RESEARCH ARTICLE OPEN ACCESS

Proactive Secret Sharing using a Trivariate Polynomial

Chinneli Ashwini, Aalaya Seshadri,
chinneliashwini4@gmail.com
aalaya6@gmail.com

ABSTRACT
Secret sharing technique is a tool in cryptography which refers to distribution of a secret data among a group of n participants .The secret can be reconstructed by combining the individual share. To reconstruct secret, minimum of any t threshold subgroup or more shares are combined together. By secret sharing technique we can acquire secured and decentralized communication. The shares of the participants may be compromised because of huge exchange of messages. Secret sharing technique can be easily implemented by using polynomials. We propose a proactive secret sharing scheme, where shares are distributed and renewed periodically without changing the secret. This scheme also allows us to reconstruct and recover the share if share is lost. The share can also be verified to ensure its validity. Major contribution of the paper is implementing Proactive secret sharing scheme using Elliptic Curve cryptography and Trivariate polynomial [1].

Index Terms: Elliptic Curve cryptography, Secret Sharing, Proactive Secret Sharing.

I. INTRODUCTION

ELLIPTIC CURVE CRYTOGRAPHY (ECC) was first proposed by Neil Koblitz and Victor Miller in 1985. ECC is a public-key cryptography approach based on the algebraic structure of elliptic curves over finite fields.ECC provides equivalent security with smaller keys compared to non-ECC cryptography and also it reduces storage and transmission requirements. For example, a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key. The security of ECC depends on the elliptic curve logarithm problem, a solution which is infeasible if modulus is large. Security depends on computation of a point multiplication and it is hard to compute the multiplicand given the original and product points [7][8][11].

ECC uses two algebraic structures, an abelian group and a field. A group **{G,.}**,is a set of elements with binary operation (.).If pair of elements (a,b) are in G then element (a.b) is also in G. A group is said to be an abelian group if it satisfies properties like Closure, Associative, Identity element, Inverse element and Commutative. An abelian group has been defined over elliptic curves with addition operation that shows how points on the curve can be added to get another point on curve. Field is a set of elements with two binary operations (addition and multiplication). It can be a non-infinite field of real numbers, GF(p),where p is of prime order. Elliptic curve point multiplication is operation of adding a point along with elliptic curve to itself repeatedly [7].

Geometric description of Point Addition

Let E be an Elliptic curve equation $y^2 = x^3+ax+b$ with two distinct points P and Q results in negation of the point on the curve E ,P + Q = -R .We consider the mirror image (w.r.t x axis) of third point of intersection[11].$P=(x_p,y_p)$,$Q=(x_q,y_q)$
Therefore $P+Q=R=(x_r, y_r)$.
$X_r = \lambda^2 - x_p - x_q$.
$Y_r = \lambda (x_p - x_r) - y_p$.
$\lambda = (y_q - y_p)/(x_q - x_p)$.

Secret sharing was first invented by Adi Shamir and George Blakley independently. In Shamir's Secret sharing technique the secret information is distributed among a group of participants and only authorized subgroup (threshold number of participants) are permitted to reconstruct the secret[2][4].

Suppose the secret is divided among n participants and to recover the secret only threshold value (k) participants are required, this protocol is called as (k,n) threshold protocol. It is impossible to recover the secret with k-1 or less participants.

Blakley's secret sharing scheme is geometric in nature, where a secret is a point in an m-dimensional space, and n-shares are constructed with each share defining a hyper plane in this space. By finding the intersection of any m of these planes, the secret i.e., the point of intersection is obtained [9].

The shares distributed among the participants can be verified by using Verifiable secret sharing technique [3]. By this method we can

ensure the share obtained is acceptable and later used for reconstruction of secret.

Earlier the process of controlling and coordinating the whole share generation and allocation of shares among participants was through certification authority (CA). The role of CA is to distribute the individual share to each participant and ensuring that no participant gets any information about the actual secret. The dealer is responsible to protect the secret and renew the secret in case of loss of share or if share gets compromised. The goal of our paper is

1) To distribute the role of central authority among shareholders and build a decentralized process (without CA).
2) To construct a secure long lived communication by using our Proactive Secret sharing scheme which construct, distribute, verify, re-cover and renew the shares but the actual secret remains unchanged.

