LWE

"Search" LWE $_{n,m,q,\chi}$

$\forall$ nu PPT $\mathcal{A}$,

$$\Pr_{\substack{A \leftarrow \mathbb{Z}_q^{m \times n} \\ s \leftarrow \mathbb{Z}_q^{n \times 1} \\ e \leftarrow \chi^m}} \left[\mathcal{A}(A, As+e) \rightarrow s \right] = \text{negl}(n)$$

n = sec. param
$m = \text{poly}(n, \log q)$
$q = O(2^n)$
χ = S.D. $\rightarrow$

"Decision" LWE $_{n,m,q,\chi}$

$\forall$ nu PPT $\mathcal{A}$,

$$\Pr_{\substack{A \leftarrow \mathbb{Z}_q^{m \times n} \\ s \leftarrow \mathbb{Z}_q^{n \times 1} \\ e \leftarrow \chi^m}} \left[\mathcal{A}(A, As+e) = 1 \right] - \Pr_{\substack{A \leftarrow \mathbb{Z}_q^{m} \\ b \leftarrow \mathbb{Z}_q^{n}}} \left[\mathcal{A}(A, b) = 1 \right] = \text{negl}(n)$$

LWE-hardness $\Rightarrow$ SIS hardness

SIS-hardness $\overset{?}{\Rightarrow}$ LWE-hardness

In Summary,

$$A, As+e \approx_c A, b$$

$$A \leftarrow \mathbb{Z}_q^{m \times n}, \; s \leftarrow \mathbb{Z}_q^{n \times 1}, \; e \leftarrow \chi^{m \times 1}, \; b \leftarrow \mathbb{Z}_q^{n \times 1}$$

$$\begin{bmatrix} A \end{bmatrix} \begin{bmatrix} As+e \end{bmatrix} \approx \begin{bmatrix} A \end{bmatrix} \begin{bmatrix} b \end{bmatrix}$$

Rename

$A^T \longrightarrow A$

$$A, s^T A + e^T \approx_c A, b^T$$

$$A \leftarrow \mathbb{Z}_q^{n \times m}$$

$$\begin{bmatrix} A \\ As+e \end{bmatrix} \approx_c \begin{bmatrix} A \\ b \end{bmatrix}$$

$$\begin{bmatrix} & A & \\ & & \end{bmatrix}$$

$$b = \begin{bmatrix} s^T A + e^T & \end{bmatrix}$$

If you don't know s, then b is (ind. from) random.

If you know s, then given A, b is easily computable (almost!)

Use b to mask message!

m can be 1.

pvt key $\longrightarrow$ s

Enc $\longrightarrow$ A, $As + e + \mu\left(\frac{q}{2}\right)$

Dec(s) $\longrightarrow$ compute As. Recover μ.

Public-key Encryption (Regev)

m will need to be $\geq n \log q$.

$$pk = \begin{bmatrix} A \\ s^T A + e^T \end{bmatrix}$$

$sk = s$

Given "just" pk (no "s"!), you should be able to generate a mask.

And given sk, ct. It should be possible to recover the mask for ct.

To ENCRYPT,

compute

$$\begin{bmatrix} A \\ b \end{bmatrix}_{(n+1)\times m} \cdot \underbrace{\begin{bmatrix} & r & \\ & \vdots & \\ & 0/1 & \end{bmatrix}}_{m\times 1}$$

$$= \begin{bmatrix} Ar \\ br \end{bmatrix}_{(n+1)\times 1}$$ ← use this as a mask.

$$ct = \begin{bmatrix} Ar \\ br \end{bmatrix} + \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ \hline msg \end{bmatrix} \pmod q$$

$c_2 \leftarrow [\,br\,]$

To Decrypt → compute $s^T Ar$.

output. $c_2 \oplus s^T Ar$

$$ct = \begin{bmatrix} Ar \\ [b^T r + \mu \lfloor \frac{q}{2} \rfloor] \end{bmatrix}$$

By LWE, $b^T = s^T A + e^T \approx$ uniform.

$$= \begin{bmatrix} A \\ b^T \end{bmatrix}, \quad ct = \begin{bmatrix} Ar \\ [b^T r + \mu \lfloor \frac{q}{2} \rfloor] \end{bmatrix}$$ where $b^T = s^T A + e^T$

$$\overset{c}{\approx} \text{(by LWE)} \begin{bmatrix} A \\ b^T \end{bmatrix}, \quad ct = \begin{bmatrix} Ar \\ [b^T r + \mu \lfloor \frac{q}{2} \rfloor] \end{bmatrix}$$ where $b^T \leftarrow \mathbb{Z}_q^{1 \times m}$

If r has sufficiently low guessing prob, $\sim 2^{-m}$.

