Constructing Provably Secure ID-based Beta Cryptographic Scheme in Random Oracle

Chandrashekhar Meshram[1], Sarita Gajbhiye Meshram[1] and Cheng-Chi Lee[2,3]
(Corresponding author: Cheng-Chi Lee)

Department of Mathematics and Computer Science, Rani Durgawati University[1]
Saraswati Vihar, Pachpedi, Jabalpur 482001, India
Department of Library and Information Science,Fu Jen Catholic University[2]
510 Jhongjheng Road, Taipei 24205, Taiwan, R.O.C.
Department of Photonics and Communication Engineering,Asia University[3]
Wufeng Shiang, Taichung, Taiwan 413, R.O.C.
(Email: cs_meshram@rediffmail.com,cclee@blue.lins.fju.edu.tw)
(Received Jan. 24, 2017; revised and accepted June 5, 2017)

Abstract

In this study, we propose a new ID-based beta cryptosystem scheme secure under selective identity adaptive chosen ciphertext security (IND-sID-CCA) under assumption in the random oracle model. We demonstrate that our scheme outperforms the other existing schemes in terms of security, computational cost and the length of public key.

Keywords: Discrete Logarithm Problem; Generalized Discrete Logarithm Problem; ID-based Cryptosystem; Integer Factorization Problem and Beta Cryptosystem; Public key Cryptosystem

1 Introduction

Shamir [24] introduced the idea of ID-based cryptography to simplify the key management problem in 1984. Two efficient ID-based cryptosystem schemes were proposed by Cocks [7] and Boneh and Franklin [6] in 2001. In their seminal paper [5], Boneh and Franklin used a category of bilinear maps as the basis of their construction. This leads a number of ID-based cryptosystem schemes [2, 3, 26], among others based on bilinear maps. Few ID-based cryptosystem schemes [1, 10, 12] have been proposed after 2003. But in these schemes, the public key of each user is not only an identity, but also some random number selected either by the user or by the trusted authority. But which makes the ID-based cryptosystem an active research field in recent years.

The first efficient ID-based cryptosystem scheme was proposed by Boneh and Franklin [5, 6]. The novel approach they use is based on a class of bilinear maps. Following their work, a number of ID-based cryptosystem scheme using bilinear maps were proposed. For example,Waters [12] presented an efficient and secure ID-based cryptosystem scheme without random oracles; Boneh and Boyen [2] designed a secure ID-based cryptosystem scheme without random oracles; Boneh and Boyen [3] gave another efficient ID-based encryption scheme without random oracles, which is secure in the selective identity model.

Meshram *et al.* [17, 20, 22] presented some new efficient ID-based cryptographic schemes and ID-based mechanisms based on discrete logarithm problem, generalized discrete logarithm problem and integer factorization problem. The security of this schemes are solving the hardness of discrete logarithm problem, generalized discrete logarithm problem and integer factorization problem simultaneously. Meshram and Meshram [18, 19] investigate the new variant of ID-based beta cryptographic scheme and transformation process such as public key cryptographic scheme transfer to ID-based cryptographic scheme without developing new ID-based scheme.

Meshram [14, 15, 16] presented new provably secure ID-based cryptographic scheme, new variant of ID-based beta cryptographic scheme, and efficient scheme based on integer factorization problem and discrete logarithm problem. It is as low as ElGamal scheme. Meshram and Obaidat [21] also showed new variant of ID-based cryptographic scheme such as quadratic-exponentiation randomized cryptographic scheme. Recently, Meshram *et al.* [23] projected new ID-based cryptographic scheme based on partial discrete logarithm problem. Liu and Ye [11] presented new variations as homomorphic universal re-encryptor for ID-based cryptography. In similar manner Wang *et al.* [25] presented efficient ID-based proxy multi signature using cubic residues.

