Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 67-72, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.67.72

A Review of Secret Sharing Schemes

K.N. Sandhya Sarma, Hemraj S. Lamkuche and S. Umamaheswari
School of IT and Science, Dr. G.R. Damodaran College of Science, Coimbatore, Nadu-641014, Tamil Nadu, India

Corresponding Author: K.N. Sandhya Sarma, School of IT and Science, Dr. G.R. Damodaran College of Science, Coimbatore, Nadu-641014, Tamil Nadu, India

ABSTRACT

A secret sharing scheme is a method for increasing the security of a critical data. The cryptographic secret key used for protecting the data is shared between a group of participants by a dealer in the distribution process; such that specific subgroups (access structure) of the share holders can recover the secret by pooling their shares in the reconstruction process. In this study, we have analyzed various secret sharing schemes and classified based on their characteristics.

Key words: Secret sharing, classification, threshold

INTRODUCTION

Shamir (1979) information security and network security requires secret sharing in any application used. Threshold (t,n) secret sharing scheme allows a dealer to distribute a secret value S to 'n' players; such that atleast (t<n) players are required to reconstruct the secret. Polynomial interpolation and hyper plane geometry are the two different types with secret sharing.

Almost all forms of communication and the information storage today, are in the digital form. Security in the digital media has been a matter of serious concern. This has resulted in the development of encryption and cryptography. Mathematicians, cryptographers and security engineers involve themselves more in secret sharing. A secret sharing scheme starts with a secret (S) and then dividing the secret into two or more pieces (s_i). The size of the secret is H(S) and of ith share is $H(s_i)$ where H is Shannon's entropy. The pieces of information are called shares and the process responsible for the division is called dealer. The dealer assigns share s_i to the participant P_i. The secret may be uniquely determined only by certain pre-determined subgroups of users which constitute the access structure and is denoted by Γ. The process responsible for the recovery of the secret information from an access structure (allowed coalition) is called a combiner. Two properties of secret sharing are:

- **Recoverability:** Given any t shares of the secret S, we can recover the secret S
- **Secrecy:** Given any<t shares, absolutely nothing are learned about S

In this study, analysis of various secret sharing schemes has been carried out and analysed and based on their characteristics it has been classified.

RELATED STUDY

Secret Sharing was proposed with the motivation of protecting and securing secret key in cryptography. Shamir (1979) formed the foundation for secret sharing and since then, several secret sharing schemes were developed. Few of them are discussed here.

Classification/variants on secret sharing: Secret Sharing Schemes can be classified into various categories according to different criteria. In terms of number of secrets to be shared, two classes can be identified-single secrets and multiple secrets (Blundo *et al*., 1993).

In terms of share's capabilities, two classes can be identified-same weighted shares and multi weighted shares. In Shamir's hierarchical secret sharing scheme the dealer assigns a larger number of shares to users at higher levels of hierarchy, so that higher level users hold more shares than lower level users. Tassa (2007) improved this concept by distinguishing the hierarchical level qualitatively i.e., the secret share of a higher level users contains more information about original secret than a lower level users. Based on the abilities the secret sharing can be classified into:

- **Proactive secret sharing:** Ostrovsky and Yung (1991) proposed Proactive security. This concept was applied to secret sharing by Hezberg *et al*. (1995). In this method, new shares are used and old shares are not considered which helps in updating the shares periodically
- **Dynamic secret sharing:** The ability to change the access structure. The dealer has the ability to change a particular access structure out of a given set and/or to allow the participants to reconstruct different secret (in different time instants)
- **Secret sharing with veto capability:** It is the ability to block the reconstruction. It is a feature where qualified set can prevent any other set of participants from reconstructing the secret key

Depending on the computation power of the participants we have:

- **Computational secret sharing:** Participants (and the dealer) are computationally bounded. Eg: Krawczyk (1993), CSS allows achieving better information rate. Information rate (ρ) is defined as the ratio between average length of the share (in bits) given to the participants and the length of the secret
- **Verifiable secret sharing:** Dealers and players involved in plain secret sharing, some may or may not follow the protocol. As per verifiable secret sharing, honest players should be able to recover the secret and corrupted players should get no information on it

