CSCI 1515 Applied Cryptography

This Lecture:

- SWHE from LWE (GSW, Continued)
- SWHE from RLWE (BFV)
- Private Information Retrieval (PIR)

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers
- from LWE (GSW)
- from RLWE (BFV)

Step 2: Bootstrapping

Learning With Errors (LWE) Assumption

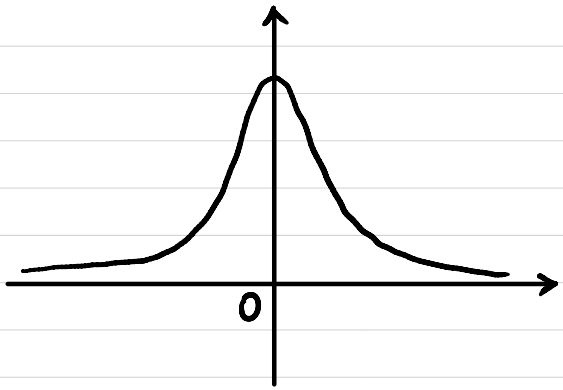
$n \sim$ security parameter

$q \sim 2^{n^\epsilon}$

$m = \Theta(n \log q)$

χ: distribution over $\mathbb{Z}_q$

(concentrated on "small integers")

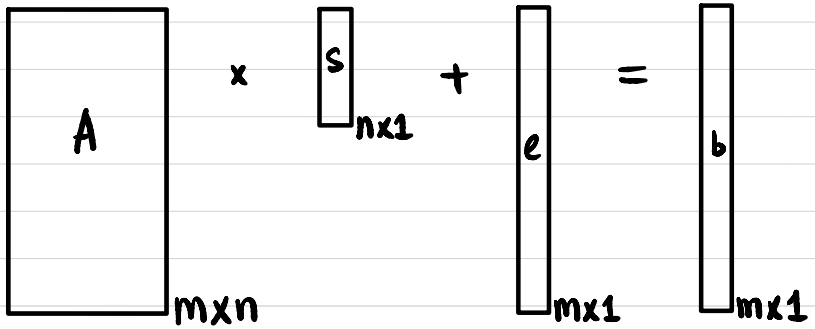


$$\Pr[|e| > \alpha \cdot q \mid e \leftarrow \chi] \leq \text{negl}(n)$$

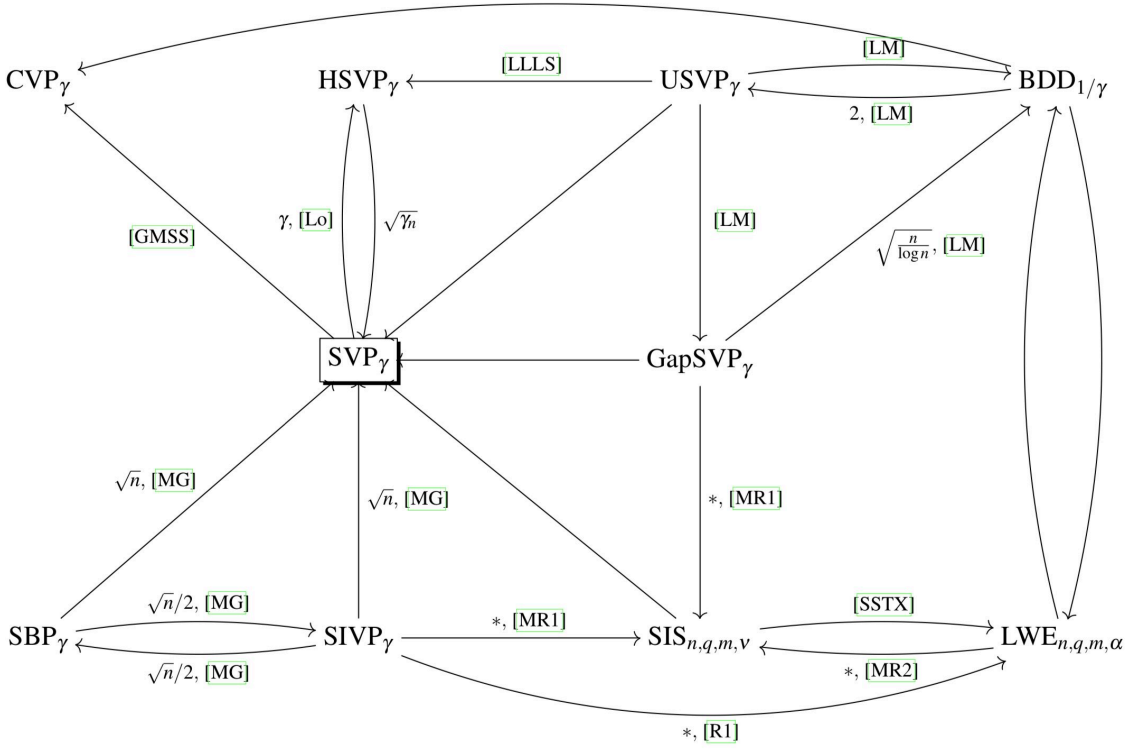
