Cryptology ePrint Archive: Report 2011/251

Concurrently Secure Computation in Constant Rounds

Sanjam Garg and Vipul Goyal and Abhishek Jain and Amit Sahai

Abstract: We study the problem of constructing concurrently secure computation protocols in the plain model, where no trust is required in any party or setup. While the well established UC framework for concurrent security is impossible to achieve in this setting, a meaningful notion of concurrent security based on \emph{super-polynomial simulation} (SPS) is achievable and has been extensively studied [Pas03,PS04,BS05,LPV09,CLP10]. The recent work of [CLP10] obtains a concurrently secure computation protocol in the plain model with SPS security under standard assumptions, but requires a number of rounds of interaction that is polynomial in the security parameter.

In this work, we obtain the first concurrently secure computation protocol in the plain model with SPS security that uses only a \emph{constant} number of rounds and requires only \emph{standard assumptions}. To accomplish our result, we introduce a new proof technique that significantly reduces the demands placed on ``rewinding techniques" employed in previous work. We believe that our techniques are of independent interest and likely to be applicable in other settings related to secure concurrent composition.

Category / Keywords: foundations / secure multi-party computation, protocol composition, universal composability, super-polynomial simulation

Date: received 20 May 2011

Contact author: sanjamg at cs ucla edu

Available formats: PDF | BibTeX Citation

Version: 20110523:025823 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]