A Novel Untraceable Blind Signature Based on Elliptic Curve Discrete Logarithm Problem

Debasish Jena, Sanjay Kumar Jena and Banshidhar Majhi
Department of Computer Sc. & Engg.
National Institute of Technology
Rourkela, INDIA

Summary

In this paper, a novel Blind Signature Scheme (BSS) has been proposed. The scheme is based on Elliptic Curve Discrete Logarithm Problem (ECDLP). It allows a requester to obtain signature from a signer on any document, in such a way that the signer learns nothing about the message that is being signed. The scheme utilizes the inherent advantage of Elliptic Curve Cryptosystem in terms of smaller key size and lower computational overhead to its counterpart public cryptosystems such as RSA and ElGamal. The scheme has been proved to be robust, untraceable and correct. The proposed scheme can be used in various applications like E-voting, digital cash etc where anonymity of requester is required.

Key words:
Blind signature, Elliptic Curve, ElGamal, Digital Signature, RSA.

1. Introduction

In today's commercial environment, transaction over Internet must be used in conjunction with the security services of authentication and non-repudiation of origin of request(s) sent from a requester so as to prevent fraudulent action by the signer. The above said security services can be achieved by the cryptography protocol called Digital Signature. A digital signature scheme provides a way for signer to sign messages using his private key so that the signatures can later be verified by anyone else by using public key of signer.

Blind signature is a special form of digital signature, which was introduced by David Chaum in 1982 [1], in which the content of a message is blinded before signature. Blind signatures are widely used in many important cryptographic services, especially in those services that emphasize the privacy of users, such as electronic voting over Internet and untraceable payment services [2, 3]. In blind signature scheme, signer signs on the blind message using his/her private key and anyone can verify the legitimacy of the signature using signer's public key. Unlike a normal digital signature scheme, however, the signer does not learn which messages he is actually signing. This procedure can be well explained with an example taken from the familiar world of paper documents. The paper analog of a blind signature can be implemented with carbon paper lined envelopes. Putting a signature on the outside of such an envelope leaves a carbon copy of the signature on a slip of paper within the envelope [2].

The Blind Signature scheme normally satisfies the following properties [2, 4, 5].

1. *Correctness:* the correctness of the signature of a message signed through the signature scheme can be checked by anyone using the signer's public key.
2. *Authenticity*: a valid signature implies that the signer deliberately signed the associated message.
3. *Unforgeability*: only the signer can give a valid signature for the associated message.
4. *Non-re-usability*: the signature of a document can not be used on another document..
5. *Non-repudiation*: the signer can not deny having signed a document that has valid signature.
6. *Integrity*: ensure the contents have not been modified.
7. *Blindness:* the content of the message should be blind to the signer; the signer of the blind signature does not see the content of the message.
8. *Untraceability:* the signer of the blind signature is unable to link the message-signature pair even when the signature has been revealed to the public.

Blind signature scheme suggested by Camenisch et al. [6] is based on Discrete Logarithm Problem (DLP) has been proved by Harn [7] that it does not satisfy the untraceability property. Another blind signature scheme suggested by Mohammed et al. [8] is based on ElGamal, has also been proved by Hwang et al. [9] that it does not satisfy correctness property. In this scheme when the

Manuscript received June 5, 2007
Manuscript revised June 20, 2007

requester obtained the blinded signature from the signer, he/she could not unblind it to acquire the desired signature.

In this paper, we propose a new untraceable BSS based on ECDLP. The proposed scheme is based on a variation of the ElGamal signature scheme which satisfies all the properties of BSS.

The organization of this paper is as follows. In the Section 2, the concept of Blind Signature which is first proposed by Dr. Chaum's based on RSA is discussed. Basic concept of Elliptic Curve is discussed in Section 3. In Section 4, Discussion on Elliptic Curve Digital Signature based on variation of ElGamal signature scheme has been made and subsequently, the proposed scheme is elaborated. The validity of the proposed BSS has been made in section 5. Finally, Section 6 describes the concluding remarks.

