

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

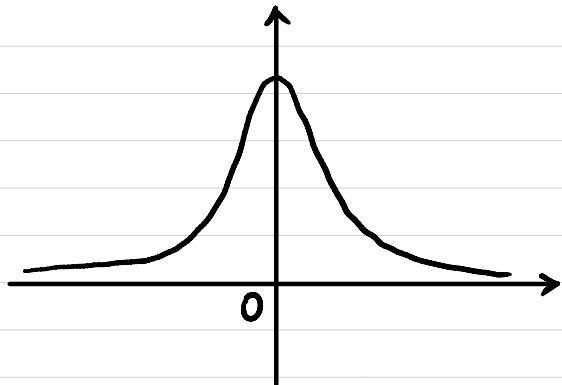
$n \sim$ security parameter

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

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

χ : distribution over \mathbb{Z}_q

(concentrated on "small integers")



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

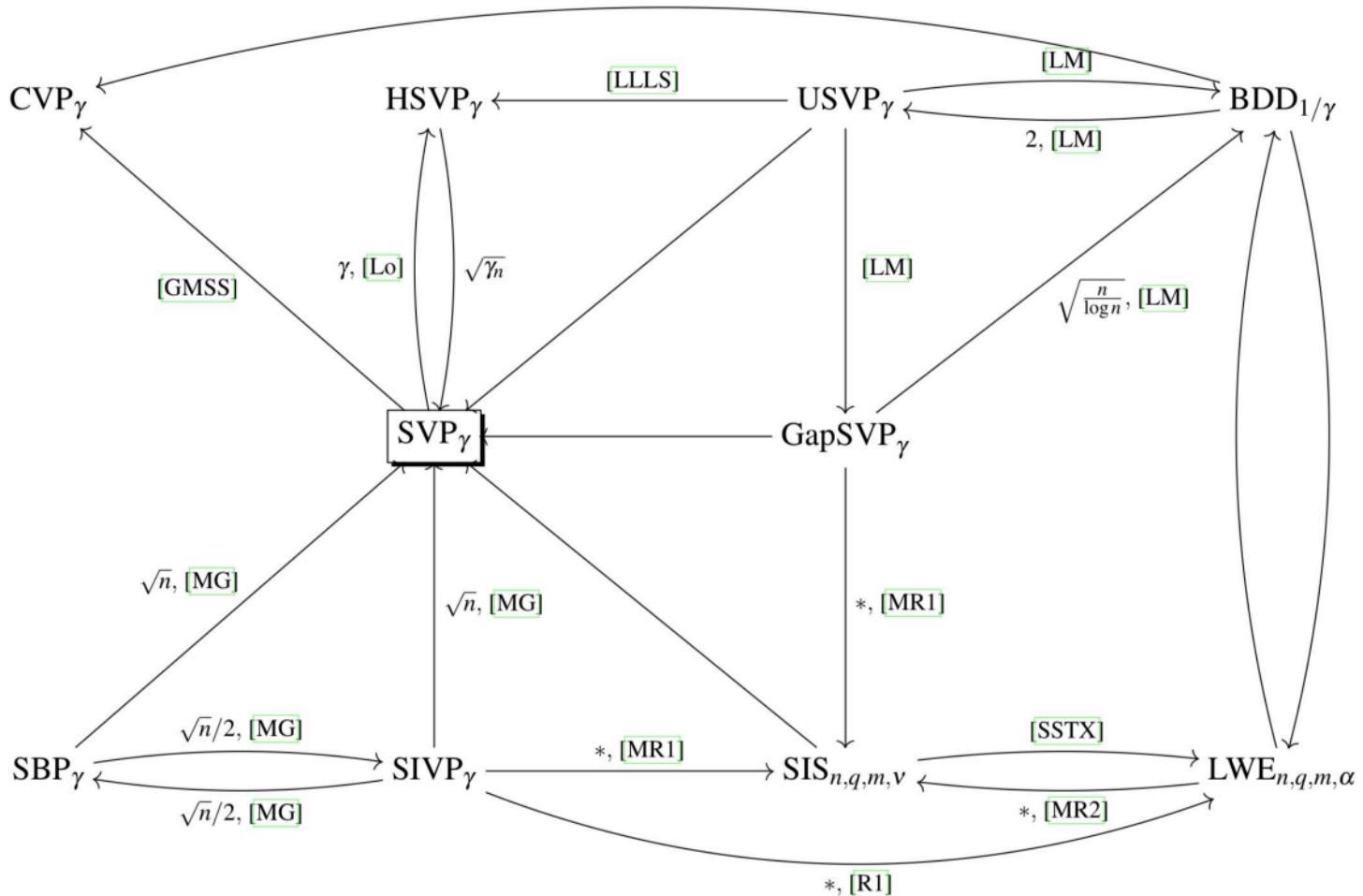
$\alpha \ll 1$

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

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

$$\begin{array}{c|c|c|c|c} A & \times & s_{n \times 1} & + & e_{m \times 1} \\ \hline m \times n & & & & m \times 1 \\ \hline & & & & m \times 1 \end{array} = b_{m \times 1}$$

