Multiparty computation (MPC) is a fundamental problem in cryptography and distributed computing. It allows a set of mutually distrusting parties to jointly compute on private information without revealing any of that information.

There are thus two natural conditions for MPC protocols. First, the parties should only learn the desired output and nothing else. Second, each party should receive the correct output even if some parties deviate from the protocol arbitrarily.

Due to its generality, MPC can model almost any cryptographic task, such as e-voting, e-auctions, e-cash, coin-tossing, encryption, authentication, contract signing, and privacy-preserving data-mining. So the issue of possibility and feasibility of MPC is fundamental to the theory of secure distributed computing.

Motivation

Goal of an MPC Protocol

The left-hand side depicts a scenario in which all the parties communicate their private inputs to a central, trusted server, which performs the computation and communicates the output back to the parties. However, a trusted third party may not always be available; a secure protocol is needed which realises the computation without requiring explicit communication of secrets, as per the right-hand side. It should also be able to mitigate against ‘foul play’ on the part of potentially dishonest parties.

Contributions

The group has been active in both the theoretical exploration of MPC and the development of improved practical implementations of MPC protocols.

In recent years, members have been working on three projects, with different collaborators, to bring down the computation time of a widely used MPC benchmark from 19 minutes to 4 seconds and then to 200 milliseconds, aided by recent breakthroughs in fully homomorphic encryption.

Another particular focus of our research has been the design of efficient MPC protocols in asynchronous networks, a far more challenging problem than in the straightforward synchronous scenario. To this end we have explored new primitives and recently developed a very simple and efficient framework for the offline phase—the key stage in any MPC protocol.

Application: Electronic Voting

In e-Voting it is vital to produce a correct tally whilst ensuring the secrecy of the individual votes.

Funding and Collaboration

- EPSRC via grant EP/I03126X/1.
- DARPA via the PROCEED project.
- European Commission via ECRYPT II
- ERC via Advanced Grant CRIPTO.
- European Commission via the CACE project.
- Academic Collaborators:
  - University of Aarhus, ETH Zurich, Bar-Ilan University, University of Haifa, TU Darmstadt.
- Industrial Collaborators:
  - IBM TJ Watson.