$\alpha \ll 1$

LWE$[n, m, q, \chi]$:

$A \xleftarrow{\$} \mathbb{Z}_q^{m \times n} \quad s \xleftarrow{\$} \mathbb{Z}_q^{n} \quad e \leftarrow \chi^m$



$$(A,\ b = As + e) \overset{c}{\approx} (A,\ b' \xleftarrow{\$} \mathbb{Z}_q^m)$$

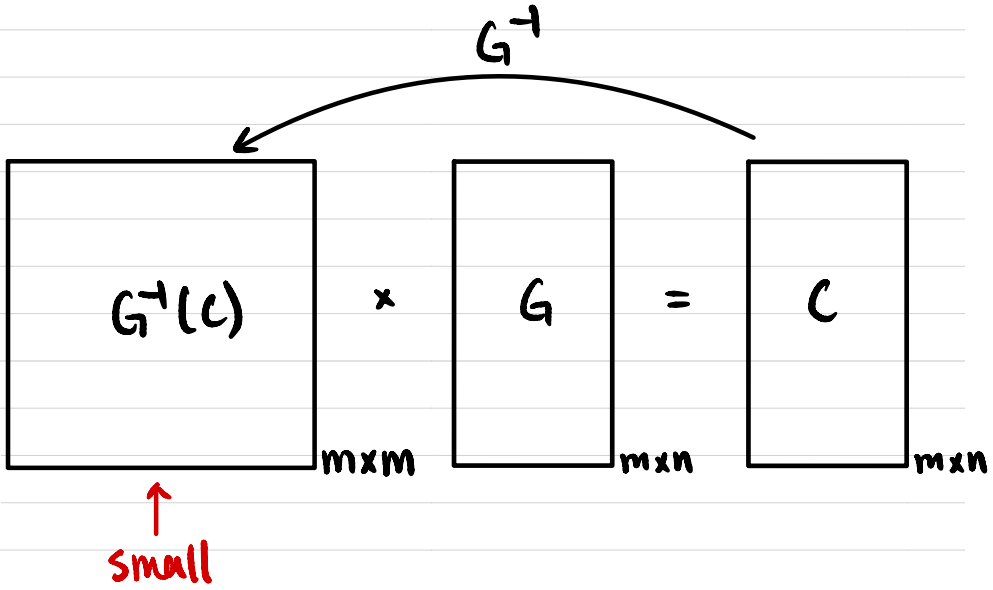

CVP_γ
HSVP_γ
[LLLS]
USVP_γ
[LM]
$\mathrm{BDD}_{1/\gamma}$
2, [LM]
[GMSS]
γ, [Lo]
$\sqrt{\gamma_n}$
[LM]
$\sqrt{\frac{n}{\log n}}$, [LM]
SVP_γ
GapSVP_γ
$\sqrt{n}$, [MG]
$\sqrt{n}$, [MG]
$*$, [MR1]
$\sqrt{n}/2$, [MG]
SBP_γ
SIVP_γ
$*$, [MR1]
$\mathrm{SIS}_{n,q,m,\nu}$
[SSTX]
$\mathrm{LWE}_{n,q,m,\alpha}$
$\sqrt{n}/2$, [MG]
$*$, [MR2]
$*$, [R1]

