Almost Optimal KP and CP-ABE for Circuits from Succinct LWE

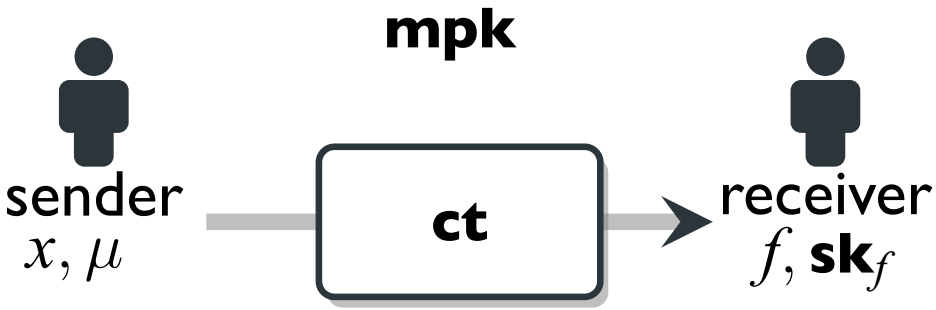
Hoeteck Wee

NTT Research

attribute-based encryption

key-policy

[GPSW06,SW05,BSW07]

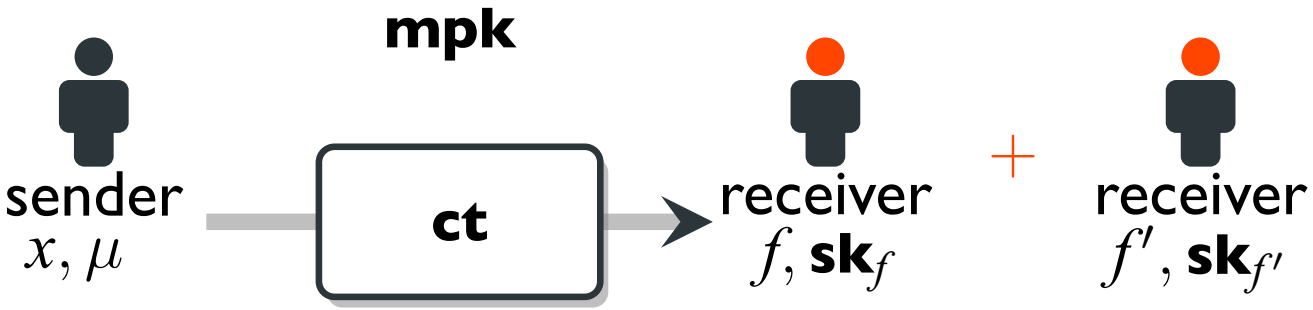


learns $\mu \Leftrightarrow f(x) = 0$

attribute-based encryption

key-policy

[GPSW06,SW05,BSW07]



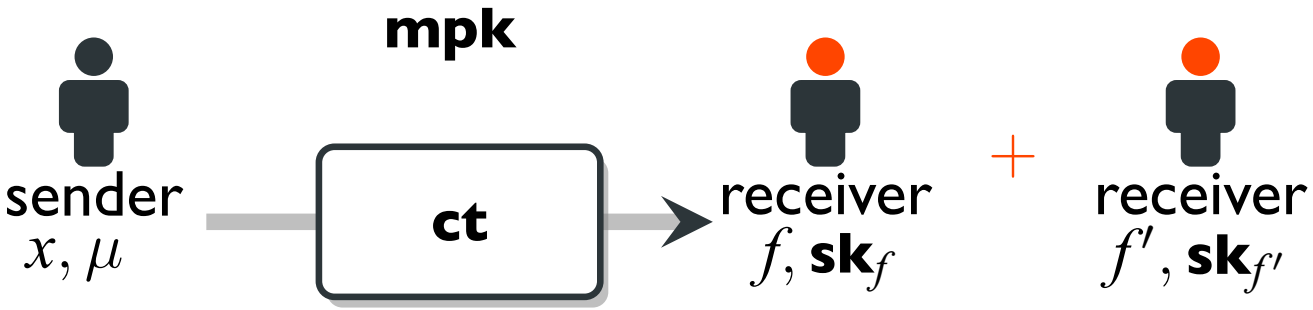
learns $\mu \Leftrightarrow f(x) = 0$

security against **collusions**

attribute-based encryption

key-policy

[GPSW06,SW05,BSW07]



