A Novel Verifiable Multi-Secret Sharing Scheme Based on Elliptic Curve Cryptography

Nisha Patel, Prakash D.Vyavahare, Manish Panchal

Department of Electronics and Telecommunication Engineering
S. G. S. Institute of Technology and Science, Indore, India
Email: {nishapatel910622, prakash.vyavahare, hellopanchal}@gmail.com

***Abstract*—Multi-secret sharing schemes are used to protect multiple secrets by distributing them among many participants in such a manner that they can be reconstructed only by certain authorized group of participants. The scheme proposed by Lin-Yeh is one such method, which is based on Shamir's threshold scheme. In this paper a Verifiable Multi-Secret Sharing Scheme is proposed which is based on Shamir's threshold scheme, Elliptic Curve Discrete Logarithm Problem (ECDLP), and Double knapsack algorithm. The proposed scheme exhibits all the advantages of Lin-Yeh's scheme in which each participant has only one secret share for reconstructing multiple secrets. Additionally, the scheme does not require secure channel in secret share distribution phase since each participant's share is selected by participant himself. The scheme can also detect malicious participants during verification phase. The main advantage of ECDLP as compared to Rivest, Shamir and Adleman (RSA) and Discrete Logarithm Problem (DLP) is that it offers the same level of security for a smaller key size, thereby reducing processing overheads with lesser requirement of memory and bandwidth with faster implementation. Therefore, it can provide an efficient and secure mechanism for key management in public key systems.**

Keywords– Multi-Secret Sharing Scheme; Double Knapsack Algorithm; Shamir's Threshold Scheme; Malicious Participant Detection; ECDLP.

I. INTRODUCTION

Secret sharing schemes are important in protecting secret information from being lost, destroyed, modified and from unauthorized access. In a secret sharing scheme, the secret is distributed among the participants, and only an authorized group of participants can reconstruct the secret. In the case of (t, n) threshold secret sharing scheme, a secret is distributed to n participants and t (or more than t) participants can reconstruct the secret. The secret sharing schemes are used in different applications like image processing, bank vault opening, inter-continental ballistic missiles launch, and electronic transactions authentication.

In 1979, the secret sharing scheme was proposed independently by Shamir [1] and Blakley [2]. Blakley's scheme is based on the principle of linear projective geometry and Shamir's scheme is based on Lagrange interpolating polynomial. The common limitations of these schemes are: (i) At a time only one secret can be shared. (ii) To distribute the secrets, secure channel is needed. (iii) After the reconstruction of secret, the participant's share is disclosed to all. For sharing another secret, new secret share is redistributed to the participants over a secure channel. (iv) There is no mechanism to detect malicious participants. Shamir's scheme consumes lot of time and also costs for storage requirement. Therefore, it is used in sharing data of small size like the encryption key [3].

Several multi-secret sharing schemes based on strong mathematical structure are presented to remove these limitations, such as polynomial equations based Lin-Yeh method [4], secure one way function - He-Dawson method [5], matrix projection - Li Bai method [6] and many more. In Li Bai's method, the organization of secrets are in a square matrix. Therefore, the number of secrets must be a square of a number. If the number of secrets are not square, then the secret matrix is stuffed by dummy secrets.

He and Dawson [5] proposed a multi-secret sharing scheme based on one-way function, which uses successive one-way functions to share multiple secrets. Geng et al. [7] showed that He-Dawson scheme was actually one-time-use scheme and proposed a new multi-secret sharing scheme with multi-policy. The scheme proposed by Geng et al. is secure and multi-use system. Lin and Yeh [4] proposed a dynamic multi-secret sharing scheme, which is efficient than Geng et al. scheme in terms of computation complexity.

