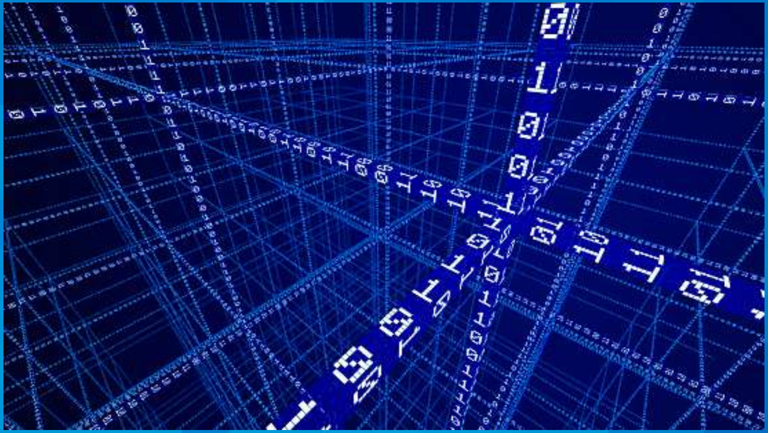

Computational Ring-LWR problem

Long Chen, Zhenfeng Zhang, Zhenfei Zhang

中國科学院 CHINESE ACADEMY OF SCIENCES

OnBoardSecurity

Motivation

- Ring LWR forms (one of) the most efficient solutions
  - Round 2/5, Saber, Lizard, etc.
  - (Partially) based on Decisional R-LWR problem
- No hardness result on polynomial modulus
- One of Peikert’s open problems in PQC

Our result

- New problem: Computational R-LWR problem
  - Given (g,g^a,g^b), it’s hard to find g^ab
  - Given {a, b_i = Round(as_i)}, it’s hard to find Round(a s_i s_j)
  - Preserves average/worst case reduction
- Reduced from R-LWE; but more efficient
  - Rounding vs errors
  - Uniform secrets
- Gives great confident to NIST submissions
  - Does not support any submitted parameters though