Tompa and Woll (1988) initially introduces cheating in secret sharing, Individual user tricks other users by using fault shares, that is adopted in Shamir's (k,n) scheme. Ogata *et al*. (1995), finally provides an efficient mode of detecting cheating in secret sharing:

- **Robust secret sharing:** Recovering correct secrets in the presence of more number of faulty and corrupted shares is employed in this scheme. It allows the secret to be reconstructed in the presence of an active adversary who is to corrupt shares. McEliece and Sarwate (1981), found first solution to the problem of designing Robust Secret Sharing

Based on the techniques used different classes of secret sharing can be identified:

- **Polynomial based secret sharing:** This scheme involves polynomials and interpolations, particularly Lagrange's interpolation (Shamir, 1979), Birkhoff interpolation (Tassa, 2007) for splitting and reconstructing the secret. Shares are evaluations of a randomly generated polynomial
- **CRT schemes:** Its rely on Chinese Remainder Theorem. CRT based Asmuth and Bloom (1983), secret sharing scheme shares the secret S among 'n' parties by modulator arithmetic such that any 't' users can reconstruct the secret by the CRT
- **Anonymous secret sharing:** Here the identities of the participants are not required for reconstruction of the secret. The secret can be reconstructed without the knowledge of which participant holds which share
- **Systematic block code based secret sharing:** Multiple groups of secrets are packed into a group of large secrets by using the CRT and then shared by constructing a secret polynomial such that its coefficients are those large secrets (Chien *et al*., 2000)
- **Black box secret sharing:** Schemes those are independent of the structure of the group or its order. Black-box secret sharing was introduced by Desmedt *et al*. (1995)
- **Visual secret sharing:** Schemes of secrets and the shares are images. Here the picture is cut in to 'n' shares, only if an "n" shares are put together it makes the visible picture if not results in an image of different form

COMPARISON OF SECRET SHARING SCHEMES

A secret sharing scheme could be either 'perfect', 'non-perfect' or 'ramp'. It is a protocol to where t denotes the cardinality, s means secret and n denotes the participant. Only if the participant rate is greater than the cardinality then the secret could be retrieved (Benaloh and Leichter, 1989). Various classifications of secret sharing schemes are mentioned in Table 1.

Table 2 shows some of the schemes and their characteristics. Some schemes are "easy to add new shares".

APPLICATIONS OF SECRET SHARING

Secret Sharing has broad applications in the situations where access to important resources has to be protected. Applications includes:

- Byzantine agreement
- E-voting
- Key management in network security
- Multi party secure computation
- Threshold cryptography
- Distributed certificate authorities

Table 1: Classification of secret sharing schemes

Perfect secret sharing schemes	Benaloh, Feldman, Herzberg, Pedersen, Shamir
Non-perfect secret sharing schemes	Asmuth-Bloom, Brickell, Ghodosi, Iftene, Mignotte
Ramp secret sharing schemes	Blakely, Bai, Franklin, Pang

