Unbounded ABE for Circuits from LWE, Revisited

Valerio Cini, Hoeteck Wee

NTT Research
↓
Bocconi

NTT Research

Attribute-Based Encryption [SW05,GPSW06]

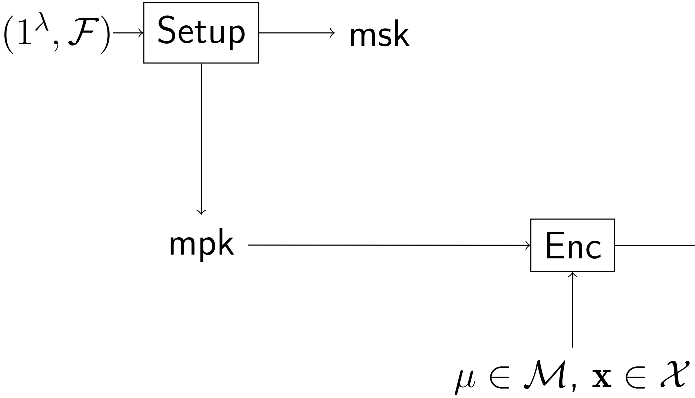
Attribute-Based Encryption [SW05,GPSW06]

$(1^\lambda, \mathcal{F}) \longrightarrow \boxed{\text{Setup}}$

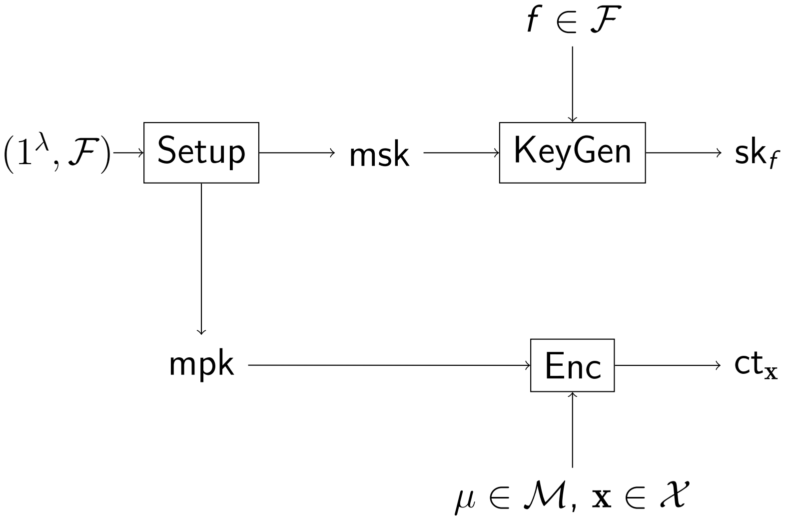
Attribute-Based Encryption [SW05,GPSW06]

$$
\begin{tikzcd}
(1^\lambda, \mathcal{F}) \arrow[r] & \boxed{\mathsf{Setup}} \arrow[r] \arrow[d] & \mathsf{msk} \\
 & \mathsf{mpk} &
\end{tikzcd}
$$

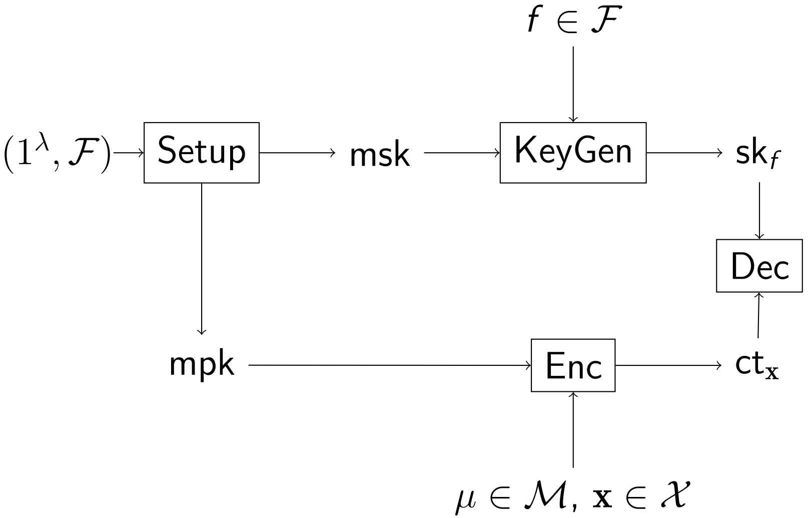
Attribute-Based Encryption [SW05,GPSW06]



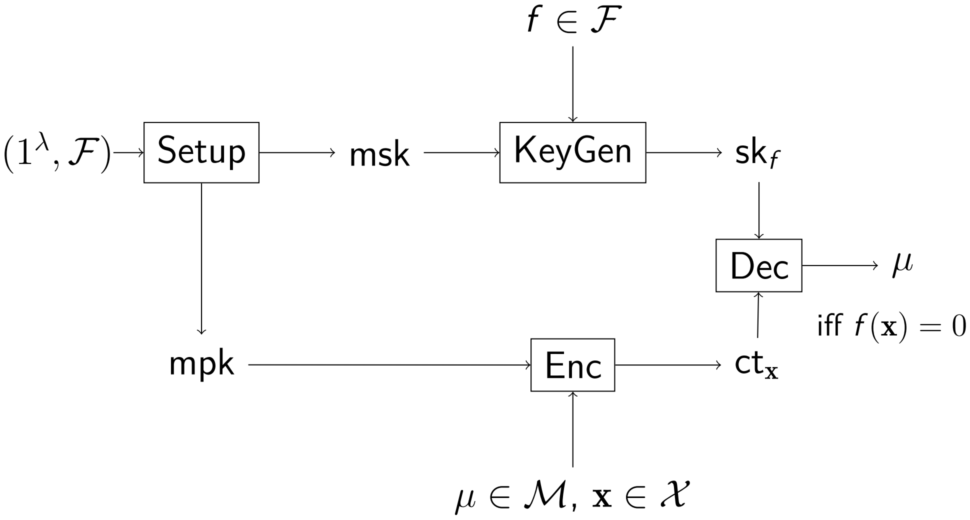
Attribute-Based Encryption [SW05,GPSW06]



