JOURNAL OF THEORETICAL PHYSICS & CRYPTOGRAPHY
www.IJTPC.org/Publications

Construction of a Randomized RSA-type Cryptosystem in Quadratic Remaindering Group.

[1]Hyonjong Kim, [2]Yongsok Kim and [3]Cholguk Ri
[1,2,3]Faculty of Mathematics, Kim Il Sung University, D.P.R.K

ABSTRACT
In this paper, A fully secure RSA-type cryptosystem is presented. Standard RSA model is only secure against passive attacks. Thus recently there are many studies for randomized RSA-type cryptosystems based on the standard RSA. In [1,4,5], authors introduced randomized RSA-type cryptosystems where the security is IND-CPA. In these cryptosystems, it is needed to solve the system of congruencies for finding the value of random parameter r for decryption. In this paper, we propose a randomized RSA-type cryptosystem in quadratic remaindering group. For this cryptosystem, it is not needed to solve the system of congruencies for finding the value of random parameter r for decryption. Security of this cryptosystem is IND-CPA.

Keywords
Public key encryption, standard model, cryptosystem, RSA

1. INTRODUCTION
The concept of security of a public-key cryptosystem means the indistinguishability against chosen-plaintext attacks (IND-CPA) and indistinguishability against chosen-cipertext attacks (IND-CCA). IND-CCA is classified into IND-CCA1 and IND-CCA2. For details, see [3,4,7,8,9]. Some recent studies show the relations between semantic security and indistinguishability against chosen ciphertext attacks [1,5,10]. Two typical randomized RSA-type cryptosystems are given as follows.

- RSA-Paillier cryptosystem [2]

This cryptosystem has similar efficiency with standard RSA. It is the combination of RSA algorithm and Paillier algorithm. Encryption is given as follows:

$$E : Z_n^* \times Z_n^* \to Z_{n^2}^*,$$

$$(r, m) \to r^e (1+mn) \bmod n^2.$$

Here, $n = pq$ where p and q are distinct prime numbers with the same length and satisfies $p \equiv q \equiv 3 (\bmod 4)$. e and $d (\in Z^*_{\phi(n)})$ satisfies $ed \equiv 1 (\bmod \phi(n))$ for Euler function $\phi(n) = (p-1)(q-1)$.

- Rabin-Paillier cryptosystem [6]

Encryption is given as follows:

$$E : Q_n \times Z_n^* \to Z_{n^2}^*,$$

$$(r, m) \to r^{2e} + mn \bmod n^2.$$

Here, $n = pq$ where p and q are distinct prime numbers with the same length and satisfies $p \equiv q \equiv 3 (\bmod 4)$. e and $d (\in Z^*_{\phi(n)})$ satisfies $ed \equiv 1 (\bmod \phi(n))$ for Euler function $\phi(n) = (p-1)(q-1)$. Q_n is the quadratic remaindering group generated over Z_n^*. Security of this cryptosystem is IND-CPA. It is needed to solve the system of congruencies to find the value of random parameter r for decryption in these cryptosystems.

2. CONSTRUCTION OF A RANDOMIZED RSA-TYPE CRYPTOSYSTEM OVER QUADRATIC RE MAINDERING GROUP.
In this section, we introduce a new cryptosystem which is based on the fact that order of Q_{n^2} is $n\frac{L(n)}{2}$. The algorithm is as follows.

Key generation algorithm

p, q, p', q' : Large prime numbers satisfying $p = 2p'+1$, $q = 2q'+1$, $n = pq$,

$L(n) = LCM(p-1, q-1) = 2p'q'$: Generalized Euler function,

e, d : Positive integers satisfying $ed \equiv 1 (\bmod L(n))$,

Q_n : Cyclic group generated over Z_n^* with order $\frac{L(n)}{2}$,

$\overline{g}$: Primitive element of Q_n,

Q_{n^2} : Cyclic group generated over $Z_{n^2}^*$ with order $\frac{L(n^2)}{2}$,

where $g = \overline{g}^2$ means that g is primitive element of Q_{n^2},

(n, g, e) : Public key,

(p, q, d) : Private key.

