Post-Quantum Cryptography QIC 891

Javad Doliskani
Institute for Quantum Computing

Learning from parity with errors

For integer $n > 0$ and real $\varepsilon \geq 0$, find the unknown $\mathbf{s} \in \mathbb{F}_2^n$ from a list of equations

$$\begin{aligned} \langle \mathbf{s}, \mathbf{a}_1 \rangle &\approx_\varepsilon b_1 \pmod 2 \\ \langle \mathbf{s}, \mathbf{a}_2 \rangle &\approx_\varepsilon b_2 \pmod 2 \\ &\vdots \end{aligned}$$

where the $\mathbf{a}_i \in \mathbb{F}_2^n$ are chosen independently and uniformly at random.

- Each equation is correct independently with probability $1 - \varepsilon$.
- Easy if $\varepsilon = 0$.
- Best known algorithm: Blum, Kalai, and Wasserman 2003, $O(2^{n/\log n})$.

Learning with errors (LWE)

For a prime $p = p(n)$ find the unknown $\mathbf{s} \in \mathbb{F}_p^n$ from a list of equations

$$\begin{aligned} \langle \mathbf{s}, \mathbf{a}_1 \rangle &\approx_\chi b_1 \pmod p \\ \langle \mathbf{s}, \mathbf{a}_2 \rangle &\approx_\chi b_2 \pmod p \\ &\vdots \end{aligned}$$

where the $\mathbf{a}_i \in \mathbb{F}_p^n$ are chosen independently and uniformly at random.

- The error is specified with a probability distribution $\chi : \mathbb{F}_p \to \mathbb{R}^+$. This means
$$b_i = \langle \mathbf{s}, \mathbf{a}_i \rangle + e_i$$
with e_i chosen independently according to χ
- Special case: $p = 2$, $\chi(0) = 1 - \varepsilon, \chi(1) = \varepsilon$.

Decision LWE

- LWE distribution $A_{\mathbf{s},\chi}$ on $\mathbb{F}_p^n \oplus \mathbb{F}_p$:

$$(\mathbf{a}_i, b_i)$$

  where $\mathbf{a}_i$ are uniform, $b_i = \langle \mathbf{s}, \mathbf{a}_i \rangle + e_i$ with e_i according to χ.
- Uniform distribution U on $\mathbb{F}_p^n \oplus \mathbb{F}_p$:

$$(\mathbf{a}_i, b_i)$$

  where $\mathbf{a_i}, b_i$ are uniform.

Problem

Distinguish $A_{\mathbf{s},\chi}$ and U with non-negligible advantage.

Hardness

- For appropriate choices of p, χ, there is a quantum reduction from the search $\mathrm{LWE}_{p,\chi}$ to worst-case lattice problems.
- Lattice problems are believed to be hard.
- There is a reduction from the Search to the Decision $\mathrm{LWE}_{p,\chi}$.

Theorem (Regev 2009)

If there is an efficient algorithm that solves the Decision LWE, then there exists an efficient algorithm that approximates the decision version of the shortest independent vectors problem (SIVP) to within $\tilde{O}(n/\alpha)$ in worst case.

Hardness (continued)

- Asymptotic assurance does not provide hardness of concrete instances, unless there is proper concrete analysis.
- The reduction might not be tight, i.e. the complexity polynomial has high degree in the main security parameter.

Example (Chatterjee et al. 2016)

Proposed parameters by Regev 2009: $p = n^2$, $\alpha = 1/(\sqrt{n}\log^2 n)$ which give $\gamma = \tilde{O}(n^{1.5})$. The tightness gap is

$$O(n^{11+c+d_1+2d_2})$$

- It is polynomial but it can be massive for practical parameters.
- For $n = 1024$, which is used in lwe-based systems, the above polynomial give a tightness gap of $\approx 2^{500}$.