Attribute-Based Encryption [SW05,GPSW06]



Attribute-Based Encryption [SW05,GPSW06]



Attribute-Based Encryption [SW05,GPSW06]

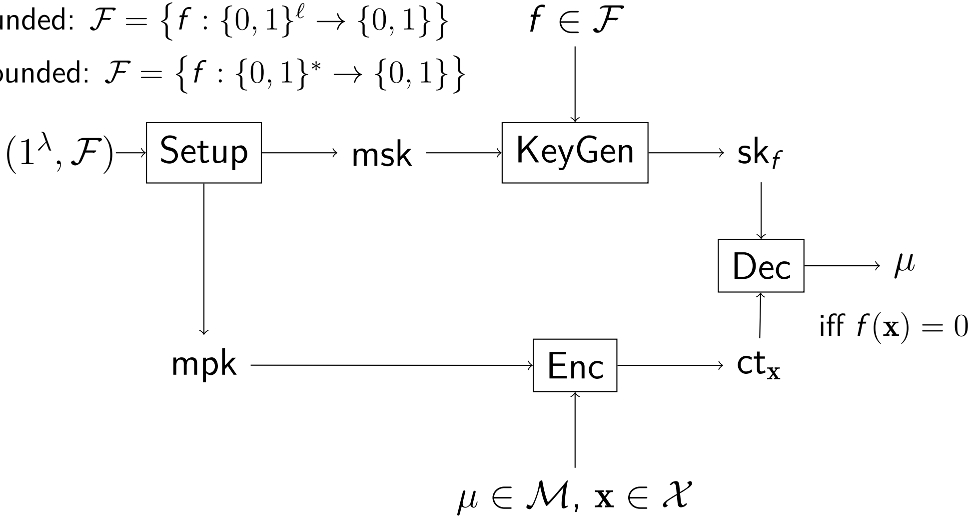
bounded: $\mathcal{F} = \left\{ f : \{0,1\}^\ell \to \{0,1\} \right\}$

$$
\begin{tikzcd}
 & & & f \in \mathcal{F} \arrow[d] & & \\
(1^\lambda, \mathcal{F}) \arrow[r] & \boxed{\mathsf{Setup}} \arrow[r] \arrow[dd] & \mathsf{msk} \arrow[r] & \boxed{\mathsf{KeyGen}} \arrow[r] & \mathsf{sk}_f \arrow[d] & \\
 & & & & \boxed{\mathsf{Dec}} \arrow[r] & \mu \\
 & \mathsf{mpk} \arrow[rr] & & \boxed{\mathsf{Enc}} \arrow[r] & \mathsf{ct}_{\mathbf{x}} \arrow[u] & \text{iff } f(\mathbf{x}) = 0 \\
 & & & \mu \in \mathcal{M},\ \mathbf{x} \in \mathcal{X} \arrow[u] & &
\end{tikzcd}
$$

Attribute-Based Encryption [SW05,GPSW06]

bounded: $\mathcal{F} = \left\{ f : \{0,1\}^\ell \to \{0,1\} \right\}$

unbounded: $\mathcal{F} = \left\{ f : \{0,1\}^* \to \{0,1\} \right\}$



State-of-the-Art

	Black-Box	Unbounded

State-of-the-Art

	Black-Box	Unbounded
[BonehGentryGorbunovHaleviNikolaenkoSegevVaikuntanathanVinayagamurthy14]		

State-of-the-Art

	Black-Box	Unbounded
[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14]	✓	✗

State-of-the-Art

	Black-Box	Unbounded
[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14]	✓	✗
[BrakerskiVaikuntanathan16]		
[GoyalKoppulaWaters16]		

State-of-the-Art

	Black-Box	Unbounded
[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14]	✓	✗
[BrakerskiVaikuntanathan16]	✗	✓
[GoyalKoppulaWaters16]	✗	✓

State-of-the-Art

	Black-Box	Unbounded
[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14]	✓	✗
[BrakerskiVaikuntanathan16]	✗	✓
[GoyalKoppulaWaters16]	✗	✓
this work	✓	✓

State-of-the-Art

	Black-Box	Unbounded
[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14]	✓	✗
[BrakerskiVaikuntanathan16]	✗	✓
[GoyalKoppulaWaters16]	✗	✓
this work	✓	✓

Why?

State-of-the-Art

	Black-Box	Unbounded
[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14]	✓	✗
[BrakerskiVaikuntanathan16]	✗	✓
[GoyalKoppulaWaters16]	✗	✓
this work	✓	✓

Why?

- No efficiency overhead or implementation hurdles

State-of-the-Art

	Black-Box	Unbounded
[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14]	✓	✗
[BrakerskiVaikuntanathan16]	✗	✓
[GoyalKoppulaWaters16]	✗	✓
this work	✓	✓

Why?

- No efficiency overhead or implementation hurdles
- Forces us to develop new ideas. May be independently useful.

State-of-the-Art

	Black-Box	Unbounded
[BonehGentryGorbunovHaleviNikolaenko SegevVaikuntanathanVinayagamurthy14]	✓	✗
[BrakerskiVaikuntanathan16]	✗	✓
[GoyalKoppulaWaters16]	✗	✓
this work	✓	✓

Why?

- No efficiency overhead or implementation hurdles
- Forces us to develop new ideas. May be independently useful.

[GKPVZ13,GVW15,GVW15,BV15,QWW18,PS19,CJJ21,...]