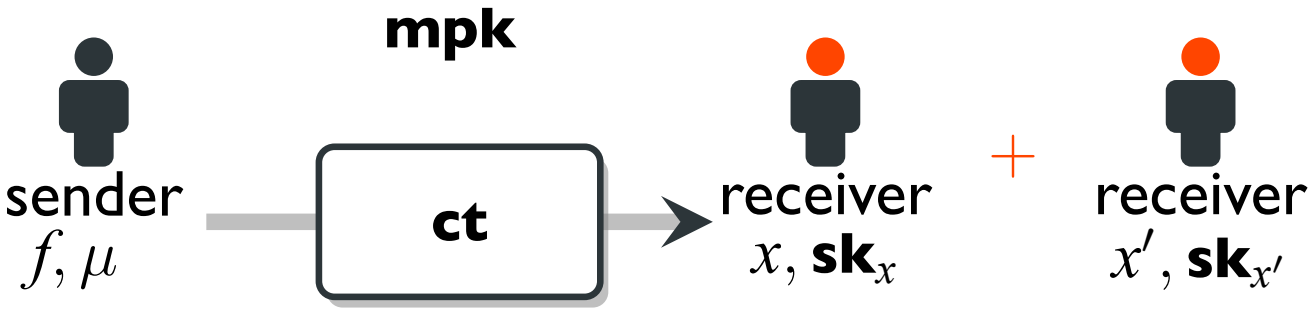
[GVW13,BGGHNSVV14]

KP-ABE for **circuits** from LWE

attribute-based encryption

ciphertext-policy

[GPSW06,SW05,BSW07]



learns $\mu \Leftrightarrow f(x) = 0$

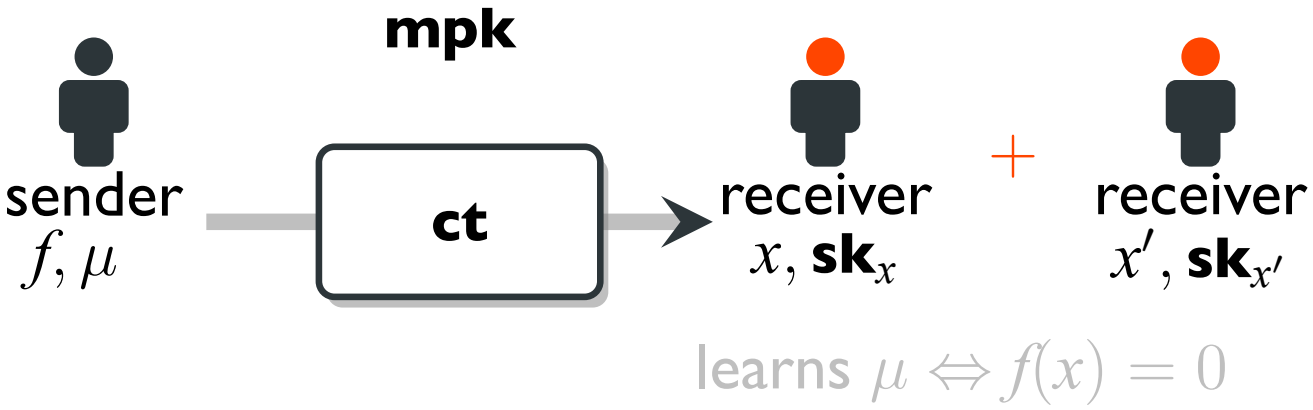
[GVW13,BGGHNSVV14]

KP-ABE for **circuits** from LWE

attribute-based encryption

ciphertext-policy

[GPSW06,SW05,BSW07]



[W22,BV22]

CP-ABE for **circuits** from evasive + tensor LWE

this work

KP-ABE & CP-ABE for **circuits** from lattices

$$|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(1)$$

$O(\cdot)$ hides poly(depth, λ) factors

this work

KP-ABE & CP-ABE for **circuits** from lattices

$|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(1)$ — *almost* **optimal**

