Cryptology ePrint Archive: Report 2011/006

Exploring the Limits of Common Coins Using Frontier Analysis of Protocols

Hemanta K. Maji and Pichayoot Ouppaphan and Manoj Prabhakaran and Mike Rosulek

Abstract: In 2-party secure computation, access to common, trusted randomness is a fundamental primitive. It is widely employed in the setting of computationally bounded players (under various complexity assumptions) to great advantage. In this work we seek to understand the power of trusted randomness, primarily in the computationally unbounded (or information theoretic) setting. We show that a source of common randomness does not add any additional power for secure evaluation of deterministic functions, even when one of the parties has arbitrary influence over the distribution of the common randomness. Further, common randomness helps only in a trivial sense for realizing randomized functions too (namely, it only allows for sampling from publicly fixed distributions), if UC security is required.

To obtain these impossibility results, we employ a recently developed protocol analysis technique, which we call the {\em frontier analysis}. This involves analyzing carefully defined ``frontiers'' in a weighted tree induced by the protocol's execution (or executions, with various inputs), and establishing various properties regarding one or more such frontiers. We demonstrate the versatility of this technique by employing carefully chosen frontiers to derive the different results. To analyze randomized functionalities we introduce a frontier argument that involves a geometric analysis of the space of probability distributions.

Finally, we relate our results to computational intractability questions. We give an equivalent formulation of the ``cryptomania assumption'' (that there is a semi-honest or standalone secure oblivious transfer protocol) in terms of UC-secure reduction among randomized functionalities. Also, we provide an {\em unconditional result} on the uselessness of common randomness, even in the computationally bounded setting.

Our results make significant progress towards understanding the exact power of shared randomness in cryptography. To the best of our knowledge, our results are the first to comprehensively characterize the power of large classes of randomized functionalities.

Category / Keywords: foundations / multi-party computation, universal composition, secure function evaluation, trusted common randomness, frontier analysis

Publication Info: TCC - 2011 (This is the full version of the paper)

Date: received 4 Jan 2011

Contact author: hemanta maji at gmail com

Available formats: PDF | BibTeX Citation

Note: Full Version of the TCC-2011 Paper

Version: 20110105:024526 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]