LWE = Learning With Errors

LWE = Learning With Errors

$\mathbf{B}$

LWE = Learning With Errors

$$\mathbf{B}, \quad \mathbf{s} \cdot \mathbf{B} + \mathbf{e}$$

LWE = Learning With Errors

$$\mathbf{B}, \quad \mathbf{s} \cdot \mathbf{B} + \mathbf{e}$$

$$\text{[Regev05]} : \quad \mathbf{s} \leftarrow \mathbb{Z}_q^n, \quad \mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}, \quad \mathbf{e} \leftarrow \chi^m$$

[BGGHNSVV14] and Attribute Dependency

$\overbrace{\boxed{\quad\quad\mathbf{A}\quad\quad}}^{\mathsf{mpk}}$ $\overbrace{\boxed{\mathbf{A}_f}}^{\mathsf{sk}_f}$

[BGGHNSVV14] and Attribute Dependency

$$\underbrace{\mathbf{s}\cdot\Big(\overbrace{\boxed{\quad\mathbf{A}\quad}}^{\textsf{mpk}} - \mathbf{x}\otimes\mathbf{G}\Big)+\mathbf{e}}_{\textsf{ct}}$$

$$\overbrace{\boxed{\mathbf{A}_f}}^{\textsf{sk}_f}$$

[BGGHNSVV14] and Attribute Dependency

$$\underbrace{\left(\mathbf{s}\cdot\left(\overbrace{\boxed{\quad\mathbf{A}\quad}}^{\mathsf{mpk}} - \mathbf{x}\otimes\mathbf{G}\right) + \mathbf{e}\right)}_{\mathsf{ct}} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}} \approx \underbrace{\mathbf{s}\cdot\left(\overbrace{\boxed{\mathbf{A}_f}}^{\mathsf{sk}_f} - f(\mathbf{x})\cdot\mathbf{G}\right)}_{\mathsf{Dec}}$$

[BGGHNSVV14] and Attribute Dependency

1. mpk : $\boxed{\mathbf{A}_0} \in \mathbb{Z}_q^{n \times m}, \boxed{\quad\mathbf{A}\quad} \in \mathbb{Z}_q^{n \times \ell m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n$, msk : $\mathbf{T}_{\mathbf{A}_0}$,

$$\underbrace{\left(\mathbf{s} \cdot \left(\overbrace{\boxed{\quad\mathbf{A}\quad}}^{\mathsf{mpk}} - \mathbf{x} \otimes \mathbf{G} \right) + \mathbf{e} \right)}_{\mathsf{ct}} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}} \approx \underbrace{\mathbf{s} \cdot \left(\overbrace{\boxed{\mathbf{A}_f}}^{\mathsf{sk}_f} - f(\mathbf{x}) \cdot \mathbf{G} \right)}_{\mathsf{Dec}}$$

[BGGHNSVV14] and Attribute Dependency

1. mpk : $\boxed{\mathbf{A}_0} \in \mathbb{Z}_q^{n\times m}$, $\boxed{\quad\mathbf{A}\quad} \in \mathbb{Z}_q^{n\times \ell m}$, $\boxed{\mathbf{b}} \in \mathbb{Z}_q^{n}$, msk : $\mathbf{T}_{\mathbf{A}_0}$,

2. ct :

$\boxed{\text{w/o error terms}}$

$$\underbrace{\left(\mathbf{s}\cdot\Big(\overbrace{\boxed{\quad\mathbf{A}\quad}}^{\mathsf{mpk}} - \mathbf{x}\otimes\mathbf{G}\Big)+\mathbf{e}\right)}_{\mathsf{ct}}\cdot\mathbf{H}_{\mathbf{A},f,\mathbf{x}} \approx \underbrace{\mathbf{s}\cdot\Big(\overbrace{\boxed{\mathbf{A}_f}}^{\mathsf{sk}_f} - f(\mathbf{x})\cdot\mathbf{G}\Big)}_{\mathsf{Dec}}$$

[BGGHNSVV14] and Attribute Dependency

1. mpk : $\boxed{\mathbf{A}_0} \in \mathbb{Z}_q^{n\times m}, \boxed{\quad \mathbf{A} \quad} \in \mathbb{Z}_q^{n\times \ell m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n,$ msk : $\mathbf{T}_{\mathbf{A}_0}$,
2. ct : $\mathbf{s}\cdot\mathbf{A}_0, \quad \mathbf{s}\cdot(\mathbf{A} - \mathbf{x}\otimes\mathbf{G}) \quad , \quad \mathbf{s}\cdot\mathbf{b}^\top + \mu\cdot\lfloor q/2\rfloor$ $\boxed{\text{w/o error terms}}$

$$\underbrace{\left(\mathbf{s}\cdot\Big(\overbrace{\boxed{\quad \mathbf{A} \quad}}^{\text{mpk}} - \mathbf{x}\otimes\mathbf{G}\Big) + \mathbf{e}\right)}_{\text{ct}} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}} \approx \underbrace{\mathbf{s}\cdot\Big(\overbrace{\boxed{\mathbf{A}_f}}^{\text{sk}_f} - f(\mathbf{x})\cdot\mathbf{G}\Big)}_{\text{Dec}}$$

[BGGHNSVV14] and Attribute Dependency

1. mpk : $\boxed{\mathbf{A}_0} \in \mathbb{Z}_q^{n\times m}, \boxed{\quad \mathbf{A} \quad} \in \mathbb{Z}_q^{n\times \ell m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n$, msk : $\mathbf{T}_{\mathbf{A}_0}$,

2. ct : $\mathbf{s}\cdot\mathbf{A}_0, \quad \mathbf{s}\cdot(\mathbf{A} - \mathbf{x}\otimes\mathbf{G}) \quad , \quad \mathbf{s}\cdot\mathbf{b}^\top + \mu\cdot\lfloor q/2 \rceil$

3. sk$_f$: $\mathbf{k}_f^\top \leftarrow \left[\mathbf{A}_0 \mid\mid \mathbf{A}_f\right]^{-1}(\mathbf{b}^\top)$

$$\underbrace{\left(\mathbf{s}\cdot\Big(\overbrace{\boxed{\quad \mathbf{A} \quad}}^{\text{mpk}} - \mathbf{x}\otimes\mathbf{G}\Big) + \mathbf{e}\right)}_{\text{ct}} \cdot \mathbf{H}_{\mathbf{A},f,\mathbf{x}} \approx \underbrace{\mathbf{s}\cdot\Big(\overbrace{\boxed{\mathbf{A}_f}}^{\text{sk}_f} - f(\mathbf{x})\cdot\mathbf{G}\Big)}_{\text{Dec}}$$