2. Blind Signature based on RSA

Let us consider standard RSA public key cryptosystems, in which the public key is denoted as a pair (e,n) and the private key is denoted as a number d. Here, the modulus n is a product of two large (secret) primes $p \& q$ and the private key d is the multiplicative inverse of e modulo $(p-1)(q-1)$. For the security of the RSA system it is assumed that both $p \& q$ are sufficiently large (e.g., > 200 digit numbers), such that it is infeasible to find either the factorization of n or the private key, d given only the public key, (e,n). Let a message $m \in [0,n]$ be given for which an RSA signature is to be produced.

Let a requester sends a message m to be signed by signer using Chaum's blind signature scheme using RSA [1]. The different phases are explained below in detail.

2.1 Blinding Phase

The requester picks a blinding factor *r*, which is a random integer between *0* and *n*, and computes the value:

$$m' = m * r^{e} \bmod n \qquad \cdots\cdots(1)$$

The requester sends *m'* to the signer. The *m'* is the message to be signed by the signer as in case of general signature without knowing the original message m.

2.2 Signing Phase:

The signer signs the message m' using his/her private key d as below:

$$s' = m'^{d} \bmod n \qquad \cdots\cdots(2)$$

The signer returns s' to the requester as the blind signature.

2.3 Extraction Phase:

The requester after receiving the *s'*, he/she extracts the signature *s* as follows:

$$\begin{aligned} s &= s'/r \bmod n \\ &= m^{d} \bmod n \end{aligned} \qquad \cdots\cdots(3)$$

$$\begin{aligned} (\because s' &= (m')^{d} \bmod n \\ &= (m * r^{e})^{d} \bmod n \\ &= m^{d} r^{ed} \bmod n) \end{aligned}$$

So, the requester finds the actual signature of m as (m,s) which satisfies (3). Fig. 1 depicts the Chaum's Blind signature scheme in terms of message communicated between requester and signer.

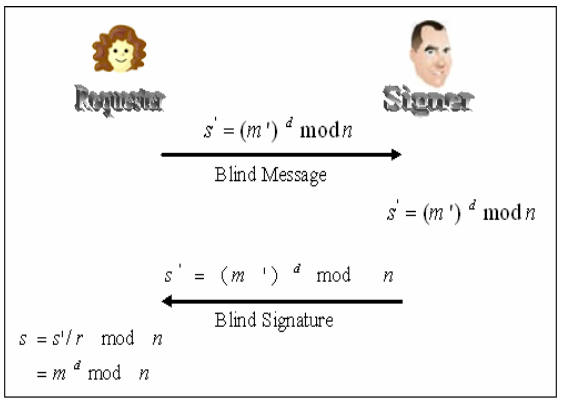

Fig.1: Chaum's Blind Signature Scheme based on RSA

3. Elliptic Curve over Finite Field

The use of Elliptic Curve Cryptography was initially suggested by Neal Koblitz [10] and Victor S. Miller [11] and after that many researchers have suggested different application of Elliptic Curve Cryptosystems. Elliptic curve cryptosystems over finite field have some advantages like the key size can be much smaller compared to other cryptosystems like RSA, Diffie-Hellman since only exponential-time attack is known so far if the curve is carefully chosen [12] and elliptic curve discrete logarithms might be still intractable even if factoring and multiplicative group discrete logarithm are broken. ECC is also computationally efficient than the first generation public key systems such as RSA and Diffie-Hellman.

3.1 Elliptic Curve Groups over F_q

A non-super singular Elliptic curve E over F_q can be written as:

$$E: \quad y2 \mod q = (x^3 + ax + b) \mod q$$
$$where\ (4a^3 + 27b) \bmod q \neq 0 \qquad \cdots\cdots(4)$$

The points $p = (x, y) \quad where\ x, y \in F_q$. $P(x, y)$ that satisfy the equation (4) together with a "point of infinity" denoted by O form an abelian group $(E,+,O)$ whose identity element is O.

