International Journal of Hybrid Information Technology
Vol.8, No.3 (2015), pp.121-132
http://dx.doi.org/10.14257/ijhit.2015.8.3.12

Factoring and Discrete Logarithm using IBC

Chandrashekhar Meshram

Department of Mathematics
RTM Nagpur University, Nagpur, India
cs_meshram@rediffmail.com

Abstract

In 1984, Shamir proposed the concept of the ID-based cryptosystem (IBC). Instead of generating and publishing a public key for each user, the ID-based scheme permits each user to choose his name or network address as his public key. This is advantageous to public-key cryptosystems because the public-key verification is so easy and direct. In such a way, a large public key file is not required. Since new cryptographic schemes always face security challenges and many integer factorization and discrete logarithm based cryptographic systems have been deployed, therefore, the purpose of this paper is to design a transformation process that can transfer the entire integer factorization problem and discrete logarithm problem based cryptosystems into the ID-based systems rather than re-invent a new system. We consider the security against a conspiracy of some entities in the proposed system and show the possibility of establishing a more secure system.

Keywords: *Cryptography, Public key Cryptosystem (PKC), IBC, Discrete Logarithm Problem (DLP) and Integer Factorization Problem (IFP)*

1. Introduction

Rapid advances in computer technology and the development of the Internet are changing the way, we conduct our daily and business lives. Secrecy is an important issue with respect to sensitive data transferred over insecure public channels. In an open network environment, secret session key needs to be shared between two users before it establishes a secret communication. While the number of users in the network is increasing, key distribution will become a serious problem. In 1976, Diffie and Hellman [4] introduced the concept of the public key distribution system (PKDS). In the PKDS, each user needs to select a secret key and compute a corresponding public key and store in the public directory. The common secrete session key, which will be shared between two users can then be determined by either user, based on his own secret key and the partner's public key. Although the PKDS provides an elegant way to solve the key distribution problem, the major concern is the authentication of the public keys used in the cryptographic algorithm.

Many attempts have been made to deal with the public key authentication issue. Kohnfelder [5] used the RSA digital signature scheme to provide public key certification. His system involves two kinds of public key cryptography: one is in modulo p, where p is a large prime number; the other is in modulo N, where N = pq, and p and q are large primes. Blom [7] proposed a symmetric key generation system (SKGS) based on secret sharing schemes. The problems of SKGS however, are the difficulty of choosing a suitable threshold value and the requirement of large memory space for storing the secret shadow of each user.

In 1984, Shamir [1] introduced the concept of an identity. In this system, each user needs to visit key authentication center (KAC) and identify himself before joining the network. Once a user's identity is accepted, the KAC will provide him with a secret key.

ISSN: 1738-9968 IJHIT

In this way, a user needs only to know the “identity” of his communication partner and the public key of the KAC, together with his secret key, to communicate with others. There is no public file required in this system. However, Shamir did not succeed in constructing an IBC, but only in constructing an ID-based signature scheme. Since then, much research has been devoted, especially in Japan, to various kinds of ID-based cryptographic schemes. Okamoto, *et al.,* [6] proposed an identity-based key distribution system in 1988, and later, Ohta [10] extended their scheme for user identification. These schemes use the RSA public key cryptosystem [14] for operations in modular N, where N is a product of two large primes, and the security of these schemes is based on the computational difficulty of factoring this large composite number N. Tsujii and Itoh [2] have also proposed an IBC based on the discrete logarithm problem with single discrete exponent which uses the ElGamal public key cryptosystem.

In 1991, Maurer and Yacobi [23] developed a non-interactive ID-based public-key distribution system. In their scheme, the public keys are self-authenticated and require no further authentication by certificates. However, some problems with this scheme were found, the scheme was modified and the final version was presented [24]. In 1998, Tseng and Jan [25] improved the scheme proposed by Maurer and Yacobi, and provided a non-interactive ID-based public-key distribution system with multi-objectives such as an ID-based signature scheme, an identification scheme, and a conference key distribution system. In their scheme, the computational complexity of the system is heavy. Therefore, it is necessary to have a powerful computational capability. Harn [13] proposed public key cryptosystem design based on factoring and discrete logarithm whose security is based factoring and discrete logarithm. In 2001, Cocks [26] used a variant of integer factorization problem to construct his ID-based encryption scheme. However, the scheme is inefficient in that a plain-text message is encrypted bit-by-bit and hence the length of the output ciphertext becomes long.

