International Journal of Information Processing, 8(2), 13-28, 2014
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

An Epitome of Multi Secret Sharing Schemes for General Access Structure

V P Binu[a], A Sreekumar[a]

[a]Department of Computer Applications, Cochin University of Science and Technology, Cochin-682022 India, Contact: binuvp@gmail.com

Secret sharing schemes are widely used now a days in various applications, which need more security, trust and reliability. In secret sharing scheme, the secret is divided among the participants and only authorized set of participants can recover the secret by combining their shares. The authorized set of participants are called access structure of the scheme. In Multi-Secret Sharing Scheme (MSSS), k different secrets are distributed among the participants, each one according to an access structure. Multi-secret sharing schemes have been studied extensively by the cryptographic community. Number of schemes are proposed for the threshold multi-secret sharing and multi-secret sharing according to generalized access structure with various features. In this survey we explore the important constructions of multi-secret sharing for the generalized access structure with their merits and demerits. The features like whether shares can be reused, participants can be enrolled or dis-enrolled efficiently, whether shares have to modified in the renewal phase *etc.*, are considered for the evaluation.

Keywords : Cheater Identification, General Access Structure, Multi-secret Sharing, Secret Sharing, Verifiability.

1. INTRODUCTION

Secret sharing schemes are important tool used in security protocols. Originally motivated by the problem of secure key storage by Shamir [1], secret sharing schemes have found numerous other applications in cryptography and distributed computing. Threshold cryptography [2], access control [3], secure multi-party computation [4] [5] [6], attribute based encryption [7] [8], generalized oblivious transfer [9] [10], visual cryptography [11] *etc.*, are the significant areas of development using the secret sharing techniques.

In secret sharing, the secret is divided among n participants in such a way that only designated subset of participants can recover the secret, but any subset of participants which is not a designated set cannot recover the secret. A set of participants who can recover the secret is called an *access structure* or *authorized set*, and a set of participants which is not an authorized set is called an *unauthorized set* or *forbidden set*. The following are the two fundamental requirements of any secret sharing scheme.

- **Recoverability:**Authorized subset of participants should be able to recover the secret by pooling their shares.
- **Privacy:**Unauthorized subset of participants should not learn any information about the secret.

Let $\mathcal{P} = \{P_i | i = 1, 2, \ldots, n\}$ be the set of participants and the secret be K. The set of all secret is represented by $\mathcal{K}$. The set of all shares $S_1, S_2, \ldots, S_n$ is represented by $\mathcal{S}$. The participants set is partitioned into two classes.

1. The class of authorized sets Γ is called the *access structure.*
2. The class of unauthorized sets $\Gamma^c = 2^{\mathcal{P}} \backslash \Gamma$

Let us assume that $\mathcal{P}, \mathcal{K}, \mathcal{S}$ are all finite sets and there is a probability distribution on $\mathcal{K}$ and $\mathcal{S}$. We use $H(\mathcal{K})$ and $H(\mathcal{S})$ to denote the entropy of $\mathcal{K}$ and $\mathcal{S}$ respectively.

according to a monotone generalized access structure. Threshold multi-secret sharing also found several applications and we prefer users to further look into it. The major concern in the multi-secret sharing is the large number of public values and the computational complexity. Only computational security can be achieved in all the schemes mentioned, where security depends on the security of some computationally hard problem. Multi-secret sharing schemes have found numerous application in implementing authentication mechanisms, resource management in cloud, multi policy distributed signatures, multi policy distributed decryption *etc.*.