SWHE from LWE (GSW)

Attempt 2 (secret-key)

Flattering Gadget:

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

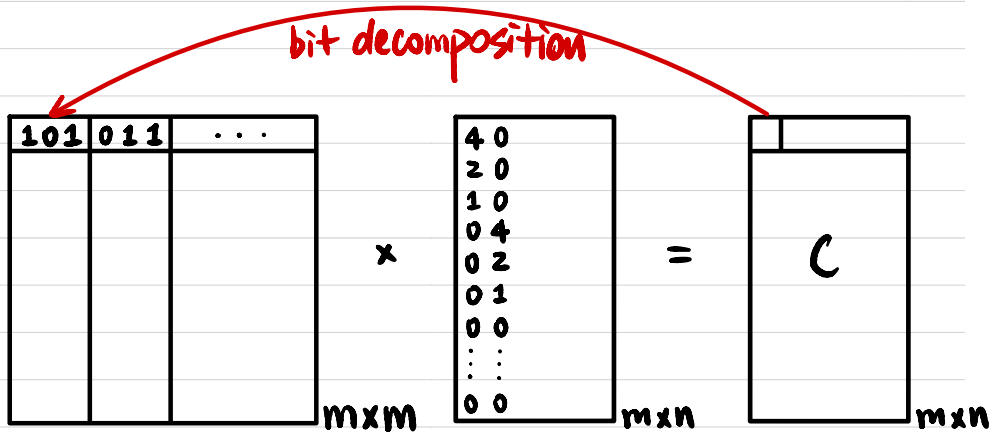


Inverse transformation

$$G^{-1}: \mathbb{Z}_q^{m \times n} \to \mathbb{Z}_q^{m \times m}$$

$\forall C \in \mathbb{Z}_q^{m \times n}$, $G^{-1}(C) = \text{small}$

$G^{-1}(C) \cdot G = C$



$m = n \cdot \log q$

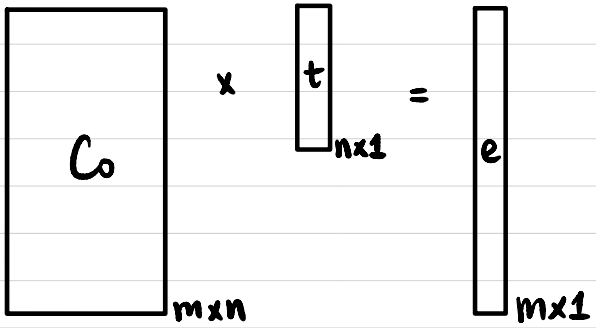
SWHE from LWE (GSW)

Attempt 2 (secret-key)

$$sk = t_{n\times 1} \begin{bmatrix} s \\ 1 \end{bmatrix}_{n\times 1}$$

$Enc_{sk}(\mu)$: $\mu \in \{0,1\}$

Sample $C_0 \in \mathbb{Z}_q^{m\times n}$ s.t. $C_0 \cdot \vec{t} = \text{small}$



$$C = C_0 + \mu \cdot G$$

↑ gadget matrix

$Dec_{sk}(C)$:

$$C\cdot\vec{t} = (C_0 + \mu\cdot G)\cdot\vec{t}$$
$$= \vec{e} + \mu\cdot(G\cdot\vec{t})$$

Homomorphism:

$$C_1\cdot\vec{t} = \mu_1\cdot(G\cdot\vec{t}) + \vec{e}_1$$
$$C_2\cdot\vec{t} = \mu_2\cdot(G\cdot\vec{t}) + \vec{e}_2$$

Additive Homomorphism?

$$C = C_1 + C_2 \Rightarrow C\cdot\vec{t} = (\mu_1+\mu_2)\cdot(G\cdot\vec{t}) + (\vec{e}_1+\vec{e}_2)$$

Multiplicative Homomorphism?