In 2004, Lee & Liao [8] design a transformation process that can transfer all of the discrete logarithm based cryptosystems into the ID-based systems rather than reinvent a new system .After 2004 several IBCs [9, 15, 19, 20-22, 33-38] have been proposed. But in these schemes, the public key of each entity is not only an identity, but also some random number selected either by the entity or by the trusted authority. In 2009, Bellare, *et al.,* [11] provides security proof or attacks for a large number of ID-based identification and signature schemes. Underlying these is a framework that on the one hand helps explain how these schemes are derived and on the other hand enables modular security analyses, thereby helping to understand, simplify, and unify previous work. In 2010, Meshram [16] has also proposed cryptosystem based on double generalized discrete logarithm problem whose security is based on double generalized discrete logarithm problem with distinct discrete exponents in the multiplicative group of finite fields. After some time, Meshram presented the modification of IBC based on the double discrete logarithm problem [17, 18] and also proposed an identity based beta cryptosystem, whose security is based on generalized discrete logarithm problem and integer factorization problem [31] after some time, Meshram, *et al.,* [32] proposed the ID-based cryptographic mechanism for generalized discrete logarithm and integer factorization problem based cryptosystem.

Based on the observation that new cryptographic schemes always face security challenges and confidentiality concerns and many integer factorization & discrete logarithm-based cryptographic systems have been deployed. The major contribution of our scheme is the key generation phase, which is just a simple transformation process with low computational complexity. No modification of the original design of the discrete logarithm and integer factorization based cryptosystems is necessary. Therefore, the new scheme has the same security as the original one, and retains all of the advantages of the ID-based system.

In this study, we design IBC for discrete logarithm problem with distinct discrete exponent and integer factorization (the basic idea of the proposed system comes on the public key cryptosystem based on discrete logarithm problem and integer factorization) because we face the problem of solving integer factorization and distinct discrete logarithm problem simultaneously in the multiplicative group of finite fields as compared to the other public key cryptosystem, where we face the difficulty of solving simultaneously the integer factoring and discrete logarithm problem in the common group. Here we describe further considerations such as the security of the system, the identification for senders. *etc.*, our scheme does not require any interactive preliminary communications in each message transmission and any assumption except the intractability of the discrete logarithm problem and integer factorization problem. (This assumption seems to be quite reasonable) Thus the proposed scheme is a concrete example of an ID–based cryptosystem which satisfies Shamir's original concept [1] in a strict sense.

2. The Public Key Encryption based on Factoring and Discrete log

Let us recall first the following lemma we will use before introducing the new scheme.
Lemma 1: let p be a prime number such that $p \equiv 2 \ mod \ 3$ .Then, the function $Z_p \rightarrow Z_p$,$x \rightarrow x^3 \ mod \ p$ is a bijection with inverse function

$$Z_p \rightarrow Z_p,$$

$$x \rightarrow x^{1/3} \ mod \ p \equiv x^{\frac{(2p-1)}{3}} (mod \ p).$$

The algorithm consists of three subalgorithms: key generation, encryption and decryption

2.1. Key Generation

1. Choose two random safe prime numbers p and , compute $N = pq$.
2. Take θ a primitive element in $Z_N^* = \{z, \gcd(z, N) = 1\}$ with order $o(\theta)$.
3. Pick a random $k < o(\theta)$ and compute $A = \theta^k (mod \ N)$.

Thus, the public key is given by (N, θ) and the private key by (k).

2.2. Encryption

To encrypt a message m, the sender proceed as follows

1. He transforms the message into $m \in Z_N$.
2. He chooses an integer $s < N$ at random.
3. Compute $C_1 = \theta^s (mod \ N)$ and $C_2 = (mA^s)^3 \ mod \ N$,send them to the receiver.

2.3. Decryption

To recover the message m from the cipher text (C_1, C_2), the receiver computes

$$m' = C_2^{\frac{1}{3}} (C_1)^{-k} \ mod \ N = m (mod \ N)$$

3. Consistency of the Algorithm

$$m' = C_2^{\frac{1}{3}} (C_1)^{-k} \ mod \ N = (\theta^{-sk} m \theta^{sk}) mod \ N = m \ mod \ N$$

Note that the equation $x^3 \equiv C_2 mod \ N$ has only one solution since it has a unique solution modulo p and a unique solution modulo q by Lemma 1. Using the Chinese

Remainder Theorem, we recover the unique solution of the equation modulo n. The fact we have here a single solution of the cubic equation is a great advantage from the Rabbin scheme where, we get four solution of the square equation.

