MedCrave
Step into the World of Research
Electrical & Electronic Technology Open Access Journal

Mini Review

Open Access
CrossMark

Secret sharing schemes

Abstract

In the (n, m)-threshold secret sharing scheme, there are n participants in the system such that at least n or more participants can easily pool their shares and reconstruct the secret. In this paper, we review some significant secret sharing schemes. In fact, we present numerous constructions for secret sharing schemes.

Keywords: threshold secret sharing scheme, multi secret sharing scheme, quantum secret sharing scheme, post quantum secret sharing scheme

Volume 2 Issue 5 - 2018

Ali Nakhaei Amroudi
Department of Mathematics and Statistics, Imam Hossein Comprehensive University, Iran

Correspondence: Ali Nakhaei Amroudi, Department of Mathematics and Statistics, Imam Hossein Comprehensive University, Iran, Tel +989139525429, Email kpnekhaei@ihu.ac.ir

Received: September 13, 2017 | **Published:** November 28, 2018

Introduction

According to Time Magazine, May 4, 1992, control of nuclear weapons in Russia involves a two-out-of-three mechanism. In order to launch a nuclear missile, the cooperation of at least two parties out of three are needed.[1] The three parties involved are the president, the Defence Minister, and the Defence Ministry. Secret sharing schemes have many other applications, such as e-voting 2 e-auction[2,3] and threshold access control.[4] In 1987, Ito, Saito and Nishizeki gave a construction which shows that there exists a perfect secret sharing scheme realizing any monotone access structure.[5] In this paper, after introducing (n, m)-threshold secret sharing, the problem of sharing some secrets simultaneously is introduced. Then we the quantum and post quantum secret sharing scheme is presented.

(t,n)- Threshold secret sharing scheme

Shamir and Blakely[6,7] proposed the first (n, m)-threshold secret sharing independently in 1979. A (n, m)-threshold secret sharing is the couple of (P; *S*) in which the secret *S* has been shared among the participants P=(P$_1$,…,P$_m$) such that every subset of P, which has at least *n* members, can retrieve *S*, and every subset of P, which has at most *n*-1 members, can not obtain any information about *S*. A secret sharing scheme is called verifiable secret sharing scheme if every participant can verify the validity of his/her share without obtaining information about *S*.[5,8]

Multi secret sharing scheme

The (k, n, m)-multi-secret sharing firstly proposed [9] In the (k, n, m)-threshold multi secret sharing scheme, there are *m* participants in the system. At least *n* or more participants can easily pool their shares and reconstruct *n* secrets at the same time[7] Shao introduced a novel verifiable multi-secret sharing scheme based on Lagrange interpolation and hash function[8] that satisfied robustness, confidentiality, n-consistence, and traceability properties. His scheme is based on Shamir's secret sharing scheme. A verifiable (k, n, m)-multi-secret sharing scheme is one (k, n, m)-multi-secret sharing scheme, which has four properties: robustness, confidentiality, *n*-consistence, and traceability.[8] Robustness means that if *n* or more participants pool their shares then they can recover the *k* secrets; confidentiality means if fewer than *n* participants pool their shares then they cannot recover the *k* secrets; n-consistence means that any *n* participants can recover the *k* secrets; finally, traceability means that any participant can trace the validation of his share.

Quantum secret sharing scheme

In quantum crytography, the security of the cryptosystems is based on the laws of quantum mechanics, instead of mathematical assumptions. The designs of Quantum Secret Sharing(QSS) schemes do not follow in general from the designs of classical schemes, since the laws of quantum mechanics have to be obeyed. In 2000 the quantum secret sharing scheme based on Monotone Span Programs (MSPs) was introduced[10,11] Quantum information theoretical model for quantum secret sharing schemes. The information theoretical description of a QSS scheme was introduced.[12] Later, several theorems were proved according to the definition.[12]

Post quantum secret sharing scheme

Many secret sharing schemes, have been introduced up to now; however some of the proposed schemes have not *n*-consistence property [9–13] and some of them are based on either RSA or DLP assumptions[7,14] whereas these assumptions are not resistant against quantum attacks.[15–22] The secret sharing schemes which is resistant against quantum attacks are called Post Quantum Secret Sharing Scheme (PQSSS). The first PQSSSs were introduced in[23,24] Recently, Nakhaei Amroudi et al. introduced some post quantum secret sharing schemes.[22]

Acknowledgments

None.

