Cryptology ePrint Archive: Report 2011/137

Towards a Game Theoretic View of Secure Computation

Gilad Asharov and Ran Canetti and Carmit Hazay

Abstract: We demonstrate how Game Theoretic concepts and formalism can be used to capture cryptographic notions of security. In the restricted but indicative case of two-party protocols in the face of malicious fail-stop faults, we first show how the traditional notions of secrecy and correctness of protocols can be captured as properties of Nash equilibria in games for rational players. Next, we concentrate on fairness. Here we demonstrate a Game Theoretic notion and two different cryptographic notions that turn out to all be equivalent. In addition, we provide a simulation based notion that implies the previous three. All four notions are weaker than existing cryptographic notions of fairness. In particular, we show that they can be met in some natural setting where existing notions of fairness are provably impossible to achieve.

Category / Keywords: Game-Theory, Secure computation, Fairness

Publication Info: This is a full version of a paper that will apear in Eurocrypt 2011.

Date: received 17 Mar 2011, last revised 23 Feb 2012

Contact author: carmit at cs au dk

Available formats: PDF | BibTeX Citation

Version: 20120223:110854 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]