On the Hardness of NTRU Problems

Yang WANG, Mingqiang WANG

Frontiers of Computer Science, DOI: 10.1007/s11704-021-1073-6

Problems & Ideas

- The worst-case hardness of NTRU problems:
  - Implicitly showed in papers discussing the construction of provably secure NTRUEncrypts.
  - Confined to Cyclotomic fields.
- Ideas:

(1) Showing that for secrets $f, g \in R$ following suitable distributions $D_{R,\alpha}$, the distribution of an NTRU instance $h = gf^{-1} mod\ qR$ is statistically closed to the uniform distribution over R_q (i.e. the DSPR assumption is statistically difficult).

(2) Reducing (decisional, *normal form*) Ring-LWE problems over corresponding number field to the NTRU problem. More precisely, if one could solve the NTRU problem corresponding to an instance h, then he could output some "short`` enough element $x, y \in R$, s.t. $hx = y\ mod\ qR$. Then, when giving an Ring-LWE instance $(h, b) \in R_q \times R_q^{\vee}$, by estimating whether $b \cdot x$ is short enough, one could solve corresponding Ring-LWE problem.

Main Contributions

- Contributions:
  - In *any algebraic number field* K, the *average-case* NTRU problem (i.e. solving NTRU problems for h coming from some distribution with non-negligible probability) is at least as hard as the (decisional) Ring-LWE problem defined over K for suitable paramters;
  - By combining known reductions, we could deduce that the *average-case* NTRU problems over K is at least as hard as the *worst-case* basic ideal lattice problems (e.g. SIVP_γ) in K;
  - In *any algebraic number field* K, solving an *average-case* $\mathrm{SVP}_{\gamma'}$ over well-structured NTRU lattices in R^2 ($R = \mathcal{O}_K$) is no easier than solving the *worst-case* SIVP_γ problems in K.