Conflicts of interest

The author declares there is no conflicts of interest.

References

1. Angsuman Das, Avishek Adhikari. An efficient multi-use multi-secret sharing scheme based on hash function. *Applied mathematics letters*. 2010;23(9):993–996.
2. Massoud Hadian Dehkordi, Samaneh Mashhadi. An efficient threshold verifiable multi-secret sharing. *Computer Standards & Interfaces*. 2008;30(3):187–190.

3. Dehkordi MH, Farzaneh Y. A New Verifiable Multi-secret Sharing Scheme Realizing Adversary Structure. *Wireless Personal Communications*. 2015;82(3):1749–1758.

4. M Ito, A Saito, T Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and communications in Japan.* 1989;72(9):56–64.

5. Stinson Douglas R. *Cryptography: theory and practice*. 2005.

6. Blakley GR. Safeguarding cryptography keys. *National Computer Conference*. 1979.

7. Dehkordi MH, Mashhadi S. New efficient and practical verifiable multi-secret sharing schemes. *Information Sciences*. 2008;178(9): 2262–2274.

8. Forouzan BA. *Cryptography & Network Security*. 2007.

9. Dehkordi MH, Mashhadi S.Verifiable secret sharing schemes based on non-homogeneous linear recursions and elliptic curves. *Computer communications*. 2008;31(9):1777–1784.

10. Olver PJ. On multivariate interpolation. *Studies in Applied Mathematics*. 2016;116(2):201–240.

11. Smith. Quantum Secret Sharing for General Access Structures. *Quantum Physics*. 2000.

12. CA Nascimento, J Muller Quade, H Imai. Improving Quantum Secret Sharing Schemes. *School of Engineering and Technology Publications*. 2001;64(4).

13. Massoud Hadian Dehkordi, Reza Ghasemi. A Lightweight Public Verifiable Multi Secret Sharing Scheme Using Short Integer Solution. *Wireless Personal Communications*. 2016;91(3):1459–1469.

14. Eslami Z, Ahmadabadi JZ. A verifiable multi-secret sharing scheme based on cellular automata. *Information Sciences*. 2010;180(15): 2889–2894.

15. Jeffrey Hoffstein , Jill Pipher , Joseph H. NTRU: a ring-based public key cryptosystem. *Lecture Notes in Computer Science.* 1998;1423:267–288.

16. Hu C, Liao X, Cheng X. Verifiable multi-secret sharing based on LFSR sequences. *Theoretical Computer Science*. 2012;445:52–62.

17. Kouzmenko R. *Generalizations of the NTRU cryptosystem.* 2006.

18. Polytechnique, Montreal, Canada.

19. Liaojun P, Huixian L, Yumin W. An efficient and secure multi-secret sharing scheme with general access structures. *Wuhan University Journal of Natural Sciences*. 2006;11(6):1649–1652.

20. Mashhadi S, Dehkordi MH. Two verifiable multi secret sharing schemes based on nonhomogeneous linear recursion and LFSR public-key cryptosystem. *Information Sciences*. 2015;294:31–40.

21. Hideki Imai, Joern Mueller Quade, Anderson CA Nascimento. A Quantum Information Theoretical Model for Quantum Secret Sharing Schemes. *Quantum Inf Comput*. 2003;5(1):69–80.

22. Amroudi AN, Zaghain A, Sajadieh M. *Wireless Pers Commun*. 2017.

23. MA Bafghi, AN Amroudi. A post quantum (n, n)-threshold secret sharing scheme using AD cryptosystem. *Annual Iranian Mathematics Conference.* 2015.

24. Saeidi Ali, Zahedi Mohammad MAhdi, Nakhaei Amroodi Ali. A (n, n)-Threshold Secret Sharing Scheme Based on GGH Cryptosystem, *International Journal of Basic Sciences & Applied Research.* 2015;4(2):106–110.

Citation: Amroudi AN. Secret sharing schemes. *Electric Electron Tech Open Acc J.* 2018;2(5):310–311. DOI: 10.15406/eetoaj.2018.02.00033