A public key system

- **Parameters:**
  - The dimension n
  - $p \in O(n^2)$, say $n^2 < p < 2n^2$, a prime
  - $m = (1+\varepsilon)(1+n)\log p$ for a constant $\varepsilon > 0$
  - $\chi = \bar{\Psi}_{\alpha(n)}$, where $\alpha(n) = 1/(\sqrt{n}\log^2 n)$, is the discrete Gaussian distribution centered around 0 with standard deviation αp
- **Private key:** $\mathbf{s} \in \mathbb{F}_p^n$ uniformly at random
- **Public key:**
  - $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \mathbb{F}_p^n$ uniformly at random
  - $e_1, \ldots, e_m \in \mathbb{F}_p$ according to χ

  The public key is $(\mathbf{a}_i, b_i)_{i=1}^m$ where $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i$

A public key system (continued)

Encryption

To encrypt a bit b:

- Choose an $t \in \{0,1\}^m$ uniformly at random
- $\mathbf{a} = \sum_{i=0}^{m-1} t_i \mathbf{a}_i$, $b' = \sum_{i=0}^{m-1} t_i b_i$
- If $b = 0$ then output $(\mathbf{a}, b')$, otherwise output $(\mathbf{a}, \lfloor p/2 \rfloor + b')$.

Decryption

To decrypt a bit $(\mathbf{a}, b')$:

- Compute $b = b' - \langle \mathbf{a}, \mathbf{s} \rangle$
- If b is closer to 0 than to $\lfloor p/2 \rfloor$ output 0, otherwise output 1.

Semantic security

Lemma (Regev 2009)

For any $\varepsilon > 0$, $m \geq (1+\varepsilon)(1+n)\log p$, if there is a poly-time algorithm A that distinguishes between the encryption of 0, 1 then there is a distinguisher D that distinguishes between $A_{\mathbf{s},\chi}$ and U for a non-negligible fraction of all $\mathbf{s}$.

- **Proof.**
  - If the distribution is U, encryption of 0 is close to uniform by *Leftover Hash Lemma.* $\Rightarrow$ Decryption is hard.
  - Build a distinguisher D based on the possibility of decryption.

The Mersenne HW system

Mersenne number

A number of the form $p = 2^n - 1$ where n is prime.

- If n is composite then p is not a prime, e.g. if $n = \ell k$ then 2^ℓ divides p.
- If p is prime it is called a Mersenne prime.
- Smallest Mersenne primes

$$2^2 - 1, 2^3 - 1, 2^5 - 1, 2^7 - 1, 2^{13} - 1, 2^{17} - 1, \ldots$$

Hamming weight

Hamming weight

$\mathrm{Ham}(A)$ = the number of 1's in the binary representation of A

Lemma (Aggarwal et al. 2017)

For $p = 2^n - 1$ and $A, B \in \mathbb{Z}/p\mathbb{Z}$:

1. $\mathrm{Ham}(A + B) \leq \mathrm{Ham}(A) + \mathrm{Ham}(B)$.
2. $\mathrm{Ham}(AB) \leq \mathrm{Ham}(A)\,\mathrm{Ham}(B)$.
3. If $A \neq 0$, $\mathrm{Ham}(-A) \leq n - \mathrm{Ham}(A)$.

The Mersenne low HW assumptions

Mersenne Low Hamming Weight Combination:

- Mersenne prime $p = 2^n - 1$, an integer $h > 0$, and independent $A, B \in_R \mathbb{Z}/p\mathbb{Z}$ of hamming weight h
- The advantage of any PPA attempting to distinguish between $(R_1, AR_1 + B)$ and (R_1, R_2) for $R_1, R_2 \in_R \mathbb{Z}/p\mathbb{Z}$ is at most $\frac{\text{poly}(n)}{2^\lambda}$.

Mersenne Low Hamming Ratio:

- Mersenne prime $p = 2^n - 1$, an integer $h > 0$, and independent $F, G \in_R \mathbb{Z}/p\mathbb{Z}$ of hamming weight h
- The advantage of any PPA attempting to distinguish between $\frac{F}{G}$ and R for $R \in_R \mathbb{Z}/p\mathbb{Z}$ is at most $\frac{\text{poly}(n)}{2^\lambda}$.