$O(\cdot)$ hides poly(depth, λ) factors

this work

KP-ABE & CP-ABE for **circuits**

$$|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(1)$$

ℓ-succinct LWE (falsifiable) [W24]

this work

KP-ABE & CP-ABE for **circuits**

$$|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(1)$$

ℓ-succinct LWE (falsifiable) [W24]

prior. KP-ABE for $f : \{0,1\}^\ell \to \{0,1\}$ [W24]

- $|\mathbf{ct}| = |\mathbf{sk}| = O(1), |\mathbf{mpk}| = O(\ell^2)$
- $|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(\ell^{2/3})$

this work

KP-ABE & CP-ABE for **circuits**

$$|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(1)$$

ℓ-succinct LWE (falsifiable) [W24]

prior. CP-ABE for $f : \{0,1\}^\ell \to \{0,1\}$ [W22,HLL24]

- $|\mathbf{mpk}| = |\mathbf{sk}| = O(\ell)$
- stronger assumptions
- weaker security notion ("very" selective)

this talk

KP-ABE & CP-ABE for **circuits**

$|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(1)$ 2

ℓ-succinct LWE (falsifiable) [W24]

prior. KP-ABE for $f : \{0,1\}^\ell \to \{0,1\}$ [W24]

– $|\mathbf{ct}| = |\mathbf{sk}| = O(1), |\mathbf{mpk}| = O(\ell^2)$ 1

– $|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(\ell^{2/3})$

this talk

KP-ABE & CP-ABE for **circuits**

$|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(1)$

ℓ**-succinct LWE (falsifiable) [W24]**

prior. KP-ABE for $f : \{0,1\}^\ell \to \{0,1\}$ **[W24]**

- $|\mathbf{ct}| = |\mathbf{sk}| = O(1), |\mathbf{mpk}| = O(\ell^2)$
- $|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(\ell^{2/3})$

ℓ-succinct LWE [W24]

$$\begin{pmatrix} \mathbf{B} & & \mathbf{W}_1 \\ & \ddots & \vdots \\ & \mathbf{B} & \mathbf{W}_\ell \end{pmatrix}$$

$$\mathbf{B}, \mathbf{W}_i \leftarrow \mathbb{Z}_q^{n \times m}$$

ℓ-succinct LWE [W24]

$$\begin{pmatrix} \mathbf{B} & & \mathbf{W}_1 \\ & \ddots & \vdots \\ & \mathbf{B} & \mathbf{W}_\ell \end{pmatrix} \begin{pmatrix} \mathbf{T}_1 \\ \vdots \\ \mathbf{T}_\ell \\ \underline{\mathbf{T}} \end{pmatrix} = \begin{pmatrix} \mathbf{G} & & \\ & \ddots & \\ & & \mathbf{G} \end{pmatrix}$$

ℓ-succinct LWE [W24]

$$\begin{pmatrix} \mathbf{B} & & \mathbf{W}_1 \\ & \ddots & \vdots \\ & \mathbf{B} & \mathbf{W}_\ell \end{pmatrix} \begin{pmatrix} \mathbf{T}_1 \\ \vdots \\ \mathbf{T}_\ell \\ \underline{\mathbf{T}} \end{pmatrix} = \begin{pmatrix} \mathbf{G} & & \\ & \ddots & \\ & & \mathbf{G} \end{pmatrix}$$

$\mathbf{sB} + \mathbf{e} \approx_c$ random, given $\mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}$

