Adaptively Secure IBE from Lattices with Asymptotically Better Efficiency

Weidan Ji[1], Zhedong Wang[1], Lin Lyu[2], Dawu Gu[1]

1 Shanghai Jiao Tong University
2 University of Wuppertal

May 12, PKC 2025

Outline

- Restriction of the previous lattice IBE framework
- Our idea to remove this restriction
- Our techniques to realize our idea
- Our new lattice IBE framework

IBE

Identity-Based Encryption (IBE) [Sha84]: a generalization of PKE, where the public key can be an arbitrary string, such as name or phone number.

- $\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$
- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}) \to (\mathsf{pk}_{\mathsf{id}}, \mathsf{sk}_{\mathsf{id}})$
- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mu) \to \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{ct}, \mathsf{sk}_{\mathsf{id}}) \to \mu$

Adaptively Secure Lattice-based IBE in the Standard Model

Adaptively secure lattice-based IBEs in the standard model follow the framework in [ABB10].

Adaptively Secure Lattice-based IBE in the Standard Model

Adaptively secure lattice-based IBEs in the standard model follow the framework in [ABB10].

There is a restriction common to all the lattice-based IBEs following this framework:

> The modulus is *quadratic* in the trapdoor norm.

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

- $\mathsf{Setup}(1^\lambda)$: $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ for $i \in [t]$,

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T_B}$$

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

- $\mathsf{Setup}(1^\lambda) : (\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ for $i \in [t]$,

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T_B}$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id}) :$
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

- $\mathsf{Setup}(1^\lambda)$: $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$ for $i \in [t]$,

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \{\mathbf{C}_i\}_{i \in [t]}\right), \quad \mathsf{msk} := \mathbf{T_B}$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i \in [t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i \mathbf{G}$, $\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id}) \cdot \mathbf{G}$

    where the keyed function F is a partitioning function [Yam17] s.t.

$$\Pr_{\boldsymbol{\kappa}}[F(\boldsymbol{\kappa}, \mathsf{id}^{(1)}) \neq 0 \wedge \cdots \wedge F(\boldsymbol{\kappa}, \mathsf{id}^{(Q)}) \neq 0 \wedge F(\boldsymbol{\kappa}, \mathsf{id}^*) = 0] \text{ is noticeable.}$$

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

- $\mathsf{Setup}(1^\lambda)$: $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ for $i \in [t]$,

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T_B}$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G},\ F(\boldsymbol{\kappa}, \mathsf{id}^*) = 0$
  - use $\mathbf{T_B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta},\ \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

- $\mathsf{Setup}(1^\lambda)$: $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ for $i \in [t]$,

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T_B}$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G},\ F(\boldsymbol{\kappa}, \mathsf{id}^*) = 0$
  - use $\mathbf{T_B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta}$, $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$
  - In the security proof, to answer the key queries, use $\mathbf{R}_{\mathsf{id}}$ and $\mathbf{T_G}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t.

$$[\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta} \text{ where } \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$$

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

- $\mathsf{Setup}(1^\lambda)$: $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ for $i \in [t]$,

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T_B}$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}$, $F(\boldsymbol{\kappa}, \mathsf{id}^*) = 0$
  - use $\mathbf{T_B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta}$, $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$

$$\mathsf{pk}_{\mathsf{id}} := ([\mathbf{B}|\mathbf{C}_{\mathsf{id}}], \mathbf{u}), \quad \mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}}.$$

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

- Setup(1^λ) : $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ for $i \in [t]$,
$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T_B}$$
- KeyGen(mpk, msk, id) :
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G},\ F(\boldsymbol{\kappa}, \mathsf{id}^*) = 0$
  - use $\mathbf{T_B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta},\ \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$
$$\mathsf{pk}_{\mathsf{id}} := ([\mathbf{B}|\mathbf{C}_{\mathsf{id}}], \mathbf{u}), \quad \mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}}.$$
- Enc$(\mathsf{mpk}, \mathsf{id}, \mu)$: $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$, $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$
$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{B}|\mathbf{C}_{\mathsf{id}}] + \mathbf{w}^\top\right).$$

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

- $\mathsf{Setup}(1^\lambda)$: $(\mathbf{B}, \mathbf{T}_\mathbf{B}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ for $i \in [t]$,

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T}_\mathbf{B}$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G},\ F(\boldsymbol{\kappa}, \mathsf{id}^*) = 0$
  - use $\mathbf{T}_\mathbf{B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta},\ \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$

$$\mathsf{pk}_{\mathsf{id}} := ([\mathbf{B}|\mathbf{C}_{\mathsf{id}}], \mathbf{u}), \quad \mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}}.$$

- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mu)$: $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$, $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top\mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] + \mathbf{w}^\top\right).$$

- To simulate the challenge ciphertext,
  - use LWE sample $\left(\mathbf{u}, \mathbf{v}^\top\mathbf{u} + y_0\right)$ to generate c_0
  - use LWE samples $\left(\mathbf{B}, \mathbf{v}^\top\mathbf{B} + \mathbf{y}^\top\right)$ and $\mathbf{R}_{\mathsf{id}^*}$ to generate $\mathbf{c}_1$ s.t. $\mathbf{w} \approx D_{\mathbb{Z}^{2m},\sigma}$ where $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

- Setup(1^λ) : $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ for $i \in [t]$,

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T_B}$$

- KeyGen(mpk, msk, id) :
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}$, $F(\boldsymbol{\kappa}, \mathsf{id}^*) = 0$
  - use $\mathbf{T_B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta}$, $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$

$$\mathsf{pk}_{\mathsf{id}} := ([\mathbf{B}|\mathbf{C}_{\mathsf{id}}], \mathbf{u}), \quad \mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}}.$$

- Enc$(\mathsf{mpk}, \mathsf{id}, \mu)$: $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$, $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{B}|\mathbf{C}_{\mathsf{id}}] + \mathbf{w}^\top\right).$$

- Dec$(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$: compute $c_0 - \mathbf{c}_1^\top \cdot \mathbf{x}_{\mathsf{id}} = \lceil \frac{q}{2} \rceil \cdot \mu + (y_0 - \langle \mathbf{w}, \mathbf{x}_{\mathsf{id}} \rangle)$.

