

# An Explication of Multifarious Secret Sharing Schemes

Sonali Patil  
Research Scholar,  
Sant Gadge Baba Amravati University,  
Amravati - 444 602, Maharashtra India

Prashant Deshmukh  
Professor and Head,  
Sipna College of Engineering and Technology,  
Amravati – 444 701, Maharashtra India

## ABSTRACT

The idea of secret sharing is to start with a secret, divide it into pieces called shares, which are then distributed amongst participants by the dealer. Only certain authorized subsets of participants can reconstruct the original secret. Applications for secret sharing schemes seem to be getting more important nowadays. For many circumstances, secret sharing has to provide more flexibility and functionality as per the need of an application. Secret Sharing has been an active research field for many years. Various secret sharing techniques have been developed to secure data, but there is a need to implement a secret sharing scheme with all augmented capabilities like general access structure, robustness against cheating shareholders, verifiability of the shares, proactive redistribution of shares etc. The intent of this paper is to explain the extended capabilities of secret sharing schemes and analyze the relation in application semantics and multifarious secret sharing schemes.

## Keywords

Security, Secret Sharing, Multi functionality, Extended Capabilities, Cryptography

## 1. INTRODUCTION

Secret Sharing Schemes (SSS) refers to method for distributing a secret amongst 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.

There are circumstances where an action is required to be executed by a group of people. For example, to transfer money from a bank a manager and a clerk need to cooperate. A ballistic missile should only be launched if three officers authorize the action. Schemes that have a group of participants that can recover a secret are known as Secret Sharing Schemes.

Secret sharing has been an active research by mathematicians as object of intrinsic interest in their own right, cryptographers as important cryptographic primitives and security engineers as technique to employ in distributed security applications. There are various kinds of secret sharing schemes like threshold schemes, schemes with general access structure, verifiable secret sharing schemes, proactive secret sharing schemes etc. As per the need of an application the secret sharing scheme should provide the extended capabilities. To achieve this there is a need of multifarious secret sharing schemes.

The rest of the paper is organized as follows. In Section 2 some definitions are discussed. Section 3 covers literature survey based on various secret sharing schemes like threshold schemes, secret sharing with general access structure, verifiable secret sharing schemes and proactive secret sharing

schemes. Section 4 discusses the usage and hurdles of secret sharing schemes with extended capabilities and also relation between application semantics and required feature of multifarious secret sharing scheme. Finally in section 5, the survey is summarized based on their comparative results.

## 2. 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 [1]. It is a measure of the amount of information that 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  $S$  whatsoever, in the information theoretic sense [2] [3].

**Ideal Secret Sharing:** Secret sharing schemes with information rate 1 are called ideal [4]. Scheme is ideal if share has the same length as secret. Ideal property can be thought as efficiency.

## 3. LITERATURE SURVEY CRUX

### 3.1 Threshold Schemes:

First threshold schemes were independently invented by both Adi Shamir [5] and George Blackley [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 management scheme. [7] [8] [9] are some threshold schemes proposed in recent years.

In old  $(t, n)$  threshold schemes the secret is shared among  $n$  participants to some prior time. For these schemes it is assumed that all the participants are honest. But in practice it can be happened that some participants are dishonest and they probably leaks secret. Chunming Tang and Zheng-an Yao [7] proposed a threshold scheme where a secret is shared forever only if not more than  $t-1$  participants are dishonest. Chou, Lin and Li [8] proposed a threshold scheme using Sudoku. Sudoku has extremely large number of solutions and this is an advantage for the scheme as it makes the scheme more secure.

In threshold schemes which involves dealer to share the secret, the dealer has to decide the threshold value. To avoid the dealers role Shi and Zong [9], proposed a method where all participants cooperate to take on the dealers role. Each participant stores one share as the same size of the secret. So the scheme is ideal. Also the scheme is perfect as it is based on Shamir's scheme. A  $(t, n)$  threshold agreement certificate is introduced in [10].

### 3.2 General Access Structure:

In the outline of threshold schemes, we wanted  $t$  out of  $n$  participants to be able to determine the key. In practice, it is often needed 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.

Let's denote  $\Gamma$  as being a set of subsets of  $P$ , and the subsets in  $\Gamma$  as being the subset of participants that should be able to compute the key. Then  $\Gamma$  is denoted as being the access structure and the subsets in  $\Gamma$  are called authorized subsets. Ito, Saito [11] provided a new methodology to overcome the problem of converting  $(t, n)$  threshold scheme to a general access structure scheme. The problem with this scheme is number of shares applied in the scheme. Sometimes the number of shares can be quite large although it is bounded. K. Srinathan [12] defined a more general notion of access hierarchies and also studied tolerability properties of access hierarchies. It is a non perfect secret sharing scheme.