4. Example

Suppose we want to cipher a message $m = 52$ with our scheme. Let's consider $p = 17$ and $q = 23$ and $N = pq = 493$. Remark that $p \equiv q \equiv 2\, mod\, 3$. Let $\theta = 13$ and choose $k = 7$. Then, the public key is given by $A = \theta^{k} (mod\, N)$., n and the private key by p, q and k. To encrypt the message $m = 52$, let's select $s = 19$. We then compute

$$C_1 = \theta^{s} (mod\, N) = 412 \text{ and } C_2 = (mA^{s})^{3}\, mod\, N = 361$$

For the decryption, we solve first the equations $x^{3} \equiv 361 mod\, 17$ an equations $x^{3} \equiv 361 mod\, 23$. The solutions of these equations are respectively $x = 13$ and $x = 9$. By the Chinese Remainder Theorem, we find $C_2^{\frac{1}{3}}\, mod\, N = 64$. We compute next $(C_1)^{-k}\, mod\, N = 463$ and find $m = 64 \times 463\, mod\, 493 = 52$.

5. Implementation of the IBC

5.1. Preparation for the Center and Each Entity

Step 1. Each entity generates a k-dimensional binary vector for his ID. We denote entity $i's$ ID by ID_i as follows:

$$\mathrm{ID}_i = (x_{i1} \quad , \quad x_{i2}, x_{i3}, x_{i4}, \dots \dots \dots, x_{ik}), x_{ij} \in \{0,1\}, (1 \leq j \leq k)$$
(1)

Each entity registers his ID with the center, and the center stores it in a public file.

Step 2.: The center publishes a one-to- one function $f(.)$ *e.g.,* to all entities. Any entity can compute the entity i's extended ID, EID_i by the following:

$$\mathrm{EID}_i = f(\mathrm{ID}_i)(mod\ N) \; = (y_{i1}, y_{i2}, y_{i3}, y_{i4}, \dots \dots \dots, y_{it}), y_{ij} \in \{0,1\}, (1 \leq j \leq t)$$
(2)

where $t = |n|$ is the number of bits of n.

Step 3. Center's secrete information: The center chooses an arbitrary large prime p and q computes $N = pq$ and also generate n-dimensional vector $\vec{a}$ over $Z^{*}_{\varphi(N)}$ which satisfies

$$\vec{a} = (a_1, a_2, a_3, \dots \dots, a_n) \tag{3}$$

$$1 \leq a_i \leq \varphi(N), \quad (1 \leq i \leq n)$$

$$aI \neq aJ \left(mod\, \varphi(N)\right), I \neq J \tag{4}$$

where I and J are n-dimensional binary vector and stores it as the centers secret information. The condition of Eq. (4) is necessary to avoid the accidental coincidence of some entities secrete keys. A simple way to generate the vector $\vec{a}$ is to use the Merkle and Hellman scheme [12].

The center chooses a super-increasing sequences corresponding to a as $a'_i\ (1 \leq i \leq n)$ satisfies

$$\textstyle\sum_{1 \leq i \leq n} a'_i < \varphi(N)$$
(5)

Step 4: The center also chooses w such that $\gcd(w, \varphi(N)) = 1$, and computes n-dimensional vector $\vec{a}$ as follows

$$a_i = a'_i w(mod\, \varphi(N))(1 \leq i \leq n), \tag{6}$$

where

$$\vec{a} = (a_1, a_2, a_3, \ldots, a_n) \qquad ,$$

(7)

Remark 1: It is clear that the vector $\vec{a}$ defined by Eq.(7) satisfies the Eqs. (3)-(4) the above scheme is one method of generating n vectors $\vec{a}$ satisfies Eqs. (3)-(4). However, another method might be possible.

Step 5: Center public information: The center chooses an arbitrary generator θ of $Z^*_{\varphi(N)}$ and computes n-dimensional vector h using generator θ corresponding to the vector.

$$h = (h_1, h_2, h_3, \ldots \ldots, h_n) \qquad ,$$

(8)

$$h_i = \theta^{a_i} mod\ N \qquad\qquad (1 \le i \le n) \qquad ,$$

(9)

The center informs each entity (N, θ, h) as public information.

