**Bulletin of Electrical Engineering and Informatics**
Vol. 4, No. 2, June 2015, pp. 160~168
ISSN: 2089-3191


# Discrete Logarithm and Integer Factorization using ID-based Encryption

**Chandrashekhar Meshram**
Department of Mathematics, RTM Nagpur University, Nagpur, India
email: cs_meshram@rediffmail.com

***Abstract***

*Shamir proposed the concept of the ID-based Encryption (IBE) in [1]. 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 anddiscrete logarithm based cryptographic systems have been deployed, therefore, the purpose of this paper is to design a transformation process that can transfer the entire discrete logarithm and integer factorization 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****: Public key Cryptosystem (PKC), ID-based Encryption (IBE), Discrete Logarithm (DL) and Integer Factorization (IF)*

## 1. Introduction

In 1984, Shamir [1] introduced the concept of an identity-based cryptography. 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. 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 ID-based cryptosystem, 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. [2] proposed an identity-based key distribution system in 1988, and later, Ohta [3] extended their scheme for user identification. These schemes use the RSA public key cryptosystem [4] 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 [5] have also proposed an ID-based cryptosystem based on the discrete logarithm problem with single discrete exponent which uses the ElGamal public key cryptosystem.

In 1991, Maurer and Yacobi [6] 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 [7]. In 1998, Tseng and Jan [8] 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 [9] proposed public key cryptosystem design based on factoring and discrete logarithm whose security is based factoring and discrete logarithm. In 2001, Bonehet. al [10] 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.

*Received October 9, 2014; Revised December 23, 2014; Accepted January 16, 2015*

In 2004, Lee & Liao [11] 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 ID-based cryptosystems [12, 13, 14, 15,16,17,18,19, 20, 21, 22, 23,24, 25, 26, 27] 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. [28] 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. 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.

As outlined in the above, unfortunately we found that the entire existing IBE scheme based on discrete logarithm and integer factorization cannot be regarded as secure. Therefore, we design IBE for discrete logarithm with distinct discrete exponent and integer factorization (the basic idea of the proposed system comes on the public key cryptosystem based on discrete logarithm and integer factorization) because we face the problem of solving integer factorization and distinct discrete logarithm 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 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 and integer factorization.(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 conept [1] in a strict sense.

The remainder of this paper is organized as follows: Section 2, presented proposed PKC based on disecrete logarithm and integer factorization. Section 3, explains consistency of the algorithm. Section 4, describes implementation of the IBE.Section 5 describes protocol of the proposed IBE. Section 6, discussed security analysis and discussion of the IBE. Section 7, discussed enhancement of security and processing cost**.** Conclusion is given in the final section8.

## 2. PKC based on DL and IF

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 $N = pq$ ,one may use methodin [29] to generate strong random primes. A function $\varphi(N) = (p-1)(q-1)$ is a phi–Euler function and an integer $g$ is primitive element in $Z_N^*$with order $n$ such that $g^{n-1} \equiv 1\ (mod N)$ .

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

**Key generation:** The key generation algorithm runs as follows (entity 1 should do the following)

1. Pick random an integer$e < N$from $Z_{\varphi(N)}^*$ such that $gcd(e, N) = 1$.
2. Select a random integer$x < N$ and Compute $y = g^x (mod N)$ .
3. Use the extended Euclidean algorithm to compute the unique integer$d$, $1 \leq d \leq \varphi(N)$ such that$ed \equiv 1\ (mod \varphi(N))$.

The public key is formed by $(N, e, y)$ and the corresponding private key is given by $(d, x)$.

**Encryption:** A entity 2 to encrypt a message $M$ to entity 1 should do the following:

1. Obtain public key $(N, e, y)$.
2. Represent the message as $M \in [1, N]$.
3. Select a random integer $x < N$.

4. Compute $C_1 = g^r(modN)$ and$C_2 = (My^{-r})^e(modN)$.
The cipher text is given by $C = (C_1, C_2)$

**Decryption:** To recover the plaintext $M$ from the cipher text$C$, entity does the following:
1. Compute $C_1^x C_2^d \equiv M(modN)$
2. Recover the plaintext M.

