A New Hope

$f(x) = x^n + 1$

$n = 2^k$

$q \equiv 1 \bmod 2n$

q is a large prime

$R_q = \mathbb{Z}/q\mathbb{Z}[x]/\langle f \rangle$

$= \mathbb{Z}[x]/\langle q, f \rangle$

$\#R_q = q^n$

$(\mathbb{Z}[x]/f)/q\mathbb{Z})$

$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$

$a_i \in \{\frac{-(q-1)}{2}, \ldots, -1, 0, 1, \ldots, \frac{q-1}{2}\}$

$\|f\|_\infty = \max |a_i|$

---

a_i = known in R_q

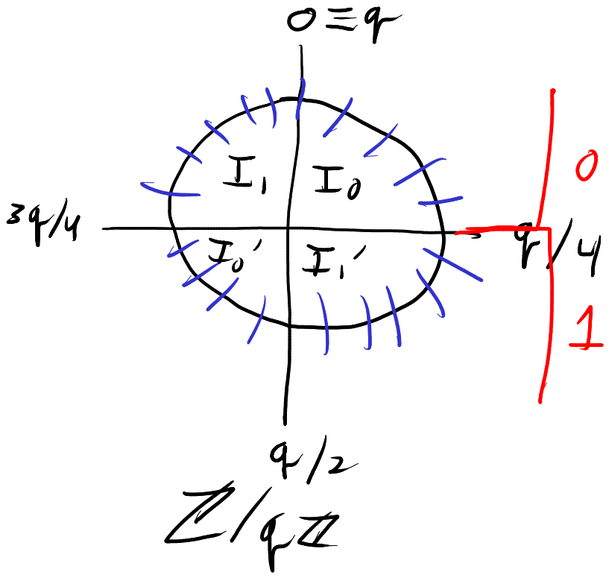
e_i = random small polys in R_q

s = known poly, $\|s\|_\infty \leq b$

set $b_i = a_i s + e_i$

Q: given set of pairs (a_i, b_i), can we find s?

Rounding and Masking



$\mathbb{Z}/q\mathbb{Z}$

$I_0 = \mathbb{Z}/q\mathbb{Z} \cap [0, q/4)$

$I_1' = \mathbb{Z}/q\mathbb{Z} \cap [q/4, q/2)$

$I_0' = \mathbb{Z}/q\mathbb{Z} \cap [q/2, 3q/4)$

$I_1 = \mathbb{Z}/q\mathbb{Z} \cap [3q/4, q)$

3 have $\frac{q-1}{4}$ elts

1 has $\frac{q+3}{4}$ elts

we won't worry about that.

Rounding

if $v \in \mathbb{Z}/q\mathbb{Z}$, then

$$\lfloor v \rceil_2 = \begin{cases} 0 & v \in I_0 \cup I_1 \\ 1 & v \in I_0' \cup I_1' \end{cases}$$

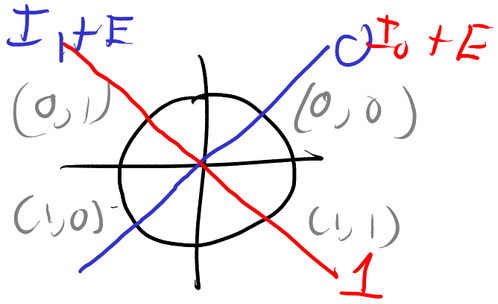
$w = v + e$

$I_0 + E = [-q/8, 3q/8)$

$I_1 + E = [-3q/8, q/8)$

Cross-rounding

$$\langle v \rangle_2 = \begin{cases} 0 & v \in I_0 \cup I_0' \\ 1 & v \in I_1 \cup I_1' \end{cases}$$



$E = [-q/8, q/8)$

$$rec(w, b) = \begin{cases} 0 & w \in I_b + E \\ 1 & else \end{cases}$$

Prop: if $w = v + e$, $e \in E$

then $rec(w, \langle v \rangle_2) = \lfloor v \rceil_2$.

e.g. if $v \in I_1'$

$\langle v \rangle_2 = 1$

$rec(w,1) = 1$

is $w \in I_1 + E$?