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

- Setup(1^λ) : $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, sample $\mathbf{u} \overset{\$}{\leftarrow} \mathbb{Z}_q^n$, $\mathbf{C}_i \overset{\$}{\leftarrow} \mathbb{Z}_q^{n\times m}$ for $i \in [t]$,

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T_B}$$

- KeyGen(mpk, msk, id) :
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G},\ F(\boldsymbol{\kappa}, \mathsf{id}^*) = 0$
  - use $\mathbf{T_B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta},\ \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$

$$\mathsf{pk}_{\mathsf{id}} := ([\mathbf{B}|\mathbf{C}_{\mathsf{id}}], \mathbf{u}), \quad \mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}}.$$

- Enc$(\mathsf{mpk}, \mathsf{id}, \mu)$: $\mathbf{v} \overset{\$}{\leftarrow} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma},\ \sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top\mathbf{u} + y_0 + \lceil q/2 \rfloor \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] + \mathbf{w}^\top\right).$$

- Dec$(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$: compute $c_0 - \mathbf{c}_1^\top \cdot \mathbf{x}_{\mathsf{id}} = \lceil \frac{q}{2} \rfloor \cdot \mu + \underbrace{(y_0 - \langle \mathbf{w}, \mathbf{x}_{\mathsf{id}} \rangle)}_{\text{error term}}$.

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

- Setup(1^λ) : $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ for $i \in [t]$,

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T_B}$$

- KeyGen(mpk, msk, id) :
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id $\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}$, $F(\boldsymbol{\kappa}, \mathsf{id}^*) = 0$
  - use $\mathbf{T_B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta}$, $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$

$$\mathsf{pk}_{\mathsf{id}} := ([\mathbf{B}|\mathbf{C}_{\mathsf{id}}], \mathbf{u}), \quad \mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}}.$$

- Enc$(\mathsf{mpk}, \mathsf{id}, \mu)$: $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$, $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{B}|\mathbf{C}_{\mathsf{id}}] + \mathbf{w}^\top\right).$$

- Dec$(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$: compute $c_0 - \mathbf{c}_1^\top \cdot \mathbf{x}_{\mathsf{id}} = \lceil \frac{q}{2} \rceil \cdot \mu + \underbrace{(y_0 - \langle \mathbf{w}, \mathbf{x}_{\mathsf{id}} \rangle)}_{\text{error term}}.$

To ensure correctness, the modulus q should be larger than the size of the error term.

Adaptively Secure Lattice-based IBE in the Standard Model

The framework in [ABB10]:

- $\mathsf{Setup}(1^\lambda)$: $(\mathbf{B}, \mathbf{T}_\mathbf{B}) \leftarrow \mathsf{TrapGen}(1^n, 1^m, q)$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ for $i \in [t]$,

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T}_\mathbf{B}$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G},\ F(\boldsymbol{\kappa}, \mathsf{id}^*) = 0$
  - use $\mathbf{T}_\mathbf{B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta},\ \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$

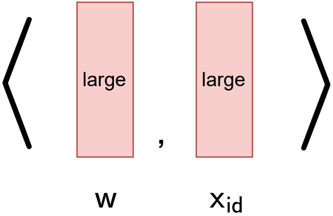
$$\mathsf{pk}_{\mathsf{id}} := ([\mathbf{B}|\mathbf{C}_{\mathsf{id}}], \mathbf{u}), \quad \mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}}.$$

- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mu)$: $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma},\ \sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top\mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] + \mathbf{w}^\top\right).$$

- $\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$: compute $c_0 - \mathbf{c}_1^\top \cdot \mathbf{x}_{\mathsf{id}} = \lceil \frac{q}{2} \rfloor \cdot \mu + \underbrace{(y_0 - \langle \mathbf{w}, \mathbf{x}_{\mathsf{id}} \rangle)}_{\text{error term}}$.

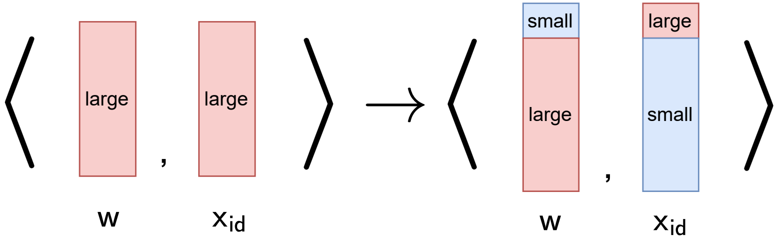
The problem we aim to solve: the modulus q is *quadratic* in $\|\mathbf{R}_{\mathsf{id}}\|$.



"large" means the Gaussian width is larger than $\|\mathbf{R}_{\mathsf{id}}\|$.

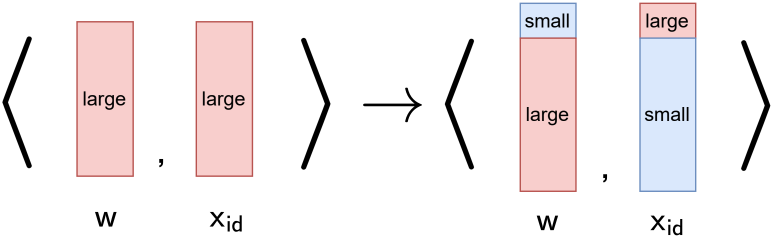
Our New Idea: Cross Multiplication

To remove this quadratic restriction, we propose a cross-multiplication design.



Our New Idea: Cross Multiplication

To remove this quadratic restriction, we propose a cross-multiplication design.

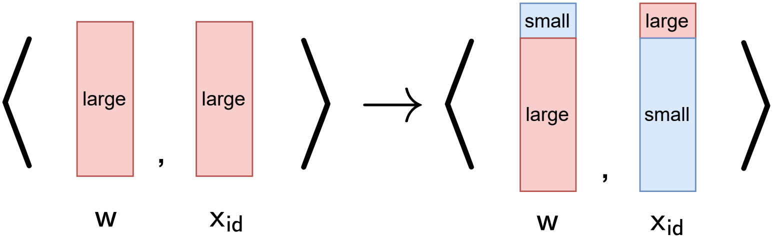


Our goal is to obtain

- a $(D_{\mathbb{Z}^n,\sigma_1}, D_{\mathbb{Z}^{2m},\sigma_2})$-hybrid error $\mathbf{w}$, $\sigma_1 \ll \sigma_2$ and only $\sigma_2 \geq \|\mathbf{R}_{\mathrm{id}}\|$.
- a $(D_{\mathbb{Z}^n,\theta_1}, D_{\mathbb{Z}^{2m},\theta_2})$-hybrid secret key $\mathbf{x}_{\mathrm{id}}$, $\theta_1 \gg \theta_2$ and only $\theta_1 \geq \|\mathbf{R}_{\mathrm{id}}\|$.

Our New Idea: Cross Multiplication

To remove this quadratic restriction, we propose a cross-multiplication design.



