Efficient Multiparty Computation from Homomorphic Threshold Cryptography

Ronald Cramer, Ivan Damgård, Jesper Buus Nielsen
Aarhus University, Dept. of Computer Science
Ny Munkegade
DK 8000 Aarhus C
Denmark
Tel. +45 89 42 33 80
Email: ivan@daimi.au.dk

27 April 2000

Keywords: Multiparty Computations, Threshold Cryptosystems.

Virtually all multiparty computation (MPC) protocols proposed to date are based on some form of verifiable secret sharing. Here, we propose basing MPC instead on threshold crypto-systems that have an additional homomorphic property.

Given any secure system with this property, we design a general MPC protocol secure when any minority of the players may deviate from the protocol. We then give two examples of threshold cryptosystems that can be used in our construction. One example is based on Paillier's probabilistic public-key system from EuroCrypt '99, another can based on assuming that the standard DDH and QRA assumptions are both true.

In the most efficient version of our construction, which requires the random oracle model, the total number of bits sent to complete the computation is $O(nk|C|)$, where n is the number of players, k is the security parameter, and $|C|$ is the size of a Boolean circuit implementing the desired computation. To the best of our knowledge, this is the most communication-efficient general MPC protocol proposed to date. Franklin and Haber (in J.Crypt. vol.9) have proposed an MPC protocol with the same complexity, but their construction is only secure when players are assumed to follow the protocol. The requirement for the random oracle model can be removed at some cost in various ways. For instance, we can obtain a protocol with complexity $O(n|C|max(k,n))$, or one with $O(n|C|p(k))$ where $p()$ is a (rather large degree) polynomial.