Encryption algorithm E

$m \in Z_n^*$: Plaintext,

$r \xleftarrow{R} Z_{\frac{L(n)}{2}}$: Random parameter,

$c = g^{nr}(1 + (m^e \bmod n)n) \bmod n^2$: Ciphertext.

Decryption algorithm D

$c \in Z_{n^2}$: Ciphertext

$$m = \left\lfloor \frac{(c^{\frac{L(n)}{2}} - 1)(\frac{L(n)}{2})^{-1} \bmod n^2}{n} \right\rfloor^d \bmod n$$: Plaintext

The validity of decryption is based on the following fact:

$$\left\lfloor \frac{\left\lfloor g^{n\frac{L(n)}{2}r}(1 + \frac{L(n)}{2}(m^e \bmod n)) - 1 \right\rfloor (\frac{L(n)}{2})^{-1} \bmod n^2}{n} \right\rfloor^d \bmod n$$

$$= \left\lfloor \frac{\frac{L(n)}{2}(m^e \bmod n)\left\lfloor \frac{L(n)}{2} \right\rfloor^{-1} \bmod n^2}{n} \right\rfloor^d \bmod n =$$

$m^{ed} \bmod n = m$.

The following table shows the comparison result of our work with previous works.

	Calculus over Z_n^*		Calculus over $Z_{n^2}^*$		Calculus for system of congruencies
	multiple	add	multiple	add	
[2]	$\log_2 \phi(n)$	-	3	1	need
[6]	$\log_2 \phi(n)$	-	$\log_2 \phi(n)$ +2	1	need
our system	$\log_2 \frac{L(n)}{2}$	-	$\log_2 \frac{L(n)}{2}$ +2	1	need not

3. CONCLUSION

We introduced a randomized RSA-type cryptosystem over quadratic remaindering group. In this cryptosystem, it is not needed to solve the system of congruencies to find the value of random parameter r for decryption. Moreover, the security of this cryptosystem is IND-CCA2 under certain assumption.

4. REFERENCES

[1] M. Bellare, P. Rogaway, Random oracles are practical: A p aradigm for designing efficient protocols, Proceedings of the 1st ACM Conference on Computer and Communications Security, pp.62-73, 1993.

[2] D. Catalano, R. Gennaro, N. Howgrave-Graham, P.Q. Nguy en, Pailler's cryptosystem revisited, Proceedings of the 8th ACM Conference on Computer and Communications Security, pp.206-214, 2003.

[3] B. Chevallier-Mames, M. Joye, Chosen-ciphertext secure RSA-type cryptosystems, 3rd International Conference on Provable Security, Guangzhou, China, pp.11-13, 2009.

[4] A. Das, A. Adhikari, An efficient IND-CCA2 secure Paillier-b ased cryptosystem, Information Processing Letters, Volume 112, Issue 22, pp.885-888, 2012.

[5] Y. Dodis, L. Reyzin, On the power of claw-free permutatio ns, Security in Communication Networks, pp. 55-73, 20 03.

[6] D. Galindo, S. Martin, P. Morillo, J.L. Villar, A practical publ ic key cryptosystem from Paillier and Rabin schemes, L NCS, vol. 2567, pp.279-291. 2003.

[7] D. Galindo, A note on an IND-CCA2 secure Paillier-based cryptosystem, Information Processing Letters, Volume113, Issue 22-24, pp.913-914, 2013.

[8] M. Joye, B. Libert, Efficient cryptosystems from 2^k-th power residue symbols, LNCS vol. 7881, pp.76-92, 2013.

[9] Y. Ren, D. Gu, Fully CCA2 secure identity based broadcast encryption without random oracles, Information Processing Letters, Volume 109, Issue 11, pp.527-533, 2009.

[10] Y. Watanabe, J. Shikata, H. Imai, Equivalence between se mantic security and indistinguishability against chosen c iphertext attacks, LNCS vol. 2567, pp.71-84, 2003.