Abstract:
We propose a new protocol, nicknamed TinyTable, for maliciously secure 2-party computation in the preprocessing model. One version of the protocol is useful in practice and allows, for instance, secure AES encryption with latency about 1 ms and amortized time about 0.5 microseconds per AES block on a fast cloud set-up. Another version is interesting from a theoretical point of view: we achieve a maliciously and unconditionally secure 2-party protocol in the preprocessing model for computing a Boolean circuit, where the communication complexity is $O(s)$ where $s$ is the circuit size, while the computational complexity is $O(k^\epsilon s)$ where $k$ is the statistical security parameter and $\epsilon < 1$ is a constant. For general circuits with no assumption on their structure, this is the best asymptotic performance achieved so far in this model.

In the talk, I will introduce secure computation and then sketch the protocol as well as an application. The talk therefore assumes little or no prior knowledge of cryptography.

Joint work with Jesper Buus Nielsen and Michael Nielsen