[BGGHNSVV14] and Attribute Dependency

1. mpk : $\boxed{\mathbf{A}_0} \in \mathbb{Z}_q^{n\times m}$, $\boxed{\quad\mathbf{A}\quad} \in \mathbb{Z}_q^{n\times \ell m}$, $\boxed{\mathbf{b}} \in \mathbb{Z}_q^{n}$, msk : $\mathbf{T}_{\mathbf{A}_0}$,
2. ct : $\mathbf{s}\cdot\mathbf{A}_0$, $\mathbf{s}\cdot(\mathbf{A} - \mathbf{x}\otimes\mathbf{G})$, $\mathbf{s}\cdot\mathbf{b}^\top + \mu\cdot\lfloor q/2 \rfloor$
3. sk$_f$: $\mathbf{k}_f^\top \leftarrow \left[\mathbf{A}_0 \,||\, \mathbf{A}_f\right]^{-1}(\mathbf{b}^\top)$ (i.e. $\left[\mathbf{A}_0 \,||\, \mathbf{A}_f\right]\cdot\mathbf{k}_f^\top = \mathbf{b}^\top$)

$$\Bigg(\underbrace{\mathbf{s}\cdot\Big(\overbrace{\boxed{\quad\mathbf{A}\quad}}^{\mathsf{mpk}} - \mathbf{x}\otimes\mathbf{G}\Big) + \mathbf{e}}_{\mathsf{ct}}\Bigg)\cdot\mathbf{H}_{\mathbf{A},f,\mathbf{x}} \approx \underbrace{\mathbf{s}\cdot\Big(\overbrace{\boxed{\mathbf{A}_f}}^{\mathsf{sk}_f} - f(\mathbf{x})\cdot\mathbf{G}\Big)}_{\mathsf{Dec}}$$

[BGGHNSVV14] and Attribute Dependency

1. mpk : $\boxed{\mathbf{A}_0} \in \mathbb{Z}_q^{n\times m}, \boxed{\mathbf{A}} \in \mathbb{Z}_q^{n\times \ell m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^{n},$ msk : $\mathbf{T}_{\mathbf{A}_0},$
2. ct : $\mathbf{s}\cdot\mathbf{A}_0, \quad \mathbf{s}\cdot(\mathbf{A}_f - f(\mathbf{x})\cdot\mathbf{G}), \quad \mathbf{s}\cdot\mathbf{b}^\top + \mu\cdot\lfloor q/2 \rfloor$
3. sk$_f$: $\mathbf{k}_f^\top \leftarrow [\mathbf{A}_0 \,||\, \mathbf{A}_f]^{-1}(\mathbf{b}^\top)$ (i.e. $[\mathbf{A}_0 \,||\, \mathbf{A}_f]\cdot\mathbf{k}_f^\top = \mathbf{b}^\top$)

$$\underbrace{\Big(\mathbf{s}\cdot\big(\overbrace{\boxed{\mathbf{A}}}^{\text{mpk}} - \mathbf{x}\otimes\mathbf{G}\big) + \mathbf{e}}_{\text{ct}}\Big)\cdot\mathbf{H}_{\mathbf{A},f,\mathbf{x}} \approx \underbrace{\mathbf{s}\cdot\big(\overbrace{\boxed{\mathbf{A}_f}}^{\text{sk}_f} - f(\mathbf{x})\cdot\mathbf{G}\big)}_{\text{Dec}}$$

[BGGHNSVV14] and Attribute Dependency

1. mpk : $\boxed{\mathbf{A}_0} \in \mathbb{Z}_q^{n\times m}, \boxed{\quad\quad\mathbf{A}\quad\quad} \in \mathbb{Z}_q^{n\times \ell m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^{n}$, msk : $\mathbf{T}_{\mathbf{A}_0}$,
2. ct : $\mathbf{s}\cdot\mathbf{A}_0, \quad \mathbf{s}\cdot(\mathbf{A}_f - f(\mathbf{x})\cdot\mathbf{G}), \quad \mathbf{s}\cdot\mathbf{b}^\top + \mu\cdot\lfloor q/2 \rfloor$
3. sk$_f$: $\mathbf{k}_f^\top \leftarrow \left[\mathbf{A}_0 \mid\mid \mathbf{A}_f\right]^{-1}(\mathbf{b}^\top) \quad$ (i.e. $\left[\mathbf{A}_0 \mid\mid \mathbf{A}_f\right]\cdot\mathbf{k}_f^\top = \mathbf{b}^\top$)

Problem:

$\boxed{\quad\quad\mathbf{A}\quad\quad} = \left[\mathbf{A}_1 \mid\mid \ldots \mid\mid \mathbf{A}_\ell\right]$ as long as $\mathbf{x} = \left[x_1 \mid\mid \ldots \mid\mid x_\ell\right]$

[BGGHNSVV14] and Attribute Dependency

1. mpk : $\boxed{\mathbf{A}_0} \in \mathbb{Z}_q^{n\times m}$, $\boxed{\quad\mathbf{A}\quad} \in \mathbb{Z}_q^{n\times \ell m}$, $\boxed{\mathbf{b}} \in \mathbb{Z}_q^n$, msk : $\mathbf{T}_{\mathbf{A}_0}$,
2. ct : $\mathbf{s}\cdot\mathbf{A}_0$, $\mathbf{s}\cdot(\mathbf{A}_f - f(\mathbf{x})\cdot\mathbf{G})$, $\mathbf{s}\cdot\mathbf{b}^\top + \mu\cdot\lfloor q/2\rfloor$
3. sk$_f$: $\mathbf{k}_f^\top \leftarrow \left[\mathbf{A}_0 \mid\mid \mathbf{A}_f\right]^{-1}(\mathbf{b}^\top)$ (i.e. $\left[\mathbf{A}_0 \mid\mid \mathbf{A}_f\right]\cdot\mathbf{k}_f^\top = \mathbf{b}^\top$)

