Lindell, Yehuda; **Pinkas, Benny**

Secure two-party computation via cut-and-choose oblivious transfer. (English)

Zbl 1281.94037

Ishai, Yuval (ed.), Theory of cryptography. 8th theory of cryptography conference, TCC 2011, Providence, RI, USA, March 28–30, 2011. Proceedings. Berlin: Springer (ISBN 978-3-642-19570-9/pbk). Lecture Notes in Computer Science 6597, 329-346 (2011).

Summary: Protocols for secure two-party computation enable a pair of parties to compute a function of their inputs while preserving security properties such as privacy, correctness and independence of inputs. Recently, a number of protocols have been proposed for the efficient construction of two-party computation secure in the presence of malicious adversaries (where security is proven under the standard simulation-based ideal/real model paradigm for defining security). In this paper, we present a protocol for this task that follows the methodology of using cut-and-choose to boost Yao's protocol to be secure in the presence of malicious adversaries. Relying on specific assumptions (DDH), we construct a protocol that is significantly more efficient and far simpler than the protocol of [the authors, Eurocrypt 2007. Lect. Notes Comput. Sci. 4515, 52–78 (2007; Zbl 1141.94362)] that follows the same methodology. We provide an exact, concrete analysis of the efficiency of our scheme and demonstrate that (at least for not very small circuits) our protocol is more efficient than any other known today.

The journal version has been published in J. Cryptology 25, No. 4, 680–722 (2012; Zbl 1278.94056).

For the entire collection see [Zbl 1213.94005].

MSC:

94A60 Cryptography

Full Text: DOI