As outlined above, unfortunately we found that new cryptographic model always face security challenges and confidentiality concerns. Therefore, our main contribution of this paper is to fill this gap by proposing a provably secure ID-based beta cryptographic scheme. Specifically, we will show that the security of the proposed scheme is closely, if not tightly, related to difficulty of solving generalized discrete logarithm problem and integer factorization problem. We provided an formal security proof for selective identity adaptive chosen ciphertext security (IND-sID-CCA) in the random oracle, which means that the new scheme offers better security guarantees than existing other ID-based cryptographic schemes. The proposed scheme does not use pairings (bilinear maps), resulting in high efficiency and ease of implementation, neither does it rely on the relatively new and untested hardness assumptions related to pairing-based cryptography. This makes it attractive for application in resource-constrained environments where saving in computation, communication and implementation code area is a premium.

The rest of this paper is organized as follows: The Beta cryptosystem and supporting example for it are demonstrated in Section 2 and 3 respectively. Proposed an ID-based beta cryptographic scheme with chosen ciphertext security is demonstrate in Section 4. The security examination of proposed ID-based cryptographic scheme is presented in Section 5. Discuss comparison with previous ID-based cryptographic schemes in Section 6. Finally, Section 7 concludes the paper.

2 The Beta Cryptosystem

The algorithm consists of three sub-algorithm, Key generation, Encryption and Decryption.

2.1 Key Generation

The key generation algorithm runs as follows (user 1 should do the following).

1) Select arbitrary primes q and p each roughly of the same size.

2) Calculates $N = q \star p$ and Euler-phi function $\varphi(N) = (q-1)(p-1)$.

3) Choose an arbitrary integer $e, 1 \leq e \leq \varphi(N)$ such that gcd $(e, \varphi(N)) = 1$.

4) Choose an arbitrary integer b such that $2 \leq b \leq \varphi(N) - 1$.

5) Choose an element β of the multiplicative group $\mathbb{Z}_N^*$ and calculate $y_1 = \beta^b mod(N)$.

6) By using the extended Euclidean algorithm to calculate 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, β^b) and the corresponding private key is given by (d, b, β).

2.2 Encryption

An user 2 to encrypt a message m to user 1 should do the following:

1) The message is represented as an integer in the interval $[1, N-1]$.

2) The cipher text is given by $C = (m\beta^b)^e mod(N)$.

2.3 Decryption

To recover the plaintext m from the cipher text C, user 1 should do the following:

1) Calculate $y_2 = \beta^{\varphi(N)-b} mod(N) = \beta^{-b} mod(N)$.

2) Then calculate $y_3 = (y_2)^e mod(N)$.

3) Recover the plaintext m by computing $((y_2)^e \star C)^d (modN)$.

3 Example

To make our construction easy to comprehend, we illustrate an example to show the basic principle of our proposed scheme.

Let the two primes be $q = 29$ and $p = 43$ and set $N = 1247$ and $\varphi(N) = 1176$.

3.1 Key Generation

The key generation algorithm runs as follows.

1) Select an arbitrary integer $e = 11$ and gcd $(11, 1176) = 1$.

2) Select an arbitrary integer $b = 19$.

3) Choose an element $\beta = 10$ of the multiplicative group $\mathbb{Z}_N^*$ and calculate $y_1 = \beta^b mod(N) = (10)^{19} mod\ 1247 = 427$.

4) By using the extended Euclidean algorithm to compute the unique integer $d = 107, 1 \leq d \leq \varphi(N)$ such that $11d \equiv 1(mod\ 1176)$.

The public key is formed by (N, e, β^b) and the corresponding private key is given by (d, b, β).

3.2 Encryption

An user 2 to encrypt a message m to user 1 should do the following:

1) The message $m = 1122$ is represented as an integer in the interval $[1, N-1]$.

2) The cipher text is given by $C = (m\beta^b)^e mod(N) = (479094)^{11} mod\ 1247 = 791$.

3.3 Decryption

To recover the plaintext m from the cipher text C, user 1 should do the following:

1) Calculate $y_2 = \beta^{\varphi(N)-b} mod(N) = \beta^{-b} mod(N) = 917$.
2) Then calculate $y_3 = (y_2)^e mod(N) = 483$.
3) Recover the plaintext m by computing $((y_2)^e \star C)^d (modN) = 1122$.

