3rd International Conference on Advances in Computing and Technology ICACT 2018

A New Public Key Cryptosystem

W. D. M. G. M. Dissanayake[1]

Department of Computer Engineering,Faculty of Engineering, University of Peradeniya, Sri Lanaka

In this paper a new CCA secure public key cryptosystem is presented. The introduced cryptosystem is simple and based on the factorization problem. The cryptosystem has two public keys and two private keys. Therefore two encryption algorithms and two decryption algorithms are in this system. Here, we hide the message in a matrix. This situation makes a difficult puzzle for adversaries. In this method, the public encryption key is (*e*,*r*,*n*), *e* and *r* are any prime numbers greater than 2 and less than *n*, *n* is a product of two large prime numbers. The decryption key is (*d*,*s*,*n*). *d* and *s* are multiplicative inverses of *e* modulo ϕ(*n*) and *r* modulo ϕ(*n*) respectively. We should select another integer g $(< 2m)$ and set the message m and g in a $2 * 2$ matrix X as the determinant of X is odd. We encrypt the determinant of the matrix by raising it to the *e*th power modulo n. We also have to send g for the decryption. g is encrypted by raising it to the *r*th power modulo n. When we decrypt the first ciphertext by raising it to another power *d* modulo n and the second ciphertext by raising it to another power *s* modulo n, we can find the message *m*. For an example, let $p = 7, q = 11, e = 23, r = 29$. Then, $n = pq = 7 \times 11 = 77, \phi(n) = 60$. Then for the private keys, $d = 47$ and $s = 29$. Let the message, $m = 30$ and $g = 7$. Then, $X = \begin{pmatrix} 30 & 7 \\ 1 & 2 \end{pmatrix}$. From the encryption equations, $C_1 \equiv [determinant(X)^e] \, mod \, n \equiv 53^{23} \, mod \, 77 \equiv 58$ and $C_2 \equiv [g^r] \, mod \, n \equiv 7^{29} \, mod \, 77 \equiv 63$. The decryption equations are $\text{Determinant}\,(X) \equiv [{C_1}^d] \, mod \, n \equiv 58^{47} \, mod \, 77 \equiv 53$ and $g \equiv [{C_2}^s] \, mod \, n \equiv 63^{29} \, mod \, 77 \equiv 7$. Then, using $2m - g = \text{Determinant}\,(X)$, we can find $m = 30$. If we use the fast exponentiation algorithm then the computational complexity of the cryptosystem is in polynomial time. The proposed cryptosystem is OW-CCA2 secure and also can use any standard security model to increase the security.

Keywords: public key cryptosystem; RSA cryptosystem; El-Gamal cryptosystem; IND security.

[1] Corresponding author: W.D.M.G.M. Dissanayake; Tel.: +94-76-883-8365
E-mail address: maheshi14d@gmail.com