New Graded Multilinear Maps from Lattices

Craig Gentry, Sergey Gorbunov, and Shai Halevi

Graded Encoding

- Approximating Multilinear Maps:
  - An encoding "hides" a plaintext value
  - Encoded values can be added, multiplied
  - Upto degree-k expressions, but no more
  - Can check if an expression equals zero
- Only two constructions so far [GGH,CLT]
  - Encoding is ~ homomorphic encryption
  - Zero-testing using a defective secret key

Our New Scheme

- Plaintext elements are LWE secrets
  - In matrix form S, must be small
- Encoding "related" to LWE instances
  - Can be viewed as instances of [GSW13]
- "Zero-test param" is a random matrix
  - More like a public key than a secret key
  - Can be checked at any level upto k (not just at level k)

The Main Idea

- Encoding a small secret $S_{n\times n}$ relative to a random $A_{m\times n}$ via a small $C_{m\times m}$ s.t.

$$C \times A \approx A \times S$$

  - A is an "approximate eighenspace" for C
- *Encodings can be added, multiplied*
  - $(C_1 + C_2)A \approx A(S_1 + S_2)$
  - $C_1 C_2 A \approx A S_1 S_2$
- *C encodes 0 if CA is small*

Encoding Levels

- $k+1$ random matrices $A_0, A_1, \ldots, A_k$
  - Only A_0 needs to be published
- Level-i encoding of S is a small D s.t.

$$D \times A_j \approx A_{j+i} \times S, \forall\, j \leq k - i$$

- Can still add same-level encoding
- Multiplication adds the levels
- D encodes 0 (at any level) if DA *is small*