Our goal is to obtain

- a $(D_{\mathbb{Z}^n,\sigma_1}, D_{\mathbb{Z}^{2m},\sigma_2})$-hybrid error $\mathbf{w}$, $\sigma_1 \ll \sigma_2$ and only $\sigma_2 \geq \|\mathbf{R}_{id}\|$.
- a $(D_{\mathbb{Z}^n,\theta_1}, D_{\mathbb{Z}^{2m},\theta_2})$-hybrid secret key $\mathbf{x}_{id}$, $\theta_1 \gg \theta_2$ and only $\theta_1 \geq \|\mathbf{R}_{id}\|$.

such that $\langle \mathbf{w}, \mathbf{x}_{id} \rangle =$ "small $\times$ large $+$ large $\times$ small", thus removing the quadratic restriction.

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$.

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i\mathbf{G}, \quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id}) \cdot \mathbf{G}$

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id

- In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i\mathbf{G}$, $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id}) \cdot \mathbf{G}$

small-norm $\mathbf{R}_i$ large-norm $\mathbf{R}_{\mathsf{id}}$

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i\mathbf{G}$, $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id}) \cdot \mathbf{G}$
- use $\mathbf{T}_{\mathbf{B}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta}$
  - In the security proof, to answer the key queries, use $\mathbf{R}_{\mathsf{id}}$ and $\mathbf{T}_{\mathbf{G}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t.

$$[\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta} \text{ where } \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$$

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i\mathbf{G}$, $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id}) \cdot \mathbf{G}$
- use $\mathbf{T}_{\mathbf{B}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta}$
  - In the security proof, to answer the key queries, use $\mathbf{R}_{\mathsf{id}}$ and $\mathbf{T}_{\mathbf{G}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t.

$$[\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta} \text{ where } \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$$

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathrm{id}}\|$.

- homomorphically compute $\mathbf{C}_{\mathrm{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i\mathbf{G}$, $\quad \mathbf{C}_{\mathrm{id}} = \mathbf{B}\mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id}) \cdot \mathbf{G}$
- use $\mathbf{T}_{\mathbf{B}}$ to sample a short $\mathbf{x}_{\mathrm{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathrm{id}}] \cdot \mathbf{x}_{\mathrm{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathrm{id}} \approx D_{\mathbb{Z}^{2m},\theta}$
  - In the security proof, to answer the key queries, use $\mathbf{R}_{\mathrm{id}}$ and $\mathbf{T}_{\mathbf{G}}$ to sample a short $\mathbf{x}_{\mathrm{id}}$ s.t.

$$[\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id})\mathbf{G}] \cdot \mathbf{x}_{\mathrm{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathrm{id}} \approx D_{\mathbb{Z}^{2m},\theta} \text{ where } \theta \geq \|\mathbf{R}_{\mathrm{id}}\|$$

Our idea: reduce a large-norm $\mathbf{R}_{\mathrm{id}}$ to a small-norm $\mathbf{R}_{\mathrm{id}}$.

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i\mathbf{G}$, $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id}) \cdot \mathbf{G}$
- use $\mathbf{T}_{\mathbf{B}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta}$
  - In the security proof, to answer the key queries, use $\mathbf{R}_{\mathsf{id}}$ and $\mathbf{T}_{\mathbf{G}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t.

$$[\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta} \text{ where } \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$$

Our idea: reduce a large-norm $\mathbf{R}_{\mathsf{id}}$ to a small-norm $\mathbf{R}_{\mathsf{id}}$.

- $\boxed{\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}} \rightarrow \boxed{\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}} \quad ?$

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i\mathbf{G}$, $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id}) \cdot \mathbf{G}$
- use $\mathbf{T}_{\mathbf{B}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta}$
  - In the security proof, to answer the key queries, use $\mathbf{R}_{\mathsf{id}}$ and $\mathbf{T}_{\mathbf{G}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t.

$$[\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta} \text{ where } \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$$

Our idea: reduce a large-norm $\mathbf{R}_{\mathsf{id}}$ to a small-norm $\mathbf{R}_{\mathsf{id}}$.

- $\boxed{\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}} \to \boxed{\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}}$?
- $\boxed{\mathbf{C}_{\mathsf{id}} = \begin{bmatrix} \mathbf{A} \\ \mathbf{SA}+\mathbf{E} \end{bmatrix} \mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}}$

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i \in [t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i \mathbf{G}$, $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id}) \cdot \mathbf{G}$
- use $\mathbf{T}_{\mathbf{B}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta}$
  - In the security proof, to answer the key queries, use $\mathbf{R}_{\mathsf{id}}$ and $\mathbf{T}_{\mathbf{G}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t.

$$[\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta} \text{ where } \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$$

Our idea: reduce a large-norm $\mathbf{R}_{\mathsf{id}}$ to a small-norm $\mathbf{R}_{\mathsf{id}}$.

- $\boxed{\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}} \rightarrow \boxed{\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}}$?
- $\boxed{\mathbf{C}_{\mathsf{id}} = \begin{bmatrix} \mathbf{A} \\ \mathbf{SA}+\mathbf{E} \end{bmatrix} \mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}} \rightarrow \boxed{\mathbf{C}_{\mathsf{id}} \approx \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}}$ $\surd$

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\text{id}}\|$.

- homomorphically compute $\mathbf{C}_{\text{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i\mathbf{G}$, $\quad \mathbf{C}_{\text{id}} = \mathbf{B}\mathbf{R}_{\text{id}} + F(\boldsymbol{\kappa}, \text{id}) \cdot \mathbf{G}$
- use $\mathbf{T}_\mathbf{B}$ to sample a short $\mathbf{x}_{\text{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\text{id}}] \cdot \mathbf{x}_{\text{id}} = \mathbf{u}$ and $\mathbf{x}_{\text{id}} \approx D_{\mathbb{Z}^{2m},\theta}$
  - In the security proof, to answer the key queries, use $\mathbf{R}_{\text{id}}$ and $\mathbf{T}_\mathbf{G}$ to sample a short $\mathbf{x}_{\text{id}}$ s.t.

$$[\mathbf{B}|\mathbf{B}\mathbf{R}_{\text{id}} + F(\boldsymbol{\kappa}, \text{id})\mathbf{G}] \cdot \mathbf{x}_{\text{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\text{id}} \approx D_{\mathbb{Z}^{2m},\theta} \text{ where } \theta \geq \|\mathbf{R}_{\text{id}}\|$$

Our idea: reduce a large-norm $\mathbf{R}_{\text{id}}$ to a small-norm $\mathbf{R}_{\text{id}}$.

