Regev's Cryptosystem

Post-quantum crypto (pub key)

- Lattice based crypto (Regev's)
- Code based crypto (McEliece)
- Hash based (signatures)
- Multivariate polys
- Isogenies on elliptic curves

NIST competition

Learning with errors (LWE)

"learning problem"

(A) secret $s \in \{0,1\}^n$ → (B)

$a_1 \leftarrow \{0,1\}^n$, $b_1 := a_1 \cdot s$
$a_2 \leftarrow \{0,1\}^n$, $b_2 := a_2 \cdot s$
$\vdots$
$a_m \leftarrow \{0,1\}^n$, $b_m := a_m \cdot s$ ⟶ s ?

Algo:

$A := \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix}$ ($m \times n$), $b := \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ ($m \times 1$), s ($n \times 1$)

$As := \begin{pmatrix} a_1 \cdot s \\ \vdots \\ a_m \cdot s \end{pmatrix} = b$

A is random
(B) learns A, As = b
Can Bob learn s?

⟶ Yes. Solve $As = b$ for s by Gaussian elim.

Noisy variant:

(A) sec $s \in \{0,1\}^n$ → (B)

$a_1 \leftarrow \{0,1\}^n$, $b_1 := a_1 \cdot s + e_1$ (then $e_1 = 1$ with prob $p \ll \frac{1}{2}$)
$\vdots$
$a_m \leftarrow \{0,1\}^n$, $b_m := a_m \cdot s + e_m$

For suitable small p: We have an poly time (q) algo.

If $p = \frac{1}{2}$: B cannot learn s
If $p = 0$: B can learn s
If $p \approx \frac{1}{2}$: B cannot learn s
If $p = 0$:
- If p very very close: B can learn s because no errors happen (whp)
- If p is "small-ish": (?)

For crypto applications, generalize: Instead of bits $\{0,1\}$ use $\mathbb{Z}_q = \{0, \dots, q-1\} = \{-\lfloor \frac{q}{2} \rfloor, \dots, \lfloor \frac{q}{2} \rfloor\}$

(A) sec $s \xleftarrow{R} \mathbb{Z}_q^n$

$a_1 \xleftarrow{R} \mathbb{Z}_q^n$, $b_1 := a_1 \cdot s + e_1$ ($e_1 \leftarrow \chi$ where χ is a distrib over $\mathbb{Z}_q$ outputting small numbers)
$\vdots$
$a_m \xleftarrow{R} \mathbb{Z}_q^n$, $b_m := a_m \cdot s + e_m$

$A \in \begin{pmatrix} \cdots \\ a_i \\ \cdots \end{pmatrix}$ ($m \times n$), s ($n \times 1$)

$e \in \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix} \leftarrow \chi^m$ ($m \times 1$), $b = As + e$

Computational LWE problem

Parameters: $n, m \geq q > 0$ (typically $m \gg n$), Distrib χ on $\mathbb{Z}_q$ (typically small)

Compute: $A \xleftarrow{R} \mathbb{Z}_q^{m \times n}$, $s \xleftarrow{R} \mathbb{Z}_q^n$, $e \leftarrow \chi^m$, $b := As + e$

Get: A, b

Find: s

Decisional LWE problem

Parameters: same

Compute: same, $r \xleftarrow{R} \mathbb{Z}_q^n$

Get: A, b or A, r

Find out: which of the two did you get?

∃ many variants of this, eg "ring LWE" etc.

Regev's cryptosystem

Assume: Decisional LWE hard
- $\Pr[\, |e \times \frac{q}{2}| : e \xleftarrow{R} \chi, x \xleftarrow{R} \{0,1\}^n \,]$ exp small

Params: n, m, q, χ

Secret key: $s \xleftarrow{R} \mathbb{Z}_q^n$, $sk := s$

Public key: $A \xleftarrow{R} \mathbb{Z}_q^{m \times n}$, $e \leftarrow \chi^m$, $b := As + e$
$pk = (A, b)$

Enc(μ) ($\mu \in \{0,1\}$): $x \xleftarrow{R} \{0,1\}^m$, $c_1 := A^T x$, $c_2 := xb + \mu \lfloor \frac{q}{2} \rfloor$
Output (c_1, c_2)

Dec(c_1, c_2): $s \cdot c_1 = xb - xe$ (1-1/8 of the time)
$c_2 - sc_1 = \mu \lfloor \frac{q}{2} \rfloor + xe \in \mathbb{Z}_q$

$b = As + e$
$xb = xAs + xe$
$= s^T A^T x + xe$
$= sc_1 + xe$

If $|c_2 - sc_1| < \frac{q}{4}$, return 0
else return 1

Note: Dec is not perfect! There is small prob. of dec errors

Security of Regev (IND-CPA)

Claim: Given pk, adv cannot distinguish Enc(0), Enc(1) (assuming Decisional LWE is hard)

Proof sketch

Game 1: $(pk, sk) \leftarrow KeyGen()$, $\mu \xleftarrow{R} \{0,1\}$, $\beta \leftarrow A(pk, Enc(\mu))$

$\Pr[\beta = \mu \text{ in Game 1}] \overset{?}{=} ?$

Game 2: $s \xleftarrow{R} \mathbb{Z}_q^n$, $A \xleftarrow{R} \mathbb{Z}_q^{m \times n}$, $e \leftarrow \chi^m$, $b := As + e$
$\mu \xleftarrow{R} \{0,1\}$, $x \leftarrow \{0,1\}^m$, $c_1 := A^T x$, $c_2 := xb + \mu \lfloor \frac{q}{2} \rfloor$
$\beta \leftarrow A(A, b, c_1, c_2)$

$\Pr[\beta = \mu : \text{Game 2}] = \Pr[\beta = \mu : \text{Game 1}]$

Dec-LWE guarantees: b indist. from random given A, b

Game 3: $s \xleftarrow{R} \mathbb{Z}_q^n$, $A \xleftarrow{R} \mathbb{Z}_q^{m \times n}$, $e \leftarrow \chi^m$, $b \xleftarrow{R} \mathbb{Z}_q^m$
$x \xleftarrow{R} \{0,1\}^m$, $c_1 := A^T x$, $c_2 := xb + \mu \lfloor \frac{q}{2} \rfloor$
$\beta \leftarrow A(A, b, c_1, c_2)$

$\Pr[\beta = \mu : \text{Game 3}] \approx \Pr[\beta = A(A, b, c_1, c_2)] \approx \Pr[\beta = A(\dots, x)] \cdot \Pr[\beta = \mu : \text{Game 2}]$

Changes to Game 2: $b := As + e$ ⟶ $b \leftarrow \mathbb{Z}_q^m$

$H_\infty(x \mid c_1) \geq m - |c_1| \log q = m - n \log q$

Assume: $m \gg n \log q$

For $b \xleftarrow{R} \mathbb{Z}_q^m$, $x \mapsto x \cdot b$ is UHF
$\Rightarrow$ $x \mapsto xb$ is ~~strong~~ strong rnd extractor (with $\log q$-bit output)
$\Rightarrow$ xb indist. from random

Game 4: like Game 3 but xb ⟶ r ($r \in \mathbb{Z}_q$)

$\Pr[\beta = \mu : \text{Game 4}] \approx \Pr[\beta = \mu : \text{Game 3}]$

$\Pr[\beta = \mu : \text{Game 4}] = \frac{1}{2}$

$\Rightarrow \Pr[\beta = \mu : \text{Game 1}] \approx \frac{1}{2}$

∎