Benaloh [13] tried to make general access structure simpler. He presented a view that a threshold scheme is only a particular case of general access structure. Monotone access structure is used to get general access structure. For any given polynomial  $P$ , the number of  $n$ -variable monotone formulae of size no more than  $P(n)$  is exponential in  $P(n)$ . However the total number of monotone functions on  $n$  variables is doubly exponential in  $n$ . Therefore, most monotone access structure cannot be realized with a large number of polynomial sized shares. Pang [14] proposed more efficient sharing scheme for general access structure.

Multiple secrets can be shared among participants and get retrieved from different access structures. Sai-zhi [15] proposed a low computational complexity general access structure scheme for multiple secret sharing. It is based on Shamir's secret sharing scheme and the discrete logarithm problem. Access structure can be changed dynamically without updating any participant's already allocated share.

### 3.3 Verifiable Secret Sharing Schemes

In the previous scheme we assumed that the Dealer is reliable, however, a misbehaving dealer can deal inconsistent shares to the participants, from which they will not be able to reconstruct a secret. To prevent such malicious behavior of the dealer, one needs to implement a protocol through which a consistent dealing can be verified by the recipients of shares. The problem of verifiable secret sharing [15] is to convince shareholders that their shares (collectively) are,  $t$ -Consistent, meaning that every subset of  $t$  shares out of  $n$  defines the same secret.

Of course if the shareholders would transfer their shares, they could easily confirm consistency, however this would contradict the purpose of the secret sharing scheme.

There are two versions of verifiable secret sharing protocols: Interactive proofs and non Interactive proofs. Both versions allow the validity of secret shares to be verified without their being revealed; a shareholder can obtain high confidence that he/she holds a valid share of the secret rather than a useless random number.

#### VSS: Interactive Proof

There are two different interactive proofs for VSS as per Benaloh [13]. In the first protocol we assume that the shareholders do not cheat. In the second protocol we do not assume that. But the question that one may ask is what if a conflict occurs? We cannot determine who is cheating: the Dealer or one of the shareholders.

#### VSS: Non Interactive Proof

Contrary to the previous protocols, in a Non Interactive Proof scheme [18], only the dealer is allowed to send messages, in particular the shareholders cannot talk with each other or with the dealer when verifying a share. The basic idea is that the dealer sends extra information to each participant during the distribution and each participant verifies that his/her secret share is consistent with this extra information.

Rabin et al. [18] used an information checking protocol to verify the validity of each share and thereby detect cheaters. VSS allows detecting cheating by secret participants and/or the secret dealer (e.g. [19] [20]). Verification capability is especially important, if secret consistency is crucial. Cheating can result not only in obstruction of the protocol, but also may allow dishonest parties to recover secret on their own [21]. Verification process requires presence of trusted third party or can be performed directly between parties of the protocol. When it takes place in public or uses publicly available data PVSS [22] is there.

#### Publicly Verifiable Secret Sharing:

Publicly verifiable secret sharing plays an important role in escrow-cryptosystems, electronic voting and other applications. In this paradigm, not only the shareholder himself but also everybody can verify the correctness of his share. A Publicly Verifiable Dynamic Sharing Protocol is suggested by Jai Yu [23] for Data Secure Storage.

The extensive form game theory was introduced to the secret sharing scheme to prevent participants cheating during the secret sharing process. The dealer distributed several sub-secret shadows instead of the secret shadows to each participant, from which a multi-round game model was constructed to simulate the secret sharing process. The designed game strategies made rational participants not

distinguish which round was the last one of the game and have no incentive to cheat. It ensures all participants could receive the secret, realizing the fairness. Detecting Dealer Cheating [24] and Resistance against cheating [10] describes some methods for verifying cheating. Yongquan CAI [25] proposed a cheat-proof rational secret sharing scheme applying the extensive form game to the secret sharing.  $(t, n)$  threshold agreement certificate is introduced in [10]. Based on these certificates participants cheating can be resisted. To resist Dealer cheating Chang, Chan [24] proposed a method in which the dealer is asked to generate a certificate polynomial. This certificate is used by participants to do the detection process.