Table 2: Different sharing schemes, comparison and their characteristics

References	Techniques used	Proactive	Threshold	Verifiable	Single/ multiple	Change secret	Change access schemes structure
Asmuth and Bloom (1983)	CRT based	No	Yes	No	Single	-	-
Bai (2006)	Matrix projection based	Yes	Yes	Partial	Multiple	Easy	Easy to add new share
Benaloh (1989)	Circuit based	No	No	No	Single	-	-
Blakley (1979)	Vector space based	No	Yes	No	Single	-	Easy to add new share
Brickell (1995)	Vector space based	No	No	No	Single	-	-
Feldman (2008)	Polynomial based	No	Yes	Yes	Single	-	Easy to add new share
Franklin and Yung (1992)	Polynomial based	No	Yes	No	Multiple	Easy	-
Ghodosi *et al*. (1998)	Polynomial based	No	No	No	Single	-	-
He and Dawson (1995)	Polynomial based	Yes	Yes	No	Multiple	Easy	Easy to add new share
Hezberg *et al*. (1995)	Polynomial based	Yes	Yes	No	Single		Easy to add new share
Iftene (2007)	CRT based	No	No	No	Single	-	-
Ingemarssonm and Simmous (1991)	Linear block based	No	Yes	No	Single	Easy	Easy to add new share
Jackson *et al*. (1994, 1996)	-	No	No	No	Single	-	-
Martin *et al*. (1999)	-	No	Yes	No	Single	-	Easy to add new share
Mignotte (1983)	CRT based	No	Yes	No	Single	-	-
Noar and Shamir (1995)	Visual secret sharing	-	Yes	No	Single	-	-
Pang *et al*. (2008)	Polynomial based	Yes	Yes	Yes	Multiple	Easy	-
Pedersen (1992)	Polynomial based	No	Yes	Yes	Single	-	Easy to add new share
Shamir (1979)	Polynomial based	No	Yes	No	Single	-	Easy to add new share
Steinfelda *et al*. (2004)	-	No	Yes	No	Single		Easy to add new share

- Distributed information storage
- Location privacy
- Key management in ad-hoc networks
- Information hiding
- Secure online auctions
- Fair exchange

CONCLUSION

A secret sharing scheme is evaluated by its security-that no single share will reveal the information, reconstruction accuracy whether the secret is exactly recovered without any alterations from the original (in visual cryptography, both the images should be the same), computation complexity and storage requirements. It is secure in the sense, no single share can leak any information and k-1 shares cannot reveal the secret. But this scheme is not secure against cheaters. As for reconstruction precision if one or more shares are fake, then the secret may not be reconstructed correctly by 'k' shares. The computation complexity of interpolation is $O(n\log^2 n)$.

Different schemes were introduced by researchers taking these factors and improving the Shamir's scheme.

REFERENCES

Asmuth, C. and J. Bloom, 1983. A modular approach to key safeguarding. IEEE Trans. Inf. Theory, 29: 208-210.

Bai, L., 2006. A strong ramp secret sharing scheme using matrix projection. Proceedings of the International Symposium on a W o rld of Wireless, Mobile and Multimedia Networks, June 26-29, 2006, Buffalo-Niagara Falls, USA., pp: 652-656.

Benaloh, J. and J. Leichter, 1989. Generalized secret sharing and monotone functions. Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology, August 21-25, 1988, Santa Barbara, California, USA., pp: 27-35.

Benaloh, J.C., 1989. Secret sharing homomorphisms-keeping shares of a secret. Proceedings of the Advances in Cryptology, August 1986, Santa Barbara, CA., USA., pp: 251-260.

Blakley, G.R., 1979. Safeguarding cryptographic keys. Proceedings of the National Computer Conference, June 4-7, 1979, New York, USA., pp: 313-317.

Blundo, C., A. De Santis and U. Vaccaro, 1993. Efficient sharing of many secrets. Proceedings of the 10th Annual Symposium on Theoretical Ascpects of Computer Science Wurzburg, February 25-27, 1993, Germany, pp: 692-703.

Brickell, E.F., 1995. Some ideal secret sharing schemes. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, May, 1995, Saint-Malo, France, pp: 468-475.

Chien, H.Y., J.K. Jan and Y.M. Tsen, 2000. A practical (t, n) multisecret sharing scheme. IEICE Trans. Fundam. Electron. Commun. Comput. Sci., E83: 2762-2765.

Desmedt, Y., G. Di Crescenzo and M. Burmester, 1995. Multi-plicative non-abelian sharing schemes and their application to threshold cryptography. Proceedings of the 4th International Conferences on the Theory and Applications of Cryptology Wollongong, November 28-December-1, 1994, Australia, pp: 19-32.

Feldman, P., 2008. A practical scheme for non-interactive verifiable secret sharing. Proceedings of the 28th Annual Symposium on Foundations o f Computer Science, October 12-14, 1987, USA., pp: 427-438.