II. BACKGROUND

In the field of cryptography there are several techniques to convey the information securely as it provides Confidentiality and Integrity. By using Secret sharing technique the data can be transmitted securely among group of users (shareholders).Proactive secret sharing technique is more efficient to secure the shares as the renewal of shares is periodically performed and reconstruction of secret is done by threshold number of participants. Traditional secret sharing scheme and verifiable secret sharing scheme are described below:

2.1 Shamir's Secret Sharing

In Shamir's threshold scheme (k,n) [2], Data D is divided into D1,D2,D3..... Dn among *n* participants. The computation of reconstructing the secret is carried out by polynomial interpolation. In case of trusted third party, the dealer chooses the polynomial with a degree less than threshold k-1 (if threshold value is 3, then polynomial of degree 2 is chosen). Let the polynomial chosen by dealer is :

$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_{k-1}x^{k-1}$

The secret data $D = a_0$ and shares are computed by substituting the corresponding share numbers in polynomial. Share of 1st participant = p(1), Share to 2nd participant = p(2), ..., Share to nth participant = p(n).In order to find the polynomial chosen by dealer, we need to interpolate k out of n shares as degree of polynomial is k-1.

Recovering the secret

The polynomial is computed from shares using Lagrange interpolation [10]. To recover the secret we must obtain a polynomial and consider its independent term. To calculate a_0 we have $(x_1,y_1)\ldots. (x_k,y_k)$ points and $P(x) = \sum_{j=1}^{k} y_j . L_j (x)$, Where L_j is Lagrange coefficient,

$L_j = \prod_{i=1, i\neq j}^{k} (x - x_i)/(x_j - x_i)$.

After generation of polynomial, we obtain the secure data D by substituting 0 in P(x). Shamir's scheme is generally used in applications which involve mutual cooperation of individual and must cooperate.

2.2 Feldman's verifiable secret sharing Scheme

In Shamir's scheme, dealer distributes the secure data among the participants (share holders) but dealer may misbehave and distribute inconsistent shares to shareholders, by which they cannot reconstruct the secret. To overcome such abnormal behavior of the dealer, shareholders must verify the shares distributed to them. A scheme which has been implemented to verify consistent dealing of shares is known as Verifiable secret sharing [3][6].

Verification of Shares

In Feldman's secret sharing scheme, dealer selects an element g and a polynomial P(x) with coefficients $p_0, p_1, p_2 \ldots p_{k-1}$.Broadcasts the corresponding values $g^{p_0}, g^{p_1}, g^{p_2} \ldots, g^{p_{k-1}}$ and then secretly transmits the value $x_i = P(i)$ to the i^{th} shareholder. Now each shareholder verifies his own share by checking with the following equation $g^{x_i} = g^{p_0}.g^{p_1}, g^{p_2} \ldots, g^{p_{k-1}}$

Participant accepts the share if the above g^{x_i} value holds true and sends a message accepting its share as consistent or else sends a message as an inconsistent share which means the dealer is malicious.

III. PROACTIVE SECRET SHARING

Let the initial set (N) consists of n participants. Public parameters such as additive group G of prime order q, collision resistant hash function $h: \{0, 1\}^* \rightarrow Z_q$ and the threshold value t(which determines the security level of group) are set. If we want to deal with subgroups threshold t'value must be set. Security condition is $t' \leq t \leq n$ [1].

3.1 Description of our proposal

Proactive Secret sharing technique is an efficient way to transmit the data securely[5].To make the network robust and reliable the secrets of participants must be renewed periodically, verify and recover if share is lost.

This technique consists of 5 phases
1. Share Distribution
2. Share Verification
3. Share Reconstruction
4. Share Renewal
5. Share Recovery.