The Mersenne low HW assumptions

Given a Mersenne prime $p = 2^n - 1$, an integer $h > 0$, and independent $A, B, F, G \in_R \mathbb{Z}/p\mathbb{Z}$ of hamming weight h. Let $H = \frac{F}{G}$ and $C = AH + B$.

Lemma

If Mersenne HW assumptions hold then the advantage of any PPA trying to distinguish between (H, C) and (H, R_2), where $R_2 \in_R \mathbb{Z}/p\mathbb{Z}$, is at most $\frac{\text{poly}(n)}{2^\lambda}$.

Proof: By the triangle inequality,

$$\begin{aligned}\Delta^D((H, C); (H, R_2)) \leq\ & \Delta^D((H, AH + B); (R1, AR_1 + B)) \\ & + \Delta^D((R_1, AR_1 + B); (R_1, R_2)) \\ & + \Delta^D((R_1, R_2); (H, R_2))\end{aligned}$$

The public key system

Key generation:

- For a given security parameter λ, find n, h such that $\binom{n-1}{h-1} > 2^\lambda$, and $4h^2 < n$.
- Set $p = 2^n - 1$.
- Choose independent $F, G \in_R \mathbb{Z}/p\mathbb{Z}$ of hamming weight h.
- *Private key:* G
- *Private key:* $H = \frac{F}{G}$

The public key system

Encryption

To encrypt a bit b:

- Choose $A, B \in_R \mathbb{Z}/p\mathbb{Z}$ of hamming weight h
- Output $(-1)^b(AH + B)$

Decryption

To decrypt a bit C:

- Compute $d = \mathrm{Ham}(CG)$
- If $d \leq 2h^2$ output 0; if $d \geq n - 2h^2$ output 1. Else output $\perp$.

Semantic security

Theorem (Aggarwal et al. 2017)

The scheme is semantically secure under the Mersenne Low Hamming Combination Assumption

- **Proof.**
  - Choose $A_1, B_1, A_2, B_2, \ldots, A_k, B_k$, and let $C_i^* = A_i H + B_i$.
  - Choose random $R_1, R_2, \ldots, R_k$
  - Define random variables

$$X_i = H, C_1^*, C_2^*, \ldots, C_i^*, R_{i+1}, \ldots R_k$$

  - Use the lemma and the triangle inequality.

Some concrete parameters

- For λ-bit classical, and $\frac{\lambda}{2}$-bit quantum security we need $\binom{n-1}{h-1} > 2^{\lambda}$
- Also we should have $4h^2 < n$
- So $h = \lfloor \sqrt{n}/2 \rfloor$ and $\lfloor \lambda \log_2 \binom{n-1}{h-1} \rfloor$

n	h	λ
1279	17	120
2203	23	174
3217	28	221
4253	32	260
9689	49	432

Toy example

- $n = 61$, $p = 2^{61} - 1$ is prime, $h = 3$
- $F = \texttt{0x1000000080000020}$, $G = \texttt{0x200000200080000}$
- $H = \frac{F}{G} = \texttt{0x180d2a5286f57ad7}$
- Encryption of 0:
  - $A = \texttt{0x8000000081}$, $B = \texttt{0x80008000000080}$
  - $C = (-1)^0(AH + B) = \texttt{0x19dfbff6365c3153}$
- Decryption of 0:
  - $GC = \texttt{0x140811888c003a68}$
  - $\mathrm{Ham}(GC) = 17 < 2h^2 = 18$

References I

Blum, Avrim, Adam Kalai, and Hal Wasserman (2003).
"Noise-tolerant learning, the parity problem, and the statistical query model".

Regev, Oded (2009).
"On lattices, learning with errors, random linear codes, and cryptography".

Chatterjee, Sanjit et al. (2016).
"Another Look at Tightness II: Practical Issues in Cryptography."

Aggarwal, Divesh et al. (2017).
A new public-key cryptosystem via Mersenne numbers.
Tech. rep.