Computing on Encrypted Data

- Goal: protect data while allowing computation.

Example: FHE

client $\qquad\qquad\qquad\qquad$ server

$$c \leftarrow \mathrm{Enc}_{sk}(x) \longrightarrow$$

$$\longleftarrow c^* = \mathrm{Eval}(f, c)$$

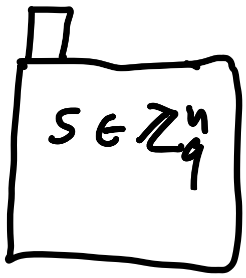
$$\mathrm{Dec}_{sk}(c^*) = f(x)$$

This class: FHE and beyond.
- ABE/FE, FHS, multi-key, obfuscation, ...
- many connections throughout crypto

Logistics: prerequisites, lectures.

Today: **Learning with Errors (LWE)**

$LWE_{n,q,\chi}$



$a_i \leftarrow \mathbb{Z}_q^n$, $e_i \leftarrow \chi$

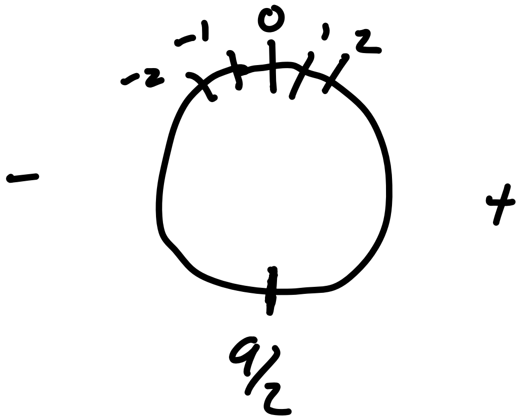
$a_i, \langle a_i, s \rangle + e_i$

O_s

χ is an "error" distribution

B-bounded: $e \leftarrow \chi$: $e \in [-B, B]$

identify $\mathbb{Z}_q$ elements with $(-q/2, \ldots, q/2]$



Search LWE assumption $\forall$ PPT $\mathcal{A}$

$$\Pr[\mathcal{A}^{O_s}(1^n) = s : s \leftarrow \mathbb{Z}_q^n] = \text{negl}(n)$$

$\Leftrightarrow \quad \forall\ m = \mathrm{poly}(n): \quad \Pr[\mathcal{A}(A, sA+e) = s] = \mathrm{negl}(n)$

$$\underbrace{\boxed{\ s\ }}_{1\times n} \xleftarrow{R} \mathbb{Z}_q^n \qquad \underbrace{\boxed{\quad A \quad}}_{n\times m} \xleftarrow{R} \mathbb{Z}_q^{n\times m}, \qquad \underbrace{\boxed{\quad e \quad}}_{1\times m} \xleftarrow{R} \chi^m$$

Decision LWE assumption: $\forall$ PPT $\mathcal{A}$

$$\left| \Pr[\mathcal{A}^{O_s}(1^n) = 1] - \Pr[\mathcal{A}^{R}(1^n) = 1] \right| = \mathrm{negl}(n)$$

$s \leftarrow \mathbb{Z}_q^n$, $\quad R$: random (a_i, b_i)

$\Leftrightarrow \quad \forall\ m = \mathrm{poly}(n) \qquad (A, sA+e) \approx (A, b)$

$s \leftarrow \mathbb{Z}_q^n, \quad A \leftarrow \mathbb{Z}_q^{n\times m}, \quad e \leftarrow \chi^m$

note: $\quad \Pr[\exists\, s', e' : \ s'A + e' = sA + e]$

$= \Pr[\exists s'\ (s'-s)A \in [-2B, 2B]^m]$

$$\leq q^n \left(\frac{4B}{q}\right)^m$$

negligible as $m \gg n$. when $q > 8B$

Related problem: Short Integer solutions (SIS)

