Algebraic Attacks against Random Local Functions and Their Countermeasures

Abstract:

Suppose that you have n truly random bits \( X=(X_1,\ldots,X_n) \) and you wish to use them to generate \( m\gg n \) pseudorandom bits \( Y=(Y_1,\ldots,Y_m) \) using a local mapping, i.e., each \( Y_i \) should depend on at most \( d=O(1) \) bits of \( x \). In the polynomial regime of \( m=n^s, s>1 \), the only known solution, originates from (Goldreich, ECCC 2000), is based on Random Local Functions: Compute \( Y_i \) by applying some fixed (public) \( d \)-ary predicate \( P \) to a random (public) tuple of distinct inputs. In this talk, we will try to understand, for any value of \( s \), how the pseudorandomness of the resulting sequence depends on the choice of the underlying predicate.

Based on joint work with Shachar Lovett.