Information Assurance and Security Letters 1 (2010) 029-034

An ID-Based Public Key Cryptosystem based on Integer Factoring and Double Discrete Logarithm Problem

Chandrashekhar Meshram[1], Shyam Sundar Agrawal[2]

[1] Department of Applied Mathematics
Shri Shankaracharya Engineering College, Junwani, Bhilai (C.G) India
Email: cs_meshram@rediffmail.com

[2]Disha Institute of Management & Technology, Raipur
Email: shyampkace@rediffmail.com

Abstract– In 1984, Shamir [1] introduced the concept of an identity-based cryptosystem. In this system, each user needs to visit a key authentication center (KAC) and identify him self before joining a communication network. Once a user is accepted, the KAC 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 KAC. There is no public file required in this system. However, Shamir did not succeed in constructing an identity based cryptosystem, but only in constructing an identity-based signature scheme. In this paper, we propose an id based cryptosystem based on the integer factoring and double discrete logarithm problem 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.

Key word: Public key Cryptosystem, Identity based Cryptosystem, Discrete Logarithm Problem, Double Discrete Logarithm Problem and Integer Factoring.

1. Introduction

In a network environment, secret session key needs to be shared between two users to establish 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 [5] 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 stored 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 [6] used the RSA digital signature scheme to provide public key certification. His system involves two kinds of public key cryptography: one is in modular p, where p is a large prime number; the other is in modular N, where N = pq, and p and q are large primes. Blom [12] 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 a based cryptosystem. Key authentication center (KAC) and identify him self before joining the network. Once a user 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 identity-based cryptosystem, but only in constructing an identity-based signature scheme. Since then, much research has been devoted, especially in Japan, to various kinds of ID-based cryptographic schemes. Okamoto et al. [11] proposed an identity-based key distribution system in 1988, and later, Ohta [13] extended their scheme for user identification. These schemes use the RSA public key cryptosystem [21] 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 ID- based cryptosystem based on the discrete logarithm problem with single discrete exponent which uses the ElGamal public key cryptosystem. Harn and Ren [32] proposed ID- based RSA for mulisignatures. Meshram & Agrawal [3] have also proposed an ID- based cryptosystem based on the double discrete logarithm problem with double distinct discrete exponent which uses the Public key cryptosystem based on the double discrete logarithm problem. Now we generalized this cryptosystem for integer factoring and discrete logarithm problem with distinct double discrete exponent because we face the

Received August 21, 2010

problem of solving integer factoring and double distinct discrete logarithm problem at the same time 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.

In this paper , we present an ID based cryptosystem based on an integer factoring and double discrete logarithm problem with distinct discrete exponent (the basic idea of the proposed system comes on the public key cryptosystem based on factoring and double discrete logarithm problem) 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.(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 Integer Factoring 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 $N = pq$ .one may use method in [25] 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 $g_1^{n-1} \equiv 1 (\mathrm{mod}\, N)$ and $g_2^{n-1} \equiv 1 (\mathrm{mod}\, N)$.
The algorithm consists of three sub algorithm, Key generation, Encryption and Decryption

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 $y_1 \equiv g_1^{\,a} (\mathrm{mod}\, N)$ and
   $y_2 \equiv g_2^{\,b} (\mathrm{mod}\, N)$.
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 the corresponding private key is given by (d, a, b).

Encryption: An 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 $\alpha_1 \equiv g_1^{\,i} (\mathrm{mod}\, N)$ and
   $\alpha_2 \equiv g_2^{\,j} (\mathrm{mod}\, N)$.
5. Compute $\beta \equiv M (y_1)^i (y_2)^j (\mathrm{mod}\, N)$.
5. Compute $C_1 \equiv \alpha_1^{\,e} (\mathrm{mod}\, N)$, $C_2 \equiv \alpha_2^{\,e} (\mathrm{mod}\, N)$ and $\gamma \equiv \beta^e (\mathrm{mod}\, N)$.

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

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

1. Compute $C_1^{\varphi(N)-a} (\mathrm{mod}\, N) = C_1^{-a} (\mathrm{mod}\, N)$ and $C_2^{\varphi(N)-b} (\mathrm{mod}\, N) = C_2^{-b} (\mathrm{mod}\, N)$.