3.1.1 Adding distinct points *P* and *Q*

The negative of the point $P = (x_1, y_1)$ is the point $-P = (x_1,-y_1)$. If $P(x_p, y_p)$ and $Q(x_q, y_q)$ are two distinct points such that P is not $-Q$, then

$$P + Q = R \qquad \cdots\cdots(5)$$
$$where \qquad R = (x_r, y_r)$$
$$s = (y_p - y_q)/(x_p - x_q) \bmod q,$$
$$s\ is\ the\ slope\ of\ the\ line\ passing$$
$$through\ P\ and\ Q.$$
$$x_r = (s^2 - x_p - x_q) \bmod q$$
$$and\ y_r = (-y_p + s*(x_p - x_r)) \bmod q$$

3.1.2 Doubling the point P

Provided that y_p is not 0,

$$2P = R(x_r, y_r) \qquad \cdots\cdots(6)$$
$$where$$
$$s = ((3x_p^{\ 2} + a)/(2y_p)) \bmod q.$$
$$x_r = (s^2 - 2x_p) \bmod q$$
$$and\ y_r = (-y_p + s*(x_p - x_r)) \bmod q$$

The Elliptic Curve Discrete Logarithm Problem *(ECDLP)* is defined as [14]:

Definition 1. Let E be an elliptic curve over a finite field F_q and let $P \in E(F_q)$ be a point of order n . Given $Q \in E(F_q)$, the elliptic curve discrete logarithm problem is to find the integer $d \in [0, n-1]$, such that $Q = dP$.

4. Proposed untraceable Blind Signature

In this section, firstly the variation of ElGamal digital signature and its subsequent extension using ECDLP has been discussed. Subsequently we shall propose a novel efficient and low computation blind signature based on Elliptic curve discrete logarithm problem.

4.1 Digital Signature using ECDLP

The proposed Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of ElGamal Digital Signature [15]. The EC variant provides smaller key sizes for similar security level.

Initially the curve parameters *(q,FR,a,b,G,n,h)* must be agreed upon by signer and receiver. Signer must have a key pair suitable for elliptic curve cryptography, consisting of a private key d_B (a randomly selected in the interval [1,n-1]) and a public key Q where $Q = d_B G$ .When a signer wants to send a signed message *m* to receiver, he/she must generate a digital signature *(r,s)* as follows

Select k randomly between [1, n-1] and generate $R, r\ and\ s$ as:

$$R = kG$$
$$wher \quad R = (x_R, y_R)$$
$$r = x_R \bmod n \quad and \quad r!= 0$$
$$s = md_B - kr \bmod n \quad and\ s!= 0 \qquad \cdots\cdots(7)$$

After receiving *(r,s)* from signer, the receiver can verify the correctness of the signature on the message by using following equation :

$$mQ = sG + rR \qquad \cdots\cdots(8)$$

4.1.1 Correctness

The verifier only verify the pair (r,s) and message m by using the above equation. The correctness of the equation $mQ = sG + rR$ is as follows:

$$s = md_B - kr$$
$$\Rightarrow md_B = s + kr$$
$$\Rightarrow md_B G = sG + rkG$$
$$\Rightarrow mQ = sG + rR$$

4.2 Blind Signature based on ECDLP

In the proposed scheme the requester requests signature from the signer, and the signer issues blind signature to the requester without knowing the content of the message.
The protocol consists of following five phases:

(a) Initialization phase
(b) Requesting phase
(c) Signing phase
(d) Extraction phase
(e) Verifying phase

In the initialization phase, the system's parameter is defined, and the signer publishes the necessary information and sends partially blind signature to requester. To obtain a signature, a requester submits an encrypted version (blinds the message) of the message to the signer in the requesting phase. In the signing phase, the signer computes the blind signature of the message, and then sends the result back to the requester. In the extraction phase, the requester extracts the signature from the result he receives in the extraction phase. Lastly, any one can verify the legitimacy of the digital signature in the verifying phase. The details of our scheme are presented as follows.