## 3. Consistency of the Algorithm

$$\begin{aligned} C_1^x C_2^d &\equiv [(My^{-r})^e]^d (g^r)^x (modN) \\ &\equiv (My^{-r})g^{rx}(modN) \\ &\equiv (Mg^{-rx})g^{rx}(modN) \\ &\equiv M(modN) \end{aligned}$$

## 4. 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 $i's$ ID by $\mathrm{ID}_i$ as follows:

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

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

***Step 2.***: The center generates two random prime numbers $p$ and $q$ ,compute

$$N = pq \quad (2)$$

Then the center chooses an arbitrary random number , $1 \le e \le \varphi(N)$ such that $\gcd(e, \varphi(N)) = 1$ where $\varphi(N) = (p-1)(q-1)$ is the Euler function of $N$, then the center publishes$(e, N)$ as the public key. Any entity can compute the entity i's extended ID, $\mathrm{EID}_i$by the following:

$$\begin{aligned} \mathrm{EID}_i &= (\mathrm{ID}_i)^e (mod\ N) \\ &= (y_{i1}, y_{i2}, y_{i3}, y_{i4}, \dots\dots\dots, y_{it}),\ y_{ij} \in \{0,1\},\ (1 \le j \le t) \end{aligned} \quad (3)$$

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

$$\vec{a} = (a_1, a_2, a_3, \dots\dots, a_n) \quad (4)$$

$$1 \le a_i \le \varphi(N), (1 \le i \le n)$$
$$aI \ne aJ\big(mod\varphi(N)\big)\ ,\ I \ne J \quad (5)$$

where $I$ and $J$ are n-dimensional binary vector and stores it as the centers secret information. The condition of equation (5) 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 [30].
The center chooses a super-increasing sequences corresponding to $a$ as $a_i'(1 \le i \le n)$ satisfies $\sum_{1 \le i \le n} a_i' < \varphi(N)$ (6)

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

$$a_i = a_i' w (mod \varphi(N)) (1 \le i \le n), \quad (7)$$

where

$$\vec{a} = (a_1, a_2, a_3, \dots, a_n), \quad (8)$$

Remark 1: It is clear that the vector $\vec{a}$ defined by Eq. (8) satisfies the Eqs. (4)-(5) the above scheme is one method of generating $n$ vectors $\vec{a}$ satisfies Eqs. (4)-(5). However, another method might be possible.

***Step 5:*** The center also chooses a unique integer $d$, $(1 \le d \le \varphi(N))$ such that

$$ed \equiv 1 \ (mod \varphi(N)) \quad (9)$$

***Step 6: Center public information*****:** The center chooses an arbitrary generator $g$ of $Z_{\varphi(N)}^*$ and computes n-dimensional vector $h$ using generator $g$ corresponding to the vector.

$$h = (h_1, h_2, h_3, \dots \dots, h_n), \quad (10)$$

$$h_i = g^{a_i} mod N (1 \le i \le n), \quad (11)$$

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

***Step 7****: **Each entity secrete key*****:** Entity $i's$ secrete keys$s_i$is computed by inner product of $a$ (the centre's secret information) and $\mathrm{EID}_i$ (entity $i's$ extended ID, see Eq.3)

$$\begin{aligned} s_i &= a \ \mathrm{EID}_i (mod \varphi(N)) \\ &= \sum_{1 \le j \le n} a_j y_{ij} \ mod \ (\varphi(N)) \end{aligned} \quad (12)$$

