

Secure Profile Matching

Pim Tuyls and Berry Schoenmakers

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. Thus, we show how to achieve *efficient* secure multiparty computation under the DDH assumption. We also consider fairness for the case of two-party computation based on homomorphic threshold cryptosystems.

In this talk, we mainly focus on a new application which we call "Secure 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 show that by using the El Gamal encryption scheme, the key generation protocol can be performed efficiently in contrast to systems based on an RSA modulus such as Paillier's cryptosystem.

Finally we mention that our approach leads to a very efficient—if not, the most efficient—solution to date for Yao's millionaires problem and non-interactive secure auctions.