Cryptology ePrint Archive: Report 2011/396

Fair Computation with Rational Players

Adam Groce and Jonathan Katz

Abstract: We consider the problem of fair two-party computation, where fairness (informally) means that both parties should learn the correct output. A seminal result of Cleve (STOC 1986) shows that fairness is, in general, impossible to achieve for malicious parties. Here, we treat the parties as rational and seek to understand what can be done.

Asharov et al. (Eurocrypt 2011) recently considered this problem and showed impossibility of rational fair computation for a particular function and a particular set of utilities. We observe, however, that in their setting the parties have no incentive to compute the function even in an ideal world where fairness is guaranteed. Revisiting the problem, we show that rational fair computation is possible (for arbitrary functions and utilities) as long as the parties have a strict incentive to compute the function in the ideal world. This gives a new example where game theory can be used to circumvent impossibility results in cryptography.

Category / Keywords: cryptographic protocols / game theory, secure computation

Date: received 22 Jul 2011

Contact author: jkatz at cs umd edu