ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

A Novel (t, n) Threshold Secret Sharing Using Dot Product of Linearly Independent Vectors

Sonali Patil[1], Prashant Deshmukh[2]

Research Scholar, Sipna College of Engineering and Technology, Amravati - 444 701, Maharashtra, India[1]

Abstract: Threshold schemes are ideally suited to situations where a group of mutually suspicious individuals with conflicting interests must cooperate. The schemes allow a user to divide portions of a secret among a participants group. Any t or more participants from a participants group of n members can cooperate to regain the original secret while (t-1) or fewer participants cannot reveal anything about the original secret. In this paper we proposed a (t, n) threshold secret sharing scheme using dot product of linearly independent vectors and Vandermonde matrix. The proposed scheme is ideal as share size is same as secret, perfect as (t-1) participants cannot retrieve any information about the secret and secure as based on dot product of problem. Also the proposed scheme can be extended for additional capabilities of secret sharing using properties of dot product of vectors.

Keywords: Secret Sharing, Network Security, Information Security, Cryptography

I. INTRODUCTION

Security of secret data is major concern in today's digitized world. We cannot trust on a single person and also if multiple people are involved then the less knowledge or power each entity has the better. Secret sharing schemes allow improving the level of protection without increasing the risk of exposure. Secret Sharing Schemes (SSS) [1] refers to method for distributing a secret among a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together, individual shares are of no use on their own. Some important concepts are defined below related to secret sharing.

- Information Rate: The information rate was studied by Stinson [1]. It is a measure of the amount of information that the participants need to keep secret in a secret sharing scheme. The information rate for a particular shareholder is the bit-size ratio (size of the shared secret) / (size of that user's share). The information rate for a secret sharing scheme itself is the minimum such rate over all participants [2]. The efficiency of a secret sharing scheme is measured by its information rate.
- Perfect: A perfect threshold scheme is a threshold scheme in which knowing only (t - 1) or fewer shares reveal no information about Secret S what so ever, in the information theoretic sense [2] [3].
- Ideal Secret Sharing: Secret sharing schemes with information rate 1 are called ideal [2]. Scheme is ideal if share has the same length as secret. Ideal property can be thought as efficiency.

In the next section we will discuss about threshold secret sharing schemes.

II. LITERATURE SURVEY CRUX

First threshold schemes were independently invented by both Adi Shamir [5] and George Blakely [6] in 1979. The definition outlined in [1] to describe what a threshold secret sharing scheme is:

Definition: Let t and n be positive integers, $t \leq n$. A (t, n) - threshold scheme is a method of sharing a key K among a set of n players (denoted by P), in such a way that any t participants can compute the value of K, but no group of t-1 participants can do so.

The value of t is chosen by a special participant which is referred to by [1] as the dealer. When D wants to share the key K among the participants in P, gives each participant some partial information referred to earlier as a share. The shares should be distributed secretly, so no participant knows the share given to any other participant. At some later time, a subset of participants $B \subseteq P$ will pool their shares in an attempt to compute the key K. Alternatively they could give their shares to a trusted authority which will perform the computation on their behalf. If $|B| \geq k$, then they should be able to compute the value of K as a function of the shares they collectively hold. Furthermore if $|B| < t$, then they should determine nothing about the value of K.

Shamir's (t, n) threshold scheme is based on Lagrange's Interpolating polynomial. This scheme is information-theoretically secure scheme. By using Shamir's threshold scheme concept we can get a very robust key

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

management scheme. Sonali and Prashant [7] [8] discussed some threshold schemes proposed in recent years. Li Bai [9] developed a threshold secret sharing scheme using matrix projection. The idea is based upon the invariance property of matrix projection.

Chunming Tang and Zheng-an Yao [10] proposed a threshold scheme based on multi-prover zero-knowledge arguments and secure multi-party computation protocol to avoid the malpractices by dishonest participants. It checks for minimum required honest participants before sharing the secret. To change the threshold value of Shamir's scheme without dealer's assistance is possible by Shi and Zhong [11]. In this scheme all participants cooperate to take on the dealer's role and to get proactive secret sharing too. Chou, Lin and Li [12] proposed a threshold scheme using Sudoku with improved security in data transfer due to large number of solutions in Sudoku.

Here Shamir's Secret Sharing, Blakley's Secret Sharing and Li Bai's Secret Sharing are discussed in detail:

Shamir secret sharing [5]:

Shamir secret sharing is based on polynomial interpolation over a finite field. Shamir developed the idea of a (t, n) threshold-based secret sharing technique ($t \leq n$). The technique allows a polynomial function of order $(t-1)$ constructed as,

$f(x) = d_0 + d_1x_1 + d_2x_2 + \ldots + d_{t-1}x_{t-1} \pmod p$, where the value d_0 is the secret and p is a prime number.