- $\boxed{\mathbf{C}_{\text{id}} = \mathbf{B}\mathbf{R}_{\text{id}} + F(\boldsymbol{\kappa}, \text{id})\mathbf{G}} \rightarrow \boxed{\mathbf{C}_{\text{id}} = \mathbf{B}\mathbf{R}_{\text{id}} + F(\boldsymbol{\kappa}, \text{id})\mathbf{G}}$?
- $\boxed{\mathbf{C}_{\text{id}} = \begin{bmatrix} \mathbf{A} \\ \mathbf{SA}+\mathbf{E} \end{bmatrix} \mathbf{R}_{\text{id}} + F(\boldsymbol{\kappa}, \text{id})\mathbf{G}} \rightarrow \boxed{\mathbf{C}_{\text{id}} \approx \mathbf{B}\mathbf{R}_{\text{id}} + F(\boldsymbol{\kappa}, \text{id})\mathbf{G}}$ $\surd$
  1. Left $\mathbf{C}_{\text{id}}$ can be seen as an GSW encryption of $F(\boldsymbol{\kappa}, \text{id})$ with large noise $\mathbf{R}_{\text{id}}$.

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathrm{id}}\|$.

- homomorphically compute $\mathbf{C}_{\mathrm{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i \mathbf{G}$, $\quad \mathbf{C}_{\mathrm{id}} = \mathbf{B}\mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id}) \cdot \mathbf{G}$
- use $\mathbf{T}_{\mathbf{B}}$ to sample a short $\mathbf{x}_{\mathrm{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathrm{id}}] \cdot \mathbf{x}_{\mathrm{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathrm{id}} \approx D_{\mathbb{Z}^{2m},\theta}$
  - In the security proof, to answer the key queries, use $\mathbf{R}_{\mathrm{id}}$ and $\mathbf{T}_{\mathbf{G}}$ to sample a short $\mathbf{x}_{\mathrm{id}}$ s.t.

$$[\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id})\mathbf{G}] \cdot \mathbf{x}_{\mathrm{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathrm{id}} \approx D_{\mathbb{Z}^{2m},\theta} \text{ where } \theta \geq \|\mathbf{R}_{\mathrm{id}}\|$$

Our idea: reduce a large-norm $\mathbf{R}_{\mathrm{id}}$ to a small-norm $\mathbf{R}_{\mathrm{id}}$.

- $\boxed{\mathbf{C}_{\mathrm{id}} = \mathbf{B}\mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id})\mathbf{G}} \rightarrow \boxed{\mathbf{C}_{\mathrm{id}} = \mathbf{B}\mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id})\mathbf{G}}$?
- $\boxed{\mathbf{C}_{\mathrm{id}} = \begin{bmatrix} \mathbf{A} \\ \mathbf{SA}+\mathbf{E} \end{bmatrix} \mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id})\mathbf{G}} \rightarrow \boxed{\mathbf{C}_{\mathrm{id}} \approx \mathbf{B}\mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id})\mathbf{G}}$ $\surd$
  1. Left $\mathbf{C}_{\mathrm{id}}$ can be seen as an GSW encryption of $F(\boldsymbol{\kappa}, \mathrm{id})$ with large noise $\mathbf{R}_{\mathrm{id}}$.
  2. Use a bootstrapping-like approach. (Incomplete Decryption)

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i\mathbf{G}$, $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id}) \cdot \mathbf{G}$
- use $\mathbf{T}_\mathbf{B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta}$
  - In the security proof, to answer the key queries, use $\mathbf{R}_{\mathsf{id}}$ and $\mathbf{T}_\mathbf{G}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t.

$$[\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta} \text{ where } \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$$

Our idea: reduce a large-norm $\mathbf{R}_{\mathsf{id}}$ to a small-norm $\mathbf{R}_{\mathsf{id}}$.

- $\boxed{\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}} \rightarrow \boxed{\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}}$?
- $\boxed{\mathbf{C}_{\mathsf{id}} = \begin{bmatrix}\mathbf{A} \\ \mathbf{SA}+\mathbf{E}\end{bmatrix}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}} \rightarrow \boxed{\mathbf{C}_{\mathsf{id}} \approx \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}}$ $\surd$
  1. Left $\mathbf{C}_{\mathsf{id}}$ can be seen as an GSW encryption of $F(\boldsymbol{\kappa}, \mathsf{id})$ with large noise $\mathbf{R}_{\mathsf{id}}$.
  2. Use a bootstrapping-like approach. (Incomplete Decryption)
  3. Obtain the right $\mathbf{C}_{\mathsf{id}}$: an encoding of $F(\boldsymbol{\kappa}, \mathsf{id})$ with small noise $\mathbf{R}_{\mathsf{id}}$.

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathrm{id}}\|$.

- homomorphically compute $\mathbf{C}_{\mathrm{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i \mathbf{G}$, $\quad \mathbf{C}_{\mathrm{id}} = \mathbf{B}\mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id}) \cdot \mathbf{G}$
- use $\mathbf{T}_{\mathbf{B}}$ to sample a short $\mathbf{x}_{\mathrm{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathrm{id}}] \cdot \mathbf{x}_{\mathrm{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathrm{id}} \approx D_{\mathbb{Z}^{2m},\theta}$
  - In the security proof, to answer the key queries, use $\mathbf{R}_{\mathrm{id}}$ and $\mathbf{T}_{\mathbf{G}}$ to sample a short $\mathbf{x}_{\mathrm{id}}$ s.t.

$$[\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id})\mathbf{G}] \cdot \mathbf{x}_{\mathrm{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathrm{id}} \approx D_{\mathbb{Z}^{2m},\theta} \text{ where } \theta \geq \|\mathbf{R}_{\mathrm{id}}\|$$

Our idea: reduce a large-norm $\mathbf{R}_{\mathrm{id}}$ to a small-norm $\mathbf{R}_{\mathrm{id}}$.

- $\boxed{\mathbf{C}_{\mathrm{id}} = \mathbf{B}\mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id})\mathbf{G}} \to \boxed{\mathbf{C}_{\mathrm{id}} = \mathbf{B}\mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id})\mathbf{G}}$?
- $\boxed{\mathbf{C}_{\mathrm{id}} = \begin{bmatrix} \mathbf{A} \\ \mathbf{SA}+\mathbf{E} \end{bmatrix} \mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id})\mathbf{G}} \to \boxed{\mathbf{C}_{\mathrm{id}} = \mathbf{B}\mathbf{R}_{\mathrm{id}} + F(\boldsymbol{\kappa}, \mathrm{id})\mathbf{G} + \mathbf{E}_{\mathrm{id}}}$

Obtain A (Mostly) Small-Norm Secret Key

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\theta}$ secret key where $\theta \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id
  - In the security proof, $\mathbf{C}_i := \mathbf{B}\mathbf{R}_i + \kappa_i\mathbf{G}$, $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id}) \cdot \mathbf{G}$
- use $\mathbf{T}_{\mathbf{B}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $[\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$ and $\mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta}$
  - In the security proof, to answer the key queries, use $\mathbf{R}_{\mathsf{id}}$ and $\mathbf{T}_{\mathbf{G}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t.

$$[\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathsf{id}} \approx D_{\mathbb{Z}^{2m},\theta} \text{ where } \theta \geq \|\mathbf{R}_{\mathsf{id}}\|$$

Our idea: reduce a large-norm $\mathbf{R}_{\mathsf{id}}$ to a small-norm $\mathbf{R}_{\mathsf{id}}$.

