FULLY HOMOMORPHIC ENCRYPTION
(FOR CLASSICAL / QUANTUM CIRCUITS)

RECAP : PUBLIC KEY ENCRYPTION

$\text{KeyGen}(1^\lambda)$: $PK = B = \underset{m\times(n+1)}{\left[\begin{array}{c|c} A & b \end{array}\right]}$ (A: $m\times n$, b: $m\times 1$)

where $A \leftarrow \mathbb{Z}_q^{m\times n}$, $b = As + e$, for $s \leftarrow \mathbb{Z}_q^{n\times 1}$, $e \leftarrow \chi^{m\times 1}$, $m = (n+1)\log q$

$SK = \left[\begin{array}{c} t \\ \hline \end{array}\right] = \begin{bmatrix} -s \\ \hline 1 \end{bmatrix}$ (t: $(n+1)\times 1$; $-s$: $n\times 1$; 1: 1×1)

Note: $Bt = -As + b = e$.

$\text{Enc}(\underset{=B}{PK}, \mu)$: Sample $\left[\longleftarrow r \longrightarrow\right]_{1\times m} \leftarrow \{0,1\}^m$

$= \left[\longleftarrow rA \longrightarrow\right]\left[rb + \mu\left\lfloor\frac{q}{2}\right\rfloor\right]_{1\times 1}$ (r: $1\times m$, A: $m\times n$)

Output $c_{1\times(n+1)} = [r.B]_{1\times(n+1)} + \left[0 \cdots \mu\left\lfloor\frac{q}{2}\right\rfloor\right]_{1\times(n+1)}$

$\text{Dec}(\underset{=t}{SK}, c)$: Compute $c.t$

$rb + \mu\left\lfloor\frac{q}{2}\right\rfloor - rAs = re + \mu\left\lfloor\frac{q}{2}\right\rfloor$

$c.t = rBt + \left[0 \cdots \mu\left\lfloor\frac{q}{2}\right\rfloor\right]\begin{bmatrix} * \\ 1 \end{bmatrix} = rBt + \mu\left\lfloor\frac{q}{2}\right\rfloor = re + \mu\left\lfloor\frac{q}{2}\right\rfloor$

Output 0 if $-\frac{q}{4} < c.t < \frac{q}{4}$

1 if $\frac{q}{4} < c.t < \frac{3q}{4}$

0 $\quad$ 1

$$c_1 = r_1 B + \left[0 \ldots \mu_1 \left\lfloor \frac{q}{2} \right\rfloor\right]$$

$$c_2 = r_2 B + \left[0 \ldots \mu_2 \left\lfloor \frac{q}{2} \right\rfloor\right]$$

To XOR plaintexts

$$(c_1 + c_2) = (r_1 + r_2) B + \left[0 \ldots (\mu_1 + \mu_2) \left\lfloor \frac{q}{2} \right\rfloor\right]$$

$$= (r_1 + r_2) B + \left[0 \ldots (\mu_1 \oplus \mu_2) \left\lfloor \frac{q}{2} \right\rfloor\right]$$

$(r_1 + r_2) \in \{0,1,2\}^m$

$$\text{Enc}(\mu_1 \oplus \mu_2) = r' B + \left[0 \ldots (\mu_1 \oplus \mu_2) \left\lfloor \frac{q}{2} \right\rfloor\right]$$

$r' \in \{0,1\}^m$

AND.

$c_1 \in \mathbb{Z}_q^{1 \times n+1}$

$c_2 \in \mathbb{Z}_q^{1 \times (n+1)}$

$c_1^T c_2 \rightarrow$ scalar

(ciphertexts must be vectors!).

$$c_1 = \left(r_1 B + \left[0 \ldots \mu_1 \left\lfloor \frac{q}{2} \right\rfloor\right]\right)$$

$$c_2 = \left(r_2 B + \left[0 \ldots \mu_2 \left\lfloor \frac{q}{2} \right\rfloor\right]\right)$$

$$c_1^T c_2 t = \left((r_1 B)^T r_2 B\right) t + \left((r_1 B)^T \left[0 \ldots \mu_2 \left\lfloor \frac{q}{2} \right\rfloor\right]\right)^t + \left(r_2 B \left[0 \ldots \mu_1 \left\lfloor \frac{q}{2} \right\rfloor\right]\right)^t + \left(\mu_1 \mu_2 \left\lfloor \frac{q}{2} \right\rfloor^2\right) t$$

$= B^T r_1^T r_2 e$

Want: $\approx$ small error $+ \mu_1 \mu_2 \left\lfloor \frac{q}{2} \right\rfloor$