4 An ID-based Beta Cryptosystem Scheme with Chosen Ciphertext Security

The major contribution of our proposed ID-based beta cryptosystem is the key generation phase. Upon the successful creation of a private key, the scheme concept can be easily implemented in encryption and decryption posses.

4.1 Setup

By taking in security parameter t this algorithm will be carried out by PKG as follows:

1) Let $N = q * p$ be a large prime number,such that $\varphi(N) = (q-1)(p-1)$ and β be an element of order N in $Z_N^\star$, x, y be PKG's secret and public keys respectively, where $y = \beta^x mod\ N$.
2) Select two random integers e and d as $1 \leq e, d \leq \varphi(N)$, such that $gcd(e, \varphi(N)) = 1$ and $ed \equiv 1(mod\varphi(N))$.
3) The PKG chosen randomly secrete information as k_i for $(1 \leq i \leq t)$, where $\Sigma_{i=1}^t k_i < \varphi(N)$ and public information K_i, where $K_i = \beta^{k_i} mod\ N$,for $(1 \leq i \leq t)$.
4) Compute the hash function $H : \{0,1\}^t \rightarrow Z_N^*$.

4.2 Exact

For a given user identity $ID \in \{0,1\}^*$, we compute the private key of the user is $\beta^{\theta_A} = vK_A^{K_A} mod\ N$, where $\theta_A = \Sigma_{i=1}^t k_i v_{Ai} mod\varphi(N)$, $K_A = \Pi_{i=1}^t K_i^{v_{Ai}} mod\ N$ and v_{Ai} is the i^{th} bit of $H(ID_A)$ for $(1 \leq i \leq t)$.

4.3 Encryption

To encrypt a message $M \in \{0,1\}^*$ for ID as follows:

1) Set the public key $V_A = \beta^{\theta_A} = vK_A^{K_A} mod\ N$, where $K_A = \Pi_{i=1}^t K_i^{v_{Ai}} mod\ N$.
2) Chosen a random integer e such that $gcd(e, \varphi(N)) = 1$.
3) Compute the ciphertext to be $C = (M\beta^{\theta_A})^e (mod\ N)$.

4.4 Decryption

Let C be the valid ciphertext encrypted by using the public key V_A. The user can decrypt ciphertext using the private key θ_A.

1) Calculate $y_2 = \beta^{-\theta_A}(mod\ N)$.
2) Compute $y_2^e = (\beta^{-\theta_A})^e (mod\ N)$.
3) Out put M as the decryption of C as

$$[(y_2)^e * C]^d (mod\ N) = [\beta^{-\theta_A e} M^e \beta^{\theta_A e}]^d (mod\ N)$$
$$= M^{ed}(mod\ N) = M(mod\ N).$$

5 Security Examination

In this section, we examine the security of ID-based beta cryptosystem scheme. The following theorem shows that ID-based beta cryptosystem scheme is IND-sID-CCA secure, if beta cryptosystem is IND-CCA secure [8] in random oracle model [9].

Definition 1. *An ID-based cryptosystem scheme, E is said to be selective identity, adaptively chosen ciphertext secure (IND-sID-CCA), if no probabilistic polynomial time (PPT) adversary* A *has a non-negligible advantage in the following game in [4].*

Theorem 1. *The identity hash function H be a random oracle. Then ID-based beta cryptosystem scheme is IND-sID-CCA secure, if beta cryptosystem [Section 2] is IND-CCA secure. Concretely, suppose there is an IND-sID-CCA rival R_1 that has advantage $\epsilon(k)$ against ID-based beta cryptosystem. Then there exists an IND-CCA rival R_2 with advantage at least $\epsilon(k)$ against beta cryptosystem. Its running time is rival $O(time(R_1))$.*

Proof. The main idea of this proof is to construct an IND-CCA rival R_2 to gain the advantage against beta cryptosystem in the following IND-CCA game.