Lin-Yeh's proposed a scheme, which is based on One-way Hash Function (OHF) and the Exclusive OR (XOR) operation, in which multiple secrets can be reconstructed with only one secret share of each participant. Lin-Yeh's scheme is efficient and flexible multi-secret sharing scheme because each participant's share is unchanged even if the secrets to be shared are changed. The major issues with Lin-Yen's scheme are: it cannot detect malicious participants and requires a secure channel during secret distribution phase. The schemes mentioned in [8][9][10] have removed these limitations, but they need a secure channel for secret distribution and are inefficient in computation.

Several verifiable schemes have been proposed for multi-secret sharing [11][12][13], in which each participant needs to keep only one secret share, using which multiple secrets can be shared. Each participant submits a pseudo secret share which is calculated from the actual share of participant for reconstruction phase. Since participants themselves generate the secret share, it reduces the overhead on dealer and also removes the requirement of secure channel between dealer and participants. However, they are based on Discrete Logarithm Problem (DLP). In DLP-based schemes one needs more number of bits to achieve higher level of security and reliability than ECDLP, which increases the requirement of memory and bandwidth [14][15].

In this paper, we propose a scheme based on Shamir's threshold scheme, Elliptic Curve Discrete Logarithm Problem [16][17], the exclusive OR operation and Double knapsack algorithm [18]. The scheme provides the efficiency and flexibil-

 ISBN: 978-1-61208-493-0

ity similar to Lin-Yeh's scheme with advantages of malicious participant detection and without secure channel between the dealer and participants during secret share distribution phase. In the scheme proposed by us the participants, who will contribute in secret reconstruction, are decided by the dealer based on a proposed algorithm which uses the exclusive OR operation. Dealer sends this information to the combiner on public channel employing double knapsack algorithm. Elliptic curve cryptosystem provides the same level of security with smaller key size than other cryptosystems and offers lesser requirement of memory and bandwidth with faster implementation [19][20]. The security of scheme proposed by Hua and Aimin [21] is dependent on hash function. The scheme proposed by us does not have dependency on other cryptographic functions, such as hash function; so the scheme is efficient for threshold applications.

TABLE I. CONVENTION AND NOTATION

A	Group containing ID's of t participants
A'	Encoded form of A by double knapsack algorithm
C	Combiner
D	Dealer
E(F_p)	Elliptic curve E defined over F_p
F_p	Field with set (0, 1, 2, ..., p-1)
G	Generator point of prime order q
ID_j	Identifier of each participant ($1 \leq j \leq n$)
P_j	j^{th} Participant ($1 \leq j \leq n$)
R_j	Pseudo secret share of participant j
S_i	i^{th} Secret ($1 \leq i \leq k$)
S_l	l^{th} group secret in Lin-Yeh's method
U_j	Total number of participants in Lin-Yeh's method
Z_q^*	Field with set (1, 2, ... , q-1)
g	A primitive element over GF(p)
h	One-way hash function
n_1, n_2	Constants used in double knapsack algorithm
p	A large prime number
t	Number of participants required in secret reconstruction
x_j	Secret share of j^{th} participant
$\oplus$	The exclusive OR operation
∞	Point at infinity on elliptic curve

The rest of this paper is organized as follows. In Section II, a review of Lin-Yeh's scheme is presented. In Section III, security weaknesses of Lin-Yeh's method are discussed, which is followed by brief description of Double knapsack algorithm in Section IV. In Section V, our proposed novel verifiable multi-secret sharing scheme based on elliptic curve cryptography is presented. The security features of the proposed scheme and its comparison with Lin-Yen method are presented in Section VI. Finally, the paper is concluded in Section VII.

II. REVIEW OF LIN-YEH'S DYNAMIC MULTI-SECRET SHARING SCHEME

There are three stages in Lin-Yen method [4], namely, (A) The system initialization stage, (B) Pseudo secret share generation stage and (C) Group secret reconstruction stage. They are explained as follows:

A. System Initialization Stage

The initialization of various public domain parameters and selection of their values is done by System Authority (SA) which is as follows:

1) p : a prime number which is large;
2) g : a primitive element over GF(p);
3) h(.) : a secure one-way hash function which produces a fixed length output for any arbitrary length of input;
4) ID_j : an identifier of the user U_j , for j = 1, 2, ... , n, where the secrets are to be shared among n participants.