REFERENCES

1. A Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612–613, 1979.
2. Y Desmedt and Y Frankel. Shared Generation of Authenticators and Signatures. *In Advances in CryptologyCRYPTO91*, pages 457–469. Springer, 1992.
3. M Naor and A Wool. Access Control and Signatures *via* Quorum Secret Sharing. *IEEE Transactions on Parallel and Distributed Systems*, 9(9):909-922, 1998.
4. M. Ben-Or, S Goldwasser and A Wigderson. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation. In *Proceedings of the* 20^{TH} *Annual ACM Symposium on Theory of Computing*, pages 1-10. ACM, 1988.
5. D Chaum, C Crepeau and I Damgard. Multiparty Unconditionally Secure Protocols. In *Proceedings of the* 20^{th} *Annual ACM Sym- posium on Theory of computing*, pages 11-19. ACM, 1988.
6. R Cramer, I Damgard and U Maurer. General Secure Multi-party Computation from any Linear Secret-Sharing Scheme. In *Advances in CryptologyEUROCRYPT 2000*, pages 316-334. Springer, 2000.
7. V Goyal, O Pandey, A Sahai and B Waters. Attribute-based Encryption for Fine-Grained Access Control of Encrypted Data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, pages 89–98. ACM, 2006.
8. J. Bethencourt, A Sahai and B Waters. Ciphertext-Policy Attribute-Based Encryption. In *IEEE Symposium on Security and Privacy*, pages 321–334, 2007.
9. T Tassa. Generalized Oblivious Transfer by Secret Sharing. *Designs, Codes and Cryptography*, 58(1):11–21, 2011.
10. B Shankar, K Srinathan and C P Rangan. Alternative Protocols for Generalized Oblivious Transfer. In *Distributed Computing and Networking*, pages 304–309. Springer, 2008.
11. M Naor and A Shamir. Visual Cryptography. In *Advances in CryptologyEUROCRYPT'94*, pages 1–12. Springer, 1995.
12. G R Blakley *et al.*,. Safeguarding Cryptographic Keys. In *Proceedings of the National Computer Conference*, vol. 48, pages 313–317, 1979.
13. R J McEliece and D V Sarwate. On Sharing Secrets and Reed-Solomon Codes. Communications of the ACM, 24(9):583–584, 1981.
14. I S Reed and G Solomon. Polynomial Codes Over Certain Finite Fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.
15. E Karnin, J Greene and M Hellman. On Secret Sharing Systems.*IEEE Transactions on Information Theory,* , 29(1):35–41, 1983.
16. J L Massey. Minimal Codewords and Secret Sharing. In *Proceedings of the* 6^{th} *Joint Swedish-Russian International Workshop on Information Theory*, pages 276–279. Citeseer, 1993.
17. M Mignotte. How to Share a Secret. In *Cryptography*, pages 371–375. Springer, 1983.
18. C Asmuth and J Bloom. A Modular Approach to Key Safeguarding. *IEEE Transactions on Information Theory*, 29(2):208–210,1983.
19. S Kothari. Generalized Linear Threshold Scheme. In *Advances in Cryptology*, pages 231–241. Springer, 1985.
20. E F Brickell. Some Ideal Secret Sharing schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 9(2):105–113, 1989.
21. G J Simmons. An Introduction to Shared Secret and/or Shared Control Schemes and Their Application. *Contemporary Cryptology: The Science of Information Integrity*, pages 441–497, 1992.
22. A Sreekumar. Secret Sharing Schemes using Visual Cryptography. *Ph.D Thesis, Cochin University of Science and Technology*, 2009.
23. J Benaloh and J Leichter. Generalized Secret Sharing and Monotone Functions. In *Ad-*

