the proper integer $\boldsymbol{w(< \frac{1}{2} log_2 n)}$, then it is possible to find the private key $(\boldsymbol{d, d_p, d_q, p, q})$ from the public key $(\boldsymbol{n, e})$ in rebalanced RSA with full exponent $\boldsymbol{e}$(i.e. $\boldsymbol{log_n e \approx 1}$) when $\boldsymbol{log_2 d_p \approx log_2 d_q \leq w}$.

Proof. In rebalanced RSA, $log_n e \approx 1$ is usually satisfied[4] for e such that $ed \equiv 1\ mod\ \lambda$ and similarly, $log_n e' \approx 1$ is satisfied for e' such that $xe' \equiv 1 mod\ \lambda$ (i.e. $k^{e'} mod\ n = \alpha$) in proposed scheme. From the assumption, there exists a polynomial time algorithm (noted as Algorithm A after this time) that finds private key (x, x_p, x_q, p, q) from public key (α, k, n) in proposed scheme.

Hence, by using Algorithm A, it is possible to propose the attack algorithm (noted as Algorithm B after this time) as follows that breaks the rebalanced RSA which has the public key (n, e) satisfying $log_n e \approx 1, log_2 d_p \approx log_2 d_q \leq w$.

Algorithm B: Attack algorithm to rebalanced RSA that uses Algorithm2.1.

Input: Public key (n, e) of rebalanced RSA such that $\frac{p-1}{2}, \frac{q-1}{2}$ are primes and $log_n e \approx 1$.

Output: Private key (d, d_p, d_q, p, q)

1. Select a generator m of G with order λ, which is a multiplicative subgroup of Z_n^*, and calculate $c(= m^e mod\ n)$. In this case, c also becomes a generator of G, because $gcd(e, \lambda) = 1$ in rebalanced RSA.

2. Search the private key(x, x_p, x_q, p, q) in polynomial time by using Algorithm A after setting $\alpha = c, k = m$. In this case, $m = c^d mod\ n,\ d_p = \square\ mod\ (p-1), d_q = d\ mod\ (q-1)$, $log_2 d_p \approx log_2 d_q \leq w$ is satisfied by the assumption and so, it is possible to find private key (d, d_p, d_q, p, q) in polynomial time.

Of course, unlike proposed scheme, the generator of group G is unknown in rebalanced RSA and so, it seems difficult to select m as a generator in step1 of Algorithm B. However, attacker can select the generator without difficulty by selecting a random element $m \in Z_n^*$ in step1, because many element of Z_n^* can become the generator of group G.

From the property of Euler function, the probability that random element $m \in Z_n^*$ becomes a generator of G is as follows.

$$P(m) > \frac{(p_1-1)(q_1-1)}{(2p_1+1)(2q_1+1)} = \frac{p_1q_1-(p_1+q_1)+1}{4p_1q_1+2(p_1+q_1)+1} \approx \frac{1}{4} \qquad (3-1)$$

Hence, attacker can find private key (d, d_p, d_q, p, q) by repeating Algorithm B about 4 times selecting m randomly in step1 and as a result, rebalanced RSA is broken in polynomial time.

(end of proof.)

However, the efficient polynomial time attacks to rebalanced RSA have not been proposed till now, even though p , q, $\frac{p-1}{2}$and $\frac{q-1}{2}$ are primes. Hence, from proposition1, it is known that the proposed scheme is secure from the small CRT exponents attacks if w is set as in rebalanced RSA with full exponent e.

In fact, it is not easy to find the $e'(= x^{-1} mod\ \lambda)$ such that $k^{e'} mod\ n = \alpha$, from the public key (α, k, n) in proposed scheme, because $log_n e' \approx 1$ is usually satisfied and so, finding e' from (α, k, n) becomes a discrete logarithm problem in Z_n^*. For the composite number $n(= pq: p$ and q are primes), discrete logarithm problem in Z_n^* is known to be not easier than factoring problem [15][16][17]. Hence, it is not possible for the attacker to obtain e' and attack2 and 3 mentioned in section2 cannot be applied to proposed scheme. However, this does not mean that the proposed scheme is more secure than rebalanced RSA with full exponent e, because attack1 mentioned in section2 can be still applied to the proposed scheme and furthermore, attack1 is more advantageous[7][8][9] than attack2 and 3 in rebalanced RSA, if $log_n e \approx 1$.

The practical attack to the proposed scheme can be described as follows.

Attacks to proposed scheme (small private CRT exponent attacks)

When $h = k^{-1} mod\ n, h_p = h\ mod\ p = \alpha^{x_p} mod\ p$.