The secret shares are the pairs of values (x_i, y_i), where $y_i = f(x_i)$, $1 \leq i \leq n$ and $0 < x_1 < x_2 \ldots < x_n \leq p - 1$.

The polynomial function f(x) is destroyed after each shareholder possesses a pair of values (x_i, y_i) so that no single shareholder knows the secret value d_0. In fact, no groups of $t - 1$ or fewer secret shares can discover the secret d_0.

On the other hand, when t or more secret shares are available, then we may set at least t linear equations $y_i = f(x_i)$ for the unknown d_i's. The unique solution to these equations shows that the secret value d_0 can be easily obtained by using Lagrange interpolation.

Blakley's Secret Sharing Scheme [6]:

Blakley's SSS uses hyper plane geometry to solve the secret sharing problem. To implement a (t, n) threshold scheme, each of the n users is given a hyper-plane equation in a t dimensional space over a finite field such that each hyper plane passes through a certain point. The intersection point of the hyper planes is the secret. When t users come together, they can solve the system of equations to find the secret.

The secret is a point in a t dimensional space and n shares are affine hyper planes that pass through this point. An affine hyperplane in a t -dimensional space with coordinates in a field F can be described by a linear equation of the following form: $a_1x_1+a_2x_2+ \ldots .. +a_tx_t=b$.

Reconstruction of original secret is simply finding the solution of a linear system of equations. The intersection point is obtained by finding the inter-section of any t of these hyper planes. The secret can be any of the coordinates of the intersection point or any function of the coordinates.

Li Bai's Secret Sharing [9]:

Li Bai developed a threshold secret sharing based upon the invariance property of matrix projection.

The scheme is divided in two phases:

Construction of Secret Shares from Secret Matrix S

1. Construct a random $m \times k$ matrix A of rank k where $m > 2(k - 1) – 1$.
2. Choose n linearly independent $k \times 1$ random vectors x_i.
3. Calculate share $v_i = (A \times x_i) \pmod p$ for $1 \leq i \leq n$, where p is a prime number.
4. Compute $\$ = (A (A'A)^{-1}A') \pmod p$.
5. Solve $R = (S - \$) \pmod p$.
6. Destroy matrix A, x_i's, \$, S and
7. Distribute n shares v_i to n participants and make matrix R publicly known.

Secret Reconstruction

1. Collect k shares from any k participants, say the shares are $v_1, v_2, \ldots, v_k$ and construct a matrix $B = [v_1\ v_2 \ldots v_k]$.
2. Calculate the projection matrix $\$ = (B (B'B)^{-1}B') \pmod p$.
3. Compute the secret $S = (\$ + R \pmod p)$.

These three methods which are discussed in detail here are compared with the proposed scheme in section IV. In the next section we will discuss the proposed method.

III. PROPOSED METHOD

The tool used for proposed method is linearly independent vectors and their dot product.

Dot Product of vectors

$$\vec{u} = \langle u_1, u_2, u_3 \rangle \text{ and } \vec{v} = \langle v_1, v_2, v_3 \rangle \text{ is}$$

$$\vec{u} \cdot \vec{v} = u_1v_1 + u_2v_2 + u_3v_3.$$

Assumptions:

Set of participants: P = {P1, P2, ... ,Pn},
Secret to be shared: S
No of Participants: n
Threshold (i.e. no of minimum participants required): t
Dealer: D

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

Construction of Secret Shares from Secret S

1. Choose a random vector X and random vector $ of size t such that S=$.X.
2. Choose Vandermode Matrix Yij where $1 \leq i \leq n$ and $1 \leq j \leq t$.
3. Compute Shares Si, where $1 \leq i \leq n$ as:

$S1=\$_1.Y_{11}+\$_2.Y_{12}+.....\$_t.Y_{1t}$
$S2=\$_1.Y_{21}+\$_2.Y_{22}+.....\$_t.Y_{2t}$
.
.
.
$Sn= \$_1.Y_{n1}+\$_2.Y_{n2}+.....\$_t.Y_{nt}$

4. Destroy Secret S and vector $.
5. Distributes n shares Si to n participants.
6. Make matrix Y and vector X publicly known.

Secret Reconstruction

Minimum t number of participants should participate to reconstruct the original secret S.
Dealer asks the shareholders to submit their shares.

Dealer selects any t participants shares S1, S2, ... St for reconstruction of the original secret.

Dealer reform Vector $ from t shares and public matrix Y. (As Si=$i.Yi1+$2.Yi2+...$t.Yit).

