“Symbolic Computations and Post-Quantum Cryptography” Online Seminar

Rong Ge

(Princeton University)

"New Algorithms for Learning in Presence of Errors ."

May 11, 12:00pm (New York Time).

Abstract:

We give new algorithms for a variety of randomly-generated instances of computational problems sing a linearization technique that reduces to solving a system of linear equations. These algorithms are derived in the context of learning with structured noise, a notion introduced in this paper. This notion is best illustrated with the learning parities with noise (LPN) problem -well-studied in learning theory and cryptography. In the standard version, we have access to an oracle that, each time we press a button, returns a random vector $ a \in GF(2)^n$ together with a bit $b \in GF(2)$ that was computed as $a\cdot u +\eta$, where $u\in GF(2)^n$ is a secret vector,and $\eta \in GF(2)$ is a noise bit that is 1 with some probability p. Say $p=1/3$. The goal is to recover u. This task is conjectured to be intractable. In the structured noise setting we introduce a slight (?) variation of the model: upon pressing a button, we receive (say) 10 random vectors $a_1, a_2, \ldots, a_{10} \in GF(2)^n$, and corresponding bits $b_1, b_2, \ldots, b_{10}$, of which at most 3 are noisy. The oracle may arbitrarily decide which of the 10 bits to make noisy. We exhibit a polynomial-time algorithm to recover the secret vector u given such an oracle. We think this structured noise model may be of independent interest in machine learning.

We discuss generalizations of our result, including learning with more general noise patterns. We also give the first nontrivial algorithms for two problems, which we show fit in our structured noise framework. We give a slightly subexponential algorithm for the well-known learning with errors (LWE) problem over $GF(q)$ introduced by Regev for cryptographic uses. Our algorithm works for the case when the gaussian noise is small; which was an open problem. We also give polynomial-time algorithms for learning the MAJORITY OF PARITIES function of Applebaum et al. for certain parameter values. This function is a special case of Goldreich's pseudorandom generator.

Next presentation: **TBA**

Algebraic
Cryptography
Center