Thesis: Efficient Protocols for Multi-Party Computation

Abstract: We demonstrate secure function evaluation protocols for branching programs, where the communication complexity is sublinear in the size of the circuit based on the circular security of the Paillier encryption scheme. We also offer a few optimizations to the scheme, including an alternative to the "Las Vegas"-style share conversion protocols of which directly checks the correctness of the computation. This allows us to reduce the number of required repetitions to achieve a desired overall error bound by a constant fraction for typical cases, and for large programs, reduces the total computation cost. We also present formal definitions for the security of perceptual hash, a general theoretical result that uses Fully Homomorphic Encryption, and a specific construction using Paillier's encryption.

Committee:

- Professor Rosario Gennaro, mentor, The City College of New York
- Professor Nelly Fazio, The City College of New York
- Professor William E. Skeith, The City College of New York

Outside Member:

- Markus Jakobsson, Security Researcher at ByteDance