$$(A, b = As + e) \stackrel{\epsilon}{\sim} (A, b' \in \mathbb{Z}_q^m)$$

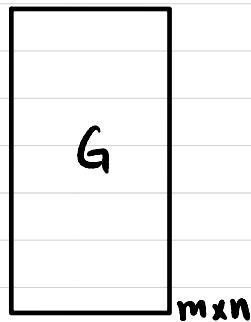


SWHE from LWE (GSW)

Attempt 2 (secret-key)

Flattening Gadget:

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



$$G^{-1} \xrightarrow{\quad} G^{-1}(c) \underset{m \times m}{\times} G \underset{m \times n}{=} c \underset{m \times n}{=}$$

Diagram illustrating the flattening gadget. A curved arrow labeled G^{-1} points to a box labeled $G^{-1}(c)$. Below it, another curved arrow labeled G^{-1} points to a box labeled c . Between the two boxes is a multiplication symbol (\times) and an equals sign ($=$). Dimensions are indicated: $G^{-1}(c)$ is $m \times m$, G is $m \times n$, and c is $m \times n$. A red arrow labeled "small" points to the $G^{-1}(c)$ box.

Inverse transformation

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

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

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

$$\xrightarrow{\text{bit decomposition}} \begin{array}{|c|c|c|} \hline 1 & 0 & 1 \\ \hline 0 & 1 & 1 \\ \hline \dots & & \dots \\ \hline \end{array} \underset{m \times m}{\times} \begin{array}{|c|c|c|} \hline 4 & 0 \\ \hline 2 & 0 \\ \hline 1 & 0 \\ \hline 0 & 4 \\ \hline 0 & 2 \\ \hline 0 & 1 \\ \hline 0 & 0 \\ \hline \vdots & \vdots \\ \hline 0 & 0 \\ \hline \end{array} \underset{m \times n}{=} c \underset{m \times n}{=}$$

Diagram illustrating the inverse transformation. A curved arrow labeled "bit decomposition" points to a matrix with binary columns (101, 011, etc.). This matrix is multiplied by a column vector (4, 2, 1, 0, 4, 0, 2, 1, 0, 0, ..., 0). The result is an equals sign followed by a box labeled c with dimensions $m \times n$.

$$m = n \cdot \log q$$

SWHE from LWE (GSW)

Attempt 2 (Secret-key)

$$SK = t_{n \times 1}$$

$$\begin{matrix} s \\ 1 \end{matrix}_{n \times 1}$$

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

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

$$\begin{matrix} C_0 \\ \hline m \times n \end{matrix} \times \begin{matrix} t \\ \hline n \times 1 \end{matrix} = \begin{matrix} e \\ \hline m \times 1 \end{matrix}$$

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

\uparrow
gadget matrix

$$\begin{aligned} Dec_{SK}(c) : C \cdot \vec{t} &= (C_0 + \mu \cdot G) \cdot \vec{t} \\ &= \vec{e} + \mu \cdot (G \cdot \vec{t}) \end{aligned}$$

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?

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

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

$a \in R_q$ $s \in R_q$ (or $s \in \chi$) $e \in \chi$

$$(a, [a \cdot s + e]_q) \stackrel{\sim}{=} (a, b \in R_q)$$

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. $a+(-a)=0$.

③ " \cdot " is distributive w.r.t " $+$:

- $\forall a, b, c \in R, a \cdot (b+c) = a \cdot b + a \cdot c$
- $\forall a, b, c \in R, (a+b) \cdot c = a \cdot c + b \cdot c$

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. $\forall a \in R, a \cdot 1 = 1 \cdot a = a$.

