AN EXPLICATION OF SECRET SHARING SCHEMES WITH GENERAL ACCESS STRUCTURE

Sonali Patil[1], Kapil Tajane[2], Janhavi Sirdeshpande[2]
[1]Assistant Professor & [2]ME Student,
Pimpri Chinchwad College of Engineering, Nigdi, Pune, India

ABSTRACT

The basic idea in secret sharing is to divide the secret key into pieces, also called as 'shares' and distribute the pieces to different persons so that certain subsets of the persons can get together to recover the key. In the outline of threshold schemes, we wanted k out of n participants to be able to determine the key. In practice, it is often needed that only certain specified subsets of the participants should be able to recover the secret. A more general situation is to specify exactly which subsets of participants should be able to determine the key and those that should not. The Access structure describes all the authorized subsets to design the access structure with required capabilities. The goal of the general access structure secret sharing scheme is to provide the flexibility to decide which specified subsets of participants will able to reconstruct the original secret and which subsets cannot. The intent of this paper is to provide an analysis of some existing General Access Structure Secret Sharing Schemes. The comparative study shows there is a need of better General Access Structure scheme to fulfil the need of applications.

KEYWORDS: *Data Security, Extended capabilities, General Access Structure, Network security, SecretSharing.*

I. INTRODUCTION

The idea of secret sharing is to start with a secret, divide it into pieces called shares, which are then distributed amongst users by the dealer. Only authorized subsets of participants can reconstruct the original secret. More formally a Secret Sharing Scheme (SSS) is a method whereby n pieces of information called shares or shadows are assigned to a secret key K in such a way that: i) The secret key can be reconstructed from certain authorized groups of shares and ii) The secret key cannot be reconstructed from unauthorized groups of shares. Electronic voting, electronic cash are good applications for general access structure.

Let's denote Γ as being a set of subsets of P, and the subsets in Γ as being the subset of participants that should be able to compute the key. Then Γ is denoted as being the access structure and the subsets in Γ are called authorized subsets. Furthermore if we let K be the set of keys and S be the share set, we use the dealer D to share a key k Є K by giving each player a share S_i Є S. Sometime later a subset of players might attempt to determine K from the shares they collectively hold.

Definition (Stinson, [5]) A perfect secret sharing scheme using the general access structure Γ, is a method of sharing a key K among a set of n participants such that P is the set of all participants, in such a way that the following two properties are fulfilled:

- If an authorized subset of participants $B \subseteq P$ pool their shares, so that they can determine the value of K.
- If an unauthorized subset of participants $C \subseteq P$ pools their shares, then they can determine nothing about the value of K.

It is noticed that a (k, n)-threshold scheme generates the access structure $\{B \subseteq P \mid |B| \geq t\}$. This structure is referred to by Stinson [5] as the threshold access structure. It is possible to generate a SSS for any access structure as long as this access structure satisfies monotone property:

- subset B Є Γ and B ⊆ C ⊆ P then C Є Γ.

In other words a superset of an authorized set is again an authorized set.

The rest of the paper is organized as follows. In Section II some definitions are discussed. Section III covers Literature Survey Crux: general access structure for secret sharing schemes. In section IV performance analysis of these schemes based on various parameters are discussed. Finally in section V, we summarize the comparative results.

II. Some Definitions

Formal foundation of secret sharing was formulated using the information theory. Two important concepts were defined based on information rate: ideal and perfect schemes.

Information Rate: The information rate was studied by Stinson [5]. 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 [6] [2]. The efficiency of a secret sharing scheme is measured by its information rate.

Ideal Secret Sharing: Secret sharing schemes with information rate 1 are called ideal [7]. Scheme is ideal if share has the same length as secret. Ideal property can be thought as efficiency.

Perfect: A perfect threshold scheme is a threshold scheme in which knowing only (t - 1) or fewer shares reveal no information about Secret S whatsoever, in the information theoretic sense [6] [2].

Qualified subset: The participants in a qualified set can collaboratively recover the secret. It is denoted by Γ_{Qual}.

Forbidden subset: The participants in a forbidden set cannot recover the secret. It is denoted by $\Gamma_{Forb.}$

III. General Access Structure Secret Sharing Schemes: Literature Survey Crux

1.1. Sonali, Kapil, Janhavi[21]:

In [21] author has implemented a simple and lossless general access (n, n) secret sharing scheme using modulo-2 operation. The scheme is ideal as created shares are of same size as original secret image. The scheme is perfect as only qualified subsets of shares can reconstruct the original secret image. The forbidden group of shareholders cannot reveal anything about the original secret image. The complexity of implemented scheme is very low as the method used to create the shares and to get general access structure is very simple. In future parallel algorithm can be used to make this scheme faster.