At the starting of the game, the IND-CCA challenger generates the public key $K_{pub} = \langle N, \beta, v \rangle$ and a private key x that satisfies $v = \beta^x mod\ N$. The challenger gives K_{pub} to rival R_2, then rival R_2 mounts an IND-CCA attack using the help of algorithm rival R_1 as follows:

Initialization. The rival outputs an identity ID_{ch} which it wishes to be challenged.

Setup. The challenger runs the *setup algorithm*. It gives the rival the resulting system parameters. It keeps the masterkey to itself.

H-queries. To respond to H-query, R_2 maintains a list of tuples $\langle ID_{Ai}, V_{Ai}, \theta_{Ai} \rangle$ which we refer to as H^{list}. The list is initially empty. When R_1 queries H at a point ID_{Ai}, R_2 responds as follows:

1) If the query on ID_{Ai} already appears on the H^{list} in a tuple of the form $\langle ID_{Ai}, V_{Ai}, \theta_{Ai} \rangle$ then R_2 responds with $H(ID_{Ai}) = v_{Ai}$ as a answer.

2) If the query is new to the H oracle, R_2 will pick a random $\theta_{Ai} \in Z_N^*$ and computes $V_{Ai} = \beta^{\theta_{Ai}} mod\ N$, else R_2 sets $\theta_{Ai} = *$ and $V_{Ai} = v$. as a answer. Here $*$ denotes a special symbol.
3) R_2 adds the tuple $\langle ID_{Ai}, V_{Ai}, \theta_{Ai} \rangle$ to H^{list} and gives back V_{Ai} to R_1.

Phase 1-Extraction queries. When R_1 asks for the private key associated to ID_{Ai}, R_2 runs the above algorithm and gets $H(ID_{Ai}) = v_{Ai}$, where $\langle ID_{Ai}, V_{Ai}, \theta_{Ai} \rangle$ is the corresponding entry in H^{list}. As $V_{Ai} = \beta^{\theta_{Ai}} mod\ N$, R_2 can retrieve the legitimate private key θ_{Ai} for ID_{Ai}. The extraction query on ID_{ch} will be denied.

Phase 1-Decryption queries. Let $\langle ID_{Ai}, C_i \rangle$ be a decryption query issued by adversary R_1, where C is ciphertext of beta cryptosystem. R_2 responds to the query as follows:

1) If $\langle ID_{Ai} \neq ID_{ch} \rangle$, then R_2 runs H-query algorithm such that of the form $\langle ID_{Ai}, V_{Ai}, \theta_{Ai} \rangle$ be the corresponding tuple on H^{list}. Next it uses the private key θ_{Ai} to respond to the decryption query.
2) If $\langle ID_{Ai} = ID_{ch} \rangle$, then R_2 forwards the decryption query with $\langle C_i \rangle$ and then relays the challenger's response back to R_1.

Challenge. Once R_1 decides that Phase 1 is over it outputs two messages M_0 and M_1 which it wishes to be challenged on. Algorithm R_2 responds as follows:

1) R_2 gives the challenger M_0 and M_1 as the messages that it wishes to be challenged on. The challenger responds with the beta cryptosystem's ciphertext C such that C is the encryption of M_c for a random coin $c \in \{0, 1\}$.
2) Next, R_2 runs the algorithm for responding H-queries to obtain $v \in Z_N^*$ such that $H(ID_{ch}) = v$ and forwards C to R_1.

Phase 2-Extraction queries. R_2 responds the same as in Phase 1, except for the extraction query on ID_{ch}, which will be rejected.

Phase 2-Decryption queries. R_2 responds the same as in Phase 1 except the decryption query $\langle ID_{ch}, C \rangle$ will be denied.

Guess. Rival R_1 finally outputs a guess c' for c. Rival R_2 outputs c' as its guess for c.
The responses to H-queries are as in the factual attack since each response is uniformly and independent distributed in Z_N^*. All responses to private key extraction queries and decryption queries are valid. So R_2 will not abort during the simulation, the possibility of perfect simulation is 1. From these we can conclude that Rival R_1's view is identical to its view in the factual attack. By the definition of algorithm R_1 we have that $|Pr[c = c'] - 1/2| \geq \epsilon(k)$, thereby R_2 has at least advantage $\epsilon(k)$ against beta cryptosystem. This proves theorem 5.0.2 and terminates the proof.