Franklin, M. and M. Yung, 1992. Communication complexity of secure computation. Proceedings of the 24th Annual ACM Symposium on Theory of Computing, May 4-6, 1992, Canada, pp: 699-710.

Ghodosi, H., J. Pieprzyk and R. Safavi-Naini, 1998. Secret sharing in multilevel and compartmented groups. Proceedings of the 3rd Australasian Conference on Information Security and Privacy, July 13-15, 1998, Brisbane, Australia, pp: 367-378.

He, J. and E. Dawson, 1995. Multisecret-sharing scheme based on one-way function. Electron. Lett., 31: 93-95.

Hezberg, H., D. Jarecki, H. Krawzyk and M. Young, 1995. Proactive secret sharing or: How to cope with perpetual leakage. Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology, August 27-31, 1995, Springer Verlag, London, pp: 339-352.

Iftene, S., 2007. General secret sharing based on the Chinese remainder theorem with applications in e-voting. Electron. Notes Theor. Comput. Sci., 186: 67-84.

Ingemarssonm, I. and G.J. Simmons, 1991. A protocol to set up shared secret schemes without the assistance of a mutually trusted party. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques Aarhus, May 21-24, 1990, Denmark, pp: 266-282.

Jackson, W.A., K.M. Martin and C.M. O'Keefe, 1994. Multisecret threshold schemes. Proceedings of the 13th Annual International Cryptology Conference, August 22-26, 1993, Santa Barbara, California, USA., pp: 126-135.

Jackson, W.A., K.M. Martin and C.M. O'Keefe, 1996. A construction for multisecret threshold schemes. Des. Codes Cryptogr., 9: 287-303.

Krawczyk, H., 1993. Secret sharing made short. Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, August 22-26, 1993, Santa Barbara, California, USA., pp: 136-146.

Martin, K.M., J. Pieprzyk, R. Safavi-Naini and H. Wang, 1999. Changing thresholds in the absence of secure channels. Proceedings of the 4th Australasian Conference Information on Security and Privacy, April 7-9, 1999, Australia, pp: 177-191.

McEliece, R.J. and D.V. Sarwate, 1981. On sharing secrets and reed-solomon codes. Commun. ACM., 24: 583-584.

Mignotte, M., 1983. How to share a secret. Proceedings of the Workshop on Cryptography, Lecture Notes in Computer Science, March 29-April-2, 1982, Burg Feuerstein, Germany, pp: 371-375.

Noar, M. and A. Shamir, 1995. Visual Cryptography. In: Advance in Cryptography, DeSantis, A. (Ed.). Springer, Netherlands, pp: 1-12.

Ogata, W., K. Kurosawa, D.R. Stinson, 1995. Optimum secret sharing scheme secure against cheating. SIAM J. Discrete Math., 20: 79-95.

Ostrovsky, R. and M. Yung, 1991. How to withstand mobile virus attacks. Proceedings of the 10th Annual ACM Symposium on Principles of Distributed Computing, August 19-21, 1991, Montreal, Quebec, Canada, pp: 51-59.

Pang, L., H. Li, Y. Yao and Y. Wang, 2008. A verifiable (t, n) multiple secret sharing scheme and its analyses. Proceedings of the International Symposium on Electronic Commerce and Security, August 3-5, 2008, Guangzhou City, China, pp: 22-26.

Pedersen, T.P., 1992. Non-Interactive and information-theoretic secure verifiable secret sharing. Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, August 11-15, 1991, Santa Barbara, California, USA., pp: 129-140.

Shamir, A., 1979. How to share a secret. Commun. ACM, 22: 612-613.

Steinfelda, R., J. Pieprzyka and H. Wang, 2004. Lattice-Based threshold-changeability for standard shamir secret-sharing schemes. Proceedings of the 10th International Conference on the Theory and Application of Cryptology and Information Security, December 5-9, 2004, Jeju Island, Korea, pp: 170-186.

Tassa, T., 2007. Hierarchical threshold secret sharing. J. Cryptol., 20: 237-264.

Tompa, M and H. Woll, 1988. How to share a secret with cheaters. J. Cryptol., 1: 133-138.