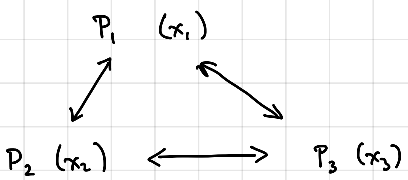
In FHE, computation is supported for data encrypted under a <u>single</u> key

↳ But in practice, data might be distributed across <u>many</u> users

<u>Question</u>: Can we compute on ciphertexts encrypted by <u>different</u> users?

<u>Application</u>: 2-round MPC (in CRS model)



1) Each party chooses a public key pk_i and encrypts $ct_i \leftarrow \text{Encrypt}(pk_i, x_i)$
2) Homomorphically evaluate f on $ct_1, \ldots, ct_n$ to obtain encryption of $f(x_1, \ldots, x_n)$ [Non-interactive]
3) Jointly decrypt computed ciphertext
   ↳ Joint decryption must involve all users who contributed a ciphertext to the computation! [Otherwise, can compromise semantic security]

<u>Syntax</u>:
$\text{Setup}(1^\lambda) \to crs$
$\text{KeyGen}(crs) \to (pk, sk)$
$\text{Encrypt}(pk, x) \to ct$
$\text{Eval}(pk_1, \ldots, pk_N, ct_1, \ldots, ct_N, C) \to ct'$
$\text{Decrypt}(sk_1, \ldots, sk_N, ct') \to x$

<u>Important</u>: Encryption only takes <u>one</u> key as input
Evaluation can take <u>any</u> sequence of public keys and ciphertexts
Decryption requires keys used during evaluation

<u>Correctness</u>: for all $x_1, \ldots, x_N$ and circuits C,
$crs \leftarrow \text{Setup}(1^\lambda)$
$(pk_i, sk_i) \leftarrow \text{KeyGen}(crs)$
$ct_i \leftarrow \text{Encrypt}(pk_i, x_i)$
$ct' \leftarrow \text{Eval}(pk_1, \ldots, pk_N, ct_1, \ldots, ct_N, C)$

$$\Pr[\text{Decrypt}(sk_1, \ldots, sk_N, ct') = C(x_1, \ldots, x_N)] = 1$$

<u>Compactness</u>: $|ct'| = \text{poly}(\lambda, d, N)$ where d is the depth of the circuit C
Does <u>not</u> depend on $|C|$ (otherwise, notion is trivial)

<u>Semantic Security</u>:

<u>adversary</u> | <u>challenger</u>

$b \in \{0,1\}$
$crs \leftarrow \text{Setup}(1^\lambda)$
$pk \leftarrow \text{KeyGen}(crs)$

$\xleftarrow{crs,\ pk}$
$\xrightarrow{x_0,\ x_1}$
$\xleftarrow{ct \leftarrow \text{Encrypt}(pk, x_b)}$

$b' \in \{0,1\}$

For all efficient $\mathcal{A}$, $|\Pr[b' = 1 \mid b = 0] - \Pr[b' = 1 \mid b = 1]| = \text{negl}(\lambda)$

Starting point: GSW (single-key) FHE scheme

pk: $A = \begin{bmatrix} \bar{A} \\ \bar{s}^T \bar{A} + e^T \end{bmatrix} \in \mathbb{Z}_q^{n \times m}$

sk: $s^T = [-\bar{s}^T \mid 1] \in \mathbb{Z}_q^n$

$s^T A = e^T \approx 0$

ct: $C = AR + x \cdot G$ where $R \xleftarrow{R} \{0,1\}^{m \times t}$ where $t = n \log q$

Decryption invariant: $s^T C \approx x \cdot s^T G$

Given $C_1 = AR_1 + x_1 G, \ldots, C_\ell = AR_\ell + x_\ell G$,

$$[C_1 \mid \cdots \mid C_\ell] \cdot H_f = C_f$$

$$\underbrace{[C_1 - x_1 G \mid \cdots \mid C_\ell - x_\ell G]}_{= A[R_1 \mid \cdots \mid R_\ell]} \cdot H_{f,x} = C_f - f(x) \cdot G$$

$C_f = A[R_1 \mid \cdots \mid R_\ell] \cdot H_{f,x} + f(x) \cdot G$

↳ encryption of $f(x)$

Suppose now we have two GSW ciphertexts encrypted under different public keys but sharing the same $\bar{A}$

this will be the CRS

$pk_1 = A_1 = \begin{bmatrix} \bar{A} \\ \bar{s}_1^T \bar{A} + e_1^T \end{bmatrix}$ $\qquad$ $pk_2 = A_2 = \begin{bmatrix} \bar{A} \\ \bar{s}_2^T \bar{A} + e_2^T \end{bmatrix}$

$sk_1 = s_1^T = [-\bar{s}_1^T \mid 1]$ $\qquad$ $sk_2 = s_2^T = [-\bar{s}_2^T \mid 1]$

Suppose $C_1 = A_1 R_1 + x_1 G$, $C_2 = A_2 R_2 + x_2 G$ $\Rightarrow$ $C_1 + C_2 = \underbrace{A_1 R_1 + A_2 R_2 + (x_1 + x_2) G}_{\text{unclear how to decrypt!}}$

Key idea: "Expand" ciphertexts so that they are encryptions under the joint secret key $s^T = [s_1^T \mid s_2^T]$.