2. Recover the plaintext M by compute $\left(C_1^{-a} C_2^{-b} \gamma\right)^d (\mathrm{mod}\, N)$.

3. Verification of the Algorithm

In Encryption: - $\alpha_1 \equiv g_1^{\,i} (\mathrm{mod}\, N)$ and $\alpha_2 \equiv g_2^{\,j} (\mathrm{mod}\, N)$, $\beta \equiv M (y_1)^i (y_2)^j (\mathrm{mod}\, N)$, $C_1 \equiv \alpha_1^{\,e} (\mathrm{mod}\, N) \equiv \left(g_1^{\,i}\right)^e (\mathrm{mod}\, N) \equiv g_1^{\,ie} (\mathrm{mod}\, N)$, $C_2 \equiv \alpha_2^{\,e} (\mathrm{mod}\, N) \equiv \left(g_2^{\,j}\right)^e (\mathrm{mod}\, N) \equiv g_2^{\,je} (\mathrm{mod}\, N)$, $\gamma \equiv \beta^e (\mathrm{mod}\, N) \equiv \left(M (y_1)^i (y_2)^j\right)^e (\mathrm{mod}\, N)$
In Decryption: -

$$C_1^{\varphi(N)-a} (\mathrm{mod}\, N) = C_1^{-a} (\mathrm{mod}\, N) = y_1^{-ie} (\mathrm{mod}\, N)$$
$$C_2^{\varphi(N)-b} (\mathrm{mod}\, N) = C_2^{-b} (\mathrm{mod}\, N) = y_2^{-je} (\mathrm{mod}\, N)$$

Then

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

4. Implementation of the ID –Based Cryptosystem

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 $A's$ ID by ID_A as follows:

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

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

Step 2.: The center generate two random prime number p and q and compute

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

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

$$EID_A \equiv (ID)^e (\mathrm{mod}\, N)$$
$$= (y_{A1}, y_{A2}, ..., y_{At}), x_{Aj} \in \{0,1\},\ (1 \le j \le t) \quad (3)$$

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

Step 3. Center's secrete information: - The center chooses an arbitrary large prime number 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

$$a = (a_1, a_2, ..., a_n), b = (b_1, b_2, ..., b_m) \quad (4)$$

$$2 \le a_i b_l \le \varphi(N) - 1,\ (1 \le i \le n), (1 \le l \le m), (m \le n)$$

$$abI \ne abJ (\mathrm{mod}(p-1)), I \ne J \quad (5)$$

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 key. A simple ways to generate the vectors a and b is to use Merkle and Hellmans scheme [24].

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

$$\sum_{1 \le il \le n} a_i' b_l' < \varphi(N), (m \le n) \quad (6)$$

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

$$a_i \equiv a_i' w (\mathrm{mod}\, \varphi(N)), (1 \le i \le n),$$
$$b_l \equiv b_l' w (\mathrm{mod}\, \varphi(N)), (1 \le l \le m) \quad (7)$$

Where

$$a = (a_1, a_2, ..., a_n), b = (b_1, b_2, ..., b_m) \quad (8)$$

Remark 1: it is clear that the vector a and b defined by (8) satisfies (4)-(5) the above scheme is one method of generating n and m dimensional vectors a and b satisfies (4)-(5). In this paper, we adopt the above scheme. However, another method might be possible.

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

$$ed \equiv 1 (\mathrm{mod}\, \varphi(N)) \quad (9)$$

Step 6: 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 .

$$h = (h_1, h_2, ..., h_n), g = (g_1, g_2, ..., g_m) \quad (10)$$

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

$$g_l = \beta^{b_l} (\mathrm{mod}\, N), (1 \le l \le m) \quad (11)$$

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

Step 7: 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)

$$s_a \equiv aEID_A (\mathrm{mod}\, \varphi(N))$$
$$= \sum_{1 \le j \le n} a_j y_{Aj} (\mathrm{mod}\, \varphi(N)) \quad (12)$$

$$s_b \equiv bEID_A (\mathrm{mod}\, \varphi(N))$$
$$= \sum_{1 \le j \le n} b_j y_{Aj} (\mathrm{mod}\, \varphi(N)) \quad (13)$$