- $\boxed{\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}} \to \boxed{\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}}$?
- $\boxed{\mathbf{C}_{\mathsf{id}} = \begin{bmatrix} \mathbf{A} \\ \mathbf{SA}+\mathbf{E} \end{bmatrix}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G}} \to \boxed{\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G} + \mathbf{E}_{\mathsf{id}}}$
- In our security proof, to answer the key queries, use $\mathbf{R}_{\mathsf{id}}$, $\mathbf{E}_{\mathsf{id}}$, $\mathbf{T}_{\mathbf{G}}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t.

$$[\mathbf{I}_n|\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G} + \mathbf{E}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathsf{id}} \approx \begin{bmatrix} D_{\mathbb{Z}^n,\theta_1} \\ D_{\mathbb{Z}^{2m},\theta_2} \end{bmatrix} \text{ where } \theta_1 \geq \|\mathbf{E}_{\mathsf{id}}\|, \theta_2 \geq \|\mathbf{R}_{\mathsf{id}}\|.$$

Obtain A (Mostly) Large-Norm Error

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\sigma}$ error where $\sigma \geq \|\mathbf{R}_{\mathsf{id}}\|$.

Obtain A (Mostly) Large-Norm Error

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\sigma}$ error where $\sigma \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- $\mathbf{v} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$. The challenge ciphertext is set to be

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{B} | \mathbf{C}_{\mathsf{id}^*} = \mathbf{B}\mathbf{R}_{\mathsf{id}^*}] + \mathbf{w}^\top\right)$$

$$\begin{aligned} \mathbf{C}_{\mathsf{id}^*} &= \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + F(\boldsymbol{\kappa}, \mathsf{id}^*)\mathbf{G} \\ &= \mathbf{B}\mathbf{R}_{\mathsf{id}^*} \end{aligned}$$

Obtain A (Mostly) Large-Norm Error

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\sigma}$ error where $\sigma \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$. The challenge ciphertext is set to be

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*}] + \mathbf{w}^\top\right)$$

  - To simulate the challenge ciphertext,
    - use LWE sample $(\mathbf{u}, \mathbf{v}^\top \mathbf{u} + y_0)$ to generate c_0
    - use LWE samples $(\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top)$ and $\mathbf{R}_{\mathsf{id}^*}$ to generate $\mathbf{c}_1$ s.t. $\mathbf{w} \approx D_{\mathbb{Z}^{2m},\sigma}$ where $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

Obtain A (Mostly) Large-Norm Error

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\sigma}$ error where $\sigma \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$. The challenge ciphertext is set to be

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top\mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top[\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*}] + \mathbf{w}^\top\right)$$

- To simulate the challenge ciphertext,
  - use LWE sample $(\mathbf{u}, \mathbf{v}^\top\mathbf{u} + y_0)$ to generate c_0
  - use LWE samples $(\mathbf{B}, \mathbf{v}^\top\mathbf{B} + \mathbf{y}^\top)$ and $\mathbf{R}_{\mathsf{id}^*}$ to generate $\mathbf{c}_1$ s.t. $\mathbf{w} \approx D_{\mathbb{Z}^{2m},\sigma}$ where $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

Our challenge ciphertext:

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top\mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top[\mathbf{I}|\mathbf{B}|\mathbf{C}_{\mathsf{id}^*} = \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + [\mathbf{w}_1^\top|\mathbf{w}_2^\top]\right)$$

$$\mathbf{C}_{\mathsf{id}^*} = \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + F(\boldsymbol{\kappa}, \mathsf{id}^*)\mathbf{G} + \mathbf{E}_{\mathsf{id}^*}$$
$$= \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}$$

Obtain A (Mostly) Large-Norm Error

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\sigma}$ error where $\sigma \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$. The challenge ciphertext is set to be

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*}] + \mathbf{w}^\top \right)$$

- To simulate the challenge ciphertext,
  - use LWE sample $(\mathbf{u}, \mathbf{v}^\top \mathbf{u} + y_0)$ to generate c_0
  - use LWE samples $(\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top)$ and $\mathbf{R}_{\mathsf{id}^*}$ to generate $\mathbf{c}_1$ s.t. $\mathbf{w} \approx D_{\mathbb{Z}^{2m},\sigma}$ where $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

Our challenge ciphertext:

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{I} | \mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + [\mathbf{w}_1^\top | \mathbf{w}_2^\top] \right)$$

- To simulate the challenge ciphertext,
  - use $\boxed{\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + \mathbf{w}_2^\top}$?

Obtain A (Mostly) Large-Norm Error

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\sigma}$ error where $\sigma \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$. The challenge ciphertext is set to be

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*}] + \mathbf{w}^\top \right)$$

- To simulate the challenge ciphertext,
  - use LWE sample $(\mathbf{u}, \mathbf{v}^\top \mathbf{u} + y_0)$ to generate c_0
  - use LWE samples $(\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top)$ and $\mathbf{R}_{\mathsf{id}^*}$ to generate $\mathbf{c}_1$ s.t. $\mathbf{w} \approx D_{\mathbb{Z}^{2m},\sigma}$ where $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

Our challenge ciphertext:

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{I}|\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + [\mathbf{w}_1^\top | \mathbf{w}_2^\top] \right)$$

- To simulate the challenge ciphertext,
  - use $\boxed{\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top [\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + \mathbf{w}_2^\top}$?
  - use $\boxed{[\mathbf{B}|\mathbf{I}], \mathbf{v}^\top [\mathbf{B}|\mathbf{I}] + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$

Obtain A (Mostly) Large-Norm Error

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\sigma}$ error where $\sigma \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$. The challenge ciphertext is set to be

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rfloor \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*}] + \mathbf{w}^\top\right)$$

- To simulate the challenge ciphertext,
  - use LWE sample $(\mathbf{u}, \mathbf{v}^\top \mathbf{u} + y_0)$ to generate c_0
  - use LWE samples $(\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top)$ and $\mathbf{R}_{\mathsf{id}^*}$ to generate $\mathbf{c}_1$ s.t. $\mathbf{w} \approx D_{\mathbb{Z}^{2m},\sigma}$ where $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

Our challenge ciphertext:

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rfloor \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{I} | \mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + [\mathbf{w}_1^\top | \mathbf{w}_2^\top]\right)$$