Step 6: Each entity secrete key: Entity $i's$ secrete keys s_i is computed by inner product of a (the centre's secret information) and EID_i (entity $i's$ extended ID, see Eq.2)

$s_i = a\ \mathrm{EID}_i(mod\ \varphi(N))$ = $\sum_{1 \le j \le n} a_j y_{ij}\ mod\ (\varphi(N))$ (10)

6. System Initialization Parameters

6.1 Center Secrete Information

a : n -dimensional vector {see Eqs. (6)-(7)}

6.2 Center Public Information

h : n -dimensional vector see Eqs. (8-9)} , N: large prime numbers , f: one –to –one function , θ : generator of $Z^*_{\varphi(N)}$.

6.3 Entity $i's$ Secretes Keys : (s_i) {see Eq. (10)}

6.4 Entity $i's$ public information: ID_i is a k −dimensional vector {see Eq. (1)}

7. Proposed IBC

Without loss of generality, we suppose that entity 2 sends message m to entity 1.

7.1 Encryption

Entity 2 generates EID_1 (entity $1's$ extended ID, see Eq.2) from ID_1. It then computes γ_1 from corresponding public information h and EID_1 :

$$\gamma_1 = \prod_{1 \le i \le n} h_i^{\ y_{1i}} (mod\ N)$$
$$= \prod_{1 \le i \le n} (\theta^{a_i})^{y_{1i}} (mod\ N)$$
$$= \theta^{\sum_{1 \le i \le n} a_i y_{1i} mod\ (\varphi(N))} (mod\ N)$$
$$= \theta^{s_1} (mod\ N)$$

(11)

Entity 2 will use γ_1 in our propose scheme. Let $m \in Z_N$ be a message to be transmitted. Entity 2 is select a random integer $r < N$ and computes the cipher text C as follows

$C = (C_1, C_2)$

$$C_1 \equiv \theta^r (mod\, N)$$

(13)

$$C_2 \equiv m(A^{s_1})^3 (mod\, N)$$

(14)

The cipher text is given by $C = (C_1, C_2)$

7.2 Decryption

To recover the plaintext m from the cipher text

Entity 1 does the following:

Computes $C_1{}^{-s_1} (mod\, N) \equiv (\theta^r)^{-s_1} (mod\, N) = (\theta^{-rs_1})(mod\, N)$

Using his secrete key s_1, recovered entity 2's the message m by Eqs. (11) and (14) to computes

$$m' = \left(C_1{}^{-s_1}\, C_2{}^{\frac{1}{3}}\right)(mod\, N) \equiv \theta^{-r\,s_1} m\, \theta^{r s_1} (mod\, N)$$
$$\equiv m\ (mod\, N)$$

8. Security Analysis and Discussion

In this section, we shall show six possible attacks by which an attacker may try to take down the new encryption scheme. For each attack, we define the attack and give reason why this attack could be failed.

The security of IBC based on the index problem in the multiplicative cyclic group $Z^*_{\varphi(N)}$, where $N = pq$ (The factorization of *N* is known only to the center.) where $\varphi(N)$ Euler function of n. In this system Coppersmith showed an attacking method [27] such that $(n+1)$ entities conspiracy can derive the center's secret information.

Attack 1 [27]: The $(n+1)$ entities i ,$(1 \le i \le n+1)$ can derive an n-dimensional vector *a'* over $Z^*_{\varphi(N)}$ which is equivalent (not necessarily identical) to the original center's secret information.

Proof: When $(n+1)$ entities' i ,$(1 \le i \le n+1)$ conspire, they have the following system of linear congruences:

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \vdots \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{bmatrix} (mod\ \varphi(N))$$

(15)

Since each EID_i is an n-dimensional binary vector, there exists an $(n+1)$-dimensional vector c over the integer ring such that

$$\textstyle\sum_{1 \le i \le n+1} c_i EID_i = 0$$

(16)

Thus we have

$$\textstyle\sum_{1 \le i \le n+1} c_i s_i = 0(mod\ \varphi(N))$$

(17)

And then

$$\textstyle\sum_{1 \le i \le n+1} c_i s_i = A\ \varphi(N)$$

(18)

If $A \neq 0$, Then the $(n+1)$entities can have an integer multiple of $\varphi(N)$, and they can find out the factorization of N.Then, a similar method with attack 1 is applicable. Hence, the center's secret information can be derived by $(n+1)$-entities conspiracy.

Furthermore, Shamir developed a more general attacking method [28] for the modified system such that $(n+2)$ entities conspiracy can derive the center's secret information with high probability.

Attack 2[28]: The $(n+2)$ entities i ,$(1 \leq i \leq n+2)$ can derive the center's secret information a with high probability.

