LECTURE 8

HOMOMORPHIC ENCRYPTION (CONTD.)

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

KeyGen$(1^n) \longrightarrow \underline{A}_{n \times m}$, $\underline{b} = As + e$

output pk $\longrightarrow B$ $\quad \left[\frac{A}{b}\right]_{(n+1)\times m}$

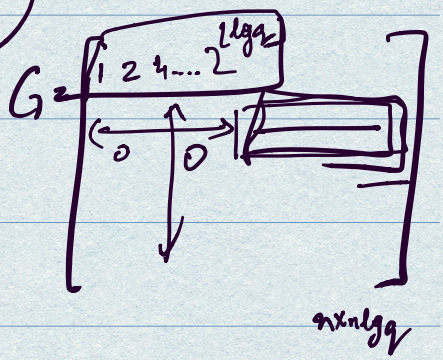
sk $\longrightarrow \underline{t} = [-s \,||\, 1]_{1\times(n+1)}$.

Invariant: $tB = e$.

$\text{Enc}(B, \mu; r) \longrightarrow$

$$\left(\quad BR + \mu G \quad \right)$$

$R \in \{0,1\}^{m\times m}$ where

$G =$ 

$$\mathrm{Dec}\left(t, \begin{bmatrix} -s \\ 1 \end{bmatrix} C\right) = tC = t_B R = eR.$$

if $\mu = 0$, tC has low norm

if $\mu = 1$, $tC - tG^T$ has low norm.

$t \cdot C = \underbrace{\langle \text{low norm term} \rangle}_{eR} + \mu t G^T$

ADDITION.

Suppose we have $C_1 = \mathrm{Enc}(\mu_1) = R_1 B + \mu_1 G^T$

$C_2 = \mathrm{Enc}(\mu_2) = R_2 B + \mu_2 G^T$

Then $C_1 + C_2 = (R_1 + R_2) B + (\mu_1 + \mu_2) G^T$

$t(C_1 + C_2) = (\text{some low norm}) + (\mu_1 + \mu_2) t G^T$

MULTIPLICATION

$$C_1 \circledast C_2 \longrightarrow \hat{C}$$

$$\text{s.t. } \hat{C} = Enc(\mu_1 \mu_2)$$

Define $C_1 \circledast C_2$ as

$$C_1^T \cdot G^{-1}(C_2)$$

$$\dim(C) = m \times (n+1) \cdot (k+1)\log q \times (n+1)$$

$$\dim(G^{-1}(C)) \Rightarrow (k+1)\log q \times (k+1)\log q$$

$C_1^T G^{-1}(C_2)$ is an $(n+1) \times (m)$ matrix

Let's compute :

$$C_{mult}$$

$$= C_1 G^{-1}(C_2)\, G^{-1}(R_2 B) + \mu_2 I$$

switch RB to BR

$$(R_1 B + \mu_1 G) \cdot G^{-1} (R_2 B + \mu_2 G) \cdot$$

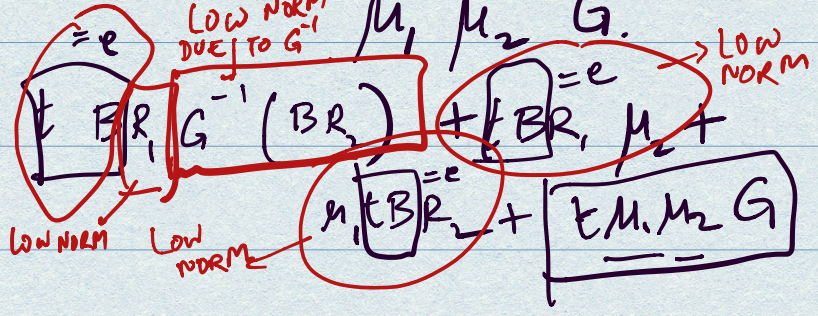
$$= R_1 B G^{-1}(R_2 B) + R_1 B \mu_2 G^{-1} G$$

$$+ \mu_1 G G^{-1} R_2 B + \mu_1 \mu_2 G G^{-1} G$$

$$\sim R_1 B G^{-1}(R_2 B) + R_1 B \mu_2 + \mu_1 R_2 B + \mu_1 \mu_2 G.$$

Left-Multiply by t.

$$t C_{mult} \sim$$



$$tBR_1 G^{-1}(BR_2) + tBR_1 \mu_2 + \mu_1 tBR_2 + t\mu_1\mu_2 G$$

We just discussed

Leveled FHE.