Table I contains other notations and conventions.

B. Pseudo Secret Share Generation Stage

SA shares k group secrets S_i , where $1 \leq i \leq k$ among n users. Following steps are performed by the SA to produce pseudo secret shares and distribute master secret shares among the participants.

1) Corresponding to each participant j choose distinct $x_j \in Z_p^*$ for j = 1, 2, ... , n, as the master secret shares.
2) For i = 1, 2, ... , k, construct a polynomial f_i(x) of degree (i-1), as f_i(x) = S_i + d_1x + ... + $d_{i-1}x^{i-1}$ where $f_i(0) = S_i$, d_1 to d_{i-1} are randomly selected integers.
3) For j = 1, 2, ... , n and i = 1, 2 ,... , k , compute V_{ij} = $f_i(ID_j)$, c_{ij} = $h^i(x_j) \oplus x_j$, R_{ij} = V_{ij} - c_{ij} mod p; Here $h^i(x_j)$ denotes i successive applications of h to x_j, symbol $\oplus$ denote the exclusive OR operation and c_{ij}'s are pseudo secret shares.
4) The master secrets x_j, for j = 1, 2, ... , n , are delivered by SA to each user U_j on secure channel and all R_{ij}'s are published.

C. Group Secret Reconstruction Stage

For reconstructing the l^{th} group secret S_l , the following steps are performed by at least l participants out of n along with the group secret combiner:

1) For j = 1, 2, ... , l each U_j calculates his pseudo secret share as c_{lj} = $h^l(x_j) \oplus x_j$, and then sends it over secure channel to the group secret combiner.
2) After receiving all c_{lj}'s, for j = 1, 2, ... , l, the l^{th} group secret is reconstructed by the group secret combiner as:

$$S_l = \left[\sum_{j=1}^{l} (c_{lj} + R_{lj}) \prod_{r=1, r\neq j}^{l} \frac{-ID_r}{ID_j - ID_r}\right] modp$$

III. SECURITY WEAKNESSES OF LIN-YEH'S METHOD

The multi-secret sharing scheme proposed by Lin-Yeh has following limitations:

1) Dealer selects the participant's secret share. Therefore, a dealer may become a cheater.
2) Secure channel is required between dealer and participants to distribute the secret share.
3) There is no mechanism to detect malicious participant.

IV. DOUBLE KNAPSACK ALGORITHM

Double knapsack algorithm is used to encode a message and make it secure over an insecure channel [18]. The algorithm is briefly described as follows:
Suppose there are two parties party 1 and party 2 who want to communicate securely.
Let r be the message to be encoded by party 1 and send to party 2.

Let l be the bit wise length of the message to be encoded.
Let n_1 be a random number which is known only to sender and receiver. They calculate a series of vectors called a_i, as $a_i = {n_1}^i$, where i = 0, 1, 2, ... , (l-1). i.e.
a_i = 1, ${n_1}^1$, ${n_1}^2$, ${n_1}^3$, ... , ${n_1}^{l-1}$
Therefore a_0 = 1, $a_1 = n_1$, ... , $a_{l-1} = {n_1}^{l-1}$
First, r is converted into binary form as:
r = b_{l-1}, b_{l-2}, b_{l-3}, ... , b_2, b_1, b_0.
Where b_{l-1} is the Most Significant Bit(MSB) and b_0 is the Least Significant Bit(LSB).
Next r is encoded as:
$R = \sum a_i b_i$
and R is sent in place of r by party 1 to party 2.
Note that only sender and recipient know the series a_i.
The r value is recovered from R in an iterative fashion as follows:
STEP 1 let k = 1
STEP 2 $R_1 = R - {n_1}^{l-k}$
STEP 3 If $R_1 \geq 0$, Then a binary bit 1 is assigned to b_{l-k} and $R = R_1$.
STEP 4 If $R_1 < 0$, then a binary bit 0 is assigned to b_{l-k}.
STEP 5 Increase the value of k by one.
STEP 6 If $k \leq l$, go to STEP 2 and if $k > l$, then end the process.
Subsequently, if we repeat the above steps on R for a different value of n_1 like n_2 then it is called the double knapsack algorithm. Double knapsack algorithm has higher security than single knapsack algorithm.

