Non-interactive and Reusable Non-malleable Commitment Schemes

Ivan Damgaard
Department of Computer Science
Aarhus University
Ny Munkegade
8000 Aarhus C.
DENMARK

Abstract

We consider non-malleable (NM) and universally composable (UC) commitment schemes in the common reference string (CRS) model. We show how to construct non-interactive NM commitments that remain non-malleable even if the adversary has access to an arbitrary number of commitments from honest players — rather than one, as in several previous schemes. We show this is a strictly stronger security notion. Our constructionis the first non-interactive scheme achieving this that can be based on the minimal assumption of existence of one-way functions. But it can also be instantiated in a very efficient version based on the strong RSA assumption. For UC commitments, we show that existence of a UC commitment scheme in the CRS model (interactive or not) implies key exchange and — for a uniform reference string — even implies oblivious transfer. This indicates that UC commitment is a strictly stronger primitive than NM. Finally, we show that our strong RSA based construction can be used to improve the most efficient known UC commitment scheme so it can work with a CRS of size independent of the number of players, without loss of efficiency.

Joint work with Jens Groth.