## 5. Protocol of the proposed IBE

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

### 5.1 Encryption

Entity 2 generates$\mathrm{EID}_1$ (entity $1's$ extended ID, see Eq.3) from $\mathrm{ID}_1$. It then computes $\gamma_1$ from corresponding public information $h$ and $\mathrm{EID}_1$ :

$$\begin{aligned} \gamma_1 &= \prod_{1 \le i \le n} h_i^{y_{1i}} (mod N) \\ &= \prod_{1 \le i \le n} (g^{a_i})^{y_{1i}} (mod N) \\ &= g^{\sum_{1 \le i \le n} a_i y_{1i} mod (\varphi(N))} (mod N) \\ &= g^{s_1} \ (mod N) \end{aligned} \quad (13)$$

Entity 2 will use $\gamma_1$ in our propose scheme. Let $M (1 \le M \le N)$ be a message to be transmitted. Entity 2 is select a random integer $r < N$ and computes the cipher text $C$ as follows

$$C = (C_1, C_2)$$

$$C_1 \equiv g^r (mod N) \quad (14)$$

$$C_2 \equiv (M y^{-r})^e (mod N) \quad (15)$$

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

### 5.2 Decryption

To recover the plaintext $M$ from the cipher text
Entity 1 does the following:
Computes $C_1{}^{s_a}(modN) \equiv (g^r)^{s_a}\ (modN)$(16)
Using his secrete key $s_1$, recovered entity 2's the message M by Eqs. (13) and (16) to computes

$$\begin{aligned}\left(C_1{}^{s_1}C_2{}^{d}\right) &\equiv g^{rs_1}[(My^{-r})^e]^d(modN)\\ &\equiv (My^{-r})g^{rs_1}(modN)\\ &\equiv (Mg^{-rs_1})g^{rs_1}(modN)\\ &\equiv M(modN)\end{aligned}$$

## 6. 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 ID-based cryptosystem 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 [31] such that $(n+1)$ entities conspiracy can derive the center's secret information.

**Attack 1** [31]: 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:

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \vdots \\ EID_{n+1} \end{bmatrix}\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{bmatrix} (mod\ \varphi(N)) \tag{17}$$

Since each $\mathrm{EID}_i$ is an n-dimensional binary vector, there exists an $(n+1)$-dimensional vector $c$over the integer ring such that

$$\sum_{1\le i\le n+1} c_i EID_i = 0 \tag{18}$$

Thus we have

$$\sum_{1\le i\le n+1} c_i s_i = 0(mod\ \varphi(N)) \tag{19}$$

And then

$$\sum_{1\le i\le n+1} c_i s_i = A\ \varphi(N) \tag{20}$$

If $A \neq 0$, 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 [32] for the modified system such that $(n+2)$ entities conspiracy can derive the center's secret information with high probability.

**Attack 2** [32]: 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 Eq. (21)

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \vdots \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{bmatrix} (mod\ \varphi(N)) \quad (21)$$

$$= Da(mod\ \varphi(N)) \quad (22)$$

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

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \vdots \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{n+1} \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_{n+1} \end{bmatrix} - \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{n+1} \end{bmatrix} \varphi(N) \quad (23)$$

Thus, Eq. (23) can be rewritten by the following:

$$\begin{bmatrix} EID_1 \\ EID_2 \\ EID_3 \\ \vdots \\ EID_{n+1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \\ -1 \end{bmatrix} = - \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{n+1} \end{bmatrix} \varphi(N) \quad (24)$$

$$= D'a' \quad (25)$$

From the assumption that the matrix $D$in Eq. (22) 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:

$$D'a' = 0(mod \varphi(N)) \quad (26)$$

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:** Anattacker wishes to obtain all secrete keys using all information available from the system. In this case, attacker needs to solve integer factorization problem and discrete logarithm problem simultaneously. The best way to factorize $N = pq$ is by using the number field sieve method (NFS) [33]. But this method is just dependent on the size of modulus$N$.It is computationally infeasible to factor a 1024-bit integer and to increase the security of our scheme; we should select strong primes [4] to avid attacks using special purpose factorization algorithms. To maintain the same security level for discrete logarithm problem with double

distinct discrete exponent, one must uses $N = pq$ with $\left(\frac{p-1}{2}\right)$ and $\left(\frac{q-1}{2}\right)$ respectively is product of two 512-bit primes.