SWHE from RLWE (BFV)

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

Ciphertext space $R_q \times R_q$

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

$a \leftarrow R_q \quad s \leftarrow X \quad e \leftarrow X$

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

sk = s

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

Sample $u, e_1, e_2 \leftarrow X$

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

$$\begin{aligned} \text{Dec}_{sk}(c): [c_0 + c_1 \cdot s]_q &= -(a \cdot s + e) \cdot u + e_1 + \Delta \cdot m + (a \cdot u + e_2) \cdot s \\ &= -e \cdot u + e_1 + \Delta \cdot m + e_2 \cdot s \\ &= [\Delta \cdot m + \text{small}]_q \end{aligned}$$

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?

$$\begin{aligned} C(s) &= C^{(1)}(s) \cdot C^{(2)}(s) \\ &= [(\Delta \cdot m_1 + e_1 + \alpha_1 \cdot q) \cdot (\Delta \cdot m_2 + e_2 + \alpha_2 \cdot q)] / \frac{q}{t} \quad \Delta = \left\lfloor \frac{q}{t} \right\rfloor \\ &= \Delta^2 \cdot m_1 m_2 + \Delta m_1 e_2 + \Delta m_1 \cdot \alpha_2 q + e_1 \cdot \Delta m_2 + e_1 e_2 + e_1 \alpha_2 q + \alpha_1 q \Delta m_2 + \alpha_1 q e_2 + \alpha_1 \alpha_2 q^2 \end{aligned}$$

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

SWHE from RLWE (BFV)

$$[C(s)]_q = c_0 + c_1 \cdot s + c_2 \cdot s^2 = \Delta \cdot m + e$$



$$[c'(s)]_q = c'_0 + c'_1 \cdot s = \Delta \cdot m + e$$

Relinearization:

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

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

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

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

$$c(s) + c_2 \cdot rlk(s) = c_0 + c_1 \cdot s + c_2 \cdot s^2 + c^2 \cdot (-s^2 + \text{small})$$

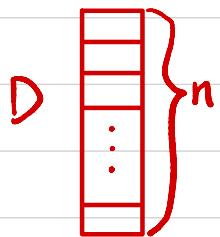


$$\sum rlk_i(s) \cdot c_2[i]$$

↑
large

Private Information Retrieval (PIR)

Server



Client



WANT: $D[i]$

While hiding i against Server

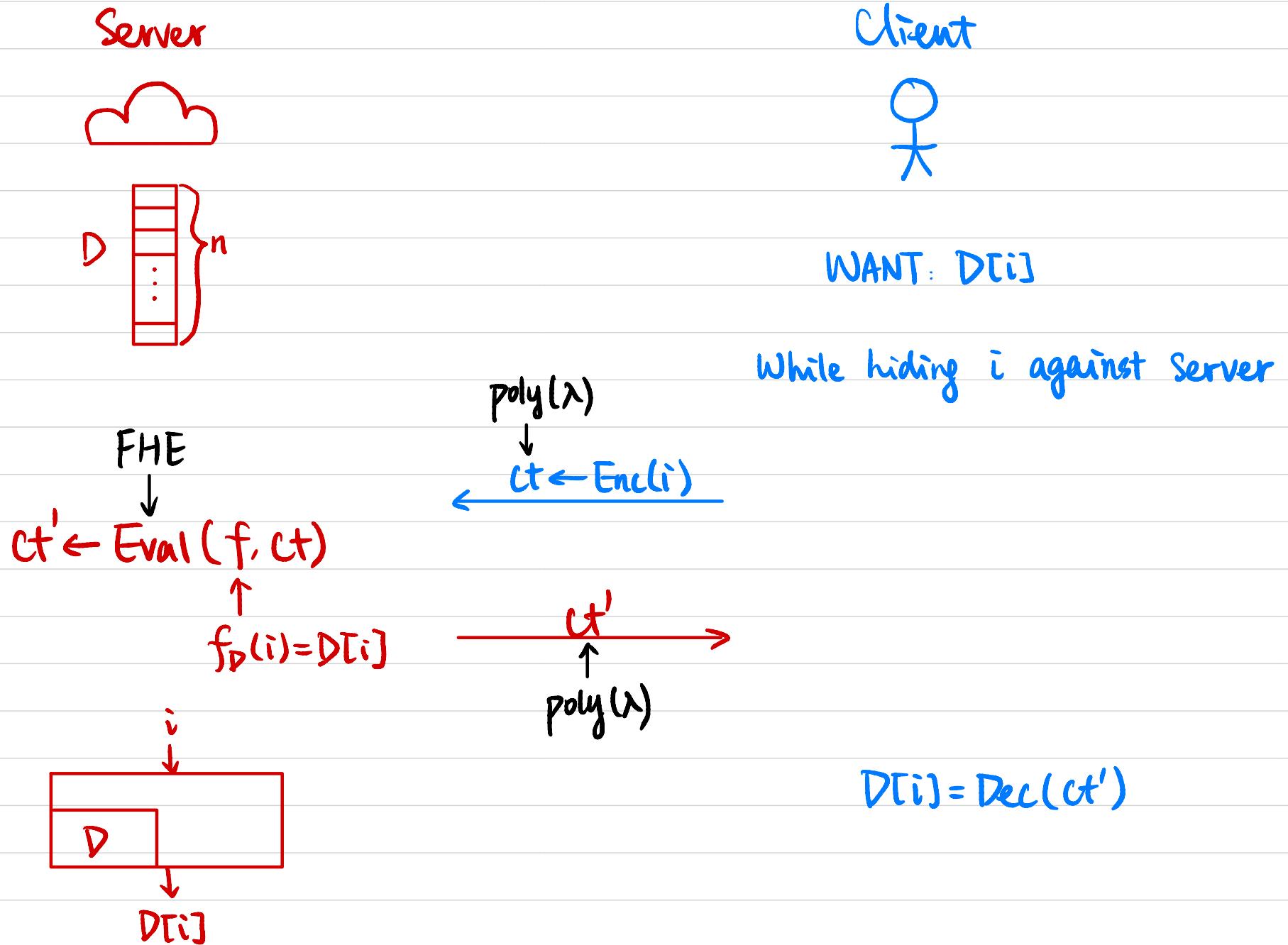
Trivial Solution:



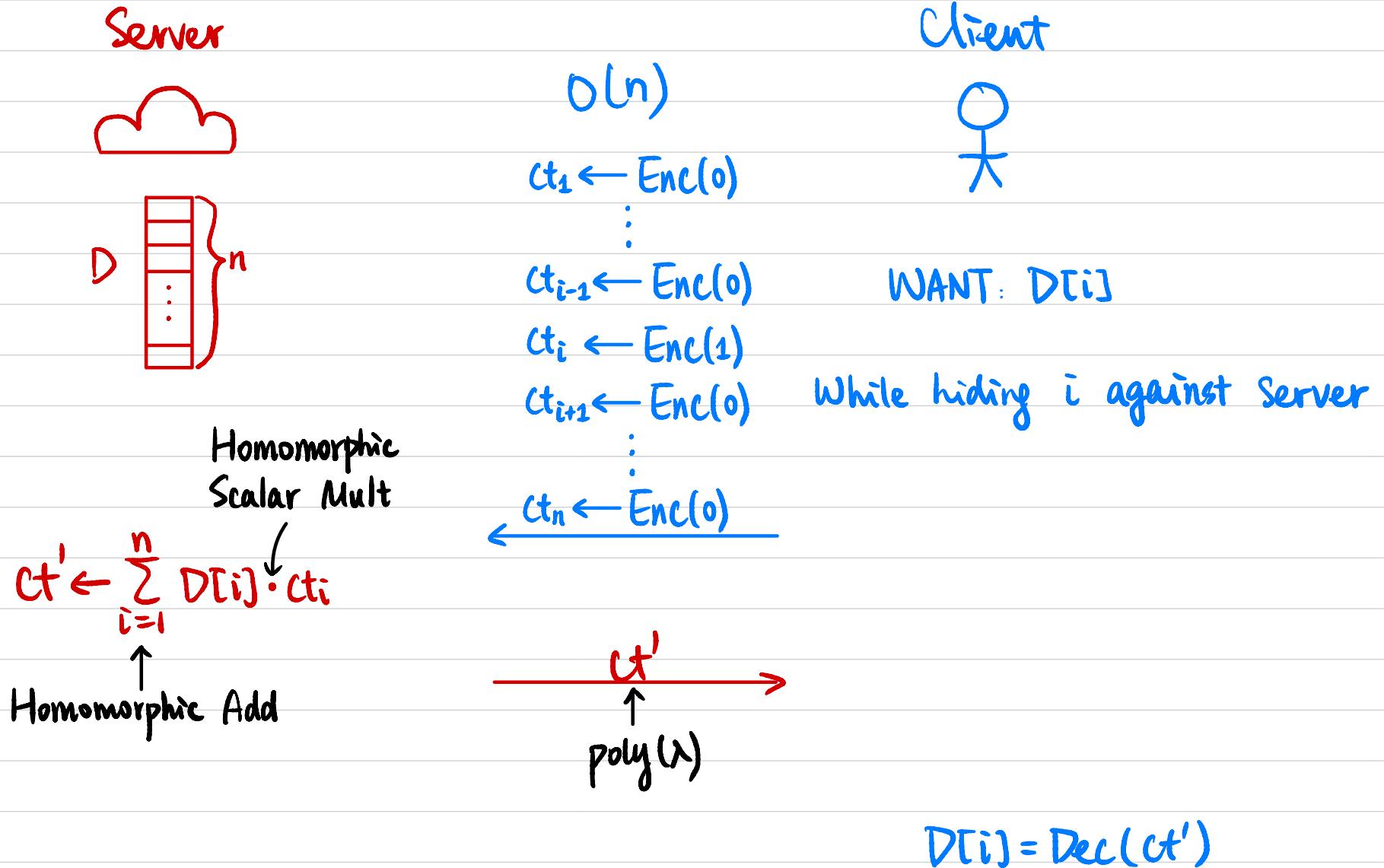
Communication complexity $O(n)$

Goal: Communication complexity $o(n)$

Private Information Retrieval (PIR)

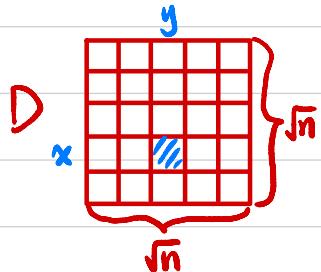


Private Information Retrieval (PIR)



Private Information Retrieval (PIR)

Server



Homomorphic
Scalar Mult

$$ct' \leftarrow \sum_{i,j=1}^{\sqrt{n}} D[i,j] \cdot ct_i^{(1)} \cdot ct_j^{(2)}$$

↑ ↑
 Homomorphic Add Homomorphic Mult

Client



WANT: $D[x,y]$

While hiding (x,y) against Server

$$\begin{array}{ll}
 ct_1^{(1)} \leftarrow \text{Enc}(0) & ct_1^{(2)} \leftarrow \text{Enc}(0) \\
 \vdots & \vdots \\
 ct_{x-1}^{(1)} \leftarrow \text{Enc}(0) & ct_{y-1}^{(2)} \leftarrow \text{Enc}(0) \\
 ct_x^{(1)} \leftarrow \text{Enc}(1) & ct_y^{(1)} \leftarrow \text{Enc}(1) \\
 ct_{x+1}^{(1)} \leftarrow \text{Enc}(0) & ct_{y+1}^{(2)} \leftarrow \text{Enc}(0) \\
 \vdots & \vdots \\
 ct_{\sqrt{n}}^{(1)} \leftarrow \text{Enc}(0) & ct_{\sqrt{n}}^{(2)} \leftarrow \text{Enc}(0)
 \end{array}$$

$$\begin{array}{c}
 \xrightarrow{\quad ct' \quad} \\