$SIS_{n,q,\beta}$: $\forall$ PPT $\mathcal{A}$ $\forall m = poly(n)$

$$\Pr_{A \leftarrow \mathbb{Z}_q^{n \times m}}\left[\mathcal{A}(A) = r \text{ s.t. } \begin{array}{l} r \in [-\beta, \beta]^m \\ r \neq 0 \\ Ar^T = 0 \end{array} \right] = negl(n)$$

$LWE_{n,q,\chi} \Rightarrow SIS_{n,q,\beta}$ as long as $\beta \cdot B \ll q$

B-bounded

Given r s.t. $A \cdot r^T = 0$

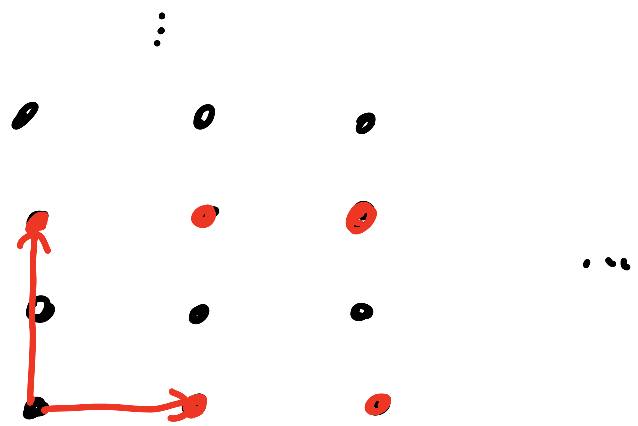
$$(sA + e) \cdot r^T = \langle e, r \rangle \quad \text{s.t} \quad |\langle e, r \rangle| \leq m \cdot \beta \cdot B$$

Connection to Lattices:

<u>Def:</u> Lattice $\mathcal{L} \in \mathbb{R}^n$ is a discrete additive subgroup of $\mathbb{R}^n$

Given basis $B = [b_1, \dots, b_k] \in \mathbb{R}^{n \times k}$

$$\mathcal{L}(B) = \{ \sum \alpha_i \cdot b_i \ : \ \alpha_i \in \mathbb{Z} \}$$



<u>Def:</u> $\lambda_1(\mathcal{L}) = \min\limits_{v \in \mathcal{L} - \{0\}} \|v\|$

SVP problem: Given B, find $v \in \mathcal{L}(B)$ s.t $\|v\| = \lambda_1(\mathcal{L}(B))$, $v \neq 0$

approximate SVP (SVP$_\gamma$) $\|v\| \le \gamma \cdot \lambda_1(\mathcal{L}(B))$

GapSVP$_\gamma$ distinguish $\lambda_1 \le 1$
$\lambda_1 \ge \gamma$

If GapSVP$_\gamma$ easy then can break LWE

$B = [\,\text{row}(A) \mid b \mid q \cdot e_1, \ldots, q \cdot e_m\,] \in \mathbb{R}^m$

If GapSVP$_\gamma$ hard on worst-case then
SIS$_{n,q,\beta}$ holds for some $\beta = \gamma / \text{poly}(n)$
$q \le \beta \cdot \text{poly}(n)$

If GapSVP$_\gamma$ hard on worst-case for quantum
LWE$_{n,q,\chi}$ holds for $q < 2^{\text{poly}(n)}$
and β-bounded χ with $\gamma = \tilde{O}(n \cdot q/\beta)$.