**Attack 4**: Assume that the attacker successfully solves the factoring problem so that he knows secrete key $d$.Thus he may obtain$C_2{}^d \equiv (My^{-r})^{ed}(modN) \equiv Mg^{-rs_1}(modN)$. Unfortunately, at this stage he still does not knows secrete $s_a$ and cannot exactact the plaintext $M$ from the above expression.

**Attack 5:** An attacker is able to obtain the secrete integer $s_1$ from $\gamma_1 \equiv g^{s_1}(modN)$ . He could derive the plaintext $M$ if and only if he manages to get $My^{-r}$,but this is impossible since he learns nothing about the integer $d$.

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

## 7. Enhancement of Security and Processing Cost

The center's secret information for the original system in Section 4 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 Binto 256 segments, every two bits, such as

$$\begin{aligned} &\mathrm{B} = (\mathrm{b}_1, \mathrm{b}_2, \mathrm{b}_3, \dots \dots \mathrm{b}_{511}, \mathrm{b}_{512}) \\ &= (\mathrm{seg}_1, \mathrm{seg}_2, \mathrm{seg}_3, \dots \dots \mathrm{seg}_{511}, \mathrm{seg}_{512}) \end{aligned} \quad (27)$$

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

$$\mathrm{h(i;jk)} = \mathrm{g}^{\mathrm{a(i;jk)}}(\mathrm{modN}) \quad (28)$$

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

$$s_k = \sum_{1 \le \mathrm{i} \le 256} a(i; \mathrm{seg_{ki}})(mod\varphi(N)) \quad (29)$$

depending on Eq.(12).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 highlysecure channel.

### 7.1 Encryption

Entity 2 computes $\gamma_1'$ ,

$$\gamma_1' = \prod_{1 \le \mathrm{i} \le 256} \mathrm{h}\left(\mathrm{i}; \mathrm{seg_{1i}}\right) \ (\mathrm{mod\ N}) \quad (30)$$

from $\mathrm{EID_1}$ and the published table. Entity 2 uses $\gamma_1'$as $\gamma_1$in the original system (in Section 4) to encrypt the message $M$.

### 7.2 Decryption

This is exactly the same as in the original system in Section 4. In the original system in Section 4, 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.