5. System Initialization Parameters

5.1 Center Secrete information

a : n -dimensional vector, b m-dimensional vector and d - is an integer {see (8)-(9)}

5.2 Center public information

h : n -dimensional vector & g m-dimensional vector {see eqn.(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 eqn. (12, 13)}

5.4 Entity $A's$ public information

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

6. Protocol of the proposed cryptosystem

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 :

$$\gamma_1 = \prod_{1\le i\le n} h_i^{\,y_{Ai}} \pmod N = \prod_{1\le i\le n} \left(\alpha^{a_i}\right)^{y_{Ai}} \pmod N$$

$$= \alpha^{\sum_{1\le i\le n} a_i y_{Ai} \bmod(\varphi(N))} \pmod N \;= \alpha^{s_a} \pmod N$$

$$\gamma_2 = \prod_{1\le l\le m} g_l^{\,y_{Al}} \pmod N = \prod_{1\le i\le n} (\beta^{b_l})^{y_{Al}} \pmod N$$

$$= \beta^{\sum_{1\le l\le m} b_l y_{Al} \bmod(\varphi(N))} \pmod N \;= \beta^{s_b} \pmod N$$

Entity B use γ_1 and γ_2 in Public key cryptosystem based on integer factoring and double discrete logarithm problem.

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

$$Y_1 \equiv \alpha^u \pmod N$$

$$Y_2 \equiv \beta^v \pmod N$$

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

And compute

$$C_1 \equiv (Y_1)^e \pmod N$$

$$C_2 \equiv (Y_2)^e \pmod N$$

$$E \equiv (\delta)^e \pmod N$$

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 $C_1^{\varphi(N)-s_a} \pmod N = C_1^{-s_a} \pmod N$

And $C_2^{\varphi(N)-s_b} \pmod N = C_2^{-s_b} \pmod N$

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

7. Security Analysis

In this section, we shall show three possible attacks by which an adversary 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.

7.1 Direct Attack

Adversary wishes to obtain all secrete keys using all information available from the system. In this case, adversary needs to solve factoring and discrete logarithm problem with double distinct discrete exponent. The best way to factorize $N = pq$ is by using the number field sieve method (NFS) [28].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 [29] 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.

7.2 Factoring Attack

Assume that the adversary successfully solves the factoring problem so that he knows secrete d . Thus he may obtain $\left(C_1^{-a} C_2^{-b} \gamma\right)^d \pmod N = M^{ed} \pmod N$.

Unfortunately, at this stage he still does not knows secrete a and b and cannot extract the plaintext M from the above expression.

7.3 Discrete log Attack

An attacker should solve a discrete logarithm problem twice to obtain the private key given the public as following:

1. In this encryption the public key is given by $(N, e, \alpha, \beta, h, g)$ and the corresponding secret key is given by (d, s_a, s_b).

   To obtain the private key (s_a) he should solve the DLP

   $$s_a \equiv \log_\alpha (\alpha^{s_a}) (\text{mod } N)$$

   To obtain the private key (s_b) he should solve the DLP

   $$s_b \equiv \log_\beta (\beta^{s_b}) (\text{mod } N)$$

   This information is equivalent to computing the discrete logarithm problem over multiplicative cyclic group $Z^*_{\varphi(N)}$ and corresponding secrete key a and b will never be revealed to the public.
2. Say that attacker is able to obtain the secret integer u and v from solve the DLP as

   $u \equiv \log_\alpha Y_1 (\text{mod } N)$ and $v \equiv \log_\beta Y_2 (\text{mod } N)$

   He could derive the plaintext M if and only if he manages to get $(C_1^{-a}, C_2^{-b}, \gamma)^d (\text{mod } N)$.
3. An attacker might try to impersonate user A by developing some relation between w and w' since

   $\gamma_1 \equiv Y^{ws_a} (\text{mod } N)$ and $\gamma_1' \equiv Y^{w's_a} (\text{mod } N)$

   Similarly

   $\gamma_2 \equiv Y^{ws_b} (\text{mod } N)$ and $\gamma_2' \equiv Y^{w's_b} (\text{mod } N)$ by knowing $\gamma_1, \gamma_2, w, w'$ the intruder can derive γ_1' and γ_2' as $\gamma_1' = \gamma_1^{w^{-1}w'} (\text{mod } N)$ and $\gamma_2' = \gamma_2^{w^{-1}w'} (\text{mod } N)$ without knowing s_a and s_b however trying to obtain w from α and β is equivalent to compute the discrete logarithm problem.