$C, Cr \overset{\text{Stat.}}{\approx} C$, uniform

$C \to \begin{bmatrix} A \\ b^T \end{bmatrix}$ $\quad \overset{\text{Stat.}}{\approx} \downarrow \text{negl}(n)$

Dual-Regev

$$pk = \underbrace{\begin{bmatrix} A \end{bmatrix}_{n \times m} \begin{bmatrix} Ar \end{bmatrix}_{n \times 1}}_{B}$$

$$r \leftarrow \{0,1\}^{m \times 1}$$

$$sk = r.$$

Enc $\rightarrow$ Sample s, e.

$$s^T B + e^T.$$

$$\begin{bmatrix} s^T \end{bmatrix}_{1 \times n} \begin{bmatrix} A \end{bmatrix}_{n \times m}, \begin{bmatrix} s^T \end{bmatrix} \begin{bmatrix} Ar \end{bmatrix}_{n \times 1}$$

$$= s^T A + e_1^T, s^T Ar + e_2$$

From ~~Regev~~ → GSW

[Gentry 09]

$$pk = \begin{bmatrix} A \end{bmatrix}$$

$$b \to [s^T A + e^T]$$

$$sk = t = [-s^T \quad 1]$$

$$t \cdot pk = \underbrace{[-s^T \; 1]}_{1 \times n+1} \begin{bmatrix} A \\ [s^T A + e^T] \end{bmatrix}_{n+1 \times m} \approx 0$$

$$Enc(pk, \mu) \to pk \cdot R + \mu G$$

$R \leftarrow \{0,1\}^{m \times m}$

G : $(n+1) \times m$ matrix

$$I_{(n+1)\times(n+1)} \otimes [1 \; 2 \; 4 \; \ldots \; 2^{\lfloor \lg q \rfloor}]$$

$$G = \begin{bmatrix} 1 & 2 & 4 & \cdots & 2^{\lfloor \log q \rfloor} & & & & & \\ & & & & & 1 & 2 & 4 & \cdots & \\ & & & & & & & & & 1 2 4 \cdots 2^{\lfloor \log q \rfloor} \end{bmatrix}$$

G^{-1} : bit-decomp.

$$G^{-1}\begin{bmatrix} v_1 \\ v_2 \end{bmatrix}_{n \times 1} \longrightarrow \begin{bmatrix} v_1 \bmod 2 \\ v_1 \bmod 4 \bmod 2 \\ \vdots \\ v_1 \bmod 2^{\lfloor \log q \rfloor} \\ v_2 \bmod 2 \\ \vdots \end{bmatrix}_{n \lfloor \log q \rfloor \times 1}$$

To Decrypt:

$sk = t = [-s^T \quad 1]$

$$tC = \underbrace{t \cdot pk \cdot R}_{\approx 0} + \mu t G$$

$\mu \, t \, G$

$\hookrightarrow \underbrace{\begin{bmatrix} -s_1 & \dots & -s_n & 1 \end{bmatrix}}_{1 \times (n+1)} \begin{bmatrix} 1 & 2 & 4 & \dots & 2^{\log q} \\ & & & & \\ & & & & \end{bmatrix}$

$(n+1) \times (n+1)\log q$

$= \mu \begin{bmatrix} -s_1 & -2s_1 & \dots & -2^{\log q} s_1 & -s_2 & -2s_2 & \dots \\ & & & & 1 & 2 & 4 \dots 2^{\log q} \end{bmatrix}$

$+$ errors

What if $Enc(\mu) \rightarrow BR + \mu \left(I \otimes \left[\frac{q}{2} \dots \frac{q}{2}\right]\right)$

Enc, Dec, Addition would all work fine

CPA - security ✓

Multiplication

FHE.

Invariant

C^* encrypting μ^*.

$tC^* \approx \mu^* tG + \text{errors}$.

$Enc \rightarrow BR + \mu G$

Also, $tB \rightarrow$ small errors, close to 0

$t(BR + \mu G) \approx \mu t G$

ADDITION

$+$.

$C_1 \quad + \quad C_2$

$C_+ = BR_1 + \mu_1 G \quad + \quad BR_2 + \mu_2 G$

$= B(R_1 + R_2) + (\mu_1 + \mu_2) G$

$t\,C_+ = \underbrace{t\,B\,(R_1 + R_2)}_{\text{small errors}} + (\mu_1 + \mu_2)\,tG$

MULTIPLICATION

$C_* = C_1 \cdot G^{-1}(C_2)$

$tC_* = t\,C_1\,G^{-1}(C_2)$

$= t\,(BR_1 + \mu_1 G) \cdot G^{-1}(C_2)$

$= (\text{errors} + \mu_1\,tG) \cdot G^{-1}(BR_2 + \mu_2 G)$

$$= (\text{errors} + \mu_1 t G) \cdot G^{-1}(BR_2 + \mu_2 G)$$

BECAUSE $G^{-1}(\ )$ has small entries!

$$\approx \text{errors}' + \mu_1 t G G^{-1}(BR_2 + \mu_2 G).$$

$$= \text{errors}' + \mu_1 t (BR_2 + \mu_2 G)$$

$$= \text{errors}' + \mu_1 t BR_2 + \mu_1 \mu_2 t G$$

$$= \text{errors}' + (\text{small errors}) + \mu_1 \mu_2 t G$$

$$\approx \mu_1 \mu_2 t G.$$

Errors w.h.p. must be $< \frac{q}{4m^2 k}$