V. PROPOSED SCHEME

The proposed scheme consists of three phases namely, (A). System initialization and secret share generation, (B). Secret construction and distribution, (C). Verification and secret reconstruction. These phases are described as follows:

A. System Initialization and Secret Share Generation

Let p be a prime number, and let F_p denote the field of integers modulo p. An elliptic curve E is defined over F_p. Let G be a point in E(F_p), and suppose that G has prime order q i.e. qG = ∞. Let P = (P_1, P_2, ... , P_n) denote the set of n participants and ID_j be the identification of j^{th} participant. Let k (k $\geq$ 1) secrets to be shared be denoted by S = (S_1, S_2, ... , S_k). Let D be the trusted dealer.
Various steps involved in construction of shares are as follows:

1) The trusted dealer selects a generator G of prime order q. The dealer publishes the system parameters (p, E, q, G) on public channel.
2) Each participant P_j (1 $\leq$ j $\leq$ n) selects a random number $x_j \in Z_q^*$ as its own secret share and computes $R_j = x_j$ G mod p. The participant sends R_j to the dealer on public channel.
3) The dealer must ensure that for any values of i and j, $R_i \neq R_j$. If D finds that $R_i = R_j$ for some i and j then, D requests to participant j to send new R_j until D gets distinct values of R_j.
4) After collecting the R_j from all the participants the dealer chooses n distinct integers $ID_j \in Z_q^*$ (1 $\leq$ j $\leq$ n) as each participants identification. D will publish (R_j, ID_j) for all j = 1, 2, ... , n.

B. Secret Construction and Distribution

Secret construction and distribution is done as follows:

1) D randomly selects a number $b_0 \in Z_q^*$ and constructs a polynomial f(x) of degree k.
f(x) = $b_0 + S_1 x + S_2 x^2 + ... + S_k x^k$ mod p
Where $S_1, S_2, ..., S_k$ are k secrets to be shared.
2) For i = 1, 2, ... , k the dealer computes f(i).
3) D chooses another random number $x_0 \in Z_q^*$ and calculates $R_0 = x_0 G$ mod p and $I_j = x_o R_j$modp for j = 1, 2, ... , n. D computes the multiplicative inverse of x_0 as x_0^{-1} by using [($x_0 * x_0^{-1}$) mod p = 1] and by employing double knapsack algorithm encodes x_0^{-1} as y_0. D publishes R_0 and transmits y_0 to combiner on public channel.
4) D will select a group of participants t out of n, which is based on the number of secrets to be shared. The secret share of this group of participants will only be used by the combiner to reconstruct the secrets. Let the group be denoted as : A = $(ID_1, ID_2, ..., ID_t)$ where $t \leq n$.
5) D will observe the co-ordinates of I_t point for all ID_t, present in group A. Point I_t is represented as $(x, y)_t$ in co-ordinate form for t^{th} participant. Note that (x, y) is a point on elliptic curve E. The value of d is calculated by application of exclusive OR operation on the co-ordinates of I_t, in different ways in order to satisfy $d > k$, as mentioned below.
The algorithm known to both D and combiner has following steps:
   a) D will select minimum value from co-ordinate $(x, y)_t$ for all t and calculate d as:
   d = $[x_1 \oplus y_2 \oplus ... \oplus x_t]$ mod p
   where for ID_1 let min$(x, y)_1 = x_1$ (i.e. for ID_1 the x co-ordinate has minimum value) , for ID_2 let min$(x, y)_2 = y_2$ (i.e. for ID_2 the y co-ordinate has minimum value) , ... , and for ID_t let min$(x, y)_t = x_t$.
   If $d < k$ then D will change the A by increasing or decreasing the number of participants in A.
   b) If D will not get $d > k$ from step (a) then D calculates d by taking only x co-ordinates of I_t for all t present in A and calculates d as :
   d = $[x_1 \oplus x_2 \oplus ... \oplus x_t]$ mod p
   c) If D is again not able to get $d > k$ from step (b) then D calculates d by taking only y co-ordinates of I_t for all t $\leq$ n and calculates d as :
   d = $[y_1 \oplus y_2 \oplus ... \oplus y_t]$ mod p
   d) Till step (c) if D does not get desired value of d then D calculates d by taking sum of x and y co-ordinates of I_t for all t and calculates d as:
   d = $[(x_1 + y_1) \oplus (x_2 + y_2) \oplus ... \oplus (x_t + y_t)]$ mod p.
6) After getting d , D will compute f(d).
7) Using the double knapsack encoding algorithm the dealer will transmit the ID_t of the selected participants group A as A' and f(d) as f(d)' over a public channel. For using this algorithm the dealer and combiner agree on two random numbers n_1 and

