Strongly Secure Quantum Ramp Secret Sharing Constructed from Algebraic Curves over Finite Fields (full version arXiv:1410.5126)

Ryutaroh Matsumoto
Department of Communications and Computer Engineering,
Tokyo Institute of Technology, Japan
ryutaroh@it.ce.titech.ac.jp

June 29, 2015

Keywords: algebraic curve, quantum secret sharing, non-perfect secret sharing, ramp secret sharing, strong security
PACS: 03.67.Dd

Secret sharing (SS) scheme encodes a secret into multiple shares being distributed to participants, so that only qualified sets of shares can reconstruct the secret perfectly [13]. The secret and shares are traditionally classical information [13], but now quantum secret and quantum shares can also be used [3, 4, 11].

In perfect SS, if a set of shares is not qualified, that is, it cannot reconstruct the secret perfectly, then the set has absolutely no information about the secret. It is well-known that the share sizes in perfect SS must be larger than or equal to that of the secret, both in classical and quantum cases. To overcome this inefficiency of storing shares, the ramp classical SS was proposed [1, 8, 14], which reduces the share sizes at the cost of allowing partial information leakage to non-qualified sets of shares. In ramp SS, a share set is said to be forbidden if it has no information about secret, while it is said to be intermediate if it is neither qualified nor forbidden [5, 14].

The first quantum ramp SS was proposed by Ogawa et al. [9], which made the share size L times smaller than its secret, where L is the number of qudits in the secret. In their study [9], there were two drawbacks. Firstly, it does not control how information is leaked to a non-qualified set of shares, and there exists an undesirable case in which an intermediate set of shares can understand a qudit in the secret, as demonstrated in [15]. To exclude such a possibility, we introduced a notion of the strong security of quantum ramp SS, which ensures no intermediate set can understand a qudit in the secret (see [15] for its formal definition) and proposed an explicit construction with the strong security.

The second drawback of [9] as well as our previous proposal [15] is that the dimension of quantum shares must be larger than that of the number of participants. When the number of participants is large, handling quantum shares become more difficult, because handling large dimensional quantum systems are generally more difficult than smaller ones. Our previous proposal [15] solved the first drawback but did not the second. The purpose of this paper is to solve the first and the second drawbacks of [9] simultaneously.

We will proceed as follows: Firstly, we modify the strong security definition given in [15], because the previous definition in [15] required that all the qualified sets are of the same size, and also that all the forbidden sets are of the same size. Secondly, we carry over the classical strongly secure ramp SS [2, 7] using algebraic curves to the quantum setting, then we prove that the proposed quantum SS has the strong security. We also present sufficient conditions for its qualified, intermediate, and forbidden sets by using the technique in [6].

Acknowledgments

This research is partly supported by the National Institute of Information and Communications Technology, Japan, and by the Japan Society for the Promotion of Science Grant Nos. 23246071 and 26289116, and the Villum Foundation through their VELUX Visiting Professor Programme 2013–2014.

References

[1] Blakley, G.R., Meadows, C.: Security of ramp schemes. In: Advances in Cryptology–CRYPTO'84, *Lecture Notes in Computer Science*, vol. 196, pp. 242–269. Springer-Verlag (1985). DOI 10.1007/3-540-39568-7_20

[2] Chen, H., Cramer, R., de Haan, R., Cascudo Pueyo, I.: Strongly multiplicative ramp schemes from high degree rational points on curves. In: N. Smart (ed.) Advances in Cryptology – EUROCRYPT 2008, *Lecture Notes in Computer Science*, vol. 4965, pp. 451–470. Springer-Verlag (2008). DOI 10.1007/978-3-540-78967-3_26

[3] Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. Phys. Rev. Lett. **83**(3), 648–651 (1999). DOI 10.1103/PhysRevLett.83.648

[4] Gottesman, D.: Theory of quantum secret sharing. Phys. Rev. A **61**(4), 042311 (2000). DOI 10.1103/PhysRevA.61.042311

[5] Iwamoto, M., Yamamoto, H.: Strongly secure ramp secret sharing schemes for general access structures. Inform. Process. Lett. **97**(2), 52–57 (2006). DOI 10.1016/j.ipl.2005.09.012

[6] Matsumoto, R.: Coding theoretic construction of quantum ramp secret sharing (2014). URL `arXiv:1405.0149v5`. (version 5 or later)

[7] Matsumoto, R.: Strong security of the strongly multiplicative ramp secret sharing based on algebraic curves. IEICE Trans. Fundamentals **E98-A**(7) (2015).

[8] McEliece, R.J., Sarwate, D.V.: On sharing secrets and Reed-Solomon codes. Comm. ACM **24**(9), 583–584 (1981). DOI 10.1145/358746.358762

[9] Ogawa, T., Sasaki, A., Iwamoto, M., Yamamoto, H.: Quantum secret sharing schemes and reversibility of quantum operations. Phys. Rev. A **72**(3), 032318 (2005). DOI 10.1103/PhysRevA.72.032318

[10] Shamir, A.: How to share a secret. Comm. ACM **22**(11), 612–613 (1979). DOI 10.1145/359168.359176

[11] Smith, A.D.: Quantum secret sharing for general access structures (2000). URL arXiv:quant-ph/0001087

[12] Stichtenoth, H.: Algebraic Function Fields and Codes, *Graduate Texts in Mathematics*, vol. 254, 2nd edn. Springer-Verlag, Berlin Heidelberg (2009). DOI 10.1007/978-3-540-76878-4

[13] Stinson, D.R.: Cryptography Theory and Practice, 3rd edn. Chapman & Hall/CRC (2006)

[14] Yamamoto, H.: Secret sharing system using (k, l, n) threshold scheme. Electronics and Communications in Japan (Part I: Communications) **69**(9), 46–54 (1986). DOI 10.1002/ecja.4410690906. (the original Japanese version published in 1985)

[15] Zhang, P., Matsumoto, R.: Quantum strongly secure ramp secret sharing. Quantum Information Processing **14**(2), 715–729 (2015). DOI 10.1007/s11128-014-0863-2