"Bit-decomposition" operation. G^{-1}

For scalar $s \in \mathbb{Z}_q$, $\xrightarrow{G^{-1}}$ write s as bitstring $s_1 s_2 \ldots s_{\log q}$

$v \in \mathbb{Z}_q^{1 \times n} = [v_1 \; v_2 \ldots v_n)$ $\xrightarrow{G^{-1}}$ $\left[\leftarrow v_1 \text{ as bitstring} \rightarrow \; \left(v_1 \bmod 2\right) \left(v_1 \bmod 4\right) \ldots \left(v_1 \bmod 2^{\lfloor \log q \rfloor}\right) \; \leftarrow v_2 \rightarrow \; \ldots \right]$ $1 \times (n \log q)$

$$A = \begin{bmatrix} \leftarrow v \rightarrow \\ \leftarrow w \rightarrow \\ \leftarrow x \rightarrow \\ \vdots \end{bmatrix}_{m \times n} \xrightarrow{G^{-1}} \begin{bmatrix} \text{bit-decomp}(v) \\ \text{bit-decomp}(w) \\ \vdots \end{bmatrix}_{m \times n \log q}$$

$$\left[(s_1 \bmod 2) \; (s_1 \bmod 4) \ldots \right] \begin{bmatrix} 1 \\ 2 \\ 4 \\ \vdots \\ 2^{\lfloor \log q \rfloor - 1} \end{bmatrix} \rightarrow s$$

$$v = \left[\leftarrow BD(v_1) \rightarrow \; \leftarrow BD(v_2) \rightarrow \; \leftarrow BD(v_3) \rightarrow \right] \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 2 & 0 \\ \vdots & 4 & \vdots \\ 2^{\lfloor \log q \rfloor - 1} & \vdots & 1 \\ | & | & 2 \\ 0 & | & 4 \\ | & | & \vdots \end{bmatrix}_{n \times q \times n} = v$$

$BD(v)$. $G \rightarrow$ (denote by vG^{-1})

$\forall$ vectors v, $vG^{-1}G = v$

FULLY HOMOMORPHIC ENCRYPTION
(FOR CLASSICAL / QUANTUM CIRCUITS)

RECAP : PUBLIC KEY ENCRYPTION

KeyGen(1^λ): $PK = B = \underset{m\times(n+1)}{\left[\begin{array}{c|c} A & b \end{array}\right]}$ (A: $m\times n$, b: $m\times 1$)

where $A \leftarrow \mathbb{Z}_q^{m\times n}$, $b = As + e$, for $s \leftarrow \mathbb{Z}_q^{n\times 1}$, $e \leftarrow \chi^{m\times 1}$, $m = (n+1)\lg q$

$SK = \left[\begin{array}{c} t \end{array}\right] = \begin{bmatrix} -s \\ 1 \end{bmatrix}$ ($-s$: $n\times 1$, 1: 1×1, t: $(n+1)\times 1$)

Note: $Bt = -As + b = e$.

$\mathrm{Enc}(\underset{=B}{PK}, \mu)$: Sample $\left[\begin{array}{c} R \end{array}\right]_{m\times m} \leftarrow \{0,1\}^{m\times m}$