### 3.4 Proactive Secret Sharing:

The Secret Sharing scheme assumes long-lived shares; however the protection provided by this scheme may be insufficient. The security in a system that is exposed to attacks and break-ins might become exhausted. Several faults might occur like secrets can be revealed, shares can gradually be corrupted / compromised, hardware failure or damage, for example reboot, power failures etc.

The goal of the pro-active security scheme is to prevent the adversary from learning the secret or from destroying it, in particular any group of  $t$  non-faulty shareholders should be

able to reconstruct the secret whenever it is necessary.

The term pro-active refers to the fact that it's not necessary for a breach of security to occur before secrets are refreshed, the refreshment is done periodically (and hence, proactively). Several PSSS have been proposed. Bai [26] used matrix projection method and Shamir's [5] scheme to get a new PSSS. Optimum secret sharing is described by Zhengjun [27]. They extend the secret  $s$  in the Shamir's scheme to an array of three elements,  $(s, e0, e1)$ , and construct two equations for checking validity. Each item in the equations should be reconstructed using Lagrange's interpolation. In this paper, the schemes are revisited by introducing a public hash function to construct equations for checking validity. The revisited scheme is more efficient because they only extend the secret to an array of two elements.

Jia Yu [28] proposed a secret sharing scheme which supports both publicly verifiable secret sharing and also enrollment ability. There is no need to expose the secret and other shares while providing a new share to new enrolled shareholder.

All these kinds of secret sharing schemes with these extended capabilities and multi functionalities draw our attention, and we are also eager to know their specific implementation methods. Following section gives performance analysis of few schemes.

## 4. PERFORMANCE ANALYSIS OF SECRET SHARING SCHEMES

Table I points to the usage of extended capability secret sharing schemes and hurdles of these schemes.

**Table I. Types of a secret sharing scheme and hurdles of those specific schemes**

Type of a scheme	Usage	Hurdles
Threshold Schemes	Group of mutually suspicious individuals with conflicting interests must cooperate.	Design of access structures is difficult.
General Access Structure Schemes	Only certain specified subsets of the participants should be able to recover the secret.	To add extra functionalities is difficult.
Verifiable Secret Sharing (Interactive Proofs)	Dealer and shareholders both interact with each other. Also shareholders can interact with each other.	Asserts a proof only to the participants of this protocol and only at the moment it is held. They cannot be legal proofs in court.
Verifiable Secret Sharing (Non Interactive Proofs)	Only dealer is allowed to send messages, in particular the shareholders cannot talk with each other or with the dealer when verifying a share.	Many of the proposed schemes are providing cheating verification but not cheater identification.
Publicly Verifiable Secret Sharing	Everybody can verify the correctness of his share.	New members can't enroll the system according to the need of actual circumstance.
Proactive Secret Sharing Schemes	Improve security through periodic executions.	Need to be more secure and efficient of course, without any information-leak or any secret change.

Table II shows application type and the required additional feature of secret sharing schemes. Few secret sharing schemes are considered for comparative study based on some parameters. Table III summarizes that:

**Table II. Application Type and Required Features of Secret Sharing Schemes**

Application Semantics	Required feature of secret sharing
Transfer money from a bank	Threshold schemes
Launching of a ballistic missile	Threshold, General Access Structure
Communications networks	Ideal, Perfect, Low complexity
Trusted Shareholders, Untrusted Dealer	Verifiable Secret Sharing
Trusted Dealer, Untrusted Shareholders	Verifiable Secret Sharing, Periodically Renew Share
Electronic voting	Publicly Verifiable Secret Sharing
Private querying of database	Low Complexity, Threshold
Collective Control	Periodically renew shares, Enroll/dis-enroll shareholders, Recover lost share
escrow-cryptosystems	Publicly Verifiable Secret Sharing
Secure Storage	Ideal, Reliable, General Access Structure

**Table III. Comparison of secret sharing schemes on various extended capabilities**

Authors	Perfect	Ideal	Flexibility	Security	Multi functionality		Extended Capabilities			
			Threshold Scheme (k, n)	Computation Time Complexity	General Access Structure	Periodically Renew Shares	Enroll / Disenroll Shareholders	Verifiability of Shares	Cheater Identification	Recover lost shares
G. Blakely [6]	No	No	Yes	Low	No	No	No	No	No	No
Tang, Yao [7]	Yes	Yes	Yes	Low	No	No	No	Yes	No	No
Chou, Lin, Li [8]	Yes	Yes	Yes	Very Low	Yes	No	Yes	No	No	No
Shi, Zhong [9]	Yes	Yes	Yes	Low	No	Yes	No	No	No	No
K. Srinathan [12]	No	Yes	Yes	High	Yes	No	No	No	No	No
Staddler [22]	Yes	Yes	Yes	High	No	No	No	No	No	No
Bai [26]	Yes	Yes	Yes	High	No	No	No	No	No	No
Jai Yu [28]	Yes	Yes	Yes	High	No	No	Yes	No	No	No