4.2.1 The initialization phase

Let *(q,FR,a,b,G,n,h)* are the curve parameter, d_B (a randomly selected in the interval [1,n-1]) and Q are private and public key of signer, respectively. Where $Q = d_B G$ which is made public. The signer randomly chooses $\tilde{k}_1, \tilde{k}_2, l_1$ and l_2 and calculates $\tilde{r}_1$ and $\tilde{r}_2$ as follows.

$$\tilde{R}_1 = \tilde{k}_1 G$$
$$\tilde{R}_2 = \tilde{k}_2 G$$
$$\tilde{R}_1 = (\tilde{x}_{r1}, \tilde{y}_{r1})$$
$$\tilde{R}_2 = (\tilde{x}_{r2}, \tilde{y}_{r2})$$
$$\tilde{r}_1 = \tilde{x}_{r1} \mod n \quad and \quad \tilde{r}_1 != 0$$
$$\tilde{r}_2 = \tilde{x}_{r2} \mod n \quad and \quad \tilde{r}_2 != 0 \qquad \cdots\cdots\cdots(9)$$

The signer sends $(\tilde{R}_1, \tilde{R}_2, l_1, l_2)$ to requester.

4.2.2 The requesting phase

After receiving, the $(\tilde{R}_1, \tilde{R}_2, l_1, l_2)$ requester randomly select four integers $a, b, w \; and \; z$ such that w is relatively prime to z i.e. $\gcd(w, z) = 1$. According to Extended Eculid's algorithm there exist two integer e and d d such that $ew + dz = 1$ [16]. Signer secret values are (e, w, d, z, a, b) .The requester computes R1 and R2 as,

$$R_1 = \tilde{R}_1 \, wal_1, \quad R_1 = (x_{r1}, y_{r1})$$
$$R_2 = \tilde{R}_2 \, zbl_2, \quad R_2 = (x_{r2}, y_{r2})$$
$$r_1 = x_{r1} \mod n \qquad \cdots\cdots\cdots(10)$$
$$r_2 = x_{r2} \mod n$$

After calculating r1 and r2 the requester blinds the message m as follows

$$\tilde{m}_1 = em\tilde{r}_1 \, r_1^{-1} r_2^{-1} a^{-1} \mod n$$
$$\tilde{m}_2 = em\tilde{r}_2 \, r_1^{-1} r_2^{-1} b^{-1} \mod n \qquad \cdots\cdots\cdots(11)$$

The requester sends the blind messages $\tilde{m}_1$ and $\tilde{m}_2$ to signer for signature.

4.2.3 The Signing Phase

In this phase, the signer computes blind signature $\tilde{s}_1$ and $\tilde{s}_2$ by using received blinds messages $\tilde{m}_1$ and $\tilde{m}_2$ as follows.

$$\tilde{s}_1 = d_B \tilde{m}_1 - r_1 \tilde{k}_1 l_i \mod n$$

$$\tilde{s}_2 = d_B \tilde{m}_2 - r_2 \tilde{k}_2 l_2 \mod n \quad \cdots\cdots\cdots (12)$$

Then the signer sends the blind signatures $\tilde{s}_1$ and $\tilde{s}_2$ to the requesters.

4.2.4 The extraction phase

After receiving the blind signatures $\tilde{s}_1$ and $\tilde{s}_2$ the requester extract the actual signature as follows

$$s_1 = \tilde{s}_1 \tilde{r}_1^{-1} r_1 r_2 wa \mod n$$

$$s_2 = \tilde{s}_2 \tilde{r}_2^{-1} r_1 r_2 zb \mod n$$

$$s = s_1 + s_2$$

$$R = R_1 + R_2$$

$$r = (r_1 * r_2) \bmod n \quad \cdots\cdots\cdots (13)$$

The pair *(r,s)* are the valid digital signature of message *m*.