$$C = G^{-1}(C_1)\cdot C_2$$
$$C\cdot\vec{t} = G^{-1}(C_1)\cdot C_2\cdot\vec{t}$$
$$= G^{-1}(C_1)\cdot(\mu_2\cdot(G\cdot\vec{t}) + \vec{e}_2)$$
$$= \mu_2\cdot G^{-1}(C_1)\cdot G\cdot\vec{t} + G^{-1}(C_1)\cdot\vec{e}_2$$
$$= \mu_2\cdot C_1\cdot\vec{t} + G^{-1}(C_1)\cdot\vec{e}_2$$
$$= \mu_2\cdot(\mu_1\cdot(G\cdot\vec{t}) + \vec{e}_1) + G^{-1}(C_1)\cdot\vec{e}_2$$
$$= \mu_2\cdot\mu_1\cdot(G\cdot\vec{t}) + \mu_2\cdot\vec{e}_1 + G^{-1}(C_1)\cdot\vec{e}_2$$

How homomorphic is it?

$\#\text{MULT} \sim \lg_m q$

Ring LWE (RLWE) Assumption

Polynomial ring $R = \mathbb{Z}[x]/(x^m+1)$ ($m = 2^k$)

↑ polynomials with integer coefficients modulo (x^m+1)

$R_q = \mathbb{Z}_q[x]/(x^m+1)$

↑ polynomials with integer coefficients modulo q and (x^m+1)

χ : "noise" distribution over R

$a \xleftarrow{\$} R_q \qquad s \xleftarrow{\$} R_q \text{ (or } s \leftarrow \chi) \qquad e \leftarrow \chi$

$$(a,\ [a \cdot s + e]_q) \overset{c}{\simeq} (a,\ b \xleftarrow{\$} R_q)$$

Def A ring is a set R with two binary operations $+, \cdot$ satisfying:

① R is an abelian group under "$+$":
- $\forall a,b \in R,\ a+b \in R$
- $\forall a,b,c \in R,\ (a+b)+c = a+(b+c)$
- $\forall a,b \in R,\ a+b = b+a$
- $\exists 0 \in R$ s.t. $\forall a \in R,\ a+0 = a$
- $\forall a \in R,\ \exists -a \in R$ s.t. $a+(-a) = 0$.

② R is a monoid under "$\cdot$":
- $\forall a,b \in R,\ a \cdot b \in R$
- $\forall a,b,c \in R,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $\exists 1 \in R$ s.t. $\forall a \in R,\ a \cdot 1 = 1 \cdot a = a$.

③ "$\cdot$" is distributive w.r.t "$+$":
- $\forall a,b,c \in R,\ a \cdot (b+c) = a \cdot b + a \cdot c$
- $\forall a,b,c \in R,\ (a+b) \cdot c = a \cdot c + b \cdot c$

SWHE from RLWE (BFV)

Plaintext space $R_t = \mathbb{Z}_t[x]/(x^k+1)$

Ciphertext space $R_q \times R_q$

$$\Delta := \left\lfloor \frac{q}{t} \right\rfloor \qquad t \ll q$$

$a \xleftarrow{\$} R_q \quad s \leftarrow \chi \quad e \leftarrow \chi$

$$pk = \left([-(a \cdot s + e)]_q, \; a \right)$$

$$sk = s$$

$Enc_{pk}(m)$: $m \in R_t$

Sample $u, e_1, e_2 \leftarrow \chi$

$$c = \left([pk_0 \cdot u + e_1 + \Delta \cdot m]_q, \; [pk_1 \cdot u + e_2]_q \right)$$

$Dec_{sk}(c)$: $[c_0 + c_1 \cdot s]_q$

$$= -(a \cancel{s} + e) \cdot u + e_1 + \Delta \cdot m + (a \cancel{u} + e_2) \cdot s$$

$$= -e \cdot u + e_1 + \Delta \cdot m + e_2 \cdot s$$

$$= [\Delta \cdot m + \text{small}]_q$$

SWHE from RLWE (BFV)

$$[C(s)]_q = c_0 + c_1 \cdot s = \Delta \cdot m + e$$

Homomorphism: $[C^{(1)}(s)]_q = \Delta \cdot m_1 + e_1$

$[C^{(2)}(s)]_q = \Delta \cdot m_2 + e_2$

Additive Homomorphism?

