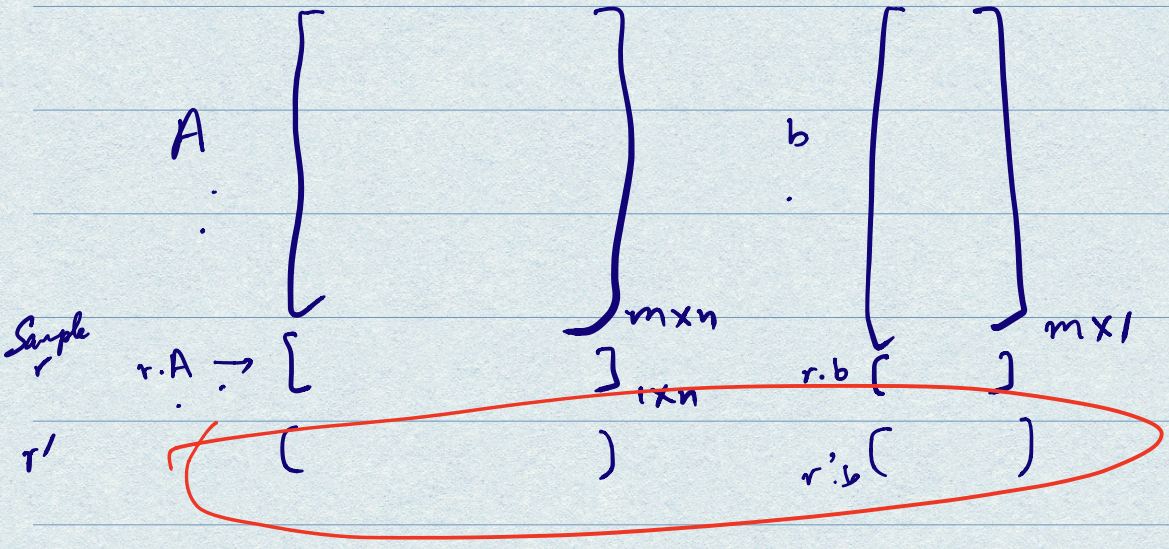
TOWARDS HOMOMORPHIC ENCRYPTION.

REGEV

$$KG \rightarrow \underbrace{\left(A \;,\; \underbrace{As+e}_{b}\right)}_{pk} \qquad \underbrace{s}_{sk}$$

$$Enc(pk, \mu; r) \rightarrow \underbrace{rA}_{rAs},\; r\left(\overbrace{b}^{Ase}\right) + \mu\left\lfloor \frac{q}{2} \right\rfloor$$



$$Dec(ct, s) \rightarrow c_2 - c_1 \cdot s$$

$ct = c_1, c_2$

$= \text{"erroneous"}\ \mu\left\lfloor \frac{q}{2} \right\rfloor$

$$ct_1 = Enc(pk, \mu_1; r_1) = \underbrace{r_1}_{1\times m} \overbrace{A}^{m\times n}, \overbrace{\left(r_1 b + \mu_1 \left\lfloor \frac{q}{2} \right\rfloor\right)}^{m\times 1}$$

$$ct_2 = Enc(pk, \mu_2; r_2) = r_2 A, \left(r_2 b + \mu_2 \left\lfloor \frac{q}{2} \right\rfloor\right)$$

$-r_2 As + r_2 As + r_2 e$

What is $ct_1 + ct_2 \pmod q$?

$$(r_1 + r_2)A, \underbrace{(r_1 + r_2)}_{\in\{0,1,2\}} b + (\mu_1 + \mu_2)\left\lfloor \frac{q}{2} \right\rfloor$$

s

$r_1 + r_2 + r_3 \ldots\ldots$

$\in \{0, 1, 2, 3\}$

what if we computed $ct_1 * ct_2$?

$$r_1 r_2 A^2, \quad r_1 r_2 b^2 + r_1 \mu_2 b \left\lfloor \frac{q}{2} \right\rfloor + r_2 \mu_1 b \left\lfloor \frac{q}{2} \right\rfloor$$

$$r_1 r_2 (As + e)^2 + \mu_1 \mu_2 \left(\left\lfloor \frac{q}{2} \right\rfloor\right)^2$$

$r_1 r_2 Ae$

BIT-DECOMPOSITION / "GADGET" TRICK

"Gadget" Matrix.

