IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-9, Sept. 2018 E-ISSN: 2347-2693

An Attribute Involved Non deterministic Cryptosystem using Composite Residuosity Class Problem

Sumalatha Gunnala[1*], D.S.R. Murthy[2], Shirisha Kakarla [3]

[1*]Department of Information Technology, SreeNidhi Institute of Science and Technology, Hyderabad, India
[2] Department of Computer Science and Engineering, Geethanjali College of Engineering and Technology, Hyderabad, India
[3] Department of Computer Science and Engineering, SreeNidhi Institute of Science and Technology, Hyderabad, India

[*]*Corresponding Author: sumalathagunnala23@gmal.com*

Available online at: www.ijcseonline.org

Accepted: 24/Sept/2018, Published: 30/Sept/2018

Abstract— In this paper, we design a public key encryption scheme, is based on the composite residuosity classes and having the property as randomization, also called as non- determinism. The non-deterministic nature of this cryptosystem produces dissimilar ciphertexts for a given same plaintext character on each iteration. The intractability of factorization of this scheme is achieved through the concept of composite residuosity class problem. The key involved in the encryption procedure of the scheme uses the credentials like unique identities of the sender to ensure the authenticity of the user. These identities, are also called attributes of the user, include email, Social Security Number (SSN) or Aadhaar number etc. While encrypting the message, the sender will use any of his identity value as a key in the procedure. The recipient can calculate this attribute value in the decryption procedure.

Keywords—Attributes, Composite residuosity classes, Decryption, Encryption, and Intractability.

I. INTRODUCTION

The first non-deterministic nature of the cryptosystem based on quadratic residuosity is proposed by Shafi-Goldwasser and Silvio-Micali [1]. The features of intractability of the quadratic residuosity class were demonstrated effectively in [1], owing to the composite integer N which is calculated as the product of large co-primes: p and q. Thus $N = pq$. It is difficult to find whether x is the quadratic residue modulo N, given the pair (x, N), where the following holds true: $x = y^2 \bmod N$ for some y. On the other end of transmission, the recipients use the factorization of N to form the secret key shared between the communicating parties, and decrypt the received ciphertext.

Later, Naccache and Stern [2] proposed a scheme based on residuosity of smooth degree in (Z/nZ)* , where n=pq; p and q are large primes. The problem of prime degree p over (Z/nZ)*, where $n=p^2q$, is investigated by Okamoto and Uchiyama [3] in 1998. In 1999, the Pascal Paillier [4], introduced is a non-deterministic asymmetric algorithm for public key cryptography, based on computing n-th residue classes [5] and is believed to be computationally difficult. With the further advancements in the applications for achieving the security and authentication of the plaintext, the composite residuosity played the key role. Unlike the quadratic nature of the [1], Pascal Paillier utilized the mathematical concepts of the composite residuosity assumption to achieve the intractability, in the aggressive manner, given the pair (z, n) and $z= y^n \bmod n^2$. The key task remains to determine whether the value of z is the n^{th} residue modulo n^2 or not.

Recently, the new probabilistic based public key cryptosystems based on prime residuosity over (Z/nZ)*, where $n=p^3q$, p and q are large primes, is introduced [6], in press. This system proves that having faster decryption procedure compare to the standard RSA [7] and variations of RSA [8] with 1024 bits. Instantly, the new scheme based on the randomized asymmetric key cryptosystem and involving attributes of the user is developed by G. Sumalatha et al [9]. In this, the encryption method combines the features of probabilistic public key system and the attribute based cryptosystem. This scheme provides the additional security by using credentials called attributes of the user like email, SSN or Aadhaar Number in encryption procedure. These attribute values will give the unique identity of the persons; the details of SSN and Aadhaar are given in [10]. By using these attributes in decryption procedure, the recipient can prove the authenticity of the sender.