Proof: When $(n+1)$ entities i ,$(1 \leq i \leq n+1)$ conspire, they have the following system of linear congruence's defied by Eq.(19)

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \vdots \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{bmatrix} (mod\ \varphi(N))$$

(19)

$$=Da(mod\ \varphi(N))$$

(20)

Assuming that the matrix D includes n linearly independent column vectors over the integer ring, there exist some positive integers c_i $(1 \leq i \leq n+1)$ such that

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \vdots \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{n+1} \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{bmatrix} - \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{n+1} \end{bmatrix} \varphi(N)$$

(21)

Thus, Eq. (21) can be rewritten by the following:

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \vdots \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \\ -1 \end{bmatrix} = - \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{n+1} \end{bmatrix} \varphi(N)$$

(22)

$$= D'a'$$

(23)

From the assumption that the matrix D in Eq. (20) includes n linearly independent column vectors over the integer ring, it follows that the matrix $D^{'}$ is nonsingular over the integer ring (*i.e.*, det $(D^{'}) \neq 0)$ with overwhelming probability, and thus, we have $a^{'} \neq (mod\ \varphi(N))$.On the other hand, we have the following system of linear congruence's:

$$D^{'}a^{'} = 0(mod\ \varphi(N))$$

(24)

If the matrix D' is nonsingular over $Z^{*}_{\varphi(N)}$, then $a' = (mod\ \varphi(N))$, and this contradicts the above results. Thus, the matrix D' is singular over $Z^{*}_{\varphi(N)}$, and we have det $(D') = 0(mod\ \varphi(N))$ with high probability. Hence, det $(D^{'})$ is divisible by $\varphi(N)$ with high probability. Furthermore, consider the case where the other $(n+1)$ entities among $(n+2)$ conspire, and define the matrix D'' in a way similar to the above. Then, det

(D'') is divisible by $\varphi(N)$ with high probability. Hence, GCD (det(D'),det (D'')) gives $e\varphi(N)$ where e is a small positive integer. By the above procedure, we can evaluate $\varphi(N)$ efficiently**.** An additional procedure to find the center's secret information is completely the same as attack 1.

Attack 3: Suppose an attacker wishes to recover all secret keys, ie p, q and k, using all informations available from the system. Then attacker needs to solve the factorization problem to find the primes p and, solve the discrete logarithm problem to find the secrete k. The best known technique to solve the FAC is by using the Number Field Sieve (NFS) [30]. Nevertheless, this method depends on the size of the modulus N. In other words, the complexity of the NFS method increases with the size of N. When $|N| = 1024$, the NFS technique is computationally infeasible. For a better security we use strong safe primes [14] p and q such that $|p| = |q| = 1024$ to maintain the same security level for the DLP over primes.

Attack 4: Assume that attacker successfully factor N. Then, he can use p and q to compute the value $m'' = C_2^{\frac{1}{3}} \, mod \, N = mA^s (mod \, N)$, by solving the cube root mod p and mod q and using the Chinese Remainder Theorem to find $C_2^{\frac{1}{3}} \, mod \, N$. However, another problem occurs: to recover the message m from mA^s, he needs to find s which is the DLP. Of course, A knows the values of p and q. But he has to solve the DLP modulo primes to find s. Since p and q are two safe primes of size 1024, the DLP modulo primes infeasible and attacker would fail.

Attack 5 Suppose attacker solves the DLP and recovers the private key. Then, he can compute θ^{sk}which is a part of the decryption but it does not suffice to recover m. To find m, attacker needs to compute $C_2^{\frac{1}{3}} \, mod \, N$. Since the factorization of n is not known, it's computationally infeasible to compute the cube root of $C_2 mod \, N$. Here again, attacker fails.

Attack 6: An attacker might try to impersonate entity 1 by developing some relation between w and w' since $\gamma_1 = Y^{ws_1} (mod \, N)$ and $\gamma_1' = Y^{w's_1} (mod \, N)$ by knowing γ_1, w, w' the attacker can derive γ_1' as $\gamma_1' = \gamma_1^{w^{-1}w'} (mod \, N)$ without knowing s_i however trying to obtain w from θ is equivalent to compute the discrete logarithm problem.

