Cryptology ePrint Archive: Report 2011/065

Fully Simulatable Quantum-Secure Coin-Flipping and Applications

Carolin Lunemann and Jesper Buus Nielsen

Abstract: We propose a coin-flip protocol which yields a string of strong, random coins and is fully simulatable against poly-sized quantum adversaries on both sides. It can be implemented with quantum-computational security without any set-up assumptions, since our construction only assumes mixed commitment schemes which we show how to construct in the given setting. We then show that the interactive generation of random coins at the beginning or during outer protocols allows for quantum-secure realizations of classical schemes, again without any set-up assumptions. As example applications we discuss quantum zero-knowledge proofs of knowledge and quantum-secure two-party function evaluation. Both applications assume only fully simulatable coin-flipping and mixed commitments. Since our framework allows to construct fully simulatable coin-flipping from mixed commitments, this in particular shows that mixed commitments are complete for quantum-secure two-party function evaluation. This seems to be the first completeness result for quantum-secure two-party function evaluation from a generic assumption.

Category / Keywords: cryptographic protocols / mixed commitment, quantum, common reference string, zero knowledge, secure function evaluation

Publication Info: Progress in Cryptology - Africacrypt 2011, pages 21-40, 2011.

Date: received 4 Feb 2011, last revised 23 Jun 2011

Contact author: carolin at cs au dk