3.2 Architecture of Our proposal

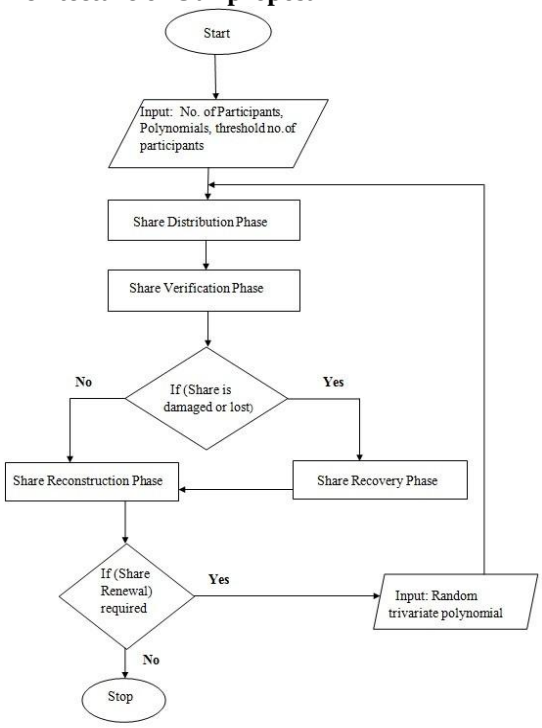

Fig 1: Block Diagram of the Proposed System

Fig 1, represents the various phases of proactive secret sharing scheme and the flow of protocol can be easily understood.

3.3 Share Distribution Protocol

In Share distribution phase each participant select a trivariate polynomial and distributes a bivariate share value by substituting the corresponding hash value of the participant in polynomial and then each participant computes his final share. It also provides commitments to other participants for verification of share. Let G be additive group and P is the generator point in G. All the participants run the following protocol [1].

1) Each participant Ni ∈ N chooses a random trivariate polynomial P_i (x, y, z) ∈ Z_q [x, y, z], with degree at most t-1 in the variables x and y, degree at most t'-1 in the variable z and symmetric with respect to variables x and y. P(x, y, z) = $\sum_{Ni \epsilon N} Pi(x,y,z)$. Let $p_{i,0} = P_i$ (0, 0, 0) and s = $\sum_{Ni \epsilon N} p_{i,0}$ = P(0, 0, 0).
2) Each participant $N_i \in N$ secretly sends to each of the other participants $N_j \in N$ the polynomial $P_{ij} = P_i$ (x, h(Nj), z) and the value $Y_i = p_{i,0} * P$. Where h(Nj) is the hash value of i^{th} participant and P is point generator in group G.

3) Each participant in $N_i \in N$ after btaining P_{ij} from all other participants, computes its final secret information $P_j(x,z)$,which is a bivariate polynomial.
$P_j(x,z)=\sum_{Ni \epsilon N} Pij(x,z)= \sum_{Ni \epsilon N} Pi(x, h(Nj), z)$.
4) Each participant $N_i \epsilon N$ secretly sends its commitment C_{ik} to all other participants $N_k \epsilon N$. $C^i_{mnj} = b^i_{mnj} * P$, where b^i_{mnj} is co-efficient multiplying $x^m y^n z^j$ in $P_i(x, y, z)$.
$C^{ik} = \sum C^i_{mnj} \_ * h(N_k)^n$.

3.4 Share Verification Protocol

Share Verification phase is important phase in proactive secret sharing technique because if the share received is incorrect the secret cannot be recovered. In this phase the shares received from other participants will be verified by using the commitment which is sent by the participant. If the shares received from all participants are correct then each participant computes the final share. If the share obtained is incorrect then share recovery can be applied and obtain correct share.

1) Each participant $N_i \epsilon N$ receives commitment C_{ik} and share $P_{ij}(x,z)$ from all other shareholders $N_k \in N$. $C^i_{mnj} = b^i_{mnj} * P$, Where b^i_{mnj} is co-efficient multiplying $x^m y^n z^j$ in $P_i(x, y, z)$. $C^{ik} = \sum C^i_{mnj} * h(N_k)^n$.
2) Each participant k calculates $\sum b^k_{mj} * P$, where b^k_{mj} is a coefficient of $x^m z^j$ in share s_{ik}.
3) Participant verifies share s_{ik} by comparing $C^{ik} = \sum b^k_{mj} * P$. If it holds true share received is correct.

3.5 Share Renewal Protocol

Share Renewal Phase is important in proactive secret sharing technique as it helps in long lived communication. In this phase, the share of each participant is renewed periodically to provide secure and robust network. The actual secret remains unchanged but shares of participants get renewed. Initial polynomials of each participant be $P_i(x, y, z)$ and share be $P_i(x, z)$.

