I.J. Information Technology and Computer Science, **2013, 06, 65-72**
Published Online May 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2013.06.09

An Efficient IBE Scheme using IFP and DDLP

Chandrashekhar Meshram
Department of Applied Mathematics, Shri Shankaracharya Engineering College, Junwani, Bhilai (C.G), India
E-mail: cs_meshram@rediffmail.com

Abstract— In 1984, Shamir introduced the concept of an identity-based encryption. In this system, each user needs to visit a private key generation (PKG) and identify him- self before joining a communication network. Once a user is accepted, the PKG will provide him with a secret key. In this way, if a user wants to communicate with others, he only needs to know the "identity" of his communication partner and the public key of the PKG. There is no public file required in this system. However, Shamir did not succeed in constructing an identity based encryption, but only in constructing an identity-based signature (IBS) scheme. In this paper, we propose an identity based encryption (IBE) based on the factorization problem (IFP) and double discrete logarithm problem (DDLP) and we consider the security against a conspiracy of some entities in the proposed system and show the possibility of establishing a more secure system.

Index Terms— Public Key Cryptosystem, Identity Based Encryption (IBE), Discrete Logarithm Problem (DLP), Double Discrete Logarithm Problem (DDLP) and Integer Factorization Problem (IFP)

I. Introduction

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 public keys used in the cryptographic algorithm.

In 1984, Shamir [1] introduced the concept of an IBE. In this system, each user needs to visit private key generation (PKG) and identify himself before joining the network. Once a user's identity is accepted, the KAC will provide him with a secret key. In this way, a user needs only to know the "identity" of his communication partner and the public key of the PKG, 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 IBE, but only in constructing an IBS scheme. Since then, much research has been devoted, especially in Japan, to various kinds of IBE 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 [12] 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 IBE based on the DLP with single discrete exponent which uses the ElGamal public key cryptosystem.

In 2001, Boneh and Franklin, Cocks [21] used a variant of integer factorization problem to construct his IBE 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 [7] 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 IBE's [8,13,17, 18, 19, 20] 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. [10] provides security proof or attacks for a large number of IBI and IBS 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 [14] has also proposed cryptosystem based on DGDLP whose security is based on DGDLP with distinct discrete exponents in the multiplicative group of finite fields. After some time Meshram presented the modification of IBE based on the DDLP [15, 16] and also proposed an identity based beta cryptosystem, whose security is based on GDLP and IFP [26] after some time Meshram et al.[27] proposed the ID-based cryptographic mechanism for GDLP and IFP based cryptosystem.

Based on the observation that new cryptographic schemes always face security challenges and confidentiality concerns and many IFP & DLP-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 IFP & DLP 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 paper, we present an IBE on an IFP and DDLP with distinct discrete exponent (the basic idea of the proposed system comes on the public key cryptosystem based on IFP and DDLP) 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 IFP and DDLP.(this assumption seems to be quite reasonable)thus the proposed scheme is a concrete example of an IBE which satisfies Shamir's original concept [1] in a strict sense.

This paper is organized into eight sections. In Section 2, public key encryption is based on IFP and DDLP. In Section 3, the discussion consistency of the algorithm is given. In Section 4, implementation of IBE is given. In Section 5, system initialization Parameters is given. In Section 6, the discussion of IBE is given. In Section 7, the discussion of the security is given. Finally, conclusions are stated in Section 8.

II. The Public Key Encryption Based on IFP and DDLP

In this section, we introduce some notation and parameters, which will be used throughout this paper:

Two large prime numbers p and q are safe primes and set $N = p * q$. One may use method in [14] to generate strong random primes. A function $\varphi(N) = (p-1)(q-1)$ is a phi–Euler function and two integers g_1 and g_2 are primitive's elements in Z_N^* with order N satisfying $g_1^{N-1} \equiv 1(\bmod N)$ and $g_2^{N-1} \equiv 1(\bmod N)$.

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

2.1 Key generation:

The key generation algorithm runs as follows (entity A should do the following)

1. Pick random an integer $e,\ 1 \le e \le \varphi(N)$ from $Z_{\varphi(N)}^*$ such that $\gcd(e, \varphi(N)) = 1$.
2. Select two random integer a and b such that $2 \le ab \le \varphi(N) - 1.$ (with no upper bounds).
3. Compute $y_1 = g_1^a (\bmod N)$ and $y_2 = g_2^b (\bmod N)$.
4. Use the extended Euclidean algorithm to compute the unique integer $d,\ 1 \le d \le \varphi(N)$ such that $ed \equiv 1(\bmod \varphi(N))$.