Can we do "unleveled" FHE?

BIG OPEN PROBLEM:

Unleveled FHE from LWE

But we know how to do

Unleveled FHE from circular LWE.

NAIVE SOLUTION: Given "noisy" ct.

Given sk, compute $m = Dec_{sk}(ct)$

"G" and output $\widehat{ct} = Enc_{pk}(C(m))$

BOOTSTRAPPING

Given sk

$ct = Enc_{pk}(sk)$

$Dec_{sk}(ct)$

$ct' = Enc_{pk}(m)$

but with low noise!

Conjecture :

GSW is "Semantically CPA" secure

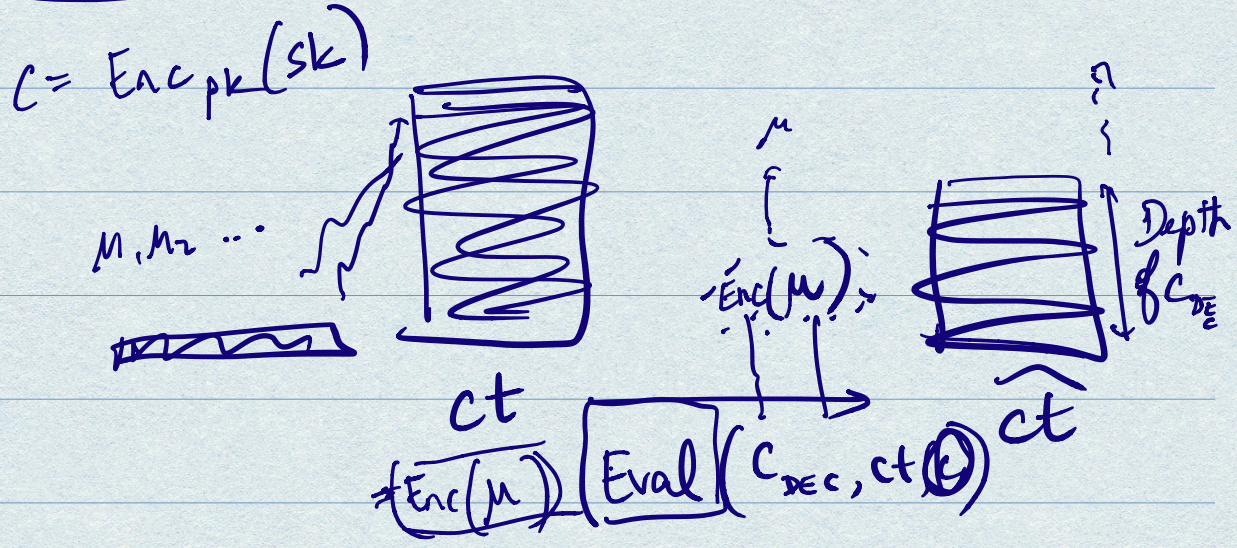