Problem:

$\boxed{\quad\mathbf{A}\quad} = \left[\mathbf{A}_1 \mid\mid \ldots \mid\mid \mathbf{A}_\ell\right]$ as long as $\mathbf{x} = \left[x_1 \mid\mid \ldots \mid\mid x_\ell\right]$

<u>want to “compress” mpk</u>

Compressing mpk

Main Idea : – delay sampling $\mathbf{A}_i$'s from setup to key-generation

– use sk_f, ct to compute $\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$ during decryption

Compressing mpk

Main Idea : – delay sampling $\mathbf{A}_i$'s from setup to key-generation

– use sk_f, ct to compute $\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$ during decryption

Warm-up:

1. mpk : $\boxed{\mathbf{A}_0}$, $\in \mathbb{Z}_q^{n \times m}$, $\boxed{\mathbf{b}} \in \mathbb{Z}_q^n$, msk : $\mathbf{T}_{\mathbf{A}_0}$,

Compressing mpk

Main Idea : – delay sampling $\mathbf{A}_i$'s from setup to key-generation

– use sk_f, ct to compute $\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$ during decryption

Warm-up:

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n \times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n,$ msk : $\mathbf{T}_{\mathbf{A}_0}, \mathbf{T}_{\mathbf{B}_0}$

Compressing mpk

Main Idea : – delay sampling $\mathbf{A}_i$'s from setup to key-generation
– use sk_f, ct to compute $\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$ during decryption

Warm-up:

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n \times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n$, msk : $\mathbf{T}_{\mathbf{A}_0}, \mathbf{T}_{\mathbf{B}_0}$
2. ct : replace $\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$ with

Compressing mpk

Main Idea : – delay sampling $\mathbf{A}_i$'s from setup to key-generation
– use sk_f, ct to compute $\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$ during decryption

Warm-up:

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n \times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n$, msk : $\mathbf{T}_{\mathbf{A}_0}, \mathbf{T}_{\mathbf{B}_0}$
2. ct : replace $\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$ with

$$\mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}$$

Compressing mpk

Main Idea : – delay sampling $\mathbf{A}_i$'s from setup to key-generation

– use sk_f, ct to compute $\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$ during decryption

Warm-up:

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n \times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n$, msk : $\mathbf{T}_{\mathbf{A}_0}, \mathbf{T}_{\mathbf{B}_0}$
2. ct : replace $\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$ with
$$\mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}$$
3. sk_f : add $\left\{ \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W}\right]^{-1}(\mathbf{V}) \right\}_{i \in [\ell]}$

Compressing mpk

Main Idea : – delay sampling $\mathbf{A}_i$'s from setup to key-generation

– use sk_f, ct to compute $\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$ during decryption

Warm-up:

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n \times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n,$ msk : $\mathbf{T}_{\mathbf{A}_0}, \mathbf{T}_{\mathbf{B}_0}$

2. ct : replace $\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$ with

$$\mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}$$

3. sk_f : add $\left\{ \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W}\right]^{-1}(\mathbf{V}) \right\}_{i \in [\ell]}$ and set $\mathbf{A}_i := \mathbf{G} \cdot \mathbf{R}_i$

Correctness

$$\underbrace{\mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}}_{\text{ciphertext}}, \qquad \underbrace{\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow [\mathbf{B}_0 \mid\mid \mathbf{W}]^{-1}(\mathbf{V})}_{\text{key}}$$

Correctness

$$\underbrace{\mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}}_{\text{ciphertext}}, \qquad \underbrace{\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W}\right]^{-1}(\mathbf{V})}_{\text{key}}$$

During decryption compute

$$\underbrace{\left[\mathbf{s}_i \cdot \mathbf{B}_0 \mid\mid \mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}\right] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}}_{\mathbf{s}_i \cdot \mathbf{V} + \mathbf{s} \cdot \mathbf{G} \cdot \mathbf{R}_i} - (\mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G})$$

Correctness

$$\underbrace{\mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}}_{\text{ciphertext}}, \qquad \underbrace{\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W}\right]^{-1}(\mathbf{V})}_{\text{key}}$$

During decryption compute

$$\underbrace{\left[\mathbf{s}_i \cdot \mathbf{B}_0 \mid\mid \mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}\right] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}}_{\mathbf{s}_i \cdot \mathbf{V} + \mathbf{s} \cdot \mathbf{A}_i} - (\mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G})$$

Correctness

$$\underbrace{\mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G},}_{\text{ciphertext}} \qquad \underbrace{\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W}\right]^{-1}(\mathbf{V})}_{\text{key}}$$

During decryption compute

$$\underbrace{\left[\mathbf{s}_i \cdot \mathbf{B}_0 \mid\mid \mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}\right] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}}_{\mathbf{s}_i \cdot \mathbf{V} + \mathbf{s} \cdot \mathbf{A}_i} - (\mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}) = \mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$$

Correctness

$$\underbrace{\mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}}_{\text{ciphertext}}, \qquad \underbrace{\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W}\right]^{-1}(\mathbf{V})}_{\text{key}}$$

During decryption compute

$$\underbrace{\left[\mathbf{s}_i \cdot \mathbf{B}_0 \mid\mid \mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}\right] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}}_{\mathbf{s}_i \cdot \mathbf{V} + \mathbf{s} \cdot \mathbf{A}_i} - (\mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}) = \mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$$

Run [BGGHNSVV14] decryption

Security?

- key $\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$ not "bounded" to index i:

Security?

- key $\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$ not "bounded" to index i: $\quad \mathbf{s} \cdot (\mathbf{A}_i - x_j \cdot \mathbf{G})$ for $j \neq i$

Security?

- key $\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$ not "bounded" to index i: $\mathbf{s} \cdot (\mathbf{A}_i - x_j \cdot \mathbf{G})$ for $j \neq i$

  $\mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G}$

  $$\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W}\right]^{-1} (\mathbf{V})$$

Security?