1) Each participant has to select a new trivariate polynomial $P`_i(x, y, z) \in Z_q[x, y, z]$ such that its free term must be zero i.e. P`(0,0,0)=0.
2) Each participant $N_i \in N$ secretly sends to each of the other participants $N_j \in N$ the polynomial. $P`_{ij}=P`_i(x,h(N_j), z)$.where $h(N_j)$ is the hash value of j^{th} node .
3) Each participant in N after obtaining $P`_{ij}$ from all other participants, each participant $N_i \in N$ computes its final secret information $P`_j(x,z)$, which is a bivariate polynomial.

$P`_j(x,z) = \sum_{Ni \epsilon N} P`_{ij}(x,z) = \sum_{Ni \epsilon N} P`_i(x, h(Nj),z)$.

4) The shares of each participant gets renewed by adding the previous share $P_j(x, z)$ with new share P`j(x,z) as Renewed share

$RS = P_j(x, z) + P`_j(x, z)$.

3.6 Share Reconstruction Protocol

In Share Reconstruction Phase, the actual secret can be reconstructed by interpolating any k (threshold) shares among n shares. By interpolation of shares (Bivariate polynomials) we acquire a polynomial as a resultant and secured data is obtained by substituting zero in polynomial since the free term is secret data.

1) Select any threshold number of shares and by applying Lagrange Interpolation. $P(x) = \sum_{j \epsilon t} P_j(x,z). l_j(x)$.

Where $l_j(x) = \pi_{m \epsilon t}(x-x_m)/(x_j-x_m)$ & $m \neq j$ and $l_j(x)$ is Lagrange coefficient.

2) Secret can be obtained by substituting zero in the polynomial P(0)=S(actual secret).

3.7 Share Recovery Protocol

In Share Recovery Phase the participants whose share is either compromised or damaged can be recovered as follows:

1) If participant N_r loses its share, then to recover the previous share. N_r requests a threshold group (t) N_M of existing participants in process.
2) If a participant $N_j \epsilon N_M$ accepts to recover the share of participant N_r, it secretly send $P_j(h(N_r), z)$ to N_r.
3) $P_j(h(N_r),z) = P(h(N_r), h(N_j), z)$ When participant N_r receives this information from t different nodes, it can obtain its secret share polynomial $P_r(x, z)$ by using Lagrange interpolation.

IV. CONCLUSION

Secret sharing scheme in field of cryptography provides a secure transmission of data. Our proposal proactive secret sharing technique using trivariate polynomials provide an effective way to transfer the data securely. Using this we can handle a decentralized communication securely for long period of time. By using Elliptic curve concept the computation for proactive secret sharing is easy. This scheme can be applied in Manets to acheive efficient decentralization and dynamicness.

REFERENCES

[1]. Paz Morillo Vanesa Daza a, Javier Herranz b. Cryptographic techniques for mobile ad-hoc networks. Computer Networks, 51:49384950, 2007.
[2]. Adi Shamir. How to share a secret. Communications of ACM, 22(11):612613, 1979.
[3]. Feldman, A Practical Scheme for Non-Interactive Verifiable Secret Sharing, Proc.of the 28th IEEE Symposium on the Foundations of Computer Science, 1987, 427-437.
[4]. Amos Beimel, Secret Sharing Schemes: Survey, Department of Computer Science,Ben-Gurion University, Isreal.
[5]. Herzberg, Jareck and, Krawczyk, Proactive Secret Sharing, IBM T.J. Watson Research Center,NY, 1995.
[6]. Michael Backes, Aniket Kate, Arpita Patra,Computational Veriable Secret Sharing.
[7]. William Stallings,"Textbook - Cryptography and Network Security"
[8]. Forouzan,"Textbook -Cryptography and Network Security"
[9]. G. Blakley. Safeguarding cryptographic keys. In Proc. Of AFIPS National Computer Conference,1979.
[10]. Jeffreys, H. and Jeffreys, B. S. "Lagrange's Interpolation Formula." 9.011 in Methods of Mathematical Physics, 3rd ed. Cambridge, England: Cambridge University Press, p. 260, 1988.
[11]. Anoop MS,"Elliptic Curve Cryptography"An Implementation Guide.

Chinneli Ashwini graduated in Computer Science and Engineering from JNTUH. She is currently pursuing M.tech from JNTUH, Hyderabad. Her research interest include secret sharing, MANET's and Security in Sensor Networks.

Seshadri Aalaya graduated in Information Technology from JNTUH, Hyderabad .Her research interest include secret sharing, Elliptic Curve Cryptography and Light- Weight Cryptography.