Cryptology ePrint Archive: Report 2011/281

Computational Verifiable Secret Sharing Revisited

Michael Backes and Aniket Kate and Arpita Patra

Abstract: Verifiable secret sharing (VSS) is an important primitive in distributed cryptography that allows a dealer to share a secret among n parties in the presence of an adversary controlling at most t of them. In the computational setting, the feasibility of VSS schemes based on commitments was established over two decades ago. Interestingly, all known computational VSS schemes rely on the homomorphic nature of these commitments or achieve weaker guarantees. As homomorphism is not inherent to commitments or to the computational setting in general, a closer look at its utility to VSS is called for. In this paper, we demonstrate that homomorphism of commitments is not a necessity for computational VSS in the synchronous or in the asynchronous communication setting. We present new VSS schemes based only on the definitional properties of commitments that are almost as good as existing VSS schemes based homomorphic commitments. Furthermore, they have significantly lower communication complexities than their (statistical or perfect) unconditional counterparts. Considering the feasibility of commitments from any claw-free permutation, one-way function or collision-resistant hash function, our schemes can be an excellent alternative to unconditional VSS in the future.

Further, in the synchronous communication model, we observe that a crucial interactive complexity measure of round complexity has never been formally studied for computational VSS. Interestingly, for the optimal resiliency conditions, the least possible round complexity in the known computational VSS schemes is identical to that in the (statistical or perfect) unconditional setting: three rounds. Considering the strength of the computational setting, this equivalence is certainly surprising. In this paper, we show that three rounds are actually not mandatory for computational VSS. We present the first two-round VSS scheme for n>= 2t+1 and lower-bound the result tightly by proving the impossibility of one-round computational VSS for t >= 2 or n >= 3t. For the remaining condition of t=1 and n >= 4, we present a one-round VSS scheme. We also include a new two-round VSS scheme using homomorphic commitments that has the same communication complexity as the well-known three-round Feldman and Pedersen VSS schemes.

Category / Keywords: cryptographic protocols / Verifiable Secret Sharing, Round Complexity, Commitments, Homomorphism

Date: received 30 May 2011

Contact author: backes at mpi-sws org, aniket@mpi-sws org, arpita@cs au dk, arpitapatra10@gmail com