Therefore,

$$h - h_p = h - \alpha^{x_p} mod\ p = jp, gcd(h - \alpha^{x_p} mod\ p, pq) = p.$$

From here, attack to rebalanced ElGamal is finalized as finding i that satisfy

$$gcd(h - \alpha^i mod\ n, n) \neq 1.$$

for all available i because CRT exponents are small.

Thus, attack 1 to rebalanced RSA is straightly applicable to rebalanced ElGamal.

Referring to [4][7][14], the following proposition is obtained.

Proposition 2: let $\boldsymbol{n = p\ q}$ ($\boldsymbol{p}$ and $\boldsymbol{q}$ are strong primes), $\boldsymbol{\lambda = lcm(p-1, q-1)}$, $\boldsymbol{x(0 < x < n)}$ be a random integer and $\boldsymbol{x_p = x\ mod\ (p-1), x_q = x\ mod\ (q-1), x_p < x_q}$.

Further, let $\boldsymbol{w}$ be the smallest integer such that $\boldsymbol{x_p \leq 2^w}$. The modulus $\boldsymbol{n}$ can be factored in time $(\boldsymbol{x_p^{1/2} log^2(n)})$, provided that $\boldsymbol{x_p \neq x_q (mod\ 2^{\lceil w/2 \rceil})}$, by using generator $\boldsymbol{\alpha}$ of subgroup of $\boldsymbol{Z_n^*}$ with order $\boldsymbol{\lambda}$ and $\boldsymbol{z = \alpha^x mod\ n}$.

(Proof) : As explained in detail in reference [4][7][14], and so skipped here. (end of Proof).

Judging with $\boldsymbol{O(x_p^{1/2} log^2(n))}$, CRT-exponents x_p and x_q should be at least 160 bits long for 1024–bit modulus and at least 264–bit modulus for 2048–bit modulus in order for this attack to match the current estimated complexity of factoring the modulus for those sizes[4][7][14].

Compared to CRT–RSA, in rebalanced RSA, encryption and decryption are not changed and only the selection range of CRT exponents is reduced. Similarly, compared to CRT–ElGamal, encryption and decryption are not changed and only the selection range of CRT exponents is reduced in proposed scheme. Referring [2], the semantic security of CRT–ElGamal depends on the DDH (Decision Diffie–Hellman) assumption in the group G which is multiplicative subgroup of $Z_n^*(n = pq$ and $p, q, \frac{p-1}{2}, \frac{q-1}{2}$ are primes) and the best known attacks for DDH is discrete logarithm attacks in cyclic subgroup of Z_n^*. If CRT exponents is reduced in CRT–ElGamal(i.e. in proposed scheme), the best known attacks for DDH is the small CRT exponents attacks. Hence, if CRT exponents are reduced reasonably considering Proposition1 and 2, DH and DDH assumption would be satisfied in the proposed scheme, too. However, it is still an open problem whether there is any new efficient attack to break the DH and DDH assumption in the proposed scheme.

3.3 Efficiency.

The encryption and decryption time comparisons of RSA, CRT–RSA, rebalanced RSA, ElGamal, CRT-ElGamal and proposed scheme are summarized in Table 1.(The comparisons were done in the similar way to reference [11].)

We used pre–calculated table that contains the main exponentiations of generator and public key and selected the random exponents with Hamming weight 99 for the 2048–bit modulus in the encryption of proposed scheme of table 1. Of course, $C_{2048}^{99} \geq 2^{567}$ is satisfied and so, referring to [5], the random exponents that have the lower hamming weight than 99 can be used in encryption.

However, even though encryption speed is increased by using the exponents which have the lower hamming weight than 99, the total processing speed is not increased for the reason of slow

decryption. Hence, we set the Hamming weight as large as possible (i.e. 99) to maximize the security of encrypted message balancing encryption speed and decryption speed.

[Table1. Encryption and decryption time comparison.]

	RSA-Basic	CRT-RSA	Rebalanced RSA	ElGamal	CRT-ElGamal	Our scheme
Public Exponent (Hamming Weight)	$2^{16}+1$ (2)	$2^{16}+1$ (2)	2048 bits (1024)	2048 bits (99)	2048 bits (99)	2048 bits (99)
Num of Multiplication in Encryption	16+1=17	16+1=17	2048×1.5=3072	99×2+1= 199	99×2+1=199	99×2+1= 199
Unit Time for Encryption	0.0056	0.0056	1	0.0648	0.0648	0.0648
Secret Exponent	2048 bits	2048 bits	2048 bits	2048 bits	2048bits	2048 bits
CRT Exponent	-	1024 bits	264 bits	-	1024 bits	264 bits
Num of Multiplication in Decryption (Modular Size)	2048 ×1.5 =3072 (2048)	2×1024×1.5 +2 =3074 (1024)	2×264×1.5+2 =794 (1024)	2048×1.5 +1=3073 (2048)	2×(1024×1.5 +1)+2=3076 (1024)	2×(264×1.5+ 1)+2=796 (1024)
Unit Time for Decryption	1	0.25	0.0648	1	0.25	0.0648
Total Processing Time Max(Encryption, Decryption)	1	0.25	1	1	0.25	0.0648

As shown in Table1, proposed scheme is more advantageous than other systems as both encryption and decryption are fast. The total processing speed of proposed scheme is 15.43times faster than rebalanced RSA and is 3.85 times faster than CRT–RSA.

