ABSTRACT

CFEM & CTIC workshop:
Theory and Practice of Secure Multiparty Computation
May 30 to June 3, 2016
Aarhus University, Denmark

Title: MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer

Marcel Keller, University of Bristol, United Kingdom

Previous protocols for arithmetic MPC with a malicious, dishonest majority required public-key cryptography operations for every multiplication. In this talk, we present how to overcome this using a recent OT extension that offers malicious security at virtually no cost.

Altogether, the overhead for malicious security in our protocol is one order of magnitude over the straight-forward semi-honest protocol based on OT extension.

The implementation of our protocol proved to be more than 200 times faster than the implementation of SPDZ for two parties. We will also present results for 100 parties, the first such results to the best of our knowledge.