- key $\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$ not "bounded" to index i: $\quad \mathbf{s} \cdot (\mathbf{A}_i - x_j \cdot \mathbf{G})$ for $j \neq i$

$$\mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G} \qquad \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W} \right]^{-1} (\mathbf{V})$$

replaced with

Security?

- key $\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$ not "bounded" to index i: $\quad \mathbf{s} \cdot (\mathbf{A}_i - x_j \cdot \mathbf{G})$ for $j \neq i$

$$\mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G} \qquad\qquad \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W}\right]^{-1}(\mathbf{V})$$

replaced with

$$\mathbf{s}_i \cdot (\mathbf{W} + i \cdot \mathbf{G}) + \mathbf{s} \cdot \mathbf{G}$$

Security?

- key $\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$ not "bounded" to index i: $\quad \mathbf{s} \cdot (\mathbf{A}_i - x_j \cdot \mathbf{G})$ for $j \neq i$

$$\mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G} \qquad \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W}\right]^{-1}(\mathbf{V})$$

replaced with

$$\mathbf{s}_i \cdot (\mathbf{W} + i \cdot \mathbf{G}) + \mathbf{s} \cdot \mathbf{G} \qquad \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W} + i \cdot \mathbf{G}\right]^{-1}(\mathbf{V})$$

Security?

- key $\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$ not "bounded" to index i: $\mathbf{s} \cdot (\mathbf{A}_i - x_j \cdot \mathbf{G})$ for $j \neq i$

$$\mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G} \qquad \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \,||\, \mathbf{W}\right]^{-1}(\mathbf{V})$$

replaced with

$$\mathbf{s}_i \cdot (\mathbf{W} + i \cdot \mathbf{G}) + \mathbf{s} \cdot \mathbf{G} \qquad \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \,||\, \mathbf{W} + i \cdot \mathbf{G}\right]^{-1}(\mathbf{V})$$

- define unique $\mathbf{A}_i$ across secret keys queries:

Security?

- key $\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$ not "bounded" to index i: $\mathbf{s} \cdot (\mathbf{A}_i - x_j \cdot \mathbf{G})$ for $j \neq i$

$$\mathbf{s}_i \cdot \mathbf{W} + \mathbf{s} \cdot \mathbf{G} \qquad \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W}\right]^{-1}(\mathbf{V})$$

replaced with

$$\mathbf{s}_i \cdot (\mathbf{W} + i \cdot \mathbf{G}) + \mathbf{s} \cdot \mathbf{G} \qquad \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W} + i \cdot \mathbf{G}\right]^{-1}(\mathbf{V})$$

- define unique $\mathbf{A}_i$ across secret keys queries: add a PRF key to msk

Construction Summary

Construction Summary

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n \times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n,$

Construction Summary

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n\times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n,$ msk : $\mathbf{T}_{\mathbf{A}_0}, \mathbf{T}_{\mathbf{B}_0}, \mathsf{k}$

Construction Summary

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n \times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n,$ msk : $\mathbf{T}_{\mathbf{A}_0}, \mathbf{T}_{\mathbf{B}_0}$, k
2. ct : $\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$

$$\left\{ \mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot (\mathbf{W} + i \cdot \mathbf{G}) + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G} \right\}_{i \in [\ell]}$$

Construction Summary

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n \times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n,$ msk : $\mathbf{T}_{\mathbf{A}_0}, \mathbf{T}_{\mathbf{B}_0}, \mathsf{k}$
2. ct : $\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$

$$\left\{\mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot (\mathbf{W} + i \cdot \mathbf{G}) + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}\right\}_{i \in [\ell]}$$

3. sk_f : $\left\{ \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W} + i \cdot \mathbf{G}\right]^{-1}(\mathbf{V}) \right\}_{i \in [\ell]}$ (randomness PRF(k, i))

Construction Summary

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n\times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n,$ msk : $\mathbf{T}_{\mathbf{A}_0}, \mathbf{T}_{\mathbf{B}_0}, \mathsf{k}$

2. ct : $$\mathbf{s}\cdot\mathbf{A}_0, \quad \mathbf{s}\cdot\mathbf{b}^\top + \mu\cdot\lfloor q/2\rfloor$$
$$\left\{\mathbf{s}_i\cdot\mathbf{B}_0, \quad \mathbf{s}_i\cdot(\mathbf{W}+i\cdot\mathbf{G})+\mathbf{s}\cdot\mathbf{G}, \quad \mathbf{s}_i\cdot\mathbf{V}+x_i\cdot\mathbf{s}\cdot\mathbf{G}\right\}_{i\in[\ell]}$$

3. sk_f : $\left\{\begin{bmatrix}\mathbf{Z}_i\\ \mathbf{R}_i\end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W}+i\cdot\mathbf{G}\right]^{-1}(\mathbf{V})\right\}_{i\in[\ell]}$ (randomness PRF(k, i))
$$\mathbf{k}_f^\top \leftarrow \left[\mathbf{A}_0 \mid\mid \mathbf{A}_f\right]^{-1}(\mathbf{b}^\top) \quad (\text{where } \mathbf{A}_i = \mathbf{G}\cdot\mathbf{R}_i)$$

Construction Summary

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n \times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n,$ msk : $\mathbf{T}_{\mathbf{A}_0}, \mathbf{T}_{\mathbf{B}_0}, \mathsf{k}$

2. ct : $\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$

$$\left\{ \mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot (\mathbf{W} + i \cdot \mathbf{G}) + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G} \right\}_{i \in [\ell]}$$

3. sk_f : $\left\{ \cancel{\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \mathbf{W} + i \cdot \mathbf{G} \right]^{-1}} (\mathbf{V}) \right\}_{i \in [\ell]}$ (randomness $\mathsf{PRF}(\mathsf{k}, i)$)

$$\mathbf{k}_f^\top \leftarrow \left[\mathbf{A}_0 \mid\mid \mathbf{A}_f \right]^{-1} (\mathbf{b}^\top) \quad \text{(where } \mathbf{A}_i = \mathbf{G} \cdot \mathbf{R}_i\text{)}$$

