Secure Computation Based on the Conditional Gate

Berry Schoenmakers
TU Eindhoven
<berry@win.tue.nl>

Pim Tuyls
Philips Research
<pim.tuyls@philips.com>

Abstract

We present new results in the framework of secure multiparty computation based on homomorphic threshold cryptosystems. We introduce the *conditional gate* as a special type of multiplication gate that can be realized in a surprisingly simple and efficient way using just standard homomorphic threshold ElGamal encryption. As addition gates are essentially for free, the conditional gate not only allows for building a circuit for any function, but actually yields very efficient circuits for a wide range of tasks (e.g., Yao's millionaires problem and variants, and applications such as 'profile matching', where two parties jointly test whether some function of their profiles exceeds a given threshold, without divulging any information on their profiles).

We also consider fairness for the case of two-party computation based on homomorphic threshold cryptosystems, and a new method for achieving private outputs in secure computations based on homomorphic threshold cryptosystems.