QIC 891 Topics in Quantum Safe Cryptography

Module 1: *Post-Quantum Cryptography*

Central candidate problems for PQC

Lecturer: Fang Song *May 10, 2016*

1 Lattice-based

Short Integer Solution ($\mathsf{SIS}_{n,q,\beta,m}$). Let $\mathbb{Z}_q$ be the additive group modulo a large integer q.

- **Given**: $A = (a_1, \ldots, a_m) \in \mathbb{Z}_q^{n\times m}, a_i \in \mathbb{Z}_q^n$.
- **Goal**: Find $x \in \mathbb{Z}_q^m$ with $\|x\| \le \beta$ s.t. $f_A(x) := Ax \pmod q = 0$.

Assumption 1. Let $A \in_R \mathbb{Z}_q^{n\times m}$ be uniformly at random, then $\mathsf{SIS}_{n,q,\beta,n}$ is hard to solve for poly-time algorithms (classical & quantum). Let $A \in_R \mathbb{Z}_q^{n\times m}$ and $x \leftarrow U$ for uniform distribution U on $\{x \in \mathbb{Z}_q^m : \|x\| \le \beta\}$), then $f_A(x)$ is hard to invert.

Learning With Errors ($\mathsf{LWE}_{n,q,\chi,m}$). Let χ be some error distribution on $\mathbb{Z}_q$.

- **Given**: (A, b), where $A = (a_1, \ldots a_m)^T \in \mathbb{Z}_q^{m\times n}, a_i \in \mathbb{Z}_q^n$ and

$$b = g_A(s,e) := As + e \pmod q \in \mathbb{Z}_q^n, \text{ with } s \in \mathbb{Z}_q^n, e \leftarrow \chi^m.$$

- **Goal**: Find s.

Assumption 2. Let $A \in_R \mathbb{Z}_q^{n\times m}$, $s \in_R \mathbb{Z}_q^n$ and $e \leftarrow \chi^m$ for some χ (e.g. rounded Gaussian $p(z) \propto e^{-\pi|z|^2/r^2}$ with $r \ge \sqrt{n}$), then $\mathsf{LWE}_{n,q,\chi,m}$ is hard to solve for poly-time algorithms (classical & quantum), i.e. $g_A(s,e)$ is hard to invert. This implies that g_A is also a pseudorandom generator (via a Search to Decision reduction) in the sense that $(A, b := g_A(s,e)) \approx_c U(\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q)$ ($\approx_c$ means "computationally hard to distinguish for any poly-time algorithms").

Remark 1. For efficiency reason, there are also Ring-based SIS and LWE problems, whose hardness relate to computational problems in structured lattices called *ideal* lattices.

2 Code-based

Let $\mathscr{C} \subseteq \mathbb{F}_2^n$ be an (n,k,d) binary linear code.
Syndrome Decoding ($\mathsf{SD}_{n,k,\beta}$). All operations are in $\mathbb{F}_2$.

- **Given**: (parity check matrix) $H \in \mathbb{F}_2^{(n-k)\times n}$ and (syndrome) $s \in \mathbb{F}_2^{n-k}$.
- **Goal**: Find $e \in \mathbb{F}_2^n$ with $\|e\| = \beta$ s.t. $f_H(x) := Hx = s$.

Assumption 3. let $H_0 \in \mathbb{F}_2^{(n-k)\times n}$ be the parity check matrix for some code $\mathscr{C}$ for which syndrome decoding is efficient (e.g., binary *Goppa* code), and $P \in_R S_n$ be a random permutation matrix. Then $g_H(\cdot)$ is hard to invert where $H := H_0 P$.

Codeword Decoding ($\mathsf{CD}_{n,k,\beta}$). (underlying McEliece PKE)

- **Given**: (generating matrix) $G \in \mathbb{F}_2^{n\times k}$ and (codeword possibly with error) $z \in \mathbb{F}_2^n$.
- **Goal**: Find $w \in \mathbb{F}_2^k$ s.t. $g_G(w) := Gw + e = z$ for some "small" error e with $\|e\| = \beta$.

Assumption 4. let $G_0 \in \mathbb{F}_2^{n\times k}$ be the generating matrix for some code $\mathscr{C}$ for which codeword decoding is efficient (e.g., binary *Goppa* code), $P \in \mathbb{F}_2^{n\times n}$ be the matrix of a random permutation $\pi \leftarrow S_n$ and $S \in_R \mathbb{F}_2^{k\times k}$ be a random invertible matrix. Then $g_G(\cdot)$ is hard to invert where $G := PG_0S$.

3 Multivariate-Polynomial-based

Multivariate Quadratic Polynomial Equations ($\mathsf{MQ}_{n,k}$). All operations are in some finite field $\mathbb{F}$.

- **Given**: $(p_i, y_i)_{i=1}^k$ where
$$p_i = \alpha_i + \sum_{j,\ell} \lambda_{ij\ell} x_j x_\ell$$
are qudratic polynomial in variables $x_1, \dots, x_n$ and $\alpha_i \in \mathbb{F}$.
- **Goal**: Find $(x_1, \dots x_n) \in \mathbb{F}^n$ s.t. $f_P(x_1, \dots, x_n) := (\dots, p_i(x_1, \dots, x_n), \dots) = (\dots, y_i, \dots)$.

Assumption 5. let P_0 be a collection of quadratic polynomials which are easy to solve. Let S and T be random affine transformations $\mathbb{F}^n \to \mathbb{F}^n$. Then $f_P(\cdot)$ is hard to invert where $P := TP_0S$.

$$\{x_i\} \to \underbrace{S \to P_0 \to T}_{P} \to \{y_i\}$$