The public key is formed by (N, e, y_1, y_2) and corresponding private key is given by (d, a, b)

2.2 Encryption:

A entity B to encrypt a message M to entity A should do the following:

1. Obtain public key (N, e, y_1, y_2)
2. Represented the message $M \in [1, N]$.
3. Select two random integer i and j such that $2 \le ij \le \varphi(N) - 1.$ (with no upper bounds)
4. Compute $\alpha_1 = g_1^i (\bmod N)$ and $\alpha_2 = g_2^j (\bmod N)$.
5. Compute $\beta \equiv M(y_1)^i (y_2)^j (\bmod N)$
6. Compute $C_1 \equiv \alpha_1{}^e (\bmod N)$, $C_2 \equiv \alpha_2{}^e (\bmod N)$ and $\gamma \equiv \beta^e (\bmod N)$.

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

2.3 Decryption:

To recover the plaintext M from the cipher text C , entity A should do the following:

1. Compute $C_1^{\varphi(N)-a} (\bmod N) = C_1^{-a} (\bmod N)$ and $C_2^{\varphi(N)-b} (\bmod N) = C_2^{-b} (\bmod N)$.
2. Recover the plaintext M by compute $\left(C_1^{-a}, C_2^{-b}, \gamma\right)^d (\bmod N)$.

III. Consistency of the Algorithm

In Encryption: - $\alpha_1 \equiv g_1{}^i (\bmod N)$ and $\alpha_2 \equiv g_2{}^j (\bmod N)$ $\beta \equiv M(y_1)^i (y_2)^j (\bmod N)$, $C_1 \equiv \alpha_1{}^e (\bmod N) \equiv \left(g_1{}^i\right)^e (\bmod N) \equiv g_1{}^{ie} (\bmod N)$,

$$C_2 \equiv \alpha_2{}^e (\bmod N) \equiv \left(g_2{}^j\right)^e (\bmod N) \equiv g_2{}^{je} (\bmod N),$$

$$\gamma \equiv \beta^e (\bmod N) \equiv \left(M(y_1)^i (y_2)^j\right)^e (\bmod N)$$

In Decryption: -

$$C_1{}^{\varphi(N)-a} (\bmod N) = C_1{}^{-a} (\bmod N) = y_1{}^{-ie} (\bmod N)$$

$$C_2{}^{\varphi(N)-b} (\bmod N) = C_2{}^{-b} (\bmod N) = y_2{}^{-je} (\bmod N)$$

Then

$$\begin{aligned}&\left(C_1{}^{-a}, C_2{}^{-b}, \gamma\right)^d (\bmod N)\\ &\quad = \left(y_1{}^{-ie}, y_2{}^{-je}, M^e y_1{}^{ie} y_2{}^{je}\right)^d (\bmod N)\\ &\quad = M^{ed} (\bmod N) = M (\bmod N)\end{aligned}$$

IV. Implementation of the IBE

4.1 Preparation for the center and each entity

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

$$ID_A = \left(x_{A1}, x_{A2}, ..., x_{Ak}\right), x_{Aj} \in \{0,1\}, \quad (1 \le j \le k) \tag{1}$$

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

Step 2.: The center also chooses an unique integer $d, 1 \le d \le \varphi(N)$ such that $ed \equiv 1(\bmod \varphi(N))$. Any entity can compute the entity $A's$ extended ID, EID_A by the following:

$$EID_A \equiv (ID)^d (\bmod N) = \left(y_{A1}, y_{A2}, ..., y_{At}\right), \quad x_{Aj} \in \{0,1\}, (1 \le j \le t) \tag{2}$$

where $t = |N|$ is the numbers of bits of N .

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

$$a = \left(a_1, a_2, ..., a_n\right), \quad b = \left(b_1, b_2, ..., b_m\right) \tag{3}$$

$$1 \le a_i b_l \le p-2, \quad (1 \le i \le n), \quad (1 \le l \le m), \quad (m \le n)$$

$$abI \ne abJ (\bmod (p-1)), I \ne J \tag{4}$$

Where I and J are n-dimensional binary vector and stores it as the centers secret information. The condition of (4) is necessary to avoid the accidental coincidence of some entities secrete key. A simple ways to generate the vectors a and b is to use Merkle and Hellmans scheme [11].

