Cryptology ePrint Archive: Report 2011/180

Highly-Efficient Universally-Composable Commitments based on the DDH Assumption

Yehuda Lindell

Abstract: Universal composability (or UC security) provides very strong security guarantees for protocols that run in complex real-world environments. In particular, security is guaranteed to hold when the protocol is run concurrently many times with other secure and possibly insecure protocols. Commitment schemes are a basic building block in many cryptographic constructions, and as such universally composable commitments are of great importance in constructing UC-secure protocols. In this paper, we construct highly efficient UC-secure commitments from the standard DDH assumption, in the common reference string model. Our commitment stage is non-interactive, has a common reference string with $O(1)$ group elements, and has complexity of $O(1)$ exponentiations for committing to a group element (to be more exact, the effective cost is that of $23\frac{1}{3}$ exponentiations overall, for both the commit and decommit stages). We present a construction that is secure in the presence of static adversaries, and a construction that is secure in the presence of adaptive adversaries with erasures, where the latter construction has an effective additional cost of just $5\frac{1}{3}$ exponentiations.

Category / Keywords: cryptographic protocols / universal composability, commitment schemes, concrete efficiency

Publication Info: This is the full version of the Eurocrypt 2011 paper.

Date: received 7 Apr 2011, last revised 12 Jul 2011

Contact author: lindell at cs biu ac il