## 8. Conclusion

In this present paper an ID-based cryptosystem 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. 1985; 84: 47-53.
[2] E Okamoto and K Tanaka. "Key distribution system based on identification information". IEEE J. Selecr. Areas Commun. 1989; 7: 481485.
[3] K Ohta. "Efficient identification and signatureschemes". Electron. Lett. 1988; 24(2): 115-116.
[4] J Gordon. "Strong RSA keys". Electron. Lett. 1984; 20(12): 514-516.
[5] S Tsujii and T Itoh. "An ID-based cryptosystem based on the discrete logarithm problem". IEEE Jounral on selected areas in communications. 1989; 7: 467-473.
[6] UM Maurer, Y Yacobi. "Non-interactive public key cryptography". Cryptology—Eurocrypt '91. New York: Springer. 1991: 498–507.
[7] UM Maurer, Y Yacobi. "A non-interactive public-key distribution system". Des Codes Cryptogr. 1996; 9(3): 305–316.
[8] YM Tseng, JK Jan. "ID-based cryptographic schemes using a non-interactive public-key distribution system". The 14th Annual Computer Security Applications Conference. 1998: 237–243.
[9] L Harn. "Public key cryptosystem design based on factoring and discrete logarithm". IEE Pro. Comput. Digit. Tech. 1994; 141(3): 193-195.
[10] 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)}.
[11] WB Lee and KC Liao. "Constructing identity-based cryptosystems for discrete logarithm based cryptosystems". Journal of Network and Computer Applications. 2004; 27: 191–199.
[12] C Meshram and S Meshram. "An identity based cryptographic model for discrete logarithm and integer factoring based cryptosystem". Information Processing Letters. 2013; 113(10): 375-380.
[13] C Meshram. "An Efficient ID-based Cryptographic Encryption based on Discrete Logarithm Problem and Integer Factorization Problem". Information Processing Letters. 2015; 115(2): 351-358.
[14] C Meshram. "Practical IBC using Hybrid-Mode Problems; Factoring and Discrete Logarithm". Bulletin of Electrical Engineering and Informatics. 2015; 4(1), pp 73- 82.
[15] C Meshram, S Meshram and C Ram. "Constructing identity-based cryptographic scheme for beta cryptosystem". International Journal of Applied Mathematics. 2012; 25(5): 609-624.
[16] C Meshram and S Meshram. "Some Modification in ID-Based Cryptosystem using IFP & DDLP". International Journal of Advanced Computer Science and Applications. 2011; 2(8): 25-29.
[17] C Meshram. "A Cryptosystem based on Double Generalized Discrete Logarithm Problem". Int. J. Contemp. Math. Sciences. 2011; 6(6): 285 -297.

[18] C Meshram. “Modified ID-Based Public key Cryptosystem using Double Discrete Logarithm Problem”. International Journal of Advanced Computer Science and Applications. 2010; 1(6): 30-34.
[19] C Meshram, X Huang and S Meshram. “Constructing Identity-based cryptographic scheme for QER cryptosystem”. International Journal of Pure and Applied Mathematics. 2012; 81(5): 737-753.
[20] 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. 2012; 81(1): 65-79.
[21] D Boneh and MK Franklin. “Identity based encryption from the Weil pairing”. SIAM Journal on Computing. 2003; 32(3): 586–615.
[22] D Boneh, R Canetti, S Halevi, and J Katz. “Chosen-ciphertext security from identity-based encryption”. SIAM Journal on Computing. 2006; 5(36): 1301–1328.
[23] C Meshram and S Meshram. “An Identity based Beta Cryptosystem”. IEEE Proceedings of 7th International Conference on Information Assurance and Security (IAS 2011). 2011: 298-303.
[24] C Meshram, S Meshram and M Zhang. “An ID-based cryptographic mechanisms based on GDLP and IFP”. Information Processing Letters. 2012; 112(19): 753-758.
[25] C Meshram and S Meshram. “A Public Key Cryptosystem based on IFP and DLP”. International Journal of Advanced Research in Computer Science. 2011; 2(5): 616-619.
[26] C Meshram and S Meshram. “PKC Scheme Based on DDLP”. International Journal of Information & Network Security. 2013; 2(2): 154-159.
[27] C Meshram. “An efficient IBE scheme using IFP and DDLP”. International Journal of Information Technology and Computer Science. 2013; 5(6): 65-72.
[28] M Bellare, C Namprempre and G Neven. “Security Proofs for Identity-Based Identification and Signature Schemes”. J. Cryptol. 2009; 22: 1–61.
[29] S Barnett. “Matrix methods for engineers and scientists”. McGraw-Hill Book Company. 1979.
[30] RC Merkle and ME Hellman. “Hiding information and signatures in trapdoor knapsacks”. IEEE Trans. Inform. Theory. 1978; IT- 24: 525-530.
[31] D Coppersmith. “Private communication”. Nov. 1987.
[32] A Shamir. “Private communication”. June 1988.
[33] AK Lenstra, HW Lenstra, MS Manesse and JM Pollard. “The number field sieve”. Proc. 22nd ACM Symp. On Theory of Computing, Baltimore, Maryland, USA. 1990: 564-572.