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

Title: Verifiable ASICs

Michael Walfish, New York University, USA

A manufacturer of custom hardware (ASICs) can undermine the intended execution of that hardware; high-assurance execution thus requires controlling the manufacturing chain. However, a trusted platform might be orders of magnitude worse in performance or price than an advanced, untrusted platform. I will describe an alternative: using verifiable computation (VC), an untrusted ASIC computes – proofs – of correct execution, which are verified by a trusted processor or ASIC. In contrast to the usual VC setup, here the prover and verifier – together – must impose less overhead than the alternative of executing directly on the trusted platform. We have instantiated this approach in physically realizable, area-efficient, high throughput ASICs (for a prover and verifier). The system, called Zebra, is based on the CMT and Allspice interactive proof protocols, themselves based on the GKR "Muggles" protocol. Zebra incorporates new observations about CMT, careful hardware design, and attention to architectural challenges. For a class of real computations, Zebra meets or exceeds the performance of executing directly on the trusted platform. Furthermore, the prover has the best throughput in the literature: tens of thousands of proofs per second.

Joint work with Riad Wahby, Max Howald, Siddharth Garg, and abhi shelat.