 \uparrow \\
 \text{poly}(\lambda)
 \end{array}$$

$$D[x,y] = \text{Dec}(ct')$$

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

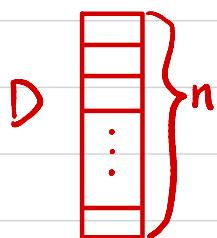
$$\# \text{Homomorphic Mult} = (d-1) \cdot n$$

$$\# \text{Homomorphic Scalar Mult} = n$$

$$\# \text{Homomorphic Add} = n$$

PIR from GSW

Server



$$\begin{aligned} ct_1 &= \text{Enc}(b_1) \\ &\downarrow \oplus \text{Enc}(1 \oplus b'_1) \\ \text{Enc}(b_1 \dot{=} b'_1) \end{aligned}$$

Client



WANT: $D[i]$

$H \in \mathbb{F}[n]$:

$$i = \overline{b'_1 b'_2 \dots b'_n}$$

Homomorphic
Scalar Mult

$$ct'_i \leftarrow D[i] \cdot \prod_{t=1}^n \text{Enc}(b_t \dot{=} b'_t)$$

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

Homomorphic Add

$$\begin{array}{c} ct_1 \leftarrow \text{Enc}(b_1) \\ \vdots \\ ct_\ell \leftarrow \text{Enc}(b_\ell) \end{array}$$

While hiding i against Server

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

$$\xrightarrow{\quad ct' \quad} \uparrow \text{poly}(\lambda)$$

$$D[i] = \text{Dec}(ct')$$