□

6 Performance Comparison of Other ID-based Cryptographic Schemes

In this section, we have discussed four most wide-used ID-based encryption schemes and compared their performance. These four ID-based cryptographic schemes are: Selective-ID Secure ID-based cryptosystem without Random Oracles [3], Boneh-Franklin ID-based cryptosystem [6], Cocks ID-based cryptosystem [7], Authenticated ID-based cryptosystem [13], and our proposed ID-based beta cryptosystem. These schemes have different performance on server for evaluating Encrypt algorithm performance, decryption algorithm performance, and computational cost. Notations used in this computation are as follows: P = airing operation, M = Modular multiplication, e = Exponentiation in G, m =Scalar or Point Multiplication in G, x = XOR operation, h = Hashing, a = addition modulo, i = inverses modulo , J = Jacobi symbol and $C(\gamma)$ = Computation cost of operation γ.

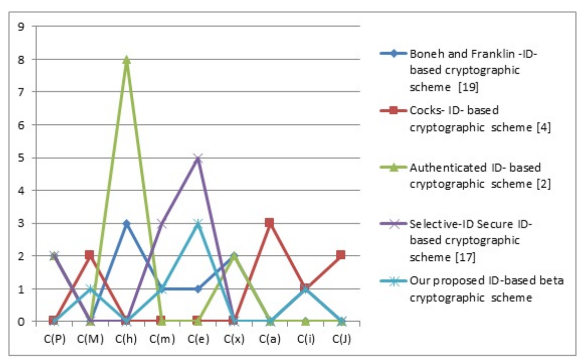

Figure 1: Computational cost

Based on our observation of Figure 1, we have observed that proposed ID-based beta cryptosystem has a better performance than other four schemes [3, 6, 7, 13] in encryption and decryption algorithms. Our proposed scheme is faster than schemes [3, 6, 7, 13] in two aspects. First, our proposed scheme needs no pairing computation in encrypt algorithm and decryption algorithm, because $\tilde{e}(P_1, P_2)$ can be pre-computed. Secondly, in the operation of mapping an identity to an element in G_1 or G_2 , the map-to-point algorithm used by scheme [6] and scheme [3] is not required because simple hash function is used in our scheme to map an identifier to an element in Z_N^*. Our proposed scheme is faster than scheme [7] in one aspect. The size of ciphertext is very large and consists of two elements of Z_N per bit of the message but the size of our proposed scheme is smaller than scheme [7] and consists of an element of Z_N^* per bit of the message.

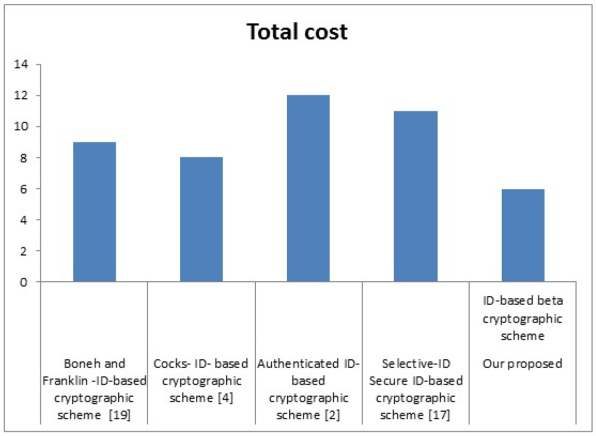

Figure 2: Total computational cost

Also, we evaluated the total computational cost of the four schemes [3, 6, 7, 13] and proposed scheme in Figure 2. We found that the computation cost of scheme [3] is near about the scheme [13] and the computation cost of scheme [7] is near about the scheme [6] and the computation cost of our proposed is much less to other four schemes and half of scheme [13]. As we know that in the Extract algorithm of scheme [6] and scheme [13], an identity string is mapped to a point on an elliptic curve and the corresponding private key is computed by multiplying the mapped point with the master key of public key generator (PKG) and Extract algorithm of our proposed scheme requires much simpler hashing than the schemes [6, 7, 13]. Hence the computational cost will reduce and therefore improves performance.