4. Conclusion

In this paper, we did not suggest the any new encryption protocols. We only described the possibility of reducing CRT exponents in CRT-ElGamal that had been suggested in previous works[2][15][16][17][18]. That is, encryption and decryption protocol of proposed scheme is the same as CRT–ElGamal. Hence, we discussed the security about the small CRT exponent attacks and described that DH and DDH assumption are not broken in proposed scheme.

Comparing to CRT–RSA, proposed scheme is almost 3.85 times faster (for the 2048 bit modulus) in total encryption processing but message expansion by a factor of 2 still remains disadvantageous. In fact, as shown in Table1, the total processing speed of CRT–ElGamal is the same as the one of CRT–RSA, but there exists a message expansion by factor of 2 compared to CRT–RSA and so, CRT–ElGamal is of no practical use compared to CRT–RSA.

However, in the case of reducing the CRT exponents, CRT–ElGamal is more advantageous than CRT–RSA in total processing speed, because encryption is not affected by reducing CRT exponents unlike CRT–RSA. By using such an advantage of CRT–ElGamal, we have proposed the fast public cryptosystem in this paper.

Reference

[1] T.ElGamal, A public key cryptosystem and signature scheme based on discrete logarithms, IEEE Transactions on Information Theory 31(1985) 469-472.

[2] D.Boneh, The decision Diffie–Hellman problem, ANTSIII, Springer LNCS 1423(1998) 48–63

[3] R.L. Rivest, A. Shamir, L. Adleman , A method for obtaining digital signatures and public – key cryptosystems, Communications of ACM 21(2)(1978) 120-126.

[4] D.Boneh , H.Shacham., Fast variants of RSA, CryptoBytes (The Technical Newsletter of RSA Laboratories)5(1) (2002) 1–9.

[5] A.Menezes , P.van Orschot , and S. Vanstone, Handbook of Applied Cryptography,CRC Press, 1996, pp.103-113.

[6] J.J.Quisquater , C.Couvreur, Fast Decipherment Algorithm for RSA Public-Key Cryptosystem, IEEE Electronics Letters 18(1982) 905-907.

[7] M.Jason Hinek , Cryptanalysis of RSA and its variants, CRC Press ,2010, pp. 139-155.

[8] E. Jochemsz, A. May, A polynomial time attack on RSA with private CRT-exponents smaller than $N^{0.073}$, In A. Menezes, editor, volume 4622 of Lecture Notes in Computer Science, Springer, 2007, pp 395-411.

[9] S.D.Galbraith, C.Heneghan, J.F.McKee, Tunable balancing of RSA, ACISP 3574(2005), 280-292.

[10] D.Bleichenbacher and A.May, New attacks on RSA with small secret CRT-exponents, In International Workshop on Public Key Cryptography(2006), 1-13.

[11] H.M.Sun, M.E.Wu, An Approach Towards Rebalanced RSA-CRT with Short Public Exponent, Cryptology ePrint Archive, Report 2005/053, 2005. http://eprint.iacr.org/.

[12] H.Wiener, Cryptanalysis of Short RSA Secret Exponents, IEEE Transactions on Information Theory 36(3) (1990) 553-558.

[13] D.Boneh, G.Durfee, Cryptanalysis of RSA with Private Key d less than $N^{0.292}$, IEEE Transactions on Information Theory 46(4) (2000) 1339-1349.

[14] D.Boneh, Twenty Years Attacks on the RSA Cryptosystem, Notices of the American Mathematical Society 46 (1999) 203-213.

[15] E.Biham, D.Boneh, O.Reingold, Breaking generalized Diffie–Hellman modulo a composite is no easier than factoring, Information Processing Letters 70(1998), 83-87

[16] K.S.McCurley, A key distribution system equivalent to factoring, Journal of Cryptology, vol.1(1988) 95-105.

[17] Z.Schmuely, Composite Diffie-Hellman public-key generating systems are hard to break, Technical Report, No.356, Computer Science Department, Technion, Israel, 1985

[18] Wei , W. , Trung , T. , Magliveras , S. , Hoffman , F. , “Cryptographic primitives based on groups of hidden order” , Tatra Mountains Mathematical Publications 29 , pp.147-155 , 2009