Require expanded ciphertext satisfies the GSW decryption invariant

$$s^T \hat{C} \approx x \cdot s^T \hat{G} \quad \text{where} \quad \hat{G} = \begin{bmatrix} G & 0^{n \times t} \\ 0^{n \times t} & G \end{bmatrix} \in \mathbb{Z}_q^{2n \times 2t}$$

(standard gadget matrix on $2n$ rows)

↑ expanded ciphertext

Difficulty: Encryption algorithm takes in one public key — does not know anything about other public keys

↳ public keys only known at evaluation time

Approach: Include a "hint" with the ciphertext

Expanded ciphertext structure:

$$\hat{C} = \begin{bmatrix} C & X \\ 0 & C \end{bmatrix}$$

where C is the original ciphertext and X is derived from the hint and pk_2

hint should still hide message

Requirement:

$$[s_1^T \mid s_2^T] \begin{bmatrix} C & X \\ 0 & C \end{bmatrix} \approx \left[x \cdot s_1^T G \;\middle|\; \underbrace{s_1^T X + s_2^T C}_{\text{need this to be } x \cdot s_2^T G} \right]$$

$$\Rightarrow [x \cdot s_1^T G \mid x \cdot s_2^T G] = x \cdot [s_1^T \mid s_2^T] \cdot \hat{G} = x \cdot s^T \hat{G}$$

<u>Key Relation:</u> $s_1^T X + s_2^T C \approx x \cdot s_2^T G$ where $C = A_1 R + x \cdot G$ $\quad (R \in \{0,1\}^{m \times m})$

Write $A_1 = \begin{bmatrix} \bar{A} \\ b_1^T \end{bmatrix}$ where $b_1^T = s_1^T \bar{A} + e_1^T \in \mathbb{Z}_q^m$

$A_2 = \begin{bmatrix} \bar{A} \\ b_2^T \end{bmatrix}$ where $b_2^T = \bar{s}_2^T \bar{A} + e_2^T \in \mathbb{Z}_q^m$

$b_2^T \approx \bar{s}_2^T \bar{A}$

Now, $s_2^T C = [-\bar{s}_2^T \mid 1] \begin{bmatrix} \bar{A} \\ b_1^T \end{bmatrix} R + x \cdot s_2^T G$

$= -\bar{s}_2^T \bar{A} R + b_1^T R + x \cdot s_2^T G$

$\approx (b_1^T - b_2^T) R + x \cdot s_2^T G$

Sufficient to choose X such that $\underbrace{s_1^T X}_{\text{looks like GSW decryption}} \approx \overbrace{(b_1^T - b_2^T)}^{\text{public vector}} R$ — encryption randomness

<u>Idea:</u> give out encryption of components of R as hint during evaluation, homomorphically compute "ciphertext" that decrypts to $(b_1^T - b_2^T) R$

Abstractly, let $T \in \{0,1\}^{m \times m}$ be a matrix.

Given encryptions of $\{T_{ij}\}_{i,j \in [m]}$ and a <u>public</u> vector $v \in \mathbb{Z}_q^m$, compute ciphertext C such that

$s^T C \approx v^T T$

Define $Z^{(ij)} \in \{0,1\}^{n \times m}$ where

$$Z^{(ij)} = \left[\frac{0^{(n-1) \times m}}{v_i \cdot e_j} \right]$$

$e_j \in \{0,1\}^m$ is j^{th} basis vector

Let $C = \sum_{i \in [m]} \sum_{j \in [m]} C_{ij} \cdot G^{-1}(Z^{(ij)})$

Observe:

$$s^T C = \sum_{i,j \in [m]} s^T C_{ij} \cdot G^{-1}(Z^{(ij)})$$

$$\approx \sum_{i,j \in [m]} T_{ij} \cdot s^T G G^{-1}(Z^{(ij)})$$

$$= s^T \sum_{i,j \in [m]} T_{ij} \cdot Z^{(ij)}$$

$$= \sum_{i,j \in [m]} T_{ij} \, [-\bar{s}^T \mid 1] \left[\frac{0^{(n-1) \times m}}{v_i e_j^T} \right]$$

$$= \sum_{i,j \in [m]} v_i \underbrace{T_{ij} \, e_j^T}$$

$\sum_{j \in [m]} T_{ij} e_j^T = t_i^T$ (i^{th} row of T)

$$= \sum_{i \in [m]} v_i \, t_i^T = v^T T$$

linear combination of rows of T