9. Enhancement of Security and Processing Cost

The center's secret information for the original system in Section 5 is derived by n entities conspiracy. In this subsection, we consider the practical countermeasure for the enhancement of the security of the system. (For simplicity, assume that n = 512 throughout this subsection.) The center partitions a 512-dimensional binary vector B into 256 segments, every two bits, such as

$$\begin{aligned} \mathrm{B} &= (\mathrm{b}_1, \mathrm{b}_2, \mathrm{b}_3, \dots \dots \mathrm{b}_{511}, \mathrm{b}_{512}) \\ &= (\mathrm{seg}_1, \mathrm{seg}_2, \mathrm{seg}_3, \dots \dots \mathrm{seg}_{511}, \mathrm{seg}_{512}) \end{aligned} \qquad (25)$$

Then, the center defines $\mathrm{a(i; jk)}\ (1 \le \mathrm{i} \le 256; \mathrm{j}, \mathrm{k} \in \{0,1\})$ appropriately, computes $\mathrm{h(i; jk)}, (1 \le \mathrm{i} \le 256; \mathrm{j}, \mathrm{k} \in \{0,1\}),$

$$\mathrm{h(i; jk)} = \theta^{\mathrm{a(i;jk)}} (\mathrm{mod\ N})$$

(26)

for each $\mathrm{seg_i}$, and publishes the table including every $\mathrm{h(i; jk)}$ to all entities. Furthermore, the center computes each entity's secret key s_k by

$$s_k = \sum_{1 \leq i \leq 256} a(i; \mathrm{seg_{ki}})(mod\ \varphi(N))$$

(27)

depending on Eq.(10).The entity k's extended identity, $\mathrm{EID_k}$, where $\mathrm{EID_k}$ is partitioned into 256 segments, every two bits such as $EID_k = (\mathrm{seg_{k1}}, \mathrm{seg_{k2}}, \mathrm{seg_{k3}}, \dots\dots \mathrm{seg_{k255}}, \mathrm{seg_{k256}})$ the center distributes it to each entity through a highly secure channel.

9.1. Encryption

Entity 2 computes γ_1' ,

$$\gamma_1' = \prod_{1 \leq i \leq 256} \mathrm{h(i; seg_{1i})}\ (\mathrm{mod\ N})$$

(28)

from $\mathrm{EID_1}$ and the published table. Entity 2 uses γ_1' as γ_1 in the original system (in Section 5) to encrypt the message m.

9.2. Decryption

This is exactly the same as in the original system in Section 5. In the original system in Section 5, the center's secret information is derived by 512 entities conspiracy, while in the above system it is derived by 1024 (= 4 x 256) entities conspiracy. Furthermore, the running cost for encryption-key generation in the above system is about half of the original system. However, the center's public information in the above system is about twice than the original system. Further generalizations, *e.g.*, each $\mathrm{EID_i}$ is partitioned into 128 segments every four bits, *etc.*, are possible.

10. Conclusion

In this present paper an IBC for integer factorization problem and discrete logarithm problem in the multiplicative group of finite fields. The proposed scheme satisfies Shamir’s original concepts in a strict sense, *i.e.*, it does not require any interactive preliminary communications in each data transmission and has no assumption that tamper free modules are available. This kind of scheme definitely provides a new scheme with a longer and higher level of security than the schemes that based on a factoring and discrete logarithm problem. The proposed scheme also requires minimal operations in encryption and decryption algorithms and thus makes it very efficient. Based on the fact that re-inventing a new scheme involves many uncertain and unknown threats, and integer factorization problem and discrete logarithm problem based schemes are widely deployed, our goal is to construct an ID-based transformation model for integer factorization problem and discrete logarithm problem based scheme rather than re-invent a new one. The concept of the ID-based system can be easily embedded into the entire integer factorization problem and discrete logarithm problem based cryptosystems without changing their original design. This solution can be directly deployed in the currently used system with very low cost. Therefore, our new scheme is more practical and has the same security as the original integer factorization problem and discrete logarithm problem based system.

References

[1] A. Shamir “Identity-based cryptosystem and signature scheme,” Advances in Cryptology: Proceedings of Crypto’ (Lecture Notes in Computer Science 196), Berlin, West Germany: Springer-Verlag, vol. 84, **(1985)**, pp. 47-53.

[2] S. Tsujii and T. Itoh “An ID-based cryptosystem based on the discrete logarithm problem”, IEEE Journal on selected areas in communications, vol. 7, **(1989)**, pp. 467-473.

[3] T. ElGmal, “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Trans. Inform. Theory, vol. 31, **(1995)**, pp. 469-472.

[4] W. Diffie and M. E. Hellman, “New direction in cryptography”, IEEE Trans. Inform. Theory, vol. 22, **(1976)**, pp. 644-654.