The center chooses a super increasing sequences corresponding to a and b as $a_i', (1 \le i \le n)$ and $b_l', (1 \le l \le m)$ satisfies

$$\sum_{1 \le il \le n} a_i' b_l' < \varphi(N), (m \le n) \tag{5}$$

Step 4: The center also chooses a w which satisfies $\gcd(w, \varphi(N)) = 1$, also compute n-dimensional vector a and m-dimensional vector b as follows

$$a_i \equiv a_i' w (\bmod \phi(N), \; (1 \le i \le n), \quad b_l \equiv b_l' w (\bmod \phi(N), \; (1 \le l \le m) \tag{6}$$

Where

$$a = \left(a_1, a_2, ..., a_n\right), \quad b = \left(b_1, b_2, ..., b_m\right) \tag{7}$$

Remark 1: it is clear that the vector a and b defined by (7) satisfies (3)-(4) the above scheme is one method of generating m and n dimensional vectors a and b satisfies (3)-(4). In this paper, we adopt the above scheme. However, another method might be possible.

Step 5: Center public information: The center chooses two arbitrary generators α and β of $Z^*_{\varphi(N)}$ and computes n-dimensional vector h using generator α & m-dimensional vector g using generator β corresponding to the vector a and b .

$$h = \left(h_1, h_2, ..., h_n\right), \quad g = \left(g_1, g_2, ..., g_m\right) \tag{8}$$

$$h_i = \left(\alpha^{ai}\right)^e (\bmod N), (1 \le i \le n),$$

$$g_i = \left(\beta^{bl}\right)^e (\bmod N), (1 \le l \le m) \tag{9}$$

The center informs each entity $(N, e, \alpha, \beta, h, g)$ as public information.

Step 6: Each entity secrete key: Entity $A's$ secrete keys s_a and s_b are given by inner product of a and b (the centre's secret information) and EID_A (entity $A's$ extended ID, see eqn.2)

$$s_a \equiv aEID_A (\mathrm{mod}\,\varphi(N)) = \sum_{1\le j\le n} a_j y_{Aj} (\mathrm{mod}\,\varphi(N)) \quad (10)$$

$$s_b \equiv bEID_A (\mathrm{mod}\,\varphi(N)) = \sum_{1\le j\le n} b_j y_{Aj} (\mathrm{mod}\,\varphi(N)) \quad (11)$$

V. System Initialization Parameters

5.1 Center Secrete information

a : n -dimensional vector, b : m-dimensional vector and d : - is an integer {see (7)-(8)}

5.2 Center public information

h : n -dimensional vector & g : m-dimensional vector {see (10-11)} p and q : large prime numbers, e : random integers , two generator α and β of $Z^*_{\varphi(N)}$.

5.3 Entity A's secrete keys

(s_a, s_b) {see (10, 11)}

5.4 Entity A's public information

ID_A is a $k-$dimensional vector {see (1)}

VI. Protocol of IBE scheme

Without loss of generality suppose that entity B wishes to send message M to entity A.

6.1 Encryption

Entity B generates EID_A (Entity $A's$ extended ID, see eqn.2) from ID_A. It then computes γ_1 and γ_2 from corresponding public information h and g and EID_A :

$$\gamma_1 = \prod_{1\le i\le n} h_i^{\,y_{Ai}} (\mathrm{mod}\,N) = \prod_{1\le i\le n} \left(\alpha^{a_i}\right)^{y_{Ai}} (\mathrm{mod}\,N)$$
$$= \alpha^{\sum_{1\le i\le n} a_i y_{Ai} \,\mathrm{mod}(\varphi(N))} (\mathrm{mod}\,N)$$
$$= (\alpha^{sa})^e (\mathrm{mod}\,N)$$

$$\gamma_2 = \prod_{1\le l\le m} g_l^{\,y_{Al}} (\mathrm{mod}\,N) = \prod_{1\le i\le n} (\beta^{b_l})^{y_{Al}} (\mathrm{mod}\,N)$$
$$= \beta^{\sum_{1\le l\le m} b_l y_{Al} \,\mathrm{mod}(\varphi(N))} (\mathrm{mod}\,N)$$
$$= (\beta^{sb})^e (\mathrm{mod}\,N)$$

Entity B use γ_1 and γ_2 in Public key cryptosystem based on IFP and DDLP.