7 Conclusion

In this article, we deals with new mechanisms for ID-based beta cryptographic scheme, whose unforgeability can be reduced to the hardness of the generalized discrete logarithm problem and integer factorization problem over multiplicative group, which are a fundamental intractable problems in cryptography. It is selective identity adaptive chosen ciphertext security (IND-sID-CCA) under assumption of generalized discrete logarithm problem and integer factorization problem over multiplicative group in random oracle. This scheme is fast than Boneh and Franklin-ID-based cryptographic scheme, Cocks- ID-based cryptographic scheme, Authenticated ID-based cryptographic scheme, Selective-ID Secure ID-based cryptographic scheme and having very low computational cost. Therefore, our new scheme is more practical and has the same security as the original discrete logarithm problem and integer factorization problem-based system.

References

[1] M. Bellare, C. Namprempre and G. Neven, "Security proofs for identity-based identification and signature scheme," *Journal of Cryptology*, vol. 22, pp. 1-61, 2009.

[2] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," *Advances in Cryptology (CRYPTO'04)*, LNCS 3152, Springer-Verlag, pp. 443-459, 2004.

[3] D. Boneh and X. Boyen, "Efficient selective-id secure identity based encryption without random Oracles," *Advances in Cryptology (Eurocrypt'04)*, LNCS 3027, Springer-Verlag, pp. 223-238, 2004.

[4] D. Boneh, R. Canetti, S. Halevi and J. Katz, "Chosen-ciphertext security from identity-based Encryption," *SIAM Journal on Computing*, vol. 36, no. 5, pp. 1301-1328, 2006.

[5] D. Boneh and M. K. Franklin, "Identity based encryption from the Weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586-615, 2003.

[6] D. Boneh and M. K. Franklin, "Identity based encryption from the Weil pairing," *Advances in Cryptology (CRYPTO'01)*, LNCS 2193, Springer-Verlag, pp. 213-229, 2001.

[7] C. Cocks, "An identity based wncryption scheme based on quadratic residues," in *International Conference on Cryptography and Coding*, LNCS 2260, Springer-Verlag, pp. 360-363, 2001.

[8] M. Hassouna, B. Barry and E. Bashier, "A new level 3 trust hierarchal certificateless public key cryptography scheme in the random oracle model," *International Journal of Network Security*, vol. 19, pp. 551-558, 2017.

[9] J. Kar, "Provably secure identity-based aggregate signcryption scheme in random oracles," *International Journal of Network Security*, vol. 17, no. 5, pp. 580-587, 2015.

[10] E. Kiltz and Y. Vahlis, "CCA2 secure IBE: Standard model efficiency through authenticated symmetric encryption," in *CT-RSA*, LNCS 4964, Springer-Verlag, pp. 221-239, 2008.

[11] L. Liu and J. Ye, "A homomorphic universal re-encryptor for identity-based encryption," *International Journal of Network Security*, vol. 19, no. 1, pp. 11-19, 2017.

[12] W. B. Lee and K. C. Liao, "Constructing identity-based cryptosystems for discrete logarithm based cryptosystems," *Journal of Network and Computer Applications*, vol. 22, pp. 191-199, 2004.

[13] B. Lynn, "Authenticated ID-based encryption," *Cryptology ePrint Archive*, Report 2002/072, 2002.

[14] C. Meshram, "An efficient ID-based cryptographic encryption based on discrete logarithm problem and

integer factorization problem," *Information Processing Letters*, vol. 115, no. 2, pp. 351-358, 2015.

[15] C. Meshram, "An efficient ID-based beta cryptosystem," *International Journal of Security and Its Applications*, vol. 9, no. 2, pp. 189-202, 2015.

[16] C. Meshram, "Factoring and discrete logarithm using IBC," *International Journal of Hybrid Information Technology*, vol. 8, no. 3, pp. 121-132, 2015.