 ISBN: 978-1-61208-493-0

n_2.

8) Then D will publish [f(1), f(2), ... , f(k), f(d)', A'].

C. Verification and Secret Reconstruction

Reconstruction of the secrets S_i (i = 1, 2, ... , k), and detection of cheater, is done by the combiner as follows :

1) Using the published information R_0 all the participants compute W_j = $x_j R_0$ and by employing double knapsack algorithm convert W_j in W_j'. Each participant delivers W_j' to the combiner on public channel. For this encoding the jth participant and combiner agree upon two random number.
2) The combiner decodes W_j from W_j' for all the participants, depending upon the knapsack constants on which the participant and combiner have agreed.
3) Now combiner decodes y_0 as x_0^{-1} by using n_1 and n_2 and checks whether $(x_0^{-1} * W_j) = R_j$ for all j = 1, 2, ... , n. If this is false then the malicious participant is detected.
4) Combiner gets [f(1), f(2), ... , f(k), f(d)', A'] from published information. Then it decodes the A' and f(d)' as A and f(d) respectively, by the knowledge of n_1 and n_2.
5) After getting group A, the combiner calculates d using the co-ordinates of W_j point of t participants by the same algorithm as used by dealer on the co-ordinates of I_j point for t participants present in group A, during secret construction phase.
6) After gathering the (k+1) data point [(1, f(1)), (2, f(2)), ... , (k, f(k)) and (d, f(d))] the combiner can reconstruct the k secrets using the following Lagrange interpolation:

$$f(x) = \left[\sum_{i=1}^{k+1} Y_i \prod_{j=1, j\neq i}^{k+1} \frac{x - X_j}{X_i - X_j}\right] modp$$

Where (X_i, Y_i) for i = 1, 2, ... , (k+1); denotes the (k+1) pairs respectively.

VI. SECURITY FEATURES AND COMPARISON OF THE PROPOSED SCHEME

A. Security Features

1) There is no role of dealer in selection of participant's secret share. Therefore, a dealer cannot become a cheater.
2) If an attacker attempts to get x_j from public information R_j, then the problem is equivalent to solving a discrete log problem on elliptic curves which is computationally hard.
3) The security of proposed scheme is based on the difficulty in solving the discrete logarithm problem on elliptic curves and finding double knapsack algorithm constants n_1 and n_2. In our scheme only D and combiner have the knowledge of A. Therefore, only the combiner can reconstruct the secrets using the Lagrange interpolation.