Let $M, (1 \le M \le N)$ be entity $B's$ message to be transmitted. Entity B select two random integer u and v such that $(2 \le uv \le \varphi(N)-1)$ and computes

$$Y_1 \equiv \alpha^u (\mathrm{mod}\,N)$$

$$Y_2 \equiv \beta^v (\mathrm{mod}\,N)$$

$$\delta \equiv M(\gamma_1)^u(\gamma_2)^v (\mathrm{mod}\,N) = M\left(Y_1^{s_a} Y_2^{s_b}\right)(\mathrm{mod}\,N)$$

And compute

$$C_1 \equiv (Y_1)^e (\mathrm{mod}\,N)$$

$$C_2 \equiv (Y_2)^e (\mathrm{mod}\,N)$$

$$E \equiv (\delta)^e (\mathrm{mod}\,N)$$

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

6.2 Decryption

To recover the plaintext M from the cipher text Entity A should do the following

Compute $C_1^{\varphi(N)-s_a} (\mathrm{mod}\,N) = C_1^{-s_a} (\mathrm{mod}\,N)$

And $C_2^{\varphi(N)-s_b} (\mathrm{mod}\,N) = C_2^{-s_b} (\mathrm{mod}\,N)$

Recover the plaintext $M = \left(C_1^{-s_a} C_2^{-s_b} E\right)^d (\mathrm{mod}\,N)$

VII. Security Analysis

The security of ID-based cryptosystem based on the indexproblem in the multiplicative cyclic group $Z^*_{\varphi(N)}$, where $N = p * q$ (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 [22] such that $(n+1)$ entities conspiracy can derive the center's secret information.

Attack 1 [22]: 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 congruence's:

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ a_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ s_{n+1} \end{bmatrix} (\bmod \varphi(N)) \tag{12}$$

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

$$\sum_{1 \le i \le n+1} c_i EID_i = 0 \tag{13}$$

Here we have

$$\sum_{1 \le i \le n+1} c_i s_i = 0 (\bmod \varphi(N)) \tag{14}$$

And thus

$$\sum_{1 \le i \le n+1} c_i s_i = A\varphi(N) \tag{15}$$

If $A \ne 0$, 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 [23] for the modified system such that $(n+2)$ entities conspiracy can derive the center's secret information with high probability.

Attack 2 [23]: The $(n+2)$ entities $i, (1 \le i \le n+2)$ can derive the center's secret information a with high probability.

Proof: When $(n+1)$ entities $i, (1 \le i \le n+1)$ conspire, they have the following system of linear congruence's defied by (16)

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ a_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ s_{n+1} \end{bmatrix} (\bmod \varphi(N)) \tag{16}$$

$$= Da (\bmod \varphi(N)) \tag{17}$$

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

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ a_{n+1} \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ s_{n+1} \end{bmatrix} - \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ c_{n+1} \end{bmatrix} \varphi(N) \tag{18}$$

Thus (18) can be rewritten by the following:

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \\ \\ \\ a_n \\ -1 \end{bmatrix} = -\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ c_{n+1} \end{bmatrix} \varphi(N) \tag{19}$$

$$= D'a' \tag{20}$$

From the assumption that the matrix D in equation (17) 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 $a' \neq (\bmod\, \varphi(N))$. On the other hand, we have the following system of linear congruence's:

$$D'a' = 0(\bmod\, \varphi(N)) \tag{21}$$

If the matrix D' is nonsingular over $Z^*_{\varphi(N)}$, then $a' = (\bmod\, \varphi(N))$, and this contradicts the above results. Thus, the matrix D is singular over $Z^*_{\varphi(N)}$, and we have det $D' = 0(\bmod\, \varphi(N))$ 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. Also, 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 IFP to find the primes p and q , solve the DDLP to find the secrete k. The best known technique to solve the IFP is by using the Number Field Sieve (NFS) [25]. 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 [12] p and q such that $|p| = |q| = 1024$ to maintain the same security level for the DDLP over primes.

Attack 4: An attacker might try to impersonate user A by developing some relation between w and w' since $\gamma_1 \equiv Y^{ws_a} (\bmod\, N)$ and $\gamma_1' \equiv Y^{w's_a} (\bmod\, N)$ Similarly $\gamma_2 \equiv Y^{ws_b} (\bmod\, N)$ and $\gamma_2' \equiv Y^{w's_b} (\bmod\, N)$ by knowing $\gamma_1, \gamma_2, w, w'$ the intruder can derive γ_1' and γ_2' as $\gamma_1' = \gamma_1^{w^{-1}w'} (\bmod\, N)$ and $\gamma_2' = \gamma_2^{w^{-1}w'} (\bmod\, N)$ without knowing s_a and s_b however trying to obtain w from α and β is equivalent to compute the DDLP.