$$[C^{(1)}(s) + C^{(2)}(s)]_q = [\Delta \cdot (m_1 + m_2) + e_1 + e_2]_q$$

Multiplicative Homomorphism?

$$C(s) = C^{(1)}(s) \cdot C^{(2)}(s)$$

$$= \left[(\Delta \cdot m_1 + e_1 + \alpha_1 \cdot q) \cdot (\Delta \cdot m_2 + e_2 + \alpha_2 \cdot q)\right] / \frac{q}{t} \qquad \Delta = \left\lfloor \frac{q}{t} \right\rfloor$$

$$= \Delta^2 \cdot m_1 m_2 + \Delta m_1 e_2 + \Delta m_1 \cdot \alpha_2 q + e_1 \cdot \Delta m_2 + e_1 e_2 + e_1 \alpha_2 q + \alpha_1 q \Delta m_2 + \alpha_1 q e_2 + \alpha_1 \alpha_2 q^2$$

WANT: $\Delta \cdot m_1 m_2 + \text{small}$

SWHE from RLWE (BFV)

$$[C(s)]_q = C_0 + C_1 \cdot s + C_2 \cdot s^2 = \Delta \cdot m + e$$

$$\downarrow$$

$$[C'(s)]_q = C_0' + C_1' \cdot s = \Delta \cdot m + e$$

Relinearization:

Relinearization key: $rlk = \left([-(a \cdot s + e + s^2)]_q,\ a\right)$

$[rlk(s)]_q = -s^2 + \text{small}$

$rlk_i = \left([-(a \cdot s + e + 2^i \cdot s^2)]_q,\ a\right)$

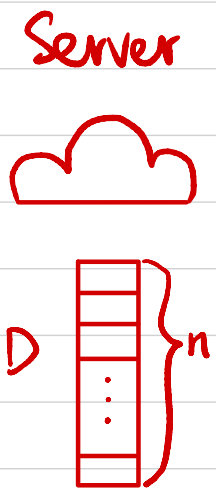
$[rlk_i(s)]_q = -2^i \cdot s^2 + \text{small}$

$$C(s) + C_2 \cdot rlk(s) = C_0 + C_1 \cdot s + \cancel{C_2 s^2} + C^2 \cdot (\cancel{-s^2} + \text{small})$$

$C_2 \cdot rlk(s)$: $\sum rlk_i(s) \cdot C_2[i]$

C^2: large

Private Information Retrieval (PIR)



WANT: D[i]

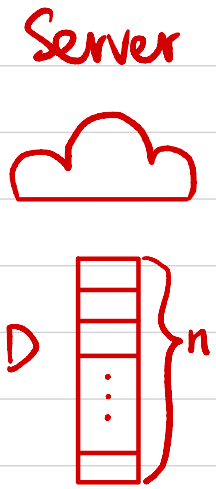
While hiding i against Server

Trivial Solution:

Communication complexity $O(n)$

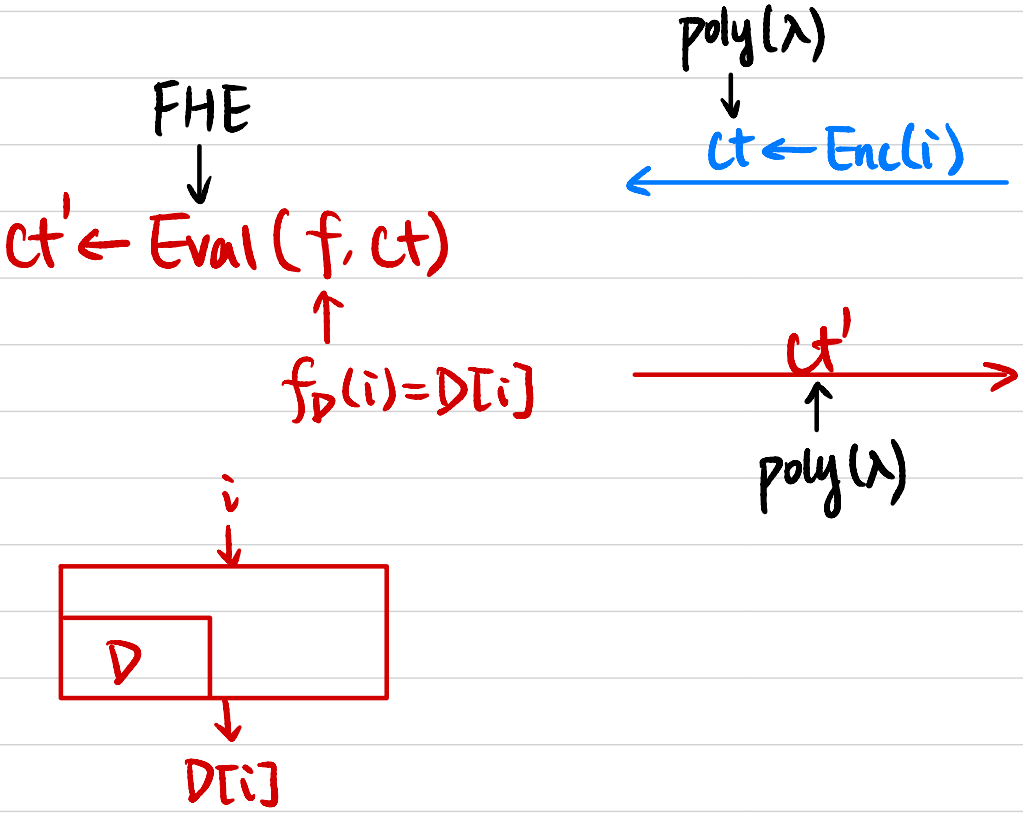
Goal: Communication complexity $o(n)$

Private Information Retrieval (PIR)



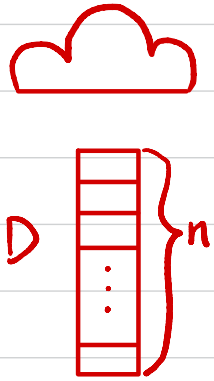
WANT: D[i]

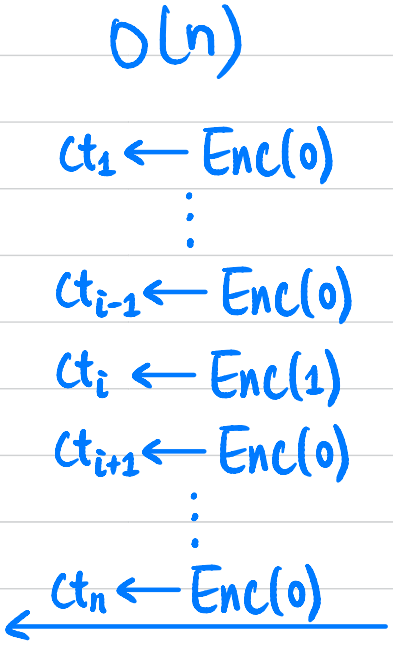
While hiding i against Server



D[i] = Dec(ct')

Private Information Retrieval (PIR)





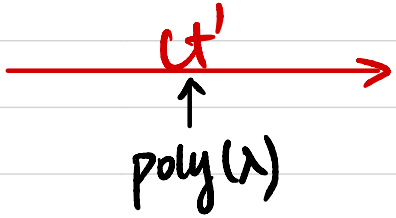
WANT: D[i]

While hiding i against Server

Homomorphic Scalar Mult

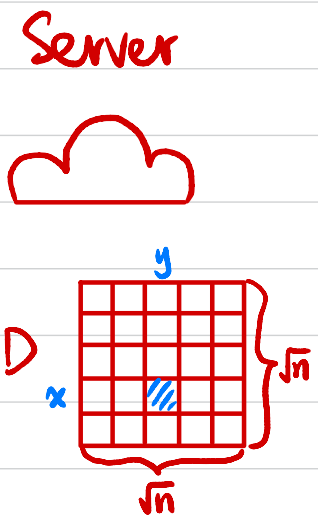
$$ct' \leftarrow \sum_{i=1}^{n} D[i] \cdot ct_i$$