In this paper, we propose a new cryptosystem that is based on the scheme introduced by Pascal Paillier [4], which involves decisional composite residuosity assumption, and the attribute based cryptosystem used in [8]. The scheme, discussed here, is constructed on the group $(Z/n^2Z)^*$, where n=pq; p, q are large prime numbers and the credentials of the user.

The plan of the paper is organized in the following way. In the Section 2, we define the Composite residuosity classes. The algorithms of the scheme are elaborated in Section 3. The illustration of the problem is given in Section 4. The conclusions are drawn out in section 5.

II. COMPOSITE RESIDUSITY CLASSES

In this section, we describe the definition of a composite residue. A composite residue, is also called an n-th residue is introduced by Paillier [4]. We set n=pq where p and q are large primes. In this case, we denote by $\phi(n)=(p-1)(q-1)$, the Euler's function. And we denote $\lambda = \text{lcm}(p-1, q-1)$ the least common multiple of p-1 and q-1 .

We denote by Z_n^2 is a residue class ring modulo n^2. And we denote by $(Z/n^2Z)^*$ its invertible element set. The set $(Z/n^2Z)^*$ is a multiplicative subgroup of Zn^2 of order $\phi(n^2)=n\phi(n)=pq(p-1)(q-1)$. For any x in $(Z/n^2Z)^*$, the following equations hold,

$$x^{\lambda} = 1 \pmod{n}, \tag{1}$$

$$x^{n\lambda} = 1 \pmod{n^2}. \tag{2}$$

lemma1: A number z is said to be an n-th residue modulo n^2 if there exists a number y in $(Z/n^2Z)^*$, such that

$$z = y^n \pmod{n^2}. \tag{3}$$

lemma2: Let g be some element of($Z/n^2Z)^*$ and denote by E the integer-valued function defined by,

$$Zn \text{ X } Zn^* \rightarrow (Z/n^2Z)^* \tag{4}$$

$$E(x,y) \rightarrow g^x y^n \pmod{n^2}, \tag{5}$$
where $x \in Zn$, $y \in Zn^*$

For the plaintext x, we employ this function E as an encryption function.

Sylow subgroups: The Sylow subgroup is defined as,

$$S= \{x< n^2 \mid x= 1 \bmod n\} \rightarrow Z_n \tag{6}$$

We define the Lagrange's function, as $L(x) = \frac{x-1}{n}$,where this function is used to map the x value, an element of the Sylow subgroup to the Z_n additive group.

For the ciphertext $c=e_g(x, y)$, we employ the rate of these two functions $L(c^{\lambda})$ and $L(g^{\lambda})$ as the decryption function.

III. DEVELOPMENT OF THE PROPOSED SCHEME

We now proceed to describe a public-key encryption scheme based on the Composite Residuosity Class Problem. Let the two larger primes are p, q and (Z/nZ)* be a multiplicative group (where n=pq). According to Chinese remainder theorem, the group (Z/nZ) formulated as,

$$(Z/nZ) = (Z/pZ) \times (Z/qZ). \tag{7}$$

The generator g is chosen from the cyclic group $(Z/n^2Z)^*$. The attribute value K, such as email, PAN or Aadhaar number, which provides the identity of the user is selected. This system has three algorithms: Initialization setup, Encryption and Decryption, and are discussed under.

Initialization Setup (): In the initialization setup (), two integers, p and q are chosen which are relatively prime to each other. Using the p and q values, the composite integer, n is calculated as p X q. Besides, the Carmichael's function λ is defined as λ= lcm ((p-1),(q-1)).The other secret is the unique attribute value K, which could be one of the user's identities. The generator g is determined from the cyclic group $(Z/n^2Z)^*$ such that gcd $(L(g^{\lambda} \bmod n^2), n)=1$. The outcome of this algorithm is the private key (p, q, λ) and the corresponding public key (n, g), which is published. The algorithm can be summarized as below:

Setup:
Step 1: Select two large prime numbers: p and q.
Step 2: Compute n=pq
Step 3: Select g ϵ $(Z/ n^2 Z)$,
such that gcd $(L(g^{\lambda} \bmod n^2), n)=1$
Step 4: Calculate λ= lcm ((p-1), (q-1))
Step 5: Select an attribute value k
Step 6: Public parameters: n, g
Step 7: Private parameters: p, q, λ, k

Encryption (n, g, m, k): For the encryption scheme, the plaintext m is chosen such that, m< n. The ciphertext c is calculated by using the following equation.

$$c = g^m k^n \bmod n^2. \tag{8}$$

where ***m*** is a plaintext and ***k*** is an user's identity value. The algorithm for computing ciphertext is given below:

Encryption:
Input: n, g, m, k
Step 1: plaintext $m < n$
Step 2: ciphertext $c = g^m k^n \bmod n^2$.

Decryption(c, p, q, λ): This function takes as input as cipher text c and private key parameters p, q and λ. In this decryption procedure, Sylow subgroups play a major role in the retrieval of the original message from the ciphertext.

The Lagrange's function L(x) defines the isomorphism between the Sylow subgroup and the Zn additive group. The plaintext elements m, is calculated by using following equation.

$$m = L(c^{\lambda} \bmod n^2)\, L^{-1}(g^{\lambda} \bmod n^2) \bmod n. \quad (9)$$

Where L(x) is defined as $L(x) = \frac{x-1}{n}$.

The attribute value k is retrieved through the following equation.

$$k = c(g^{-1})^m \bmod n \quad (10)$$

Decryption:
Input: (p, q , λ , c)
Step 1: ciphertext c < n^2

Step2: $m = L(c^{\lambda} \bmod n^2)\, L^{-1}(g^{\lambda} \bmod n^2) \bmod n.$

Step 3: $k = c(g^{-1})^m \bmod n$

IV. ILLUSTRATION

Let us consider two prime numbers as p=3 and q=5. Then the composite integer n is calculated as follows, n= pxq=15, thus n^2= 225.
Calculate λ= lcm (p-1, q-1), thus λ= lcm (2, 4) = 4.

Select a generator, g from the group (Z/n^2Z) given below, such that, gcd (L ($g^{\lambda} mod\ n^{2)}$, n) =1.
Therefore g is chosen as 13. The list of elements of the cyclic group (Z/n^2Z)* is given below.

(Z/n^2Z)*=
{1,2,4,7,8,11,13,14,16,17,19,22,23,26,28,29,31,32,34,37,38, 41,43,44,46,47,49, 52, 53, 56, 58,59,61, 62, 64, 67, 68, 71, 73, 74,76,77, 79, 82, 83, 86, 88, 89,91,92 , 94, 97, 98, 101, 103,104,106, 107, 109, 112, 113, 116, 118,119,121, 122, 124, 127, 128, 131, 133,134,136,137, 139, 142, 143, 146, 148, 149,151,152, 154, 157, 158, 161, 163, 164,166,167, 169, 172, 173, 176, 178, 179,181,182, 184, 187, 188, 191 , 193, 194,196, 197, 199, 202, 203, 206, 208,209,211, 212, 214, 217, 218, 221, 223, 224},

Let a plaintext message m= 5, and an attribute value k=4.
By applying the encryption algorithm given in section 3, the ciphertext is computed as follows,

$$c = g^m k^n \bmod n^2.$$
$$c = (13)^5\ (4)^{15} \bmod 225$$
$$c = 8557 \bmod 225.$$
$$c = 7$$

Applying the algorithm for decryption procedure, given in section 3, the plaintext message ***m*** and attribute value ***k*** are calculated as follows:

$$m = L(c^{\lambda} \bmod n^2)\, L^{-1}(g^{\lambda} \bmod n^2) \bmod n.$$
$$m = \frac{L(7^4 \bmod 225)}{L(13^4 \bmod 225)} \bmod 15$$
$$m = \frac{L(151)}{L(211)} \bmod 15$$

