Hemenway, Brett; Ostrovsky, Rafail
Efficient robust secret sharing from expander graphs. (English) [Zbl 1380.94098]

Summary: Threshold secret sharing allows a dealer to share a secret among \( n \) players so that any coalition of \( t \) players learns nothing about the secret, but any \( t+1 \) players can reconstruct the secret in its entirety. Robust secret sharing (RSS) provides the additional guarantee that even if \( t \) malicious players mangle their shares, they cannot cause the honest players to reconstruct an incorrect secret. In this work, we construct a simple RSS protocol for \( t = \left( \frac{1}{2} - \epsilon \right) n \) that achieves logarithmic overhead in terms of share size and simultaneously allows efficient reconstruction. Our shares size increases by an additive term of \( O(\kappa \log n) \), and reconstruction succeeds except with probability at most \( 2^{-\kappa} \). Previous efficient RSS protocols like that of T. Rabin and M. Ben-Or [“Verifiable secret sharing and multiparty protocols with honest majority”, in: Proceedings of the twenty-first annual ACM symposium on theory of computing, STOC ’89. New York, NY: Association for Computing Machinery (ACM). 73-85 (1989; doi:10.1145/73007.73014)] and A. Cevallos et al. [Lect. Notes Comput. Sci. 7237, 195–208 (2012; Zbl 1297.94116)] use MACs to allow each player to check the shares of each other player in the protocol. These checks provide robustness, but require significant overhead in share size. Our construction identifies the \( n \) players as nodes in an expander graph, each player only checks its neighbors in the expander graph.

MSC:

94A60 Cryptography
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)
94C15 Applications of graph theory to circuits and networks

Keywords: robust secret sharing; expander graphs; secure message transmission

Full Text: DOI

References:

[9] Cabella, S; Padrò, C; Sáez, G; ciobanu, G (ed.); Paun, G (ed.), Secret sharing schemes with detection of cheaters for a general access structure, 185-194, (1999), Berlin · Zbl 0954.94010
Jhanwar, MP, Safavi-Naini, R: Unconditionally-Secure Robust Secret Sharing with Minimum Share Size. In: Sadeghi, A-R (ed.); Cramer, R; Damgård, I; Döttling, N; Fehr, S; Kilian, J; Oswald, E; Padró, C; Rabani, Y; Safavi-Naini, R; Oswald, E (ed.); Fischlin, M (ed.), Linear secret sharing schemes from error correcting codes and universal hash functions, 313-336, (2015), Berlin - Zbl 1371.94665

Cramer, R; Damgård, I; Fehr, S; Kilian, J (ed.). On the cost of reconstructing a secret, or VSS with optimal reconstruction phase, 503-523, (2001), Berlin - Zbl 1001.94534

Cramer, R; Dodis, Y; Fehr, S; Padró, C; Wicks, D; Smart, NP (ed.). Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors, 471-488, (2008), Berlin - Zbl 1149.94433

Cramer, R; Fehr, S; Yung, M (ed.), Optimal black-box secret sharing over arbitrary abelian groups, 307-323, (2008), Berlin - Zbl 1129.94020


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.