1.2. X. Wu, W. Sun[20]:

In [20] author proposed a Random Grid (RG) based visual secret sharing scheme for general access structure. The existing RG based schemes are special cases of the proposed scheme. By using the proposed scheme complicated sharing strategy can be implemented which is fit for practical applications. In this scheme secret image is encoded into n RGs while qualified sets can recover the secret visually and forbidden sets cannot. The advanced merits provided by the proposed scheme are: no pixel expansion, no code book required and no image distortion.

1.3.Sun Hua and Wang Aimin[18]:

In [18] author proposed a new secret sharing scheme for general access structure based on Shamir's threshold scheme and elliptic curve. In this scheme each participant selects his own secret and the dealer need not deliver any secret information to each participant. The existing secret does not need to be changed when the shared secret is renewed, the access structure is modified, and participants are added or deleted. The proposed scheme is able to prevent adversaries from getting the secret and efficiently guard against the cheating among participants. It has better security and efficiency because of no secret communication required in the secret distribution phase. Multiple secrets instead of only one secret can be shared in each sharing session without redistributing participant's secret shadow. The security of scheme is based on Shamir's secret sharing scheme and discrete logarithm.

1.4. SAI-ZHI[14]:

In [14] author proposed a dynamic and verifiable multiple secrets sharing based on general access structure. The scheme allows each participant to choose his secret shadow by himself. In this scheme cheating is verifiable and it can dynamically change participant set, the qualified subset and the number of the shared secrets without refreshing any participant's secret shadow. The scheme gives additional capability of verifying the shares.

1.5.WeiYun, Zhong Pucha[13]:

In [13] author proposed a low computational, multi-stage secret sharing scheme with general access structure in which each participant has to hold one shadow only to share more than one secret. It is possible to change the participants set and access structure dynamically without updating any participants secret shadow. The proposed scheme has advantages over the existing schemes and is more practical. There are some disadvantages such as the secret shadows are chosen by the dealer. The scheme fails to prevent cheating during the reconstruction of secrets.

1.6.Surjadi Slamet, Kiki Ariyanti Sugeng, Mirka Miller[11]:

In [11] author proposed a new scheme which shows how sum labeling can be used for representing the graphs of access structure of secret sharing scheme. Here author has combined Shamir's scheme with graph access structure represented using sum graph labeling to obtain a new secret sharing scheme for general access structure. The scheme uses multiple assignments of shares. In this scheme each participant holds 2 shares at a time.

1.7.K. Srinathan [9]:

In [9] author focused on non perfect secret sharing schemes for general access structure. To handle non perfect secret sharing for general access structure is more challenging task. This scheme defines a more general notion of access hierarchies and describes their tolerability properties.

1.8.Benaloh and Leichter[4]:

In [4] author gave a simpler and more efficient way to realize general access structure schemes. They also proved that no threshold scheme is sufficient to realize secret sharing on general monotone access structures.

1.9.Ito Saito[3]:

[3] is the pioneer method for general access structure for secret sharing schemes. It is the basic scheme for general access structure based on Shamir's (k,n) threshold scheme. In proposed scheme, a secret S is divided into pieces which are shared by a set P of participants. The family { P'⊆P : P' can reconstruct the secrets} is called the general access structure of secret sharing scheme.

IV. PERFORMANCE ANALYSIS OF GAS SCHEMES

Few secret sharing schemes are considered for comparative study based on some parameters. The following table summarizes that:

Table 1: Comparative Study of GAS

GAS Schemes	Year	Ideal	Perfect	Enrolment/ Disenrollment	Multiple assignment	Reconstruction of Lost Shares
Sonali, Kapil, Janhavi [21]	2012	Yes	Yes	No	Yes	No

X. Wu, W. Sun[20]	2012	Yes	No	No	No	No
Sun Hua, Wang Aimin[18]	2010	Yes	Yes	Yes	Yes	Yes
Chou,Lin,Li[17]	2010	Yes	Yes	No	No	No
Sai- zhi[14]	2009	No	No	Yes	Yes	Yes
Wei Yun, Zhong Pucha[13]	2008	Yes	Yes	Yes	No	No
Slamet, Sugeng, Miller[11]	2006	No	Yes	No	Yes	No
K. Srinathan[9]	2002	No	No	No	No	No
Benaloh, J., and J. Leichter[4]	1988	No	No	No	No	No
Ito,Saito, Nishizeki[3]	1987	Yes	No	No	Yes	No

V. CONCLUSION

In this paper various General Access Structure secret sharing schemes are studied. Table I gives comparative study of some General Access Structure Schemes based on performance parameters like ideal, perfect, enrolment/disenrollment, multiple assignments of shares, and reconstruction of lost corrupted shares.