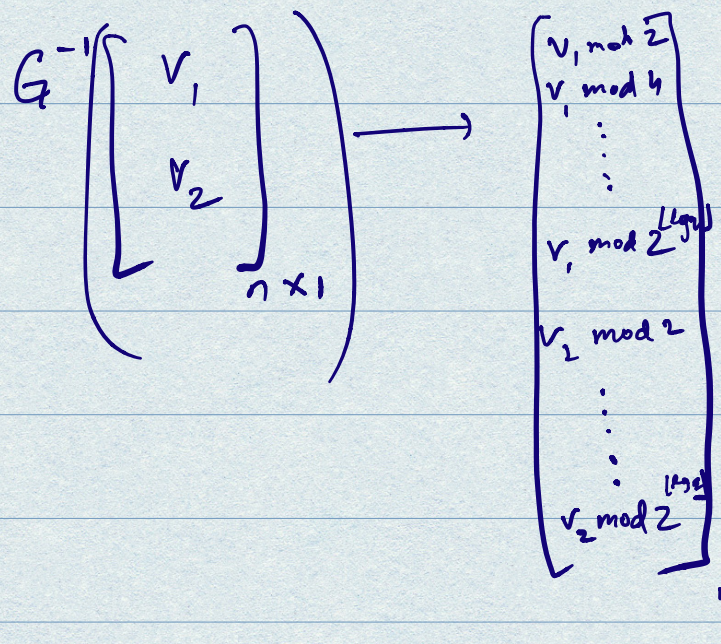
Powers-of-2-matrix.

$G = n \times (n \log q)$ matrix

$$\begin{bmatrix} 1 & 2 & 4 & \dots & 2^{\lfloor \log q \rfloor} & 0 & \dots & 0 \\ & & & & & 1 & 2 & 4 & \dots & 2^{\lfloor \log q \rfloor} & 0 & \dots \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & & \\ & & & & & & & & & & 1 & 2 & 4 & \dots & 2^{\lfloor \log q \rfloor} \end{bmatrix}$$

$n \times n \log q$

G^{-1} is the inverse "bit decomposition" operation.



(FLIPPED) LWE

Like LWE, but (A has 0/1 entries.)

$s \leftarrow \mathbb{Z}_q^n$, $e \leftarrow \chi_B^m$ (as before)

Hardness of LWE $\Rightarrow$ Hardness of Flipped LWE

"HERMITE NORMAL-FORM" LWE: Like LWE, but s is $A \leftarrow \mathbb{Z}_q^{m \times n}$, ($s \leftarrow \{0,1\}^n$), $e \leftarrow \chi_B^m$ also. "Short"

To PROVE:

dLWE is hard $\Rightarrow$ FLWE is hard.

$\Downarrow$

If FLWE can be solved, then so can dLWE.

Given dLWE sample:

A , b.

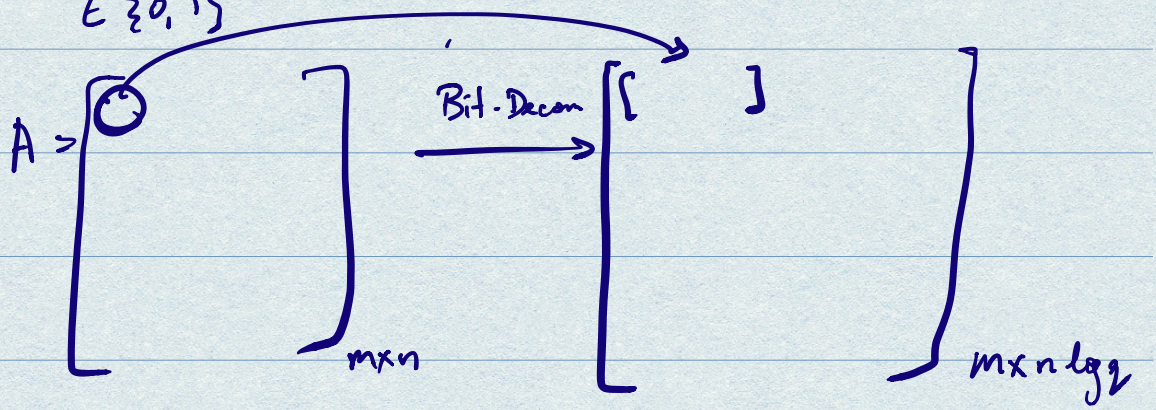
$\downarrow$

$\in \mathbb{Z}_q^{m \times n}$

convert to

$A' = \text{Bit-Decomp}(A)$.