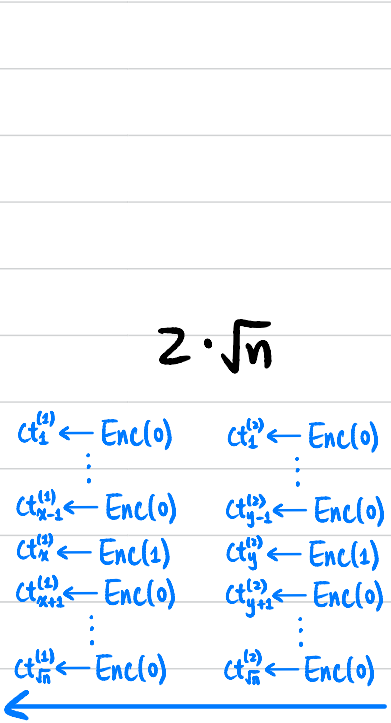
Homomorphic Add

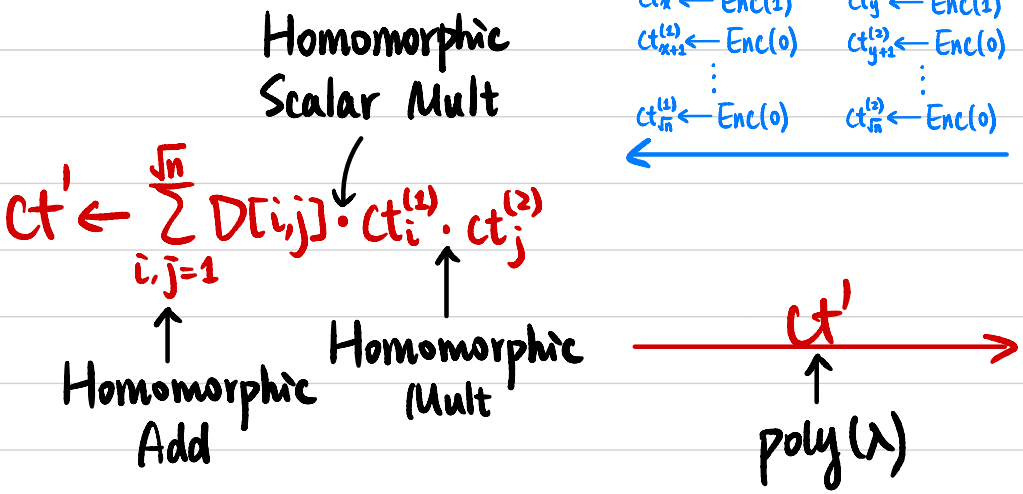


$D[i] = Dec(ct')$

Private Information Retrieval (PIR)







D[x,y] = Dec(ct')

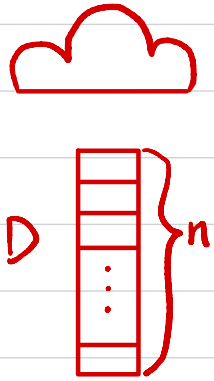
Extend to dimension d ? Communication $d \cdot \sqrt[d]{n}$

Homomorphic Mult = (d-1)·n

Homomorphic Scalar Mult = n

Homomorphic Add = n

PIR from GSW



Server

Client

$ct_1 = Enc(b_1)$

$\downarrow \oplus Enc(1 \oplus b_1')$

$Enc(b_1 \stackrel{?}{=} b_1')$

WANT: $D[i]$

$\forall i \in [n]$:

$i = \overline{b_1' b_2' \cdots b_\ell'}$

Homomorphic Scalar Mult

$ct_i' \leftarrow D[i] \cdot \prod_{t=1}^{\ell} Enc(b_t \stackrel{?}{=} b_t')$

Homomorphic Mult

$ct_1 \leftarrow Enc(b_1)$

$\vdots$

$ct_\ell \leftarrow Enc(b_\ell)$

While hiding i against Server

$i = \underbrace{\overline{b_1 b_2 \cdots b_\ell}}_{\log n}$

ct'

$poly(\lambda)$

$ct' \leftarrow \sum_{i=1}^{n} ct_i'$

Homomorphic Add

$D[i] = Dec(ct')$