Cryptology ePrint Archive: Report 2011/602

Positive Results for Concurrently Secure Computation in the Plain Model

Vipul Goyal

Abstract: We consider the question of designing concurrently self-composable protocols in the plain model. We first focus on the minimal setting where there is a party \pa which might interact with several other parties in any unbounded (polynomial) number of concurrent sessions. \pa holds a single input x which it uses in all the concurrent sessions. An analogy is a server interacting with various clients at the same time. In this ``single input" setting, we show that many (or even most) functionalities can be securely realized in the plain model. More precisely, we are able to realize all functionalities except ones which are a (weak form of) cryptographic unpredictable function. We complement our positive result by showing an impossibility result in this setting for a functionality which evaluates a pseudorandom function.

Our security definition follows the standard ideal/real world simulation paradigm (with no super polynomial simulation etc). There is no apriori bound on the number of concurrent executions.

We also show interesting extensions of our positive results to the more general setting where the honest parties may choose different inputs in different session (even adaptively), the roles that the parties assume in the protocol may be interchangeable, etc.

Prior to our work, the only positive results known in the plain model in the fully concurrent setting were for zero-knowledge.

Category / Keywords: cryptographic protocols /

Date: received 6 Nov 2011

Contact author: vipul at microsoft com

Available formats: PDF | BibTeX Citation

Version: 20111110:010039 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]