[5] L. M. Kohnfelder, “A method for certification,” Lab. Comput. Sci. Mass. Inst. Technol. Cambridge, MA, **(1978)** May.

[6] E. Okamoto and K. Tanaka, “Key distribution system based on identification information,” IEEE J. SeIecr. Areas Commun., vol. 7, **(1989)**, pp. 481-485.

[7] R. Blom, “An optimal class of symmetric key generation systems.” In Proc. Eurocryp ‘84, Pans, France, **(1984)** April 9-11, pp. 335-338.

[8] W. Lee and K. Liao, “Constructing identity-based cryptosystems for discrete logarithm based cryptosystems”, Journal of Network and Computer Applications, vol. 27, **(2004)**, pp. 191–199.

[9] M. Hwang, J. Lo and S. Lin, “An efficient user identification scheme based on ID-based cryptosystem”, Computer Standards & Interfaces, vol. 26, **(2004)**, pp. 565–569.

[10] K. Ohta, “Efficient identification and signature schemes”, Electron. Lett., vol. 24, **(1988)**, pp. 115-116.

[11] M. Bellare, C. Namprempre and G. Neven, “Security Proofs for Identity-Based Identification and Signature Schemes” J. Cryptol., vol. 22, **(2009)**, pp. 1–61.

[12] R. C. Merkle and M. E. Hellman, “Hiding information and signatures in trapdoor knapsacks” IEEE Trans. Inform. Theory, vol. 24, **(1978)**, pp. 525-530.

[13] L. Harn, “Public key cryptosystem design based on factoring and discrete logarithm”, IEEE Pro. Comput. Digit. Tech, vol. 141, **(1994)**, pp. 193-195.

[14] J. Gordon, “Strong RSA keys”, Electron. Lett., vol. 20, **(1984)**, pp. 514-516.

[15] E. Kiltz and Y. Vahlis, “CCA2 Secure IBE: Standard model efficiency through authenticated symmetric encryption”, In CT-RSA, Lecture Notes in Computer Science, vol. 4964, **(2008)**, pp. 221–239.

[16] C. Meshram, “A Cryptosystem based on Double Generalized Discrete Logarithm Problem”, Int. J. Contemp. Math. Sciences, vol. 6, **(2011)**, pp. 285 -297.

[17] C. Meshram, “Modified ID-Based Public key Cryptosystem using Double Discrete Logarithm Problem”, International Journal of Advanced Computer Science and Applications, vol. 1, **(2010)**, pp. 30-34.

[18] C. Meshram and S. Agrawal, “An ID-Based Public Key Cryptosystem based on Integer Factoring and Double Discrete Logarithm Problem”, Information Assurance and Security Letters, vol. 1, **(2010)**, pp. 29-34.

[19] R. Gangishetti, M. C. Gorantla, M. L. Das and A. Saxena, “Threshold key issuing in identity-based cryptosystems”, Computer Standards & Interfaces, vol. 29, **(2007)**, pp. 260–264.

[20] J. Sun, C. Zhang, Y. Zhang and Y. Fang, “An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks”, IEEE Tran. On Parall and Distributed Systems, vol. 27, **(2010)**, pp. 1227-1239.

[21] D. Boneh and M. K. Franklin, “Identity based encryption from the Weil pairing”, SIAM Journal on Computing, vol. 32, **(2003)**, pp. 586–615.

[22] D. Boneh, R. Canetti, S. Halevi and J. Katz “Chosen-ciphertext security from identity-based encryption”, SIAM Journal on Computing, vol. 5, **(2006)**, pp. 1301–1328.

[23] U. M. Maurer and Y. Yacobi, “Non-interactive public key cryptography”, Cryptology—Eurocrypt’91, New York: Springer, **(1991),** pp. 498–507.

[24] U. M. Maurer and Y. Yacobi, “A non-interactive public-key distribution system”, Des Codes Cryptogr., vol. 9, **(1996)**, pp. 305–316.

[25] Y. M. Tseng and J. K. Jan, “ID-based cryptographic schemes using a non-interactive public-key distribution system”, 14th Annual Computer Security Applications Conference, **(1998)**, pp. 237–243.

[26] C. Cocks, “An Identity Based Encryption Scheme Based on Quadratic Residues”, Cryptography and Coding - Institute of Mathematics and Its Applications International Conference on Cryptography and Coding Proceedings of IMA 2001, LNCS, Springer-Verlag, vol. 2260, **(2001),** pp. 360-363.

[27] D. Coppersmith, “private communication”, **(1987)** November.