4.2.5 The Verifying phase

Any one can verify the legitimacy of the digital signature (R, r, s) of message m by using (14)

$$mQ = sG + rR \quad \cdots\cdots\cdots (14)$$

The proposed scheme is diagrammatically shown in Fig. 2.

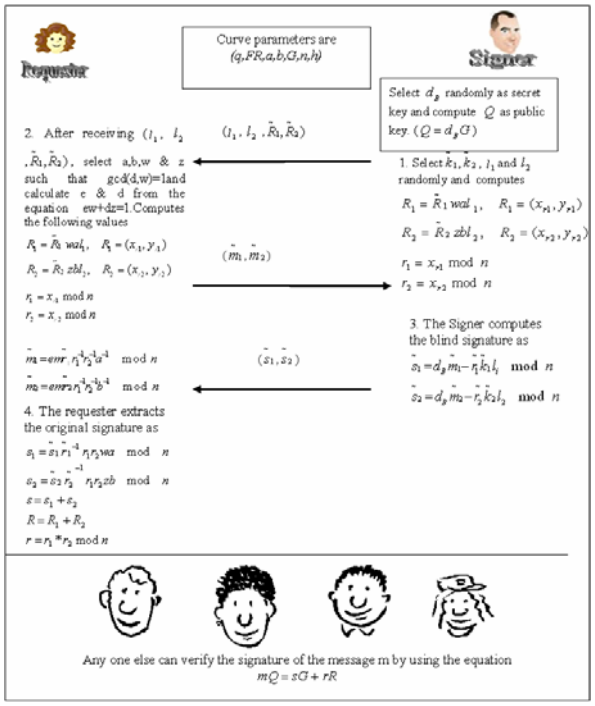

Fig.2 New Blind Signature Scheme based on ECDLP

5. Proof of properties of the proposed scheme

In this section we discuss the correctness and some of the important property of our proposed blind signature scheme.

5.1 Correctness

The correctness of our scheme can be easily verified as follows. The verifier has only digital signature *(r,s,R)* of message m for verification.
The signer computes the s by adding s_1 and s_2.
Therefore,

$$s = s_1 + s_2$$
$$= \tilde{s}_1 \tilde{r}_1^{-1} r_1 r_2 wa + \tilde{s}_2 \tilde{r}_2^{-1} r_1 r_2 zb$$
$$= \left(d_B \tilde{m}_1 - \tilde{r}_1 \tilde{k}_1 l_i \right) \tilde{r}_1^{-1} r_1 r_2 wa +$$
$$\left(d_B \tilde{m}_2 - \tilde{r}_2 \tilde{k}_2 l_2 \right) \tilde{r}_2^{-1} r_2 zb$$
$$= \left(d_B \left(em \tilde{r}_1 r_1^{-1} r_2^{-1} a^{-1} \right) - \tilde{r}_1 \tilde{k}_1 l_i \right) \tilde{r}_1^{-1} r_1 r_2 wa$$
$$+ \left(d_B \left(dm \tilde{r}_2 r_1^{-1} r_2^{-1} b^{-1} \right) - \tilde{r}_2 \tilde{k}_2 l_2 \right) \tilde{r}_2^{-1} r_1 r_2 zb$$
$$= d_B emw - \tilde{k}_1 l_i r_1 r_2 wa + d_B dzm - \tilde{k}_2 l_2 r_1 r_z zb$$
$$= d_B m(ew + dz) - r_1 r_2 (\tilde{k}_1 l_i wa + \tilde{k}_2 l_2 zb)$$
$$= d_B m - r(\tilde{k}_1 l_i wa + \tilde{k}_2 l_{2_z} zb)$$
$$(\because ew + dz = 1 \; and \; r = r_1 \, r_2)$$
$$= d_B m - r(\tilde{k}_1 l_i wa + \tilde{k}_2 l_{2_z} zb)$$