no, so rec is 1

$\lfloor v \rfloor_2 = 1$

ex: $q = 17$

$v = 7 \in I_1'$

$\lfloor v \rfloor_2 = 1, \langle \rangle_2 = 1$

$I_0 = [0, 4]$

$I_1' = [5, 8]$

$I_0' = [9, 12]$

$I_1 = [13, 16]$

$w = 11 \in I_0'$

$\lfloor w \rfloor_2 = 1$

$\langle w \rangle_2 = 0$

$rec(w, 0) = 1$

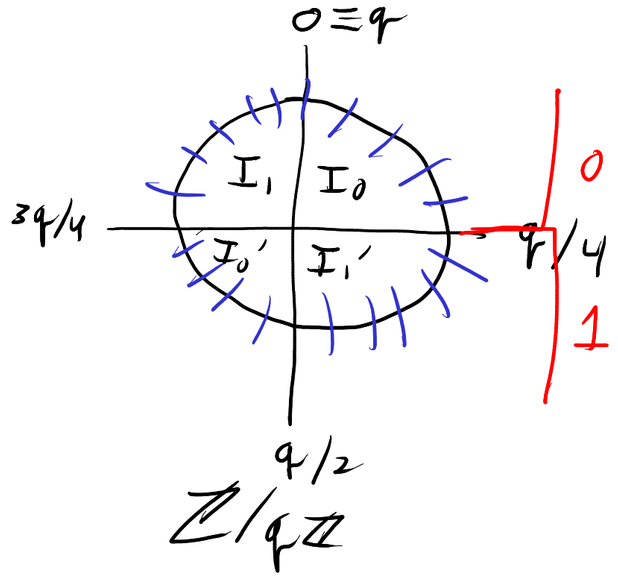
$I_0 + E = [-17/8, 3 \cdot 17/8)$

$= [-2, 6]$

$rec(w, 1) = 0$

$I_1 + E = [-3 \cdot 17/8, 17/8]$

$= [-6, 2]$



Ring-LWE Diffie-Hellman

Trusted party chooses

$n = 2^k$, q odd prime $\equiv 1 \bmod 2n$

$a \in R_q = \mathbb{Z}/q\mathbb{Z}[x]/\langle x^n + 1 \rangle$

prob dist to choose small elts of R_q

Key gen

1) Alice gens random $s_0, s_1 \in R_q$
priv key

2) computes $b = s_1 \cdot a + s_0$
pub key

encapsulation

1) Bob gens random $e_0, e_1, e_2 \in R_q$

2) computes $u = e_0 a + e_1$
$v = e_0 b + e_2$

3) computes $\mu = \lfloor v \rceil_2 \in \{0,1\}^n$

4) $\langle v \rangle_2 \in \{0,1\}^n$.

5) transmits $c = (u, \langle v \rangle_2) \in R_q \times \{0,1\}^n$

decapsulation

1) Alice computes $w = u \cdot s_1$

2) $\mathrm{rec}(w, v') = \mu$.

Prop: $\mu = \mathrm{rec}(w, v')$.

Pf / $w = e_0 a s_1 + e_1 s_1$

$v = e_0 s_1 a + e_0 s_0 + e_2$

so $w = v +$ small

so $\mathrm{rec}(w, \langle v \rangle_2) = \lfloor v \rceil_2$

$n = 4$

$q = 17$

$a = 3x^3 + 7x^2 - 5x$

---

keygen

$s_0 = x^3 + x + 1$

$s_1 = x^2 + 3x + 2$ Too Large

$b = s_1 a + s_0$

$= 6x^3 - x^2 + 5x + 2$

---

encapsulation

$e_0 = x^3 - x - 1$

$e_1 = x^2 + 2x - 2$

$e_2 = -x^3 + 2x^2 + 1$

$u = e_0 a + e_1 = 7x^3 - 4x^2 + 0x + 6$

$v = e_0 b + e_2 = -4x^3 - 8x^2 - 6x + 0$

$u = \lfloor v \rceil_2 = (0, 1, 1, 0)$

$\langle v \rangle_2 = (1, 0, 0, 0)$

Bob sends $(7x^3 - 4x^2 + 6, (1, 0, 0, 0))$

---

decapsulation

$w = (7x^3 - 4x^2 + 6)(x^2 + 3x + 2) = 2x^3 - 2x^2 - 6x - 5$

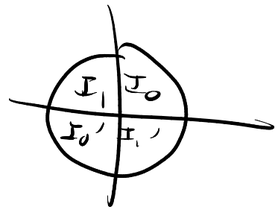
$\mathrm{rec}(w, (1, 0, 0, 0)) = (0, 0, 1, 1)$.

$I_0 = [0, 4]$

$I_1' = [5, 8]$

$I_0' = [9, 12] = [-8, -5]$

$I_1 = [13, 16] = [-4, -1]$



$I_0 + E = [-2, 6]$

$I_1 + E = [-6, 2]$

Suggested params

$n = 512$

$q = 25601$

≥ 680-bit key

$p(\text{failure}) \approx 2^{-75.72}$