Security of RLWE problems for Homomorphic Encryptions

Jung Hee Cheon

Seoul National University

About Me

- Cryptanalysis
  - Discrete Logarithms
    - Diffie-Hellman with Auxiliary Inputs [EC'06 [1]]
    - Pollard ρ Improvement [AC'09 [2]]
  - Lattice Problems
    - Mmap attacks [EC'15 [4], EC'16 [5]]
    - NTRU subfield attack [ANTS'16 [3]]

---

1. C.-, Security Analysis of the Strong Diffie-Hellman Problem.
2. CHK, Speeding Up the Pollard Rho Method on Prime Fields.
3. CJL, An Algorithm for NTRU Problems and Cryptanalysis of the GGH Multilinear Map without an encoding of zero.
4. CHLRS, Cryptanalysis of the Multilinear Map over the Integers.
5. CFLMR, Cryptanalysis of the New CLT Multilinear Map over the Integers.

About Me

- Constructions of HE
  - Integer-based HEs [EC'13 [1], EC'15 [2]]
  - HEAAN : Homomorphic Encryption for Arithmetic of Approximate Numbers [Asia'17 [3], EC'18 [4]]
    - 1st place in IDASH 17' competition [5] :
      HE based logistic regression model learning

1. CCK+, Batch Fully Homomorphic Encryption over the Integers.
2. CS, Fully Homomorphic Encryption over the Integers Revisited.
3. CKKS, Homomorphic Encryption for Arithmetic of Approximate Numbers.
4. CHKKS, Bootstrapping for Approximate Homomorphic Encryption.
5. `http://www.humangenomeprivacy.org/2017/`

Ring Learning With Errors

Ring Learning With Errors (RLWE) problem is parametrized by

$$\text{a ring } \mathcal{R}, \text{ modulus } q > 0, \text{ and error distribution } \chi$$

- $\mathcal{R} = \mathbb{Z}[X]/\Phi_m(X)$ where $\Phi_m(X) =$ the m-th cyclotomic poly.
- Set $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$.

Definition (Ring-LWE (informal))

Distinguish the following two distributions :

- Ring-LWE distribution (with secret $s \in \mathcal{R}_q$) :
  Sample $a \xleftarrow{\$} \mathcal{R}_q$, and return $(a, b) \in \mathcal{R}_q^2$ given by $b = as + e$ where $e \leftarrow \chi$.
- The uniform distribution over $\mathcal{R}_q^2$.

Parameter settings for RLWE

Error distribution χ

- Each coeff of e from a Discrete Gaussian distribution with fixed width.

Secret key s

- Polys in full $\mathcal{R}_q$
- Polys having ternary coeffs from $\{-1, 0, 1\}$
- Polys having *sparse* ternary coeffs ex) Hamming Weight 64 in HElib, sp-HEAAN.

$*$ Red letters = Current white paper standards [1]

1. `http://homomorphicencryption.org/white-papers/`

On the choice of ring

Current choices :

- The m-th cyclotomic rings with m = power of 2
  - In this case, $\Phi_m(X) = X^{m/2} + 1 \rightarrow$ Efficient.
- Other cyclotomic rings s.t. $q \equiv_m 1$ are also used (HElib).

Some other RLWE instances are being reported to be vulnerable [3] [4].

- Need to be cautious when choosing ring !

$*$ Red letters = Current white paper standards

---

1. V. Lyubashevsky and C. Peikert and O. Regev, On Ideal Lattices and Learning with Errors Over Rings, EC'10

2. C. Peikert and O. Regev and N. Stephens-Davidowitz, Pseudorandomness of Ring-LWE for Any Ring and Modulus,

3. Y. Elias and K. E. Lauter and E. Ozman and K. E. Stange, Provably Weak Instances of Ring-LWE, C'15

4. W. Castryck and I. Iliashenko and F. Vercauteren, Provably Weak Instances of Ring-LWE Revisited, EC'16

On the choice of secret

For better efficiency, some schemes further assume *sparse* secret.

- ex) HElib and sp-HEAAN : 64 nonzero coefficients out of n coeffs.

However, some attacks for LWE has been improved with sparse secrets !

- The (improved) dual attack by Albrecht [1]
- Such attacks should be considered when using sparse secret.

1. M. Albrecht, On dual lattice attacks against small-secret LWE and parameter choices in HElib and SEAL, EC'17

Security estimation for (R)LWE-based schemes

- Lattice-based algorithms :
  The dual attack, the decoding attack, the uSVP attack ...
- Finding *short vectors* in lattices : BKZ lattice reduction algorithms.

- Assess a bit-security of Ring-LWE by LWE
  - So far, no significant ring-specialized attack for current cyclotomic rings.

General problem		Additional Information
Discrete Logarithm	v.s.	Variants of DL (e.g. DLwAI)
LWE	v.s.	Ring-LWE

Thank you for listening !