ABSTRACT

CFEM & CTIC workshop:
Theory and Practice of Secure Multiparty Computation
May 30 to June 3, 2016
Aarhus University, Denmark

Title: Optimal round VSS with a non-interactive Dealer: VSS as a special case of VSR

Yvo Desmedt, University of Texas, USA

In a cloud environment the client has limited resources (e.g., pressed by time, has limited battery, etc.). In such an environment, the dealer's effort in VSS should be minimal, which means in particular, to use the least randomness possible, to generate the smallest possible shares, and to be non-interactive. In the case of non-interactive dealer, we wonder whether an ordinary secret sharing scheme can be used in the first place.

A trivial approach for the above case would be that the parties use MPC to verify consistency of their shares. In our approach, we avoid MPC and add an extra requirement that the VSS protocol should have an optimal number of rounds. We work in the setting of perfect security and use the synchronous model.

When applied to Shamir secret sharing, our techniques are achieved by

(1) extending Reed-Solomon codes, in which the decoder uses a tensor, and
(2) by regarding the problem of VSS as a special case of Verifiable Share

Redistribution (VSR), a topic introduced by Wong-Wang-Wing. Our results easily extend to the case of general adversary structure.

We also briefly discuss the potential impact of VSR on MPC.

This is a joint work with Kirill Morozov.