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

[18] C. Meshram and S. Meshram, "An identity-based cryptographic model for discrete logarithm and integer factoring based cryptosystem," *Information Processing Letters*, vol. 113, no. 10-11, pp. 375-380, 2013.

[19] C. Meshram and S. Meshram, "An identity based beta cryptosystem," in *IEEE Proceedings of 7th International Conference on Information Assurance and Security (IAS'11)*, pp. 298-303, 2011.

[20] C. Meshram, S. Meshram and M. Zhang, "An ID-based cryptographic mechanisms based on GDLP and IFP," *Information Processing Letters*, vol. 112, no. 19, pp. 753-758, 2012.

[21] C. Meshram and M. S. Obaidat, "An ID-based quadratic-exponentiation randomized cryptographic scheme," in *IEEE Proceeding of International Conference on Computer, Information and Telecommunication Systems*, pp. 1-5, 2015.

[22] C. Meshram and P. L. Powar, "An efficient identity-based QER cryptographic scheme," *Complex and Intelligent Systems*, vol. 2, no. 4, pp. 285-291, 2016.

[23] C. Meshram, P. L. Powar, M. S. Obaidat and C. C. Lee, "An IBE technique using partial discrete logarithm," *Procedia Computer Science*, vol. 93, pp. 735-741, 2016.

[24] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of CRYPTO'84*, LNCS 196, Springer-Verlag, pp. 47-53, 1984.

[25] F. Wang, C. C. Chang, C. Lin and S. C. Chang, "Secure and efficient identity-based proxy multisignature using cubic residues," *International Journal of Network Security*, vol. 18, no. 1, pp. 90-98, 2016.

[26] B. Waters, "Efficient identity-based encryption without random oracles,," *Advances in Cryptology (CRYPTO'05)*, LNCS 3494, Springer-Verlag, pp. 114-127, 2005.

Biography

Chandrashekhar Meshram received the PhD from R.T.M. Nagpur University, Nagpur (M.S.) India. Presently he is Post-Doctoral Fellow under Dr. D S Kothari postdoctoral fellow New Delhi, India. His research interested in the field of Cryptography and its Application, Statistics, Raga (Music and Statistics), Neural Network , Ad hoc Network, Number theory, Time Series Analysis and Climate Change, Mathematical modeling and Chaos Theory. 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 LifeVtime member of Internet Society (ISOC),USA, Indian Mathematical Society, Cryptology Research Society of India and Ramanujan Mathematical Society of India (RMS). He is regular reviewer of sixty International Journals and International Conferences.

Sarita Gajbhiye Meshram received M. Tech degree in Soil and water engineering in 2009 with gold medal from College of Agricultural Engineering, Jawaharlal Nehru Krishi Vishwa Vidhyalaya, Jabalpur (M.P.); and PhD Degree in Water Resource Development and Management from IIT Roorkee (U.K.) India in 2015. She is currently Dr. D.S. Kothari Post-Doctoral Fellow in the Department of Mathematics and Computer Sciences, Rani Durgawati University, Jabalpur, India. Her current research interests Include Geographical Information Systems, Rainfall-Runoff sediment yield modelling, SCS-CN. She is carrying out her research work in the field of Rainfall-Runoff, Sediment Yield, Water Quality, Application of RS and GIS Water Network and Cryptographic Protocol. He has published more than 50 research papers in refereed journals, conference and workshop proceedings, and books. She is a member of some international society and reviewer of the reputed journal.

Cheng-Chi Lee received the Ph.D. degree in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He is currently a Professor with the Department of Library and Information Science at Fu Jen Catholic University. Dr. Lee is currently as an editorial board member of International Journal of Network Security, Journal of Computer Science, Cryptography, and International Journal of Internet Technology and Secured Transactions. He also served as a reviewer in many SCIindex journals, other journals, other conferences. His current research interests include data security, cryptography, network security, mobile communications and computing, wireless communications. Dr. Lee had published over 200 scientific articles on the above research fields in international journals and conferences. He is a member of IEEE, the Chinese Cryptology and Information Security Association (CCISA), the Library Association of The Republic of China, and the ROC Phi Tau Phi Scholastic Honor Society.