B. Malicious Participant Detection

The participants themselves generate the secret share x_j, so only the participant can calculate W_j using the published information R_0. The product of x_0^{-1} and W_j ensures that W_j belongs to the j^{th} participant only. If any malicious participant tries to give false value as W_j" then it is easily caught by verifying that $x_0^{-1} * W_j'' \neq R_j$. This is achieved by the use of a integer x_0^{-1}.

Theorem : If $(x_0^{-1} * W_j = R_j)$, then P_j is true; otherwise P_j may be a cheater.

Proof : $x_0^{-1} * W_j = x_0^{-1} * (x_j R_0) = x_0^{-1} * x_j * (x_0 * G) modp = (x_j G) modp = R_j$.

C. Performance Comparison

The performance comparison of the proposed scheme with the Lin-Yeh's scheme is shown in Table II. The Lin-Yeh's multi-secret sharing scheme is based on OHF and XOR operation, successive use of hash function in the scheme contributes great complexities [22]. Lin-Yeh's scheme

TABLE II. COMPARISON OF PROPOSED SCHEME WITH LIN-YEH'S SCHEME

S.No	Characteristics	Lin-Yeh's Scheme	Proposed Scheme
1	Mathematical structure used	OHF	ECDLP
2	Detection of malicious participant	No	Yes
3	Dependent on security of other cryptographic function such as hash function	Yes	No
4	Participant selects his secret share	No	Yes
5	Secure channel requirement during share distribution	Yes	No
6	Parallel secret reconstruction	No	Yes
7	Cryptanalytic strength	Less	More
8	Computation time	Less	Comparable

uses $(k(n + k))$ one-way hash functions and $(k(k - 2))$ modular multiplication computations [4]. As compared to the other operations, the time for performing the modular addition and the XOR operation is ignored, because they are negligible. The proposed scheme's complexity is mainly based on polynomial interpolation and the point multiplication computation on elliptic curve. The proposed scheme uses $(4n + 1)$ point multiplication computation on elliptic curve. Point multiplication is the most important and most basic operation in elliptic curve cryptosystem, and we have methods to speed up the computation [23]. Interpolation operations are the common property in the schemes, which are based on Shamir's secret sharing scheme. we have efficient algorithms [24], using them the performance of our proposed scheme is improved largely. Especially, when the degree of the polynomial f(x) is only 1, only two pairs of (1, f(1)) and (d, f(d)) are required to reconstruct the secret S, which largely reduces the computational complexity. The complexity due to double knapsack algorithm is acceptable, because it is important in order to detect the malicious participant. In addition, the proposed scheme does not need secure channel. Therefore, proposed scheme has more cryptanalytic strength and offers higher security.

VII. CONCLUSION AND FUTURE WORK

In this paper, a verifiable multi-secret sharing scheme, which is based on Shamir's threshold scheme and elliptic curve discrete logarithm problem is proposed. The scheme offers the advantages over Lin-Yeh's scheme with verification feature of

 ISBN: 978-1-61208-493-0

given shares and reduction in the cost of secure communication channel, required during secret distribution phase. The increase in computational complexity due to ECDLP is acceptable due to various advantages of Elliptic Curve Cryptosystem over other Cryptosystems. Therefore, the proposed scheme provides an efficient and secure mechanism for key management in public key systems. Key recovery mechanisms, distributed information storage and secure protocols, such as access control can be efficiently implemented by the proposed scheme.

The scheme proposed in this paper requires a trusted combiner during secret reconstruction and verification phase to detect malicious participants. The scheme can be modified in future, such that it does not require a trusted combiner.

REFERENCES

[1] A. Shamir, "How to share a secret?" Communication of the ACM, vol. 22, pp. 612-613, 1979.

[2] G. Blakley, "Safeguarding cryptographic keys," Proc AFIPS 1979 Nalt Conf, New York: AFIPS Press, vol. 48, pp. 313-317, 1979.