- To simulate the challenge ciphertext,
  - use $\boxed{\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + \mathbf{w}_2^\top}$?
  - use $\boxed{[\mathbf{B}|\mathbf{I}], \mathbf{v}^\top [\mathbf{B}|\mathbf{I}] + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + \mathbf{w}_2^\top}$ $\surd$

Obtain A (Mostly) Large-Norm Error

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\sigma}$ error where $\sigma \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$. The challenge ciphertext is set to be

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*}] + \mathbf{w}^\top \right)$$

  - To simulate the challenge ciphertext,
    - use LWE sample $(\mathbf{u}, \mathbf{v}^\top \mathbf{u} + y_0)$ to generate c_0
    - use LWE samples $(\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top)$ and $\mathbf{R}_{\mathsf{id}^*}$ to generate $\mathbf{c}_1$ s.t. $\mathbf{w} \approx D_{\mathbb{Z}^{2m},\sigma}$ where $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

Our challenge ciphertext:

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{I} | \mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + [\mathbf{w}_1^\top | \mathbf{w}_2^\top] \right)$$

  - To simulate the challenge ciphertext,
    - use $\boxed{\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + \mathbf{w}_2^\top}$?
    - use $\boxed{[\mathbf{B}|\mathbf{I}], \mathbf{v}^\top [\mathbf{B}|\mathbf{I}] + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + \mathbf{w}_2^\top}$ $\checkmark$

Intuition: $[\mathbf{B}|\mathbf{I}] \cdot \begin{bmatrix} \mathbf{I} & \mathbf{R}_{\mathsf{id}^*} \\ \mathbf{0} & \mathbf{E}_{\mathsf{id}^*} \end{bmatrix} = [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}]$

Obtain A (Mostly) Large-Norm Error

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\sigma}$ error where $\sigma \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$. The challenge ciphertext is set to be

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*}] + \mathbf{w}^\top\right)$$

  - To simulate the challenge ciphertext,
    - use LWE sample $(\mathbf{u}, \mathbf{v}^\top \mathbf{u} + y_0)$ to generate c_0
    - use LWE samples $(\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top)$ and $\mathbf{R}_{\mathsf{id}^*}$ to generate $\mathbf{c}_1$ s.t. $\mathbf{w} \approx D_{\mathbb{Z}^{2m},\sigma}$ where $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

Our challenge ciphertext:

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top \mathbf{D}[\mathbf{I}|\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + [\mathbf{w}_1^\top|\mathbf{w}_2^\top]\right)$$

  - To simulate the challenge ciphertext,
    - use $\boxed{\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top [\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + \mathbf{w}_2^\top}$?
    - use $\boxed{[\mathbf{B}|\mathbf{I}], \mathbf{v}^\top [\mathbf{B}|\mathbf{I}] + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top [\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + \mathbf{w}_2^\top}$ $\surd$

Obtain A (Mostly) Large-Norm Error

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\sigma}$ error where $\sigma \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$. The challenge ciphertext is set to be

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rfloor \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*}] + \mathbf{w}^\top\right)$$

- To simulate the challenge ciphertext,
  - use LWE sample $(\mathbf{u}, \mathbf{v}^\top \mathbf{u} + y_0)$ to generate c_0
  - use LWE samples $(\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top)$ and $\mathbf{R}_{\mathsf{id}^*}$ to generate $\mathbf{c}_1$ s.t. $\mathbf{w} \approx D_{\mathbb{Z}^{2m},\sigma}$ where $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

Our challenge ciphertext:

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rfloor \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top \mathbf{D}[\mathbf{I}|\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + [\mathbf{w}_1^\top|\mathbf{w}_2^\top]\right)$$

- To simulate the challenge ciphertext,
  - use $\boxed{\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top [\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + \mathbf{w}_2^\top}$?
  - use $\boxed{[\mathbf{B}|\mathbf{I}], \mathbf{v}^\top [\mathbf{B}|\mathbf{I}] + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top [\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + \mathbf{w}_2^\top}$ $\surd$
  - use $\boxed{[\mathbf{D}\mathbf{B}|\mathbf{D}], \mathbf{v}^\top \mathbf{D}[\mathbf{B}|\mathbf{I}] + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top \mathbf{D}[\mathbf{I}|\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + [\mathbf{w}_1^\top|\mathbf{w}_2^\top]}$

Obtain A (Mostly) Large-Norm Error

Let's recall how the previous framework obtains a $D_{\mathbb{Z}^{2m},\sigma}$ error where $\sigma \geq \|\mathbf{R}_{\mathsf{id}}\|$.

- $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w} \leftarrow D_{\mathbb{Z}^{2m},\sigma}$. The challenge ciphertext is set to be

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*}] + \mathbf{w}^\top \right)$$

  - To simulate the challenge ciphertext,
    - use LWE sample $(\mathbf{u}, \mathbf{v}^\top \mathbf{u} + y_0)$ to generate c_0
    - use LWE samples $(\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top)$ and $\mathbf{R}_{\mathsf{id}^*}$ to generate $\mathbf{c}_1$ s.t. $\mathbf{w} \approx D_{\mathbb{Z}^{2m},\sigma}$ where $\sigma \geq \|\mathbf{R}_{\mathsf{id}^*}\|$

Our challenge ciphertext:

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top \mathbf{D}[\mathbf{I} | \mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + [\mathbf{w}_1^\top | \mathbf{w}_2^\top] \right)$$

  - To simulate the challenge ciphertext,
    - use $\boxed{\mathbf{B}, \mathbf{v}^\top \mathbf{B} + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + \mathbf{w}_2^\top}$?
    - use $\boxed{[\mathbf{B}|\mathbf{I}], \mathbf{v}^\top [\mathbf{B}|\mathbf{I}] + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\boxed{\mathbf{v}^\top [\mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] + \mathbf{w}_2^\top}$ $\checkmark$
    - use $\boxed{[\mathbf{D}\mathbf{B}|\mathbf{D}], \mathbf{v}^\top \mathbf{D}[\mathbf{B}|\mathbf{I}] + \mathbf{y}^\top}$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ $\rightarrow$ $\mathbf{v}^\top \mathbf{D}[\mathbf{I} | \mathbf{B} | \mathbf{B}\mathbf{R}_{\mathsf{id}^*} + \mathbf{E}_{\mathsf{id}^*}] +$ $\boxed{[\mathbf{w}_1^\top | \mathbf{w}_2^\top] \approx \begin{bmatrix} D_{\mathbb{Z}^n,\sigma_1} \\ D_{\mathbb{Z}^{2m},\sigma_2} \end{bmatrix}}$

Our New IBE Framework

Our framework:

- $\mathsf{Setup}(1^\lambda)$: $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{2n \times 2m}$ for $i \in [t]$, $\mathbf{D} \xleftarrow{\$} \mathbb{Z}_q^{n \times n}$