Finally,

$$s = d_B m - r(\tilde{k}_1 l_i wa + \tilde{k}_2 l_{2_z} zb) \qquad \cdots\cdots(15)$$

Now multiplying both sides of (15) *by generator G we have*

$$sG = d_B mG - r(\tilde{k}_1 l_i wa + \tilde{k}_2 l_{2_z} zb)G$$
$$\Rightarrow sG = Qm - r(\tilde{k}_1 l_i waG + \tilde{k}_2 l_{2_z} zbG)$$
$$\Rightarrow sG = Qm - r(R_1 + R_2)$$
$$\Rightarrow sG = Qm - rR$$
$$\Rightarrow sG + rR = Qm$$

5.2 Blindness

As requester randomly select six blinding factors $(e_x, w_x, d_x, z_x, a_x, b_x)$ to compute the blind message $(\tilde{m}_1, \tilde{m}_2)$, so the form the blind messages $(\tilde{m}_1, \tilde{m}_2)$ the signer can not compute the original message as it is based on ECDLP.

5.3 Untraceability

The signer cannot link the signature to the message as signer only has the information i.e. $(\tilde{m}_{1x}, \tilde{m}_{2x}, \tilde{r}_{1x}, \tilde{r}_{2x}, \tilde{k}_{1x}, \tilde{k}_{2x}, \tilde{s}_{1x}, \tilde{s}_{2x}, l_{1x}, l2_x)$ for all blinded messages, where $x = 1,2,\cdots,n.$ If a requester reveals the signatures of a message and its signature i.e. ((m_x, r_x, s_x, R_x) to public, from this information the signer can only compute two values $\tilde{e}_x, \tilde{a}_x^{-1}$ *and* $\tilde{d}_x, \tilde{b}_x^{-1}$, where $\tilde{e}_x, \tilde{a}_x^{-1} = \tilde{m}_{1x} \tilde{m}_x^{-1} \tilde{r}_{1x}^{-1} \tilde{r}_x \bmod q$ and $\tilde{d}_x, \tilde{b}_x^{-1} = \tilde{m}_{2x} \tilde{m}_x^{-1} \tilde{r}_{2x}^{-1} \tilde{r}_x \bmod q$ corresponding to each information stored $(\tilde{m}_{1x}, \tilde{m}_{2x}, \tilde{r}_{1x}, \tilde{r}_{2x}, \tilde{k}_{1x}, \tilde{k}_{2x}, \tilde{s}_{1x}, \tilde{s}_{2x}, l_{1x}, l2_x)$. Therefore, without the knowledge of the secret information of the requester i.e. $(e_x, w_x, d_x, z_x, a_x, b_x)$ can not trace the blind signature.

6. Conclusion

This paper suggests a secure and efficient blind signature scheme based on the Elliptic Curve Discrete Logarithm Problem. The scheme has been proved to be secure, robust and untraceable. As the scheme is based on ECDLP, it achieves the same security with fewer bits key as compared to RSA. In addition, it has low-computation requirements. It can also be applied to applications like electronic voting systems and untraceable digital cash where anonymity of the signer is a requirement.

Acknowledgments

This research was supported by Department of Communication and Information Technology, Government of India under Information Security Education and Awareness project and being carried out at department of Computer Science and Engineering, NIT Rourkela, INDIA.