Dealer reconstructs the original secret S by taking the dot product of vectors $ and public vector X.

The scheme can be extended for other additional capabilities of secret sharing due to following properties of Dot Product:

1. The commutative property holds : $\vec{u} \cdot \vec{v} = \vec{v} \cdot \vec{u}$.
2. The distributive property holds : $\vec{u} \cdot (\vec{v} + \vec{w}) = \vec{u} \cdot \vec{v} + \vec{u} \cdot \vec{w}$
3. $c(\vec{u} \cdot \vec{v}) = c\vec{u} \cdot \vec{v} = \vec{u} \cdot c\vec{v}$
4. $\vec{0} \cdot \vec{v} = \vec{0}$
5. $\vec{v} \cdot \vec{v} = \|\vec{v}\|^2$

The proposed scheme is compared with other existing threshold schemes in next section.

IV. COMPARATIVE RESULTS

The proposed scheme is compared with existing Threshold Secret Sharing Schemes like Shamir's Secret Sharing, Blakley's Secret Sharing and Li Bai's Secret Sharing.

TABLE 1: COMPARATIVE STUDY

Parameters	Secret Sharing Schemes			
	Shamir's Secret Sharing	**Blakley's Secret Sharing**	**Li Bai's Secret Sharing**	**Proposed Scheme**
Perfect	Yes	No	No	Yes
Ideal	Yes	Yes	Yes	Yes
Security of scheme	Less	Less	Less	More(*)
Multiple Secret Sharing	No	No	Yes	Yes(**)

1. The actual secret is shared directly in Shamir's SSS, Blakleys SS and Li Bai's Secret Sharing. But in proposed Secret Sharing Scheme the actual secret is not shared right away but the dot product of an intermediate secret vector is shared among the participants
2. The proposed scheme can be used for multiple secret sharing by making vector $ as a secret values

V. CONCLUSION

In this paper we have proposed a secure (t, n)-threshold secret sharing scheme. The scheme is perfect because knowledge of (t - 1) or fewer shares does not narrow the range of possible values that the secret could take. The scheme is ideal because the information rate (size of the shared secret) / (size of that user's share) = 1. The security of the secret is guaranteed by the dot product problem. Also using the properties of dot product the scheme can be extended to proactive and verifiable secret sharing.

REFERENCES

[1] D. R. Stinson,"Cryptography:Theory and Practice",CRC Press, Boca Raton 1995.
[2] Menezes, A., P. van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996, pp. 524-528
[3] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," vol. IT-29, no. 1, pp. 35–41, Jan. 1983.
[4] Y. Desmedt and Y. Frankel, "Threshold cryptosystems", In Proc. of CRYPTO'89 , volume 435 of LNCS , pages 307–315. Springer-Verlag, 1990.
[5] Shamir,A., "How to Share a Secret", Communications of the ACM, vol.22, no.11, 1979.
[6] G. Blakely, "Safeguarding cryptographic keys", presented at the Proceedings of the AFIPS 1979 National Computer Conference, vol. 48, Arlington, VA, June 1997, pp. 313–317.
[7] Sonali Patil, Dr. Prashant Deshmukh, "An Explication of Multifarious Secret Sharing Schemes", International Journal of

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

Computer Applications IJCA USA, Volume 46– No.19, May 2012 ISSN: 0975 – 8887.

[8] Sonali Patil, Prashant Deshmukh**,** "Analyzing Relation in Application Semantics and Extended Capabilities for Secret Sharing Schemes", International Journal of Computer Science Issues, IJCSI, Mauritious, Volume 9, Issue 3, May 2012 ISSN: 1694-0784.

[9] Li Bai, "A strong ramp secret sharing scheme using matrix projection," presented at the Second International Workshop on Trust, Security and Privacy for Ubiquitous Computing, Niagara-Falls, Buffalo, NY, 2006.

[10] Chunming Tang, Zheng-an Yao, "A New (*t, n*)-Threshold Secret Sharing Scheme", International Conference on Advanced Computer Theory and Engineering, IEEE 2008 p. 920-924.

[11] Runhua Shi, Hong Zhong, "A Secret Sharing Scheme with the Changeable Threshold Value", International Symposium on Information Engineering and Electronic Commerce, IEEE 2009 p. 233-236.

[12] Yung-Chen Chou, Chih-Hung Lin, Pao-Ching Li, Yu-Chiang Li, "A (2, 3) Threshold Secret Sharing Scheme Using Sudoku", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE 2010.

BIOGRAPHY

Sonali Patil pursuing Ph.D. from Amravati University. Her research interests include secret sharing, data security. She has published several papers. Currently she is working as an Assistant Professor at Computer Enginering Department in PCCOE, Akurdi, Pune.