“Symbolic Computations and Post-Quantum Cryptography”
Online Seminar

Zvika Brakerski

(*Stanford University)*

"Fully Homomorphic Encryption from LWE."

Nov 10, 12:00pm (New York Time).

Abstract:

In fully homomorphic encryption, it is possible to transform an encryption of a message, m, into an encryption of any (efficient) function of that message, $f(m)$, without knowing the secret key. This property makes it into a very useful cryptographic building block.
In the talk, we will show how to construct fully homomorphic encryption from the learning with errors (LWE) assumption. Thus, by known reductions, our scheme is based on the worst case hardness of short vector problems in arbitrary lattices.
We introduce two novel techniques: re-linearization and dimension-modulus reduction, which enable us to deviate from two fundamental concepts that ruled the design of all previous candidate schemes:
1. We show that the ``squashing paradigm'' is not needed to achieve full homomorphism.
2. We show that Gentry's bootstrapping theorem is not necessary for achieving ``leveled'' fully homomorphic encryption (a variant where the parameters of the scheme grow with the depth of the circuit to be evaluated). Nevertheless, using the bootstrapping theorem is still necessary to get a non-leveled scheme, it also improves efficiency and considerably weakens the underlying hardness assumption. Specifically, our scheme (using bootstrapping) can be based on the hardness of quasi-polynomial approximation to short vector problems.
The talk is based on two works: a joint work with Vinod Vaikuntanathan, and a joint work with Craig Gentry and Vinod Vaikuntanathan.

Next presentation: **Dec 8, 2011.** Pseudorandom Functions and Lattices
Chris Peikert *(Georgia Institute of Technology)*

Algebraic Cryptography Center