References

[1] D. Chaum, *Blind Signature Systems*, U.S. Patent 4,759,063, 19 Jul 1988.
[2] D. Chaum, 'Blind *signatures for untraceable payments'*. Advances in cryptology, CRYPTO'82, Lect. Notes Computer Science, (Springer-Verlag, 1998), pp. 199-203

[3] D. Chaum,A. Fiat and M. Naor, *'Untraceable electronic cash'*. Advances in cryptology, CRYPTO'RX, Lect. Notes Computer Science, (Springer-Verlag, 1990), pp. 319-327
[4] Chun-I Fan, W.K. Chen, and Y. S. Yeh, *"Randomization enhanced Chaum's blind signature scheme,"* Computer Communications, vol. 23, pp. 1677–1680, 2000.
[5] Zuhua Shao, *"Improved user efficient blind signatures,"* Electronics Letters, vol. 36, no. 16, pp. 1372–1374, 2000.
[6] J. Camenisch, J. Piveteau, and M. Stadler, *"Blind signatures based on discrete logarithm problem,"* in Advancesin Cryptology, EUROCRYPT'94, pp. 428–432, Lecture Notes in Computer Science, 950, 1994.
[7] L. Harn, *"Cryptanalysis of the blind signatures based on the discrete logarithm problem,"* IEE ElectronicLetters, pp. 1136–1137, 1995.
[8] E. Mohammed, A. E. Emarah, and K. El-Shennawy, *"A blind signatures scheme based on ElGamal signature,"* in IEEE/AFCEA EUROCOMM 2000 Information Systems for Enhanced Public Safety and Security, pp. 51–53, 2000.
[9] Min-Shiang Hwang and Yuan-Liang Tang Yan-Chi Lai. *"Comment on "A BlindSignatureScheme Based On ElGamal Signature"*. Technical Report CYUT-IM-TR-2001-010, CYUT, Aug. 2001.
[10] N. Koblitz, *"Elliptic Curve Cryptosystems"*, Mathematics of Computation ,48,1987pp.203-209
[11] V. Miller, *"Uses of Elliptic Curve in Cryptography*", Advances in Cryptography, Proceedings of Crypto'85, Lectures notes on Computer Sciences,218, Springer – Verlag, 1986, pp.417-426
[12] N. Koblitz, *"CM-Curves with Good Cryptographic Properties "*, Proceeding of Crypto'91,1992
[13] Darrel Hankerson, Alferd Menzes, Scott Vanstone, Guide *to Elliptic Curve Cryptography*, Springer
[14] C.Popesu ,*"A Secure Key Agreement Protocol Using Elliptic Curves"*, International Journal of Computers and Applications, Vol 27,2005
[15] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
[16] Doug Stinson, "*Cryptography Theory and Practice*", Second Edition, CRC Press, Inc, 2002.

Debasish Jena was born in 18th December, 1968. He received his B Tech degree in Computer Science and Engineering, his Management Degree and his MTech Degree in 1991, 1997 and 2002 respectively. He has joined Centre for IT Education as Assistant Professor since 01.02.2006. He has registered for Ph.D. at NIT, Rourkela on 15th January 2007.In addition to his responsibility, he was also IT, Consultant to Health Society, Govt. of Orissa for a period of 2 years from 2004 to 2006.His research areas of interest are Information Security , Web Engineering, Bio-Informatics and Database Engineering,

Dr. S.K. Jena was born in 28 April, 1954. He received his Ph.D. from Indian Institute of Technology, Bombay and M.Tech from Indian Institute of Technology, Kharagpur. He has joined National Institute of Technology as Professor in the Department of Computer Science and Engineering in 2002. Currently he is working as Professor and Head of Computer Science and Engineering department. He has more than 35 publications in International Journals and conferences. His research areas of interest are Database Engineering, Distributed Computing, Parallel algorithm, Information Security and Data Compression.

B.Majhi is presently working as a professor in the department of computer science & engineering in NIT Rourkela. He has completed 16 years of teaching in NIT Rourkela and 3 years of Industry experience in a reputed firm. He has completed his M.Tech and Ph.D. in Computer Science & Engineering from NIT Rourkela and Sambalpur University respectively. He has 13 research publications in international and national journals and more than 30 publications in national/international conferences to his credit. His research areas include soft computing applications, image processing, and cryptography.