Construction Summary

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n \times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n,$ msk : $\mathbf{T}_{\mathbf{A}_0}, \mathbf{T}_{\mathbf{B}_0}, \mathsf{k}$

2. ct : $\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$

$$\{\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})\}_{i \in [\ell]}$$

3. sk$_f$: $\cancel{\left\{ \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \,||\, \mathbf{W} + i \cdot \mathbf{G}\right]^{-1}(\mathbf{V}) \right\}_{i \in [\ell]}}$ (randomness PRF(k, i))

$$\mathbf{k}_f^\top \leftarrow \left[\mathbf{A}_0 \,||\, \mathbf{A}_f\right]^{-1}(\mathbf{b}^\top) \quad (\text{where } \mathbf{A}_i = \mathbf{G} \cdot \mathbf{R}_i)$$

Construction Summary

1. mpk : $\boxed{\mathbf{A}_0}, \boxed{\mathbf{B}_0}, \boxed{\mathbf{W}}, \boxed{\mathbf{V}} \in \mathbb{Z}_q^{n \times m}, \boxed{\mathbf{b}} \in \mathbb{Z}_q^n,$ msk : $\mathbf{T}_{\mathbf{A}_0}, \mathbf{T}_{\mathbf{B}_0}$, k

2. ct : $\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rceil$

$$\{\mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})\}_{i \in [\ell]} = \mathbf{s} \cdot (\mathbf{A} - \mathbf{x} \otimes \mathbf{G})$$

3. sk$_f$: $\cancel{\left\{ \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \,||\, \mathbf{W} + i \cdot \mathbf{G}\right]^{-1}(\mathbf{V}) \right\}_{i \in [\ell]}}$ (randomness PRF(k, i))

$$\mathbf{k}_f^\top \leftarrow \left[\mathbf{A}_0 \,||\, \mathbf{A}_f\right]^{-1}(\mathbf{b}^\top) \quad \text{(where } \mathbf{A}_i = \mathbf{G} \cdot \mathbf{R}_i\text{)}$$

Security Proof

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\left\{ \mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot (\mathbf{W} + i \cdot \mathbf{G}) + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G} \right\}_{i \in [\ell]}$$

Security Proof

- Hybrids over $i \in [\ell]$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\left\{ \mathbf{s}_i \cdot \mathbf{B}_0, \quad \mathbf{s}_i \cdot (\mathbf{W} + i \cdot \mathbf{G}) + \mathbf{s} \cdot \mathbf{G}, \quad \mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G} \right\}_{i \in [\ell]}$$

Security Proof

- Hybrids over $i \in [\ell]$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\mathbf{s}_i \cdot \mathbf{B}_0, \qquad \mathbf{s}_i \cdot (\mathbf{W} + i \cdot \mathbf{G}) + \mathbf{s} \cdot \mathbf{G}$$

$$\mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}$$

Security Proof

- Hybrids over $i \in [\ell]$ $\qquad \mathbf{W} = \mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i - i \cdot \mathbf{G} \qquad (\tilde{\mathbf{W}}_i \leftarrow \chi^{m \times m})$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rceil$$

$$\mathbf{s}_i \cdot \mathbf{B}_0, \qquad \mathbf{s}_i \cdot (\mathbf{W} + i \cdot \mathbf{G}) + \mathbf{s} \cdot \mathbf{G}$$

$$\mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}$$

Security Proof

- Hybrids over $i \in [\ell]$ $\qquad \mathbf{W} = \mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i - i \cdot \mathbf{G} \qquad (\tilde{\mathbf{W}}_i \leftarrow \chi^{m \times m})$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\mathbf{s}_i \cdot \mathbf{B}_0, \qquad \mathbf{s}_i \cdot \mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + \mathbf{s} \cdot \mathbf{G}$$

$$\mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}$$

Security Proof

- Hybrids over $i \in [\ell]$ $\qquad \mathbf{W} = \mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i - i \cdot \mathbf{G} \qquad (\tilde{\mathbf{W}}_i \leftarrow \chi^{m \times m})$

$$\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \chi^{2m \times m},$$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\mathbf{s}_i \cdot \mathbf{B}_0, \qquad \mathbf{s}_i \cdot \mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + \mathbf{s} \cdot \mathbf{G}$$

$$\mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}$$

Security Proof

- Hybrids over $i \in [\ell]$ $\quad \mathbf{V} := \left[\mathbf{B}_0 \mid\mid \underbrace{\mathbf{W} + i \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i}\right] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$

$$\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \chi^{2m \times m},$$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\mathbf{s}_i \cdot \mathbf{B}_0, \qquad \mathbf{s}_i \cdot \mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + \mathbf{s} \cdot \mathbf{G}$$

$$\mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}$$

Security Proof

- Hybrids over $i \in [\ell]$ $\qquad \mathbf{V} := \left[\mathbf{B}_0 \mid\mid \underbrace{\mathbf{W} + i \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i}\right] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$

$$\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \chi^{2m \times m}, \quad \begin{bmatrix} \mathbf{Z}_j \\ \mathbf{R}_j \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \underbrace{\mathbf{W} + j \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + (j-i) \cdot \mathbf{G}}\right]^{-1}(\mathbf{V}) \quad (j \neq i)$$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\mathbf{s}_i \cdot \mathbf{B}_0, \qquad \mathbf{s}_i \cdot \mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + \mathbf{s} \cdot \mathbf{G}$$

$$\mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}$$

Security Proof

- Hybrids over $i \in [\ell]$ $\quad \mathbf{V} := [\mathbf{B}_0 \,||\, \underbrace{\mathbf{W} + i \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i}] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$

$$\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \chi^{2m \times m}, \quad \begin{bmatrix} \mathbf{Z}_j \\ \mathbf{R}_j \end{bmatrix} \leftarrow [\mathbf{B}_0 \,||\, \underbrace{\mathbf{W} + j \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + (j-i) \cdot \mathbf{G}}]^{-1}(\mathbf{V}) \quad (j \neq i)$$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\underbrace{\mathbf{s}_i \cdot \mathbf{B}_0}_{\mathbf{c}_{1,i}}, \qquad \underbrace{\mathbf{s}_i \cdot \mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + \mathbf{s} \cdot \mathbf{G}}_{\mathbf{c}_{2,i}}$$