VI. FUTURE WORK

There is a lot advancing in the field of secret sharing. Applications for secret sharing schemes seem to be getting more important. The comparative study shows that to add extra functionalities like enrolment and disenrollment of shareholders, renewing of existing shares is difficult with general access structures. In future a better general access structure secret sharing can be implemented with all the extended capabilities.

REFERENCES

[1] Shamir, A., “How to Share a Secret”, Communications of the ACM, vol.22, no.11, 1979.

[2] E. D. Karnin, J. W. Greene, and M. E. Hellman, “On secret sharing systems,” vol. IT-29, no. 1, pp. 35–41, Jan. 1983.

[3] Mitsuru Ito, Akira Saito, Takao Nishizeki, “Secret Sharing Scheme: Realizing General Access Structure”, GLOBECOM IEEE 1987.

[4] Benaloh, J., and J. Leichter, Generalized secret sharing and monotone functions, CRYPTO '88, Springer Verlag, pp. 27-35.

[5] D. R. Stinson, “Cryptography: Theory and Practice”, CRC Press, Boca Raton 1995.

[6] Menezes, A., P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996, pp. 524-528

[7] P. Paillier, “On ideal non-perfect secret sharing schemes,” in Security Protocols Workshop, 1997, pp. 207–216.

[8] 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.

[9] K. Srinathan, N. Tharani Rajan, and C. Pandu Rangan, “Non-perfect secret sharing over general access structures,” in INDOCRYPT, 2002, pp. 409–421

[10] Pang, L.-J., Li, H.-X., Wang, Y.-M., “A secure and efficient secret sharing scheme with general access structures”, Lecture Notes in Computer Science v 4223 LNAI, Fuzzy Systems and Knowledge Discovery - Third International Conference, FSKD 2006, Proceeding 2006, p. 646-649.

[11] Surjadi Slamet, Kiki Ariyanti Sugeng, Mirka Miller “Sum Graph Based Access Structure In a Secret Sharing Scheme” Journal of Prime Research in Mathematics Vol. 2(2006),1113-119.

[12] 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.

[13] WEI Yun, ZHONG Pucha:” A multi-stage secret sharing scheme with general access structures” 978-1-4244-2108-4/08/$25.00 © 2008 IEEE

[14] Sai-zhi Ye, Guo-xiang Yao, Quan-long Guan, “A multiple secret sharing scheme with general access structure, International Symposium on Intelligent Ubiquitous Computing and Education, 2009 IEEE

[15] 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.

[16] Chao-Wen Chan, Chin-Chen Chang, Zhi-Hui Wang, “Cheating Resistance for Secret Sharing”, International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009 IEEE p. 840-846..

[17] 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.

[18] Sun Hua and Wang Aimin ,” A Multi-Secret Sharing Scheme with General Access Structures based on Elliptic Curve” 3rd International Conference on Advanced Computer Theory and Engineering 2010 IEEE

[19] Sonali Patil, Prashant Deshmukh ”An Explication of Multifarious Secret Sharing Schemes”International Journal of Computer Applications (0975 – 8887) Volume 46– No.19, May 2012.

[20] X. Wu and W. Sun “Visual secret sharing for general access structures by random grids”IEEE Dec2012.

[21] Sonali Patil, Kapil Tajane, Janhavi Sirdeshpande “General Access Structure For Modulo-2 Secret Sharing Scheme” International Journal of Engineering Research & Technology(2278-0181) Volume 1, Issue 8, October-2012.

AUTHORS 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 Engineering Department in PCCOE, Akurdi, Pune.

Kapil Tajane received Bachelor degree in Computer Science & Engg from Amravati University. Currently doing Master of Computer Engg. from Pune University.

Janhavi Sirdeshpande received Bachelor degree in Computer Science & Engg from Marathwada University. Currently doing Master of Computer Engg. from Pune University