

Factoring
 $N = pq$

DLP
 $g^x = h$

SVP
 $\lambda_1(\Lambda) = \min_{v \in \Lambda \setminus \{0\}} \|v\|$

CVP
 $\text{dist}(t, \Lambda) = \min_{v \in \Lambda} \|t - v\|$

SIS
 $Ax \equiv 0 \pmod{q}, \|x\| \text{ small}$

LWE
 $As + e \equiv b \pmod{q}$

Codes
 $He^T = s$

Isogeny
 $\varphi : E_1 \rightarrow E_2$

Hard Problems in Cryptography

Mathematical Foundations for Post-Quantum Cryptography

Factorization · Discrete Logarithm · Lattices · Codes · Isogenies · Multivariate · Hash

Ji, Yonghyeon