VIII. Conclusion

We discussed IBE based on IFP and DDLP in the multiplicative group. 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 that based on a IFP and DDLP in the multiplicative group. It is also requires minimal operations in encryption and decryption algorithms and thus makes it is very efficient. The present paper provides the special result from the security point of view, because we faced the problem of solving factoring with double and triple distinct discrete logarithm problem simultaneously at the same time in the multiplicative group as compared to the other public key cryptosystem.

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, 1985, vol. 84, pp. 47-53.

[2] S. Tsujii, and T. Itoh "An ID-based cryptosystem based on the discrete logarithm problem" IEEE Jounral on selected areas in communications, 1989 vol. 7, pp. 467-473.

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

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

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

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

[7] Wei-Bin Lee and Kuan-Chieh Liao “Constructing identity-based cryptosystems for discrete logarithm based cryptosystems” Journal of Network and Computer Applications, 2004, vol. 27, pp. 191–199.

[8] Min-Shiang Hwang, Jung-Wen Lo and Shu-Chen Lin “An efficient user identification scheme based on ID-based cryptosystem” Computer Standards & Interfaces, 2004, vol. 26, pp. 565–569.

[9] K. Ohta, “Efficient identification and signatureschemes.” *Electron. Lett.,* 1988,vol. 24, no. 2, pp. 115-116.

[10] Mihir Bellare , Chanathip Namprempre and Gregory Neven “Security Proofs for Identity-Based Identification and Signature Schemes” J. Cryptol. , 2009, vol. 22, pp. 1–61.

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

[12] J. Gordon “Strong RSA keys” Electron. Lett. .1984, vol.20, no.12, pp. 514-516.

[13] Eike Kiltz and Yevgeniy Vahlis. “CCA2 Secure IBE: Standard model efficiency through authenticated symmetric encryption” In CT-RSA, Vol. 4964 of Lecture Notes in Computer Science 2008, pp 221–239. Springer.

[14] Chandrashekhar Meshram “A Cryptosystem based on Double Generalized Discrete Logarithm Problem” Int. J. Contemp. Math. Sciences, 2011, Vol. 6, no. 6, 285 -297.

[15] Chandrashekhar Meshram “Modified ID-Based Public key Cryptosystem using Double Discrete Logarithm Problem” International Journal of Advanced Computer Science and Applications, 2010,Vol. 1, No.6, pp.30-34.

[16] Chandrashekhar Meshram & Shyam Sundar Agrawal “An ID-Based Public Key Cryptosystem based on Integer Factoring and Double Discrete Logarithm Problem” Information Assurance and Security Letters, 2010, vol.1,pp. 29-34.

[17] Raju Gangishetti, M. Choudary Gorantla, Manik Lal Das, Ashutosh Saxena “Threshold key issuing in identity-based cryptosystems” Computer Standards & Interfaces, 2007, vol.29, pp.260–264.

[18] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang“An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks” IEEE Tran. On Parall. and Distributed Systems, 2010, vol.27, no.9,pp. 1227-1239.

[19] Dan Boneh and Matthew K. Franklin. “Identity based encryption from the Weil pairing” SIAM Journal on Computing, 2003, Vol.32 (3), pp.586–615.

[20] Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz “Chosen-ciphertext security from identity-based encryption” SIAM Journal on Computing, 2006,Vol.5 (36), pp.1301–1328.

[21] 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 2260, pp. 360-363, Springer-Verlag, (2001)}.

[22] D. Coppersmith “private communication” Nov. 1987.

[23] A. Shamir “private communication” June 1988.

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

[25] 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.

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

[27] Chandrashekhar Meshram, Suchitra A.Meshram and Mingwu Zhang “An ID-based cryptographic mechanisms based on GDLP and IFP” Information Processing Letters, 2012, vol. 112, no 19, pp. 753–758.

Author Profile

Chandrashekhar Meshram received the M.Sc and M.Phil degrees, from Pandit Ravishankar Shukla University, Raipur (C.G.) in 2007 and 2008, respectively and pursuing PhD from R.T.M. Nagpur University, Nagpur (M.S.) India. Presently he is teaching as an Assistant Professor in Department of Applied Mathematics, Shri

Shankaracharya Engineering College, Junwani, Bhilai, (C.G.) 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.

How to cite this paper: Chandrashekhar Meshram,"An Efficient IBE Scheme using IFP and DDLP", International Journal of Information Technology and Computer Science(IJITCS), vol.5, no.6, pp.65-72, 2013. DOI: 10.5815/ijitcs.2013.06.09