ℓ-succinct LWE [W24]

$$\begin{pmatrix} \mathbf{B} & & \mathbf{W}_1 \\ & \ddots & \vdots \\ & \mathbf{B} & \mathbf{W}_\ell \end{pmatrix} \begin{pmatrix} \mathbf{T}_1 \\ \vdots \\ \mathbf{T}_\ell \\ \underline{\mathbf{T}} \end{pmatrix} = \begin{pmatrix} \mathbf{G} & & \\ & \ddots & \\ & & \mathbf{G} \end{pmatrix}$$

$$\mathbf{sB} + \mathbf{e} \approx_c \text{ random, given } \mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}$$

claim. LWE $=$ 1-succinct LWE $\Leftarrow$ 2-succinct LWE

$\Leftarrow \cdots \Leftarrow$ ℓ-succinct LWE $\Leftarrow$ evasive LWE

ℓ-succinct LWE [W24]

$$\begin{pmatrix} \mathbf{B} & & \mathbf{W}_1 \\ & \ddots & \vdots \\ & \mathbf{B} & \mathbf{W}_\ell \end{pmatrix} \begin{pmatrix} \mathbf{T}_1 \\ \vdots \\ \mathbf{T}_\ell \\ \underline{\mathbf{T}} \end{pmatrix} = \begin{pmatrix} \mathbf{G} & & \\ & \ddots & \\ & & \mathbf{G} \end{pmatrix}$$

$\mathbf{sB} + \mathbf{e} \approx_c$ random, given $\underbrace{\mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}}_{\mathbf{pp}_\ell}$

KP-ABE for circuits [W24]

$$|\mathbf{ct}| = |\mathbf{sk}| = O(1), |\mathbf{mpk}| = O(\ell^2)$$

from ℓ-succinct LWE

vector commitment [W24]

$$\mathsf{com}^{\mathsf{vc}}_{\ell}(\mathbf{x} \in \{0,1\}^{\ell}) \rightarrow \mathbf{C}_{\mathbf{x}} \in \mathbb{Z}_q^{n \times m}$$

vector commitment [W24]

$$\mathsf{com}^{\mathsf{vc}}_{\ell}(\mathbf{x} \in \{0,1\}^{\ell}) \to \mathbf{C_x} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C_x} \qquad \overbrace{\mathbf{x} \otimes \mathbf{G}}^{n \times \ell m} \qquad \overbrace{\mathbf{Z_x}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{x})}$$

vector commitment [W24]

$$\mathsf{com}^{\mathsf{vc}}_{\ell}(\mathbf{x} \in \{0,1\}^{\ell}) \to \mathbf{C}_{\mathbf{x}} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_{\mathbf{x}} \overbrace{\mathbf{V}_{\ell}}^{\mathsf{ver}^{\mathsf{vc}}(1^{\ell})} = \mathbf{x} \otimes \mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{\mathbf{x}}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{x})}$$

where $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$

vector commitment [W24]

$$\mathsf{com}^{\mathsf{vc}}_{\ell}(\mathbf{x} \in \{0,1\}^{\ell}) \to \mathbf{C}_{\mathbf{x}} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_{\mathbf{x}} \overbrace{\mathbf{V}_{\ell}}^{\mathsf{ver}^{\mathsf{vc}}(1^{\ell})} = \mathbf{x} \otimes \mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{\mathbf{x}}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{x})}$$

where $\mathbf{Z}_{\mathbf{x}}, \mathbf{V}_{\ell} \in \mathbb{Z}_q^{m \times \ell m}$ low-norm

vector commitment [W24]

$$\mathsf{com}^{\mathsf{vc}}_{\ell}(\mathbf{x} \in \{0,1\}^{\ell}) \to \mathbf{C}_{\mathbf{x}} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_{\mathbf{x}} \overbrace{\mathbf{V}_{\ell}}^{\mathsf{ver}^{\mathsf{vc}}(1^{\ell})} = \mathbf{x} \otimes \mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{\mathbf{x}}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{x})}$$

where $\mathbf{Z}_{\mathbf{x}}, \mathbf{V}_{\ell} \in \mathbb{Z}_q^{m \times \ell m}$ low-norm

vector commitment [W24]

$$\mathsf{com}^{\mathsf{vc}}_{\ell}(\mathbf{x} \in \{0,1\}^{\ell}) \to \mathbf{C}_{\mathbf{x}} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_{\mathbf{x}} \overbrace{\mathbf{V}_{\ell}}^{\mathsf{ver}^{\mathsf{vc}}(1^{\ell})} = \mathbf{x} \otimes \mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{\mathbf{x}}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{x})}$$