[3] A. Abdallah and M. Salleh, "Secret sharing scheme security and performance analysis," International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering, pp. 173-180, 2015.

[4] H. Y. Lin and Y. S. Yeh, "Dynamic multi-secret sharing scheme," International Journal of Contemporary Mathematical Sciences, vol. 3, pp. 37-42, 2008.

[5] J. He and E. Dawson, "Multistage secret sharing based on one-way function," Electron. Lett., Vo1. 30, pp. 1591-1592, 1994.

[6] L. Bai, "A strong ramp secret sharing scheme using matrix Projection," Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 652-656, 2006.

[7] Y. J. Geng, X. H. Fan, and F. Hong, "A new multi-secret sharing scheme with multi-policy," The 9th International Conference on Advanced Communication Technology, Vol. 3, pp. 1515-1517, 2007.

[8] F. Wang, L. Gu, S. Zheng, Y. Yang, and Z. Hu, "A novel verifiable dynamic multi-policy secret sharing scheme," Advanced Communication Technology (ICACT), The 12th International Conference, Vol. 2, pp. 1474-1479, 2010.

[9] D. Zhao, H. Peng, C. Wang, and Y. Yang, "A secret sharing scheme with a short share realizing the (t, n) threshold and the adversary structure," Computers and Mathematics with Applications, Vol. 64, Issue 4, pp. 611-615, August 2012.

[10] H. Pilaram and T. Eghlidosy, "An efficient lattice based multi-stage secret sharing scheme," in press, IEEE 2015.

[11] J. J. Zhao, J. Z. Zhang, and R. Zhao, "A practical verifiable multi-secret sharing scheme," Computer Standards and Interfaces, vol. 29, pp. 138-141, 2007.

[12] J. Qu, L. Zou, and J. Zhang, "A practical dynamic multi-secret sharing scheme," Information Theory and Information Security (ICITIS), pp. 629-631, 2010.

[13] A. Nalwaya, P. D. Vyavahare, and M. Panchal, "Veriable dynamic multi-secret sharing scheme," International Conference on Security and Management (SAM), pp. 186-188, 2013.

[14] M. Amara and A. Siad, "Elliptic curve cryptography and its applications," 7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA), pp. 247-250, 2011.

[15] L. D. Singh and T. Debbarma, "A new approach to elliptic curve cryptography," International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), pp. 78-82, 2014.

[16] D. Hankerson, A. Menezes, and S. Vanstone, "Guide to Elliptic Curve Cryptography," Springer, 2004.

[17] B. Qing-hai, Z. Wen-bo, J. Peng, and L. Xu, "Research on design principles of elliptic curve public key cryptography and its implementation," International Conference on Computer Science and Service System, pp. 1224-1227, 2012.

[18] R. R. Ramasamy, M. A. Prabakar, M. I. Devi, and M. Suguna, "Knapsack based ECC encryption and decryption," International Journal of Network Security, vol. 9, pp. 218-226, Nov. 2009.

[19] W. Stallings, "Cryptography and Network Security," Pearson, 2012.

[20] R. Markan and G. Kaur, "Literature survey on elliptic curve encryption techniques," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, pp. 906-909, 2013.

[21] S. Hua and W. Aimin, "A multi secret sharing scheme with general access structures based on elliptic curve," 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol. 2, pp. 629 632, 2010.

[22] A. Das and A. Adhikari, "An efficient multi-use multi-secret sharing scheme based on hash function," Applied Mathematics Letters, vol. 23, pp. 993-996, April 2010.

[23] R. M. Avanzi, H. Cohen, and C. Doche, "Handbook of Elliptic and Hyperelliptic Curve Cryptography", Chapman and Hall/CRC Press, 2005.

[24] K. H. Rosen, "Elementary Number Theory and Its Applications", Addison-Wesley, MA, 1993.

 ISBN: 978-1-61208-493-0