Cryptology ePrint Archive: Report 2011/611

Adaptive and Concurrent Secure Computation from New Notions of Non-Malleability

Dana Dachman-Soled and Tal Malkin and Mariana Raykova and Muthuramakrishnan Venkitasubramaniam

Abstract: We present a unified framework for obtaining general secure computation that achieves adaptive- Universally Composable (UC)-sec
Our framework captures essentially all previous results on adaptive concurrent secure computation, both in relaxed models (e.g., quasi-polynom
time simulation), as well as trusted setup models (e.g., the CRS model, the imperfect CRS model). This provides conceptual simplicity and insig
into what is required for adaptive and concurrent security, as well as yielding improvements to set-up assumptions and/or computational assump
Moreover, using our framework we provide first constructions of concurrent secure computation protocols that are adaptively secure in the timi
model, and in the non-uniform simulation model.

Conceptually, our framework can be viewed as an adaptive analogue to the recent work of Lin, Pass and Venkitasubramaniam [STOC `09], w
considered only non-adaptive adversaries. Their main insight was that stand-alone non-malleability was sufficient for UC-security. A main conce
contribution of this work is, quite surprisingly, that it is indeed the case even when considering adaptive security.

A key element in our construction is a commitment scheme that satisfies a new notion of non-malleability. The notion of concurrent equivocal no
malleable commitments, intuitively, guarantees that even when a man-in-the-middle adversary observes concurrent equivocal commitments and
decommitments, the binding property of the commitments continues to hold for commitments made by the adversary. This notion is stronger tha
standard notions of concurrent non-malleable commitments which either consider only specific commits (e.g., statistically-binding) or specific
scenarios (e.g., the commitment phase and the decommitment phase are executed in a non-overlapping manner). Previously, commitments that s
our definition, have been constructed in setup models, but either require existence of stronger encryption schemes such as CCA-secure encrypti
require independent ``trapdoors" provided by the setup for every pair of parties to ensure non-malleability. We here provide a construction that
eliminates these requirements and require only a single trapdoor.

Category / Keywords: foundations / non-malleability, adaptive adversaries, UC-security

Date: received 10 Nov 2011

Contact author: dg2342 at columbia edu

Available formats: PDF | BibTeX Citation

Version: 20111115:174636 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]