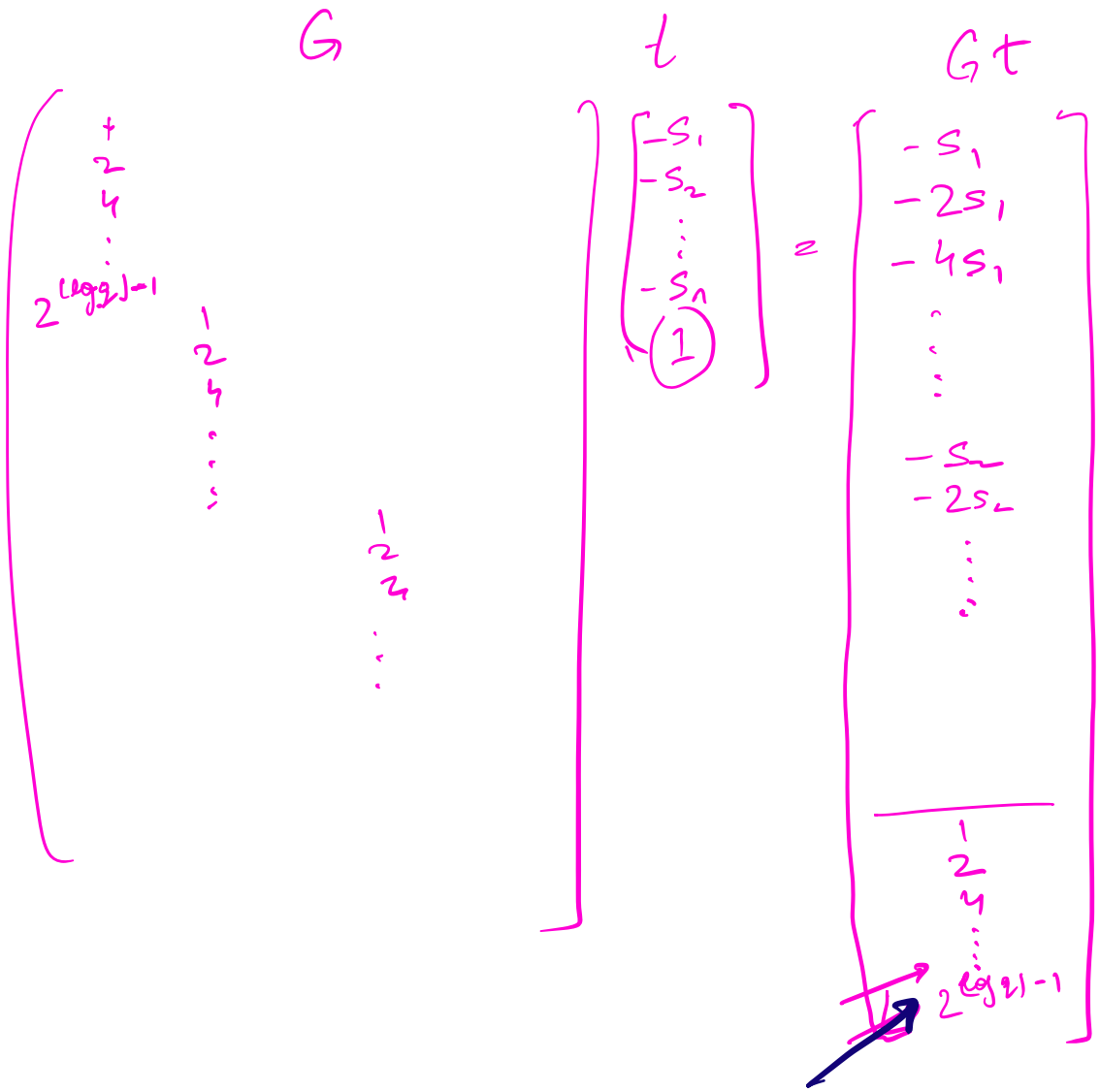
Output $C_{m\times(n+1)} = [RB]_{m\times(n+1)} + \mu G_{(n+1)\lg q \times (n+1)}$ ($= m$)

$\mathrm{Dec}(\underset{=t}{SK}, C)$: Compute $C \cdot t$

$Ct = RBt + \mu Gt$ $\left[\begin{array}{c} \not{s} \\ 1 \end{array}\right] = RBt + \mu Gt = Re + \mu Gt$.

Output 0 if $-\frac{q}{4} < c\cdot t < \frac{q}{4}$

1 if $\frac{q}{4} < c\cdot t < \frac{3q}{4}$


G
t
Gt
1
2
4
$2^{\lfloor \log_2 n \rfloor - 1}$
$-s_1$
$-s_2$
$-s_n$
1
$-s_1$
$-2s_1$
$-4s_1$
$-s_n$
$-2s_n$
$2^{\lfloor \log_2 n \rfloor - 1}$

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

$$C_1^{(m \times (n+1))} = R_1 B + \mu_1 G$$

$$C_2^{(m \times (n+1))} = R_2 B + \mu_2 G$$

$C_1 G^{-1}$ has dimension $m \times (n+1)\log q = m \times m$.

To multiply, $C^* = (C_1 G^{-1})\, C_2$

Decrypting C^* gives:

$$C^* t = (C_1 G^{-1}) C_2 t = (C_1 G^{-1})(R_2 e + \mu_2 G t)$$

$$= C_1 G^{-1} R_2 e + C_1 G^{-1} \mu_2 G t$$

$$= C_1 G^{-1} R_2 e + \mu_2 C_1 G^{-1} G t$$

$$= (C_1 G^{-1}) R_2 e + \mu_2 C_1 t$$

$$= (C_1 G^{-1}) R_2 e + \mu_2 (R_1 e + \mu_1 G t)$$

$$= \underbrace{(C_1 G^{-1}) R_2 e}_{\text{low norm}} + \mu_2 \mu_1 G t + \underbrace{\mu_2 R_1 e}_{\text{low norm}}$$

$$= \mu_1 \mu_2 G t + (\text{low norm})$$