Code on graph-based Asynchronous Verifiable Secret Sharing

Hugo Delavenne*[1] and Lola-Baie Mallordy[2]

[1]Geometry, arithmetic, algorithms, codes and encryption – LIX CNRS, Ecole Polytechnique, Institut Polytechnique de Paris, L'Institut National de Recherche en Informatique et e n Automatique (INRIA) – France

[2]Geometry, arithmetic, algorithms, codes and encryption – LIX CNRS, Ecole Polytechnique, Institut Polytechnique de Paris, L'Institut National de Recherche en Informatique et e n Automatique (INRIA) – France

Résumé

Verifiable Secret Sharing (VSS) schemes usually consider synchronous communication, which cannot always be the case on real networks where packets can be lost or parties arbitrarily delayed. Allowing asynchrony adds a large overhead complexity cost: the dealer and communication complexity is in $O(n^2 \log n)$ in state of the art n-parties Asynchronous VSS (AVSS) schemes, whereas there are synchronous schemes with only linear communications. To ensure that all honest parties agree on the same secret and are ready for reconstruction, AVSS schemes essentially perform a broadcast protocol. While this immediately bounds the overall communication complexity of the protocol to be at least in $O(n^2)$, this method enables to reach the maximum threshold of malicious parties of $t = n/3$. However, a smaller threshold t may be sufficient for some use cases, and one may want to take advantage of this. We consider a statistical scheme, meaning that the correctness and termination properties are only guaranteed with good probability. We propose a new method to transform any linear VSS scheme into a statistical AVSS. We build a statistical AVSS protocol Bonneval-on-Arc where each party only communicates with d neighbours, a situation that we model by a d-regular graph. We obtain quasilinear communication complexity for the dealer, and sublinear complexity for each party, and a corruption threshold $t < n/(d+2)$ as a tradeoff.

*Intervenant