8. Conclusion

In this present paper an ID-based cryptosystem based on factoring and double discrete logarithm problem with distinct discrete exponents 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 that based on a factoring and double discrete logarithm problem with distinct discrete exponents. The proposed scheme 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 face the problem of solving factoring with double and triple distinct discrete logarithm problem at the same time in the multiplicative group of finite fields as compared to the other public key cryptosystem. In other words, one must break the factoring and discrete logarithm problem with double distinct exponent systems simultaneously to break our proposed system because we face the difficulty of solving the traditional discrete logarithm problem in the common groups.

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 pp. 47-53, 1985.

[2]. S. Tsujii, and T. Itoh "An ID-Based Cryptosystem based on the Discrete Logarithm Problem"*IEEE Jounral on selected areas in communications*, vol. 7 pp 467-473, 1989.

[3]. C.S.Meshram and S.S.Agrawal "An ID-Based Cryptosystem based on the Double Discrete Logarithm Problem" *International Journal of Computer Science and Network Security*, vol.10 no.7 pp.8-13, 2010.

[4]. T. ElGmal "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Trans. Inform. Theory*, vol. 31, pp 469-472, 1995.

[5]. W. Diffie and M.E. Hellman, "New direction in Cryptography", *IEEE Trans.Inform.Theory*, vol. 22, pp 644-654, 1976.

[6]. L. M. Kohnfelder, "A method for certification," *Lab. Comput. Sci. Mass. Inst. Technol*. Cambridge, MA, May 1978.

[7]. Y. Desmedt and J. J. Quisquater, "Public-key system based on the (Is there a difference between DES and difficulty of tampering Advances in Cryptology: *Proceedings of Crypto '86 (Lec- RSA?),*" in lecture Notes in Computer Science 263). Berlin, West Germany: Springer-Verlag, pp. 111-117, 1987.

[8]. H. Tanaka, "A realization scheme for the identity-based cryptosystem "Advances in Cryptology: *Proceedings of Crypto '87 (Lecture Springer- Notes in Computer Science 293).* Berlin, West-Germany Springer Verlag, pp. 340-349, 1988.

[9]. S. Tsujii, T. Itoh, and K. Kurosawa, "ID-based cryptosystem using discrete logarithm problem," *Electron. Lett.*, vol. 23. No. 24, pp 1318- 1320, 1987.

