Cryptology ePrint Archive: Report 2011/535

Multiparty Computation from Somewhat Homomorphic Encryption

I. Damgard and V. Pastro and N.P. Smart and S. Zakarias

Abstract: We propose a general multiparty computation protocol secure against an active adversary corrupting up to $n-1$ of the n players. The protocol may be used to compute securely arithmetic circuits over any finite field $\F_{p^k}$. Our protocol consists of a preprocessing phase that is both independent of the function to be computed and of the inputs, and a much more efficient online phase where the actual computation takes place. The online phase is unconditionally secure and has total computational (and communication) complexity linear in n, the number of players, where earlier work was quadratic in n. Hence, the work done by each player in the online phase is independent of n and moreover is only a small constant factor larger than what one would need to compute the circuit in the clear. It is the first protocol in the preprocessing model with these properties. We show a lower bound implying that for computation in large fields, our protocol is optimal. In practice, for 3 players, a secure 64-bit multiplication can be done in 0.05 ms. Our preprocessing is based on a somewhat homomorphic cryptosystem. We extend a scheme by Brakerski et al., so that we can perform distributed decryption and handle many values in parallel in one ciphertext. The computational complexity of our preprocessing phase is dominated by the public-key operations, we need $O(n^2/s)$ operations per secure multiplication where s is a parameter that increases with the security parameter of the cryptosystem. Earlier work in this model needed $\Omega(n^2)$ operations. In practice, the preprocessing prepares a secure 64-bit multiplication for 3 players in about 13 ms, which is 2-3 order of magnitude faster than the best previous results.

Category / Keywords: cryptographic protocols /

Date: received 30 Sep 2011, last revised 23 Feb 2012

Contact author: ivan at cs au dk,vpastro@cs au dk,zarah@cs au dk,nigel@cs bris ac uk

Available formats: PDF | BibTeX Citation

Version: 20120223:182853 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]