L(x) is given as

$$L(x) = \frac{x-1}{n}$$
$$L(151) = \left(\frac{151-1}{15}\right) = \frac{150}{15} = 10.$$
$$L(211) = \left(\frac{211-1}{15}\right) = \frac{210}{15} = 14.$$
$$m = \left(10 \times 14^{-1} \bmod 15\right)$$
$$m = 5$$
$$k = (c) \times (g^{-1})^m \bmod n$$
$$k = 7 \times (13^{-1})^5 \bmod 15$$
$$k = 7 \times 7^5 \bmod 15$$
$$k = 4$$

Here the original message ***m*** and the attribute value ***k*** are retrieved successfully. With the received attribute value of k, the recipient can ensure the authenticity of the sender.

V. CONCLUSION

In this paper, an attribute involved public cryptosystem is developed, based on the composite residuosity class assumption and the intractability of the factorization. This scheme involves the features of probabilistic cryptosystem and credentials (attribute value) of the sender. Here, the receiver can obtain the attribute value by using decisional composite residuosity assumption, which can be cross verified with the attribute value communicated. This ensures the authenticity of the sender. The partial homomorphism is the additional advantage that is achieved in this system.

REFERENCES

[1] S. Goldwasser and S. Micali., "Probabilistic Encryption", in Journal of Computer and System Sciences, 28, pp 270–299, 1984.
[2] D. Naccache and J. Stern, "A New Cryptosystem based on Higher Residues" , in Proc. of the 5th CCCS, pp 59–66. ACM press, 1998.
[3] T. Okamoto and S. Uchiyama, "A new public key cryptosystem as secure as factoring", in Proc. Eurocrypt '98, pp 310–318, 1998.
[4] P. Paillier, "Public-Key Cryptosystems Based on Discrete Logarithms Residues", in Eurocrypt '99, LNCS 1592, pp 223–238. Springer-Verlag, 1999.
[5] J C. Benaloh, "Verifiable Secret-Ballot Elections", PhD Thesis, Yale University, 1988.

[6] G. Sumalatha, D.S.R. Murthy and K. Shirisha , "A Secure Intractable Public Key Cryptosystem Involving p-Sylow Subgroup" , International journal of Network Security, in press.
[7] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", in Communications of the ACM, 21(2), pp120–126, 1978.
[8] V. Kapoor, "*Data Encryption and Decryption Using Modified RSA Cryptography Based on Multiple Public Keys and 'n'prime Number*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.35-38, 2013.
[9] Sumalatha Gunnala, Shirisha Kakarla and Sreerama Chandra Murthy Dasika , "An Attribute Involved Public Key Cryptosystem Based on p-Sylow Subgroups and Randomization" , Journal of Applied Computer Science & Mathematics , vol. 12, Issue 1/2018, pp 34-38, 2018.
[10] Sarita Sharma, Rakesh Gaherwal, "*Comparative Study and Analysis of Unique Identification Number and Social Security Number*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.1, pp.27-30, 2017.

Authors Profile

G. Sumalatha is currently working as Associate Professor in the Department of Information Technology, SreeNidhi Institute of Science and Technology (SNIST), Hyderabad, India. She is pursuing PhD in JNTUH. Her research interests include Information security, cryptography and compilers. She published thirteen research papers in reputed International Journals.

D.S.R. Murthy is presently working as Professor in the Department of Computer Science and Engineering (CSE), Geethanjali College of Engineering and Technology, Hyderabad, India. He published a text book on **C and Data structures.** He also published number of research papers in various international journals. Currently he is guiding six research scholars for their PhD. His research interests include Image cryptography, network security.

K. Shirisha is currently working as Professor in the Department of Computer Science and Engineering (CSE), SreeNidhi Institute of Science & Technology (SNIST), Hyderabad, India. Her research interests include Information security, cryptography, database security, and data mining. She published nineteen research papers in reputed International Journals. She stood University topper in the M.Tech.(CSE).

