Cryptology ePrint Archive: Report 2011/174

On-line secret sharing

Laszlo Csirmaz and Gabor Tardos

Abstract: In a perfect secret sharing scheme the dealer distributes shares to participants so that qualified subsets can recover the secret, while unqualified subsets have no information on the secret. In an on-line secret sharing scheme the dealer assigns shares in the order the participants show up, knowing only those qualified subsets whose all members she have seen. We often assume that the overall access structure (the set of minimal qualified subsets) is known and only the order of the participants is unknown. On-line secret sharing is a useful primitive when the set of participants grows in time, and redistributing the secret when a new participant shows up is too expensive. In this paper we start the investigation of unconditionally secure on-line secret sharing schemes. The complexity of a secret sharing scheme is the size of the largest share a single participant can receive over the size of the secret. The infimum of this amount in the on-line or off-line setting is the on-line or off-line complexity of the access structure, respectively. For paths on at most five vertices and cycles on at most six vertices the on-line and offline complexities are equal, while for other paths and cycles these values differ. We show that the gap between these values can be arbitrarily large even for graph based access structures. We present a general on-line secret sharing scheme that we call first-fit. Its complexity is the maximal degree of the access structure. We show, however, that this on-line scheme is never optimal: the on-line complexity is always strictly less than the maximal degree. On the other hand, we give examples where the first-fit scheme is almost optimal, namely, the on-line complexity can be arbitrarily close to the maximal degree. The performance ratio is the ratio of the on-line and off-line complexities of the same access structure. We show that for graphs the performance ratio is smaller than the number of vertices, and for an infinite family of graphs the performance ratio is at least constant times the square root of the number of vertices.

Category / Keywords: foundations / secret sharing; online algorithm; complexity; entropy

Publication Info: Submitted to Design, Codes, and Cryptography

Date: received 5 Apr 2011

Contact author: csirmaz at degas ceu hu

Available formats: PDF | BibTeX Citation

Version: 20110405:085914 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]