[28] A. Shamir, “private communication”, **(1988)** June.

[29] S. Barnett, “Matrix methods for engineers and scientists”, McGraw-Hill Book Company, **(1979)**.

[30] A. K. Lenstra, H. W. Lenstra, M. S. Manesse and J. M. Pollard, “The number field sieve”, Proc. 22nd ACM Symp. On Theory of Computing, Baltimore, Maryland, USA, **(1990)**, pp. 564-572.

[31] C. Meshram and S. A. Meshram, “An Identity based Beta Cryptosystem”, IEEE Proceedings of 7th International Conference on Information Assurance and Security (IAS 2011), **(2011)** December 5-8, pp. 298-303.

[32] C. Meshram, S. A. Meshram and M. Zhang, "An ID-based cryptographic mechanisms based on GDLP and IFP", Information Processing Letters, vol. 112, **(2012)**, pp. 753–758.

[33] C. Meshram and S. Meshram, "An identity based cryptographic model for discrete logarithm and integer factoring based cryptosystem", Information Processing Letters, vol. 113, **(2013)**, pp. 375-380.

[34] C. Meshram, "An Efficient ID-based Cryptographic Encryption based on Discrete Logarithm Problem and Integer Factorization Problem", Information Processing Letters, vol. 115, **(2015),** pp. 351-358.

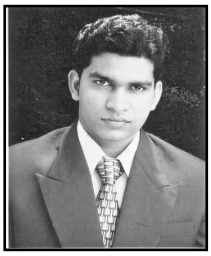
[35] C. Meshram, X. Huang and S. Meshram, "Constructing Identity-based cryptographic scheme for QER cryptosystem", International Journal of Pure and Applied Mathematics, vol. 81, no. 5, **(2012)**, pp. 737-753.

[36] C. Meshram, X. Huang and S. Meshram, "New Identity-based cryptographic scheme for IFP and DLP based cryptosystem", International Journal of Pure and Applied Mathematics, vol. 81, no. 1, **(2012),** pp. 65-79.

[37] C. Meshram, S. Meshram and C. Ram, "Constructing identity-based cryptographic scheme for beta cryptosystem", International Journal of Applied Mathematics, vol. 25, no. 5, **(2012)**, pp. 609-624.

[38] C. Meshram and S. Meshram, "Some Modification in ID-Based Cryptosystem using IFP & DDLP", International Journal of Advanced Computer Science and Applications, vol. 2, no. 8, **(2011)**, pp. 25-29.

Authors



Chandrashekhar Meshram, He received the M.Sc and M. Phil degrees, from Pandit Ravishankar Shukla University, Raipur (C.G.) in 2007 and 2008, respectively and PhD from R.T.M. Nagpur University, Nagpur (M.S.) India. Presently he is teaching as an Assistant Professor in Department of Applied Mathematics, Gyan Ganga Institute of Technology and Sciences, Jabalpur (M.P.), India. His research interested in the field of Cryptography and its Application, Boundary value problem, Statistics, Raga (Music and Statistics), Neural Network, Ad hoc Network, Number theory, Environmental chemistry, Mathematical modeling, Thermo elasticity, Solid Mechanics and Fixed point theorem. He is a member of International Association of Engineers (IAENG), Hong Kong, World Academy of Science, Engineering and Technology (WASET), New Zealand, Computer Science Teachers Association (CSTA), USA, Association for Computing Machinery (ACM), USA, International Association of Computer Science and Information Technology(IACSIT), Singapore, European Association for Theoretical Computer Science (EATCS), Greece, International Association of Railway Operations Research (IAROR), Netherland, International Association for Pattern Recognition (IAPR), New York, International Federation for Information Processing (IFIP), Austria, Association for the Advancement of Computing in Education (AACE), USA, International Mathematical Union (IMU) Berlin, Germany, European Alliance for Innovation (EAI), International Linear Algebra Society (ILAS) Haifa, Israel, Science and Engineering Institute (SCIEI), Machine Intelligence Research Labs (MIR Labs), USA, Society: Intelligent Systems, KES International Association, United Kingdom, Universal Association of Computer and Electronics Engineers (UACEE), The Society of Digital Information and Wireless Communications (SDIWC) and Life – time member of Internet Society (ISOC), USA, Indian Mathematical Society, Cryptology Research Society of India and Ramanujan Mathematical Society of India (RMS) and editor in chief of IJRRWC, UK and managing editor of IJCMST, India. He is regular reviewer of thirty International Journals and International Conferences.