even if pk is modified to

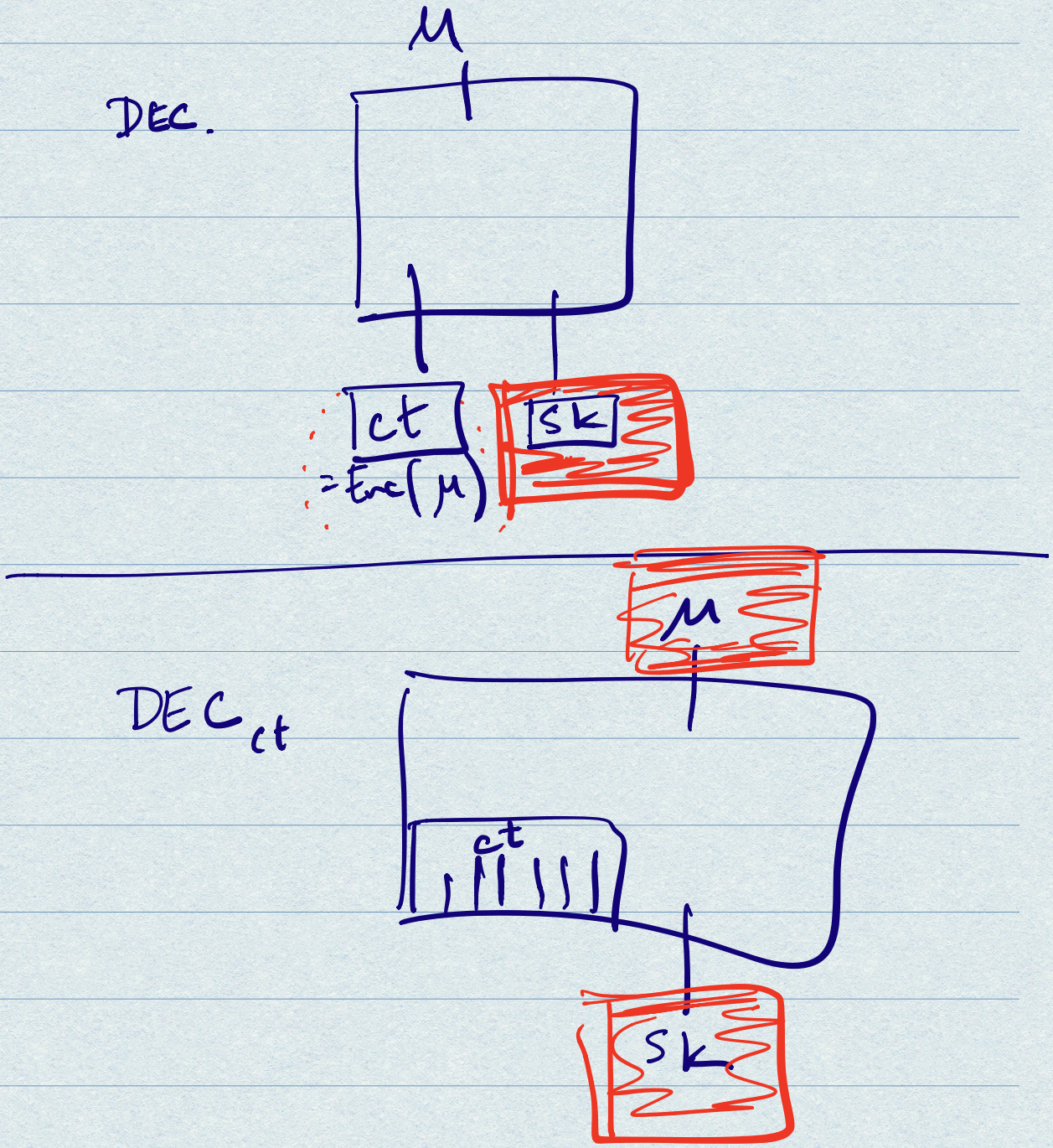
$(pk, Enc_{pk}(sk))$.

LWE + other assumptions

⇓

Unleveled FHE.





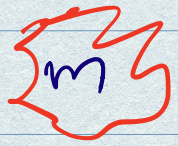
Hom-Eval $_{Dec_{ct}}\left(Enc_{pk}(sk)\right) = Enc(\mu)$

(pk_1, sk_1) ~ NOT HOMOMORPHIC

(pk_2, sk_2) ~ IS HOMOMORPHIC

$ct = Enc_{pk_1}(m)$

$ct_2 = Enc_{pk_2}(sk_1)$



$Eval_{Dec_{ct}}(ct_2)$

$ct_3 = Enc_{pk_2}(m)$.