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \mathbf{D}, \{\mathbf{C}_i\}_{i \in [t]}\right), \quad \mathsf{msk} := \mathbf{T_B}.$$

Our New IBE Framework

Our framework:

- $\mathsf{Setup}(1^\lambda)$: $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{2n\times 2m}$ for $i \in [t]$, $\mathbf{D} \xleftarrow{\$} \mathbb{Z}_q^{n\times n}$

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \mathbf{D}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T_B}.$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id
  - In the security proof, $\mathbf{C}_i := \left[\begin{smallmatrix}\mathbf{A}\\ \mathbf{SA}+\mathbf{E}\end{smallmatrix}\right]\mathbf{R}_i + \kappa_i\mathbf{G}$, $\mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G} + \mathbf{E}_{\mathsf{id}}$

Our New IBE Framework

Our framework:

- $\mathsf{Setup}(1^\lambda)$: $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{2n \times 2m}$ for $i \in [t]$, $\mathbf{D} \xleftarrow{\$} \mathbb{Z}_q^{n \times n}$

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \mathbf{D}, \{\mathbf{C}_i\}_{i \in [t]}\right), \quad \mathsf{msk} := \mathbf{T_B}.$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i \in [t]}$ and id $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G} + \mathbf{E}_{\mathsf{id}}$
  - use $\mathbf{T_B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $\mathbf{D}[\mathbf{I}_n|\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$, $\mathbf{x}_{\mathsf{id}} := \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} \approx \begin{bmatrix} D_{\mathbb{Z}^n, \theta_1} \\ D_{\mathbb{Z}^{2m}, \theta_2} \end{bmatrix}$

  - In the security proof, to answer the key queries, use $\mathbf{R}_{\mathsf{id}}$, $\mathbf{E}_{\mathsf{id}}$, $\mathbf{T_G}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t.

$$[\mathbf{I}_n|\mathbf{B}|\mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\boldsymbol{\kappa}, \mathsf{id})\mathbf{G} + \mathbf{E}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u} \text{ and } \mathbf{x}_{\mathsf{id}} := \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} \approx \begin{bmatrix} D_{\mathbb{Z}^n, \theta_1} \\ D_{\mathbb{Z}^{2m}, \theta_2} \end{bmatrix}, \text{ only } \theta_1 \geq \|\mathbf{E}_{\mathsf{id}}\|$$

Our New IBE Framework

Our framework:

- $\mathsf{Setup}(1^\lambda)$: $(\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{2n\times 2m}$ for $i \in [t]$, $\mathbf{D} \xleftarrow{\$} \mathbb{Z}_q^{n\times n}$

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \mathbf{D}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T_B}.$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\kappa, \mathsf{id})\mathbf{G} + \mathbf{E}_{\mathsf{id}}$
  - use $\mathbf{T_B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $\mathbf{D}[\mathbf{I}_n|\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$, $\mathbf{x}_{\mathsf{id}} := \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} \approx \begin{bmatrix} D_{\mathbb{Z}^n,\theta_1} \\ D_{\mathbb{Z}^{2m},\theta_2} \end{bmatrix}$, $\theta_1 \geq \|\mathbf{E}_{\mathsf{id}}\|$

$$\mathsf{pk}_{\mathsf{id}} := (\mathbf{D}[\mathbf{I}|\mathbf{B}|\mathbf{C}_{\mathsf{id}}], \mathbf{u}), \quad \mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}}.$$

- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mu)$: $\mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n$, $y_0 \leftarrow D_{\mathbb{Z},\delta}$, $\mathbf{w}_1 \leftarrow D_{\mathbb{Z}^n,\sigma_1}$, $\mathbf{w}_2 \leftarrow D_{\mathbb{Z}^{2m},\sigma_2}$, $\sigma_2 \geq \|\mathbf{E}_{\mathsf{id}^*}\|$

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top \cdot \mathbf{D}[\mathbf{I}|\mathbf{B}|\mathbf{C}_{\mathsf{id}}] + [\mathbf{w}_1^\top|\mathbf{w}_2^\top]\right).$$

- To simulate the challenge ciphertext,
  - use LWE sample $(\mathbf{u}, \mathbf{v}^\top\mathbf{u} + y_0)$ to generate c_0
  - use LWE samples $([\mathbf{DB}|\mathbf{D}], \mathbf{v}^\top[\mathbf{DB}|\mathbf{D}] + \mathbf{y}^\top)$, $\mathbf{R}_{\mathsf{id}^*}$, $\mathbf{E}_{\mathsf{id}^*}$ to generate $\mathbf{c}_1$ s.t. $\begin{bmatrix} \mathbf{w}_1 \\ \mathbf{w}_2 \end{bmatrix} \approx \begin{bmatrix} D_{\mathbb{Z}^n,\sigma_1} \\ D_{\mathbb{Z}^{2m},\sigma_2} \end{bmatrix}$

Our New IBE Framework

Our framework:

- $\mathsf{Setup}(1^\lambda) : (\mathbf{B}, \mathbf{T_B}) \leftarrow \mathsf{TrapGen}$, sample $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{C}_i \xleftarrow{\$} \mathbb{Z}_q^{2n\times 2m}$ for $i \in [t]$, $\mathbf{D} \xleftarrow{\$} \mathbb{Z}_q^{n\times n}$

$$\mathsf{mpk} := \left(\mathbf{B}, \mathbf{u}, \mathbf{D}, \{\mathbf{C}_i\}_{i\in[t]}\right), \quad \mathsf{msk} := \mathbf{T_B}.$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathsf{id})$:
  - homomorphically compute $\mathbf{C}_{\mathsf{id}}$ from $\{\mathbf{C}_i\}_{i\in[t]}$ and id $\quad \mathbf{C}_{\mathsf{id}} = \mathbf{B}\mathbf{R}_{\mathsf{id}} + F(\kappa, \mathsf{id})\mathbf{G} + \mathbf{E}_{\mathsf{id}}$
  - use $\mathbf{T_B}$ to sample a short $\mathbf{x}_{\mathsf{id}}$ s.t. $\mathbf{D}[\mathbf{I}_n|\mathbf{B}|\mathbf{C}_{\mathsf{id}}] \cdot \mathbf{x}_{\mathsf{id}} = \mathbf{u}$, $\mathbf{x}_{\mathsf{id}} := \begin{bmatrix}\mathbf{x}_1\\ \mathbf{x}_2\end{bmatrix} \approx \begin{bmatrix} D_{\mathbb{Z}^n,\theta_1}\\ D_{\mathbb{Z}^{2m},\theta_2}\end{bmatrix}$, $\theta_1 \geq \|\mathbf{E}_{\mathsf{id}}\|$

$$\mathsf{pk}_{\mathsf{id}} := (\mathbf{D}[\mathbf{I}|\mathbf{B}|\mathbf{C}_{\mathsf{id}}], \mathbf{u}), \quad \mathsf{sk}_{\mathsf{id}} := \mathbf{x}_{\mathsf{id}}.$$