$\in \{0,1\}^{m' \times n'}$



Attempt 1. $b' = b$.

$$b_{m\times 1} = A_{m\times n}\, s_{n\times 1} + e_{m\times 1}$$

$$\stackrel{?}{=} A' s' + e'$$

(A', b) for $b = A's' + e'$, $s' \in \mathbb{Z}_q^{n\log q \times r}$ is NOT a FLWE sample!

(Wrong distribution, see below)

Q1. Is $As \stackrel{?}{=} A's'$ for some s'

$a_1 s_1 + a_2 s_2 + \cdots a_n s_n$

where $A' = \text{Bit-Decomp}(A)$.

Yes, for $s' = \begin{bmatrix} s_1 \\ 2s_1 \\ 4s_1 \\ \vdots \\ 2^{\lfloor \log q \rfloor} s_1 \\ s_2 \\ 2s_2 \\ \vdots \\ s_n \end{bmatrix}$

$b' = b$ (is not good, because (A', b') is not FLWE)

$= \underbrace{b}_{= A's'} + A'\hat{s}$ where $\hat{s} \xleftarrow{\$} \mathbb{Z}_q^{n \log q \times 1}$

Is (A', b') a FLWE sample?

1. Is $b' = A's'' + e'$ for some s''?

Yes, for $s'' = (\hat{s} + s') \bmod q$.

How is s'' distributed?

Because entries of $\vec{s}$ are uniform mod q, so are entries of s''.

BACK TO MULTIPLICATION.

A DIFFERENT VARIANT OF REGEV.

(Gentry, Sahai and Waters).

Leveled Fully-Homomorphic Encryption

Set $m = (n+1)\log q$

KeyGen $\rightarrow$ $A_{m \times n}$, $b = As + e$

output $pk = B = [A \| b]_{m \times (n+1)}$

$sk = t = \begin{bmatrix} -s \\ 1 \end{bmatrix}_{(n+1) \times 1}$

Enc $(pk, \mu ; r) \rightarrow$

Sample R as a matrix with random 0/1 entries.

$R \xleftarrow{\$} \{0,1\}^{m \times m}$.

Output $(RB) + \mu G^T$ $\hookrightarrow (n+1)\log q \times (n+1)$

$m \times (n+1)$

$$\text{Dec}(t, c) = \underset{\downarrow}{Ct}$$

$$= RB \begin{bmatrix} -s \\ 1 \end{bmatrix} + \mu G^T t \qquad (t \downarrow)$$

We showed: $Bt = e$

$$= R \left[A \,\|\, b \right] \begin{bmatrix} -s \\ 1 \end{bmatrix} + \mu G^T t$$

$$= R \underbrace{(-As + b)}_{= e} + \mu G^T t$$

$$= \underline{(R \cdot e)} + \boxed{\mu G^T t}$$

If $\mu = 0$, Ct is low norm

If $\mu = 1$, w.h.p. Ct is NOT low norm

To decrypt, compute Ct and check if its close to 0 or close to $G^T t$.

$$C_1 = R_1 B + \mu_1 G^T$$

$$C_2 = R_2 B + \mu_2 G^T$$

$$\hat{C} = C_1 * C_2 = R_1 R_2 B^2 + R_1 \mu_2 G^T + R_2 \mu_1 G^T + \mu_1 \mu_2 (G^T)^2$$

BAD!

What is $\hat{C} \cdot t$?

$R_1 R_2 B^2 t$

$\downarrow$

$= R_1 R_2 \overset{\downarrow}{B} e$

$\uparrow$

this is bad.

INSTEAD,

$$\hat{C} = C_1 * G^{-1}(C_2).$$