vances in Cryptology CRYPTO88, pages 27–35. Springer, 1990.
24. M Ito, A Saito and T Nishizeki. Secret Sharing Scheme Realizing General Access Structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.
25. A Beimel. Secret-Sharing Schemes: A Survey. In *Coding and Cryptology*, pages 11–46. Springer, 2011.
26. E F Brickell and D M Davenport. On the Classification of Ideal Secret Sharing Schemes.*Journal of Cryptology*, 4(2):123–134, 1991.
27. D R Stinson. An Explication of Secret Sharing Schemes. *Designs, Codes and Cryptography*, 2(4):357–390, 1992.
28. M Karchmer and A Wigderson. On Span Programs. In *Proceedings of the* 8^{th} *Annual Conference on Structure in Complexity Theory* , pages 102–111, 1993.
29. W A Jackson and K M Martin. Cumulative Arrays and Geometric Secret Sharing Schemes. In *Advances in Cryptology AUSCRYPT'92*, pages 48–55. Springer, 1993.
30. H Ghodosi, J Pieprzyk, R Safavi-Naini and H Wang. On Construction of Cumulative Secret Sharing Schemes. In *Information Security and Privacy*, pages 379–390. Springer, 1998.
31. S Long, J Pieprzyk, H Wang and D S Wong. Generalised Cumulative Arrays in Secret Sharing. *Designs, Codes and Cryptography*, 40(2):191–209, 2006.
32. M Franklin and M Yung. Communication Complexity of Secure Computation. In *Proceedings of the* 24^{th} *annual ACM Symposium on Theory of Computing*, pages 699–710, 1992.
33. C Blundo, A De Santis and U Vaccaro. Efficient Sharing of Many Secrets. In *STACS* 93, pages 692–703. Springer, 1993.
34. W A Jackson, K M Martin and C M OKeefe. Multisecret Threshold Schemes. In *Advances in Cryptology CRYPTO93*, pages 126–135. Springer, 1994.
35. J He and E Dawson. Multisecret-Sharing Scheme Based on One-Way Function. *Electronics Letters*, 31(2):93–95, 1995.
36. L Harn. Efficient Sharing (Broadcasting) of Multiple Secrets. *IEE Proceedings-Computers and Digital Techniques*, 142(3):237-240, 1995.
37. C Cachin. On-Line Secret Sharing. In *Cryptography and Coding*, pages 190–198. Springer,1995.
38. O Goldreich, S Micali and A Wigderson. How to Play any Mental Game. In *Proceed ings of the* 19^{th} *Annual ACM Symposium on Theory of Computing*, pages 218–229. ACM, 1987.
39. L Lamport. Password Authentication with Insecure Communication. *Communications of the ACM*, 24(11):770–772, 1981.
40. R Pinch. On-Line Multiple Secret Sharing. *Electronics Letters*, 32(12):1087–1088, 1996.
41. H Ghodosi, J Pieprzyk, G Chaudhry and J Seberry. How to Prevent Cheating in Pinch's Scheme. *Electronics Letters*, 33(17):1453–1454, 1997.
42. C Y Yeun and C J Mitchell. How to Identify All Cheaters in Pinchs Scheme. *Proceedings of JWIS98, Singapore*, pages 129–133, 1998.
43. R J Hwang and C C Chang. An Online Secret Sharing Scheme for Multi-Secrets. *Computer Communications*, 21(13):1170–1176,1998.
44. H M Sun. On-Line Multiple Secret Sharing Based on a One-Way Function. *Computer Communications*, 22(8):745–748, 1999.
45. A Das and A Adhikari. An Efficient Multiuse Multi-Secret Sharing Scheme Based on Hash Function. *Applied Mathematics Letters*, 23(9):993–996, 2010.
46. P S Roy and A Adhikari. Multi-Use Multi-Secret Sharing Scheme for General Access Struc ture. *Annals of the University of Craiova Mathematics and Computer Science Series*, 37(4):50–57, 2010.
47. J. Herranz, A Ruiz and G Saez. New Results and Applications for Multi-Secret Sharing Schemes. *Designs, Codes and Cryptography*, pages 1–24, 2013.
48. J Herranz, A Ruiz and G Saez. Sharing Many Secrets with Computational Provable Security. *Information Processing Letters*, 2013.

V P Binu is a Research Scholar in the Department of Computer Applications, Cochin University of Science and Technology(CUSAT). He Holds a Bachelor Degree in Computer Science and Engineering and Masters Degree in Computer and Information Science. His research area includes Cryptography, Secret Sharing and Security.

A Sreekumar received his MTech Degree in Computer Science and Engineering from IIT Madras, in 1992 and Ph.D in Cryptography from Cochin University of Science and Technology, in 2010. He joined as a Lecturer in the Department of Computer Applications, CUSAT, in 1994 and currently he is working as an Associate Professor. He had more than 20 years of teaching experience. His research interest includes Cryptography, Secret Sharing Schemes and Number Theory.