- $\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}, \mu) : \mathbf{v} \xleftarrow{\$} \mathbb{Z}_q^n, y_0 \leftarrow D_{\mathbb{Z},\delta}, \mathbf{w}_1 \leftarrow D_{\mathbb{Z}^n,\sigma_1}, \mathbf{w}_2 \leftarrow D_{\mathbb{Z}^{2m},\sigma_2}, \sigma_2 \geq \|\mathbf{E}_{\mathsf{id}^*}\|$

$$\mathsf{ct} := \left(c_0 := \mathbf{v}^\top \mathbf{u} + y_0 + \lceil q/2 \rceil \cdot \mu, \quad \mathbf{c}_1^\top := \mathbf{v}^\top \cdot \mathbf{D}[\mathbf{I}|\mathbf{B}|\mathbf{C}_{\mathsf{id}}] + [\mathbf{w}_1^\top | \mathbf{w}_2^\top]\right).$$

- $\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})$: compute $c_0 - \mathbf{c}_1^\top \cdot \mathbf{x}_{\mathsf{id}} = \lceil \frac{q}{2} \rfloor \cdot \mu + \left(y_0 - \left\langle \begin{bmatrix}\mathbf{w}_1\\ \mathbf{w}_2\end{bmatrix}, \begin{bmatrix}\mathbf{x}_1\\ \mathbf{x}_2\end{bmatrix}\right\rangle\right)$

By cross multiplication, we successfully remove the quadratic restriction.

Our Results

Scheme	mpk	Modulus	Gaussian width of sk_{id}
[ALW+21]	$\omega(1)$	$\tilde{O}(n^{11.5})$	$\tilde{O}(n^5)$
[Abl24]	$\omega(\frac{\log \lambda}{\log \log \lambda})$	$\tilde{O}(n^{9.5})$	$\tilde{O}(n^{4.5})$

Table: Efficiency Improvement in Lattice-Based IBEs: Before and After Our Framework.

Our Results

Scheme	mpk	Modulus	Gaussian width of sk_{id}
[ALW+21]	$\omega(1)$	$\tilde{O}(n^{11.5}) \rightarrow \tilde{O}(n^{8})$	$\tilde{O}(n^{5}) \rightarrow \tilde{O}(n^{1.5})$
[Abl24]	$\omega(\frac{\log \lambda}{\log \log \lambda})$	$\tilde{O}(n^{9.5}) \rightarrow \tilde{O}(n^{7.5})$	$\tilde{O}(n^{4.5}) \rightarrow \tilde{O}(n^{1.5})$

Table: Efficiency Improvement in Lattice-Based IBEs: Before and After Our Framework.

Our Results

Scheme	mpk	Modulus	Gaussian width of $\mathsf{sk}_{\mathsf{id}}$
[ALW+21]	$\omega(1)$	$\tilde{O}(n^{11.5}) \to \tilde{O}(n^{8})$	$\tilde{O}(n^{5}) \to \tilde{O}(n^{1.5})$
[Abl24]	$\omega(\frac{\log\lambda}{\log\log\lambda})$	$\tilde{O}(n^{9.5}) \to \tilde{O}(n^{7.5})$	$\tilde{O}(n^{4.5}) \to \tilde{O}(n^{1.5})$

Table: Efficiency Improvement in Lattice-Based IBEs: Before and After Our Framework.

Our new IBE framework is general — it is not restricted to any specific partition function, nor limited to integer or ring settings.

In our paper, we apply our framework to the IBE in [ALW+21] to keep the asymptotically smallest mpk size.

Conclusion

In our work,

1. we propose two novel sampling algorithms to get hybrid secrets and errors;
2. we remove the restriction that the moduli of previous lattice IBE are quadratic in the trapdoor norm;
3. we propose a new lattice IBE framework which significantly reduces the modulus and the Gaussian width of $\mathsf{sk}_{\mathsf{id}}$.

Conclusion

In our work,

1. we propose two novel sampling algorithms to get hybrid secrets and errors;
2. we remove the restriction that the moduli of previous lattice IBE are quadratic in the trapdoor norm;
3. we propose a new lattice IBE framework which significantly reduces the modulus and the Gaussian width of $\mathsf{sk}_{\mathsf{id}}$.

https://eprint.iacr.org/2025/253

Conclusion

In our work,

1. we propose two novel sampling algorithms to get hybrid secrets and errors;
2. we remove the restriction that the moduli of previous lattice IBE are quadratic in the trapdoor norm;
3. we propose a new lattice IBE framework which significantly reduces the modulus and the Gaussian width of $\mathsf{sk}_{\mathsf{id}}$.

https://eprint.iacr.org/2025/253

Thank you! Q&A

References I

[ABB10] Shweta Agrawal, Dan Boneh, and Xavier Boyen. "Efficient Lattice (H)IBE in the Standard Model". In: *EUROCRYPT 2010*. Ed. by Henri Gilbert. Vol. 6110. LNCS. Springer, 2010, pp. 553–572. URL: https://doi.org/10.1007/978-3-642-13190-5_28.

[Abl24] Parhat Abla. "Identity-Based Encryption from LWE with More Compact Master Public Key". In: *CT-RSA 2024*. Ed. by Elisabeth Oswald. Vol. 14643. LNCS. Springer, 2024, pp. 319–353. URL: https://doi.org/10.1007/978-3-031-58868-6_13.

[ALW+21] Parhat Abla et al. "Ring-Based Identity Based Encryption - Asymptotically Shorter MPK and Tighter Security". In: *TCC 2021*. Ed. by Kobbi Nissim and Brent Waters. Vol. 13044. LNCS. Springer, 2021, pp. 157–187. URL: https://doi.org/10.1007/978-3-030-90456-2_6.

[Sha84] Adi Shamir. "Identity-Based Cryptosystems and Signature Schemes". In: *CRYPTO '84*. Ed. by G. R. Blakley and David Chaum. Vol. 196. LNCS. Springer, 1984, pp. 47–53. URL: https://doi.org/10.1007/3-540-39568-7_5.

References II

[Yam17] Shota Yamada. "Asymptotically Compact Adaptively Secure Lattice IBEs and Verifiable Random Functions via Generalized Partitioning Techniques". In: *CRYPTO 2017*. Ed. by Jonathan Katz and Hovav Shacham. Vol. 10403. LNCS. Springer, 2017, pp. 161–193. URL: https://doi.org/10.1007/978-3-319-63697-9_6.