[10]. S. C. Pohlig and M. E. Hellman, “An improved algorithm for computing logarithms over GF (p) and its cryptographic significance,” *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 106-110, 1978.
[11]. E. Okarnoto and K. Tanaka, “Key distribution system based on identification information,” *IEEE J. SeIecr. Areas Commun.* , 1989, vol. 7, pp.481485, May 1989.
[12]. R. Blorn, “An optimal class of symmetric key generation systems.” *In Proc. Eurocryp ‘84*, Pans, France, 1984, Apr. 9-11, pp. 335-338.
[13]. K. Ohta, “Efficient identification and signature schemes.” *Electron. Lett.*, vol. 24, no. 2, pp. 115-116, 1988.
[14]. Wei-Bin Lee and Kuan-Chieh Liao “Constructing identity-based cryptosystems for discrete logarithm based cryptosystems” *Journal of Network and Computer Applications*, vol. 27, pp. 191–199, 2004.
[15]. Min-Shiang Hwang, Jung-Wen Lo and Shu-Chen Lin “An efficient user identification scheme based on ID-based cryptosystem” *Computer Standards & Interfaces*, vol. 26, pp. 565–569, 2004.
[16]. Eun-Kyung Ryu and Kee-Young Yoo “On the security of efficient user identification scheme” *Applied Mathematics and Computation*, vol.171, pp. 1201–1205, 2005.
[17]. Mihir Bellare , Chanathip Namprempre and Gregory Neven “Security Proofs for Identity-Based Identification and Signature Schemes” *J. Cryptol*., vol. 22, pp. 51–61, 2009.
[18]. K. Koyama and K. Ohta, “Identity-based conference key distribution system,” in Advances in Cryptology: *Proceedings of Crypto ‘87* (Lecture Notes in Computer Science 293). Berlin, West Germany: Springer- Verlag, pp. 175-184, 1988.
[19]. T. EIGamal, “A public-key cryptosystem and a signature scheme based on discrete logarithm,” *IEEE Trans. Inform. Theory*, vol. IT- 31, pp. 469-472, 1985.
[20]. S. C. Pohlig and M. E. Hellman, “An improved algorithm for computing logarithms over GF (p) and its cryptographic significance,” *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 106-110, 1978.
[21]. K. Nakamura, E. Okamoto, K. Tanaka, and S. Miura, “private communication” Aug. 1987.
[22]. D. Coppersmith, “private communication” Aug. 1987.
[23]. R. L. Rivest, A. Shamir and L. Adelman, “A method for obtaining digital signatures and public-key cryptosystem,” *Comrnun. ACM*, vol. 21, no. 2, pp. 120-126, 1978.
[24]. R. C. Merkle and M. E. Hellman, “Hiding information and signatures in trapdoor knapsacks” *IEEE Trans. Inform. Theory*, vol. IT- 24, pp. 525-530, 1978.
[25]. S. Barnett, “Matrix methods for engineers and scientists” *McGraw-Hill Book Company*, 1979.
[26]. S.Tsujii,J.Chao and K.Araki, “A Simple ID-Based Scheme for Key Sharing” IEEE Jounral on Selected Area in Communication,vol.11,no.5, pp.730-734, 1993.
[27]. L.Harn, “Public key cryptosystem design based on factoring and discrete logarithm” *IEE Pro. Comput. Digit. Tech*, vol.141, no.3, pp.193-195, 1994.
[28]. 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*, pp. 564-572, 1990.
[29]. J. Gordon “Strong RSA keys” Electron. Lett., vol.20, no.12, pp. 514-516, 1984.
[30]. S.Narayan and U.Parampalli, “Efficient identity based signatures in the standard model” *IET Inf. Secur*. vol.2, no.4, pp. 108-118, 2008.
[31]. A. Kiayias and H.S.Zhou “Hidden identity based signatures” *IET Inf. Secur*. vol.3, no.3, pp. 119-127, 2009.
[32]. L. Harn and J. Ren “Efficient identity based RSA multisignatures” *computer and security*, vol.27, pp. 12-15, 2008.
[33]. 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*, vol.27, no.9,pp. 1227-1239, 2010.

Author Biographies

Chandrashekhar Meshram is teaching as an Assistant Professor in Department of Applied Mathematics, Shri Shankaracharya Engineering College, Junwani, Bhilai (C.G) India. He received the M.Sc (Maths) and M.Phil (Cryptography) degrees, from Pandit Ravishankar Shukla University, Raipur, Chhattisgarh, India in 2007 and 2008, respectively. He is doing his research in the field of Cryptography and its Application. He is a member of International Association of Engineers, Hong Kong, Computer Science Teachers Association (CSTA, ACM), USA and International Association of Computer Science and Information Technology (IACSIT), Singapore and Life -time member of Indian Mathematical Society and Cryptology Research Society of India.

Shyam SundarAgrawal is working as an Associate Professor in the Department of Applied Mathematics in Disha Institute of Management & Technology, Raipur, India. He received the M.Sc (Maths) and Ph.D Degree from Sambalpur University, Orissa, India in 1997 and 2008, respectively. He is doing his research where his interest includes Decision Making under Fuzzy Logic, Combinatorics and Cryptography. He is a member of IMS, ISTE India and International Association of Engineers. Computer Science Teachers Association (CSTA, ACM), USA and International Association of Computer Science and Information Technology (IACSIT), Singapore.