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

Title: Privacy-Preserving Outsourcing by Distributed Verifiable Computation

Meilof Veeningen, Philips Research, The Netherlands

Verifiable computation allows a client to outsource computations to a worker with a cryptographic proof of correctness of the result that can be verified faster than performing the computation. Recently, the Pinocchio system achieved faster verification than computation in practice for the first time.
Unfortunately, Pinocchio and other efficient verifiable computation systems require the client to disclose the inputs to the worker, which is undesirable for sensitive inputs. We first explain Pinocchio, and then show how to solve its privacy problems by distributing the Pinocchio system to three (or more) workers, that each individually do not learn which inputs they are computing on. This is achieved by exploiting the almost linear structure of Pinocchio proofs, letting each worker essentially perform the work for a single Pinocchio proof; verification by the client remains the same.