Crypto from LWE and SIS

CRHF from SIS: $h_A(x) = A \cdot x$

$A \leftarrow \mathbb{Z}_q^{n \times m}$, $x \in \{0,1\}^m$

Given collision $x \neq x'$:

$$A(x - x') = 0 \qquad x - x' \in [-1,1]^m.$$

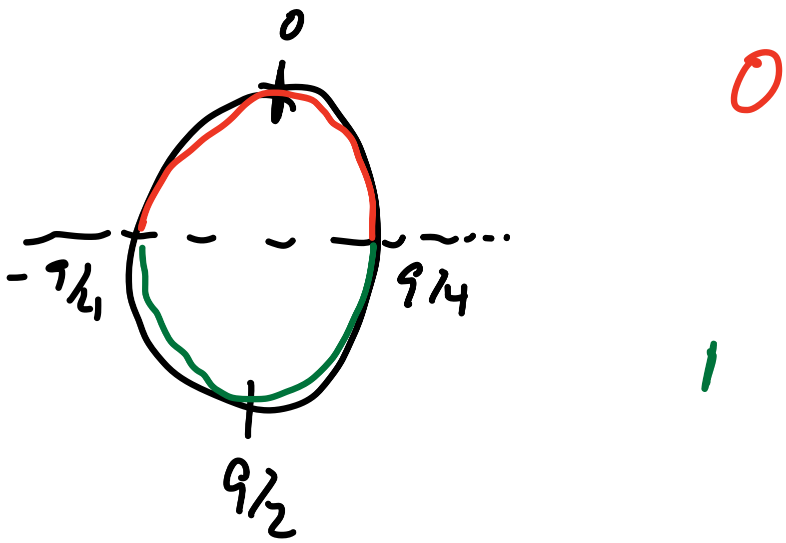
Symmetric-Key Enc from LWE:

Secret-Key : $s \leftarrow \mathbb{Z}_q^n$

$\mathrm{Enc}_s(\mu)$: $\left(a, \langle a,s\rangle + e + \mu \cdot \lceil q/2 \rceil\right)$

$a \leftarrow \mathbb{Z}_q^n$, $e \leftarrow \chi$

$\mathrm{Dec}_s(ct = (a, b))$: $\mathrm{round}_q(b - \langle a, s\rangle)$



correct if $B < q/4$

Public-Key Enc from LWE:

$\mathrm{KeyGen}(1^n)$: $pk = (A, b = sA + e)$
$sk = s$

$\mathrm{Enc}_{pk}(\mu)$: $r \leftarrow \{0,1\}^m$
$a^* = A \cdot r^T$
$b^* = b \cdot r^T + \mu \cdot \lceil \frac{q}{2} \rceil$

output (a^*, b^*)

$$\mathrm{Dec}_{sk}(a^*, b^*) = \mathrm{round}_q(b^* - \langle a^*, s \rangle)$$

Correctness: $b^* - \langle a^*, s \rangle =$

$$(sA + e) \cdot r^T + \mu \lceil q/2 \rceil - sAr^T$$

$$= e \cdot r^T + \mu \cdot \lceil q/2 \rceil$$

need: $\| e \cdot r^T \| \leq q/4$

$$\Leftarrow \quad B \leq q/4 \cdot m$$

Security: Hybrid argument

H0: (pk, ct) :

$pk = (A, b)$ $\quad$ $ct \leftarrow Enc_{pk}(\mu)$

$b = A \cdot s + e$

H1: (pk', ct) :

$pk = (A, b)$ $\quad$ $ct \leftarrow Enc_{pk}(\mu)$

$b \leftarrow \mathbb{Z}_q^m$

$H0 \approx H1$ by LWE

H2: (pk', ct')

$pk = (A, b)$ $\quad$ $ct' \leftarrow \mathbb{Z}_q^{n+1}$

$b \leftarrow \mathbb{Z}_q^m$

$H1 \approx H2$ stat close by LHL

$$\begin{array}{cc} m & \\ \bar{A} = \begin{bmatrix} A \\ b \end{bmatrix} & n+1 \end{array} \qquad ct := \bar{A} \cdot r + \begin{bmatrix} 0 \\ \mu \cdot \lceil q/2 \rceil \end{bmatrix}$$

by LHL $\bar{A} \cdot r$ is random and indep of $\bar{A}$.

H2 does not depend on μ.