### 3. CONCLUSION

In this paper several multifarious features of secret sharing schemes such as general access structure, verifiability of

shares, cheater identification, enroll and dis-enroll of shareholders, recover lost or corrupted shares and periodically renew shares are discussed. Table I summarizes the given

literature survey crux by pointing usage and hurdles extended capability secret sharing schemes. Table II summarizes application semantics and required extended capability feature of secret sharing schemes. Table III gives comparison of few secret sharing schemes based on some parameters like complexity measure, perfect, ideal and extended capabilities. There is a lot advancing (steadily but surely) in the field of secret sharing. Applications for secret sharing schemes seem to be getting more important. The requirement is to extend the research for implementing better multifarious secret sharing scheme as per the need of various application semantics.

#### 4. 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] P. Paillier, "On ideal non-perfect secret sharing schemes," in Security Protocols Workshop, 1997, pp. 207–216.
- [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 1979, pp. 313–317.
- [7] 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.
- [8] 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.
- [9] 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.
- [10] 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.
- [11] Mitsuru Ito, Akira Saito, Takao Nishizeki, "Secret Sharing Scheme: Realizing General Access Structure", GLOBECOM IEEE 1987.
- [12] K. Srinathan, N. Tharani Rajan, and C. Pandu Rangan, "Non-perfect secret sharing over general access structures," in INDOCRYPT, 2002, pp. 409–421.
- [13] Benaloh, J., and J. Leichter, Generalized secret sharing and monotone functions, CRYPTO '88, Springer Verlag, pp. 27-35.
- [14] 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.
- [15] 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.
- [16] Stadler, M., "Publicly verifiable secret sharing", Lecture notes in Computer Science, 1997, 190-199.
- [17] P. Feldman, A practical scheme for non-interactive verifiable secret sharing. IEEE Symposium on Foundations of Computer Science, pages 427--437. IEEE, 1987
- [18] Rabin, T., and M. Ben-Or, Verifiable secret sharing and multiparty protocols with honestmajority, Proceedings of the 21st ACM Symposium on the Theory of Computing, 1989, pp.73-85.
- [19] T. P. Pedersan, "Non-Intractive and Information-Theoretic Secure Verifiable Secret Sharing", Lecture notes in Comuter Science, 1992, pp.129-140 (Advances in Cryptology – CRYPTO' 91).
- [20] C. Dwork, "On verification in Secret Sharing", Lecture notes in Comuter Science, 1992, pp.114-128 (Advances in Cryptology – CRYPTO' 91).
- [21] Tompa, M., and Woll, H. "How to share a secret with cheaters", Journal of Cryptology, Vol.1, No.2, 1998, pp.133-138.
- [22] M. Stadler, "Publicly Verifiable Secret Sharing", Lecture notes in Computer Science, 1997, 190-199 (Advances in Crptology – EUROCRYPT'96).
- [23] Jia Yu, Fanyu Kong, Rong Hao, Zhen Cheng, "A Publicly Verifiable Dynamic Sharing Protocol for Data Secure Storage", Ninth International Conference on Web-Age Information Management 2008 IEEE.
- [24] Chin-Chen Chang, Chao-Wen Chan, "Detecting Dealer Cheating in Secret Sharing Systems", Proceedings of the Twenty-Fourth Annual International Computer Software & Applications Conference (COMPSAC'00), IEEE 2000.
- [25] Yongquan CAI, Xiaofeng REN, "A Cheat-proof Rational Secret Sharing Scheme", Journal of Computational Information Systems, (2011) p. 88-96, January 2011.
- [26] Bai, L. and Zou, X. (2009) 'A Proactive Secret Sharing Scheme in matrix projection method', Int. J. Security and Networks, Vol. 4, No. 4, pp.201–209.
- [27] Zhengjun Cao, Olivier Markowitch, "Two Optimum Secret Sharing Schemes Revisited", International Seminar on Future Information Technology and Management Engineering, 2008 IEEE, p. 157-160.
- [28] Jia Yu, Fanyu Kong, Rong Hao, "Publicly Verifiable Secret Sharing with Enrollment Ability", ACIS, IEEE 2007.