Speaker: Shai Halevi, IBM research

Title: Fully Homomorphic Encryption with Polylog Overhead

We show that homomorphic evaluation of (wide enough) arithmetic circuits can be accomplished with only polylogarithmic overhead. Namely, we present a construction of fully homomorphic encryption (FHE) schemes that for security parameter $\secparam$ can evaluate any width-$\Omega(\secparam)$ circuit with t gates in time $t\cdot polylog(\secparam)$.

To get low overhead, we use the recent batch homomorphic evaluation techniques of Smart-Vercauteren and Brakerski-Gentry-Vaikuntanathan, who showed that homomorphic operations can be applied to "packed" ciphertexts that encrypt vectors of plaintext elements. In this work, we introduce permuting/routing techniques to move plaintext elements across these vectors efficiently. Hence, we are able to implement general arithmetic circuit in a batched fashion without ever needing to "unpack" the plaintext vectors.

We also introduce some other optimizations that can speed up homomorphic evaluation in certain cases. For example, we show how to use the Frobenius map to raise plaintext elements to powers of~p at the "cost" of a linear operation.

Joint work with Craig Gentry and Nigel Smart.