$$\mathbf{s}_i \cdot \mathbf{V} + x_i \cdot \mathbf{s} \cdot \mathbf{G}$$

Security Proof

- Hybrids over $i \in [\ell]$ $\qquad \mathbf{V} := [\mathbf{B}_0 \mid\mid \underbrace{\mathbf{W} + i \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i}] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$

$$\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \chi^{2m \times m}, \begin{bmatrix} \mathbf{Z}_j \\ \mathbf{R}_j \end{bmatrix} \leftarrow [\mathbf{B}_0 \mid\mid \underbrace{\mathbf{W} + j \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + (j-i) \cdot \mathbf{G}}]^{-1}(\mathbf{V}) \quad (j \neq i)$$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\underbrace{\mathbf{s}_i \cdot \mathbf{B}_0}_{\mathbf{c}_{1,i}}, \qquad \underbrace{\mathbf{s}_i \cdot \mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + \mathbf{s} \cdot \mathbf{G}}_{\mathbf{c}_{2,i}}$$

$$[\mathbf{c}_{1,i} \mid\mid \mathbf{c}_{2,i}] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} - \mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$$

Security Proof

- Hybrids over $i \in [\ell]$ $\qquad \mathbf{V} := [\mathbf{B}_0 \mid\mid \underbrace{\mathbf{W} + i \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i}] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$

$$\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \chi^{2m \times m}, \quad \begin{bmatrix} \mathbf{Z}_j \\ \mathbf{R}_j \end{bmatrix} \leftarrow [\mathbf{B}_0 \mid\mid \underbrace{\mathbf{W} + j \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + (j-i) \cdot \mathbf{G}}]^{-1}(\mathbf{V}) \quad (j \neq i)$$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\underbrace{\mathbf{s}_i \cdot \mathbf{B}_0}_{\mathbf{c}_{1,i}}, \qquad \underbrace{\mathbf{c}_{1,i} \quad \cdot \tilde{\mathbf{W}}_i + \mathbf{s} \cdot \mathbf{G}}_{\mathbf{c}_{2,i}}$$

$$[\mathbf{c}_{1,i} \mid\mid \mathbf{c}_{2,i}] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} - \mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$$

Security Proof

- Hybrids over $i \in [\ell]$ $\qquad \mathbf{V} := \left[\mathbf{B}_0 \,||\, \underbrace{\mathbf{W} + i \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i}\right] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$

$$\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \chi^{2m \times m}, \quad \begin{bmatrix} \mathbf{Z}_j \\ \mathbf{R}_j \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \,||\, \underbrace{\mathbf{W} + j \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + (j-i) \cdot \mathbf{G}}\right]^{-1}(\mathbf{V}) \quad (j \neq i)$$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\mathbf{c}_{1,i}\,, \qquad \underbrace{\mathbf{c}_{1,i} \cdot \tilde{\mathbf{W}}_i + \mathbf{s} \cdot \mathbf{G}}_{\mathbf{c}_{2,i}}$$

$$\left[\mathbf{c}_{1,i} \,||\, \mathbf{c}_{2,i}\right] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} - \mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$$

Security Proof

- Hybrids over $i \in [\ell]$ $\quad \mathbf{V} := \left[\mathbf{B}_0 \mid\mid \underbrace{\mathbf{W} + i \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i}\right] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$

$$\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \chi^{2m \times m}, \begin{bmatrix} \mathbf{Z}_j \\ \mathbf{R}_j \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \underbrace{\mathbf{W} + j \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + (j-i) \cdot \mathbf{G}}\right]^{-1}(\mathbf{V}) \quad (j \neq i)$$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\mathbf{c}_{1,i}\ , \qquad \mathbf{c}_{2,i}$$

$$\left[\mathbf{c}_{1,i} \mid\mid \mathbf{c}_{2,i}\right] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} - \mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$$

Security Proof

- Hybrids over $i \in [\ell]$ $\qquad \mathbf{V} := \left[\mathbf{B}_0 \mid\mid \underbrace{\mathbf{W} + i \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i}\right] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix}$

$$\begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} \leftarrow \chi^{2m \times m}, \begin{bmatrix} \mathbf{Z}_j \\ \mathbf{R}_j \end{bmatrix} \leftarrow \left[\mathbf{B}_0 \mid\mid \underbrace{\mathbf{W} + j \cdot \mathbf{G}}_{\mathbf{B}_0 \cdot \tilde{\mathbf{W}}_i + (j-i) \cdot \mathbf{G}}\right]^{-1}(\mathbf{V}) \quad (j \neq i)$$

$$\mathbf{s} \cdot \mathbf{A}_0, \quad \mathbf{s} \cdot \mathbf{b}^\top + \mu \cdot \lfloor q/2 \rfloor$$

$$\mathbf{c}_{1,i}\ , \qquad\qquad \mathbf{c}_{2,i}$$

$\boxed{\text{run [BGGHNSVV14] security proof}}$

$$\left[\mathbf{c}_{1,i} \mid\mid \mathbf{c}_{2,i}\right] \cdot \begin{bmatrix} \mathbf{Z}_i \\ \mathbf{R}_i \end{bmatrix} - \mathbf{s} \cdot (\mathbf{A}_i - x_i \cdot \mathbf{G})$$

Conclusion

- Unbounded attribute-based encryption from LWE

Conclusion

- Unbounded attribute-based encryption from LWE
- Unbounded inner product predicate encryption from LWE

Conclusion

- Unbounded attribute-based encryption from LWE
- Unbounded inner product predicate encryption from LWE
- Other applications?

Conclusion

- Unbounded attribute-based encryption from LWE
- Unbounded inner product predicate encryption from LWE
- Other applications?

Thank you!