construction. crs: $\mathbf{pp}_{\ell} = \mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}$

vector commitment [W24]

$$\mathsf{com}^{\mathsf{vc}}_{\ell}(\mathbf{x} \in \{0,1\}^{\ell}) \to \mathbf{C}_{\mathbf{x}} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_{\mathbf{x}} \overbrace{\mathbf{V}_{\ell}}^{\mathsf{ver}^{\mathsf{vc}}(1^{\ell})} = \mathbf{x} \otimes \mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{\mathbf{x}}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{x})}$$

construction. crs: $\mathbf{pp}_{\ell} = \mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}$

$$\mathbf{C}_{\mathbf{x}} := \sum x_i \mathbf{W}_i, \ \mathbf{V}_{\ell} = \underline{\mathbf{T}}, \ \mathbf{Z}_{\mathbf{x}} := \sum x_i \mathbf{T}_i$$

vector commitment [W24]

$$\mathsf{com}^{\mathsf{vc}}_{\ell}(\mathbf{x} \in \{0,1\}^{\ell}) \to \mathbf{C}_{\mathbf{x}} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_{\mathbf{x}} \overbrace{\mathbf{V}_{\ell}}^{\mathsf{ver}^{\mathsf{vc}}(1^{\ell})} = \mathbf{x} \otimes \mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{\mathbf{x}}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{x})}$$

construction. crs: $\mathbf{pp}_{\ell} = \mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}$

$\Rightarrow$ **KP-ABE** for circuits

$$|\mathbf{mpk}| = |\mathbf{pp}_{\ell}| = O(\ell^2), \quad |\mathbf{ct}| = |\mathbf{sk}| = O(1)$$

vector commitment [W24]

$$\mathsf{com}_\ell^{\mathsf{vc}}(\mathbf{x} \in \{0,1\}^\ell) \to \mathbf{C}_\mathbf{x} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_\mathbf{x} \overbrace{\mathbf{V}_\ell}^{\mathsf{ver}^{\mathsf{vc}}(1^\ell)} = \mathbf{x} \otimes \mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_\mathbf{x}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{x})}$$

this work. crs: $\mathbf{pp}_{2m^2} = \mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}$

$\Rightarrow$ **KP-ABE** for circuits

$$|\mathbf{mpk}| = |\mathbf{pp}_\ell| = O(\ell^2), \quad |\mathbf{ct}| = |\mathbf{sk}| = O(1)$$

vector commitment [W24]

$$\mathsf{com}^{\mathsf{vc}}_{\ell}(\mathbf{x} \in \{0,1\}^{\ell}) \to \mathbf{C}_{\mathbf{x}} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_{\mathbf{x}} \overbrace{\mathbf{V}_{\ell}}^{\mathsf{ver}^{\mathsf{vc}}(1^{\ell})} = \mathbf{x} \otimes \mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{\mathbf{x}}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{x})}$$

this work. crs: $\mathbf{pp}_{2m^2} = \mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}$

$\Rightarrow$ **KP-ABE** for circuits

$$|\mathbf{mpk}| = |\mathbf{pp}_{2m^2}| = O(1), |\mathbf{ct}| = |\mathbf{sk}| = O(1)$$

matrix commitment

$$\mathsf{com}^{\mathsf{mx}}_{L}(\mathbf{M} \in \mathbb{Z}_q^{n \times L}) \rightarrow \mathbf{C_M} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C_x} \overbrace{\mathbf{V}_\ell}^{\mathsf{ver}^{\mathsf{vc}}(1^\ell)} = \mathbf{x} \otimes \mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z_x}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{x})}$$

matrix commitment

$$\mathsf{com}_L^{\mathsf{mx}}(\mathbf{M} \in \mathbb{Z}_q^{n \times L}) \to \mathbf{C_M} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C_M} \overbrace{\mathbf{V}_L}^{\mathsf{ver}^{\mathsf{vc}}(1^L)} = \mathbf{M} - \mathbf{B} \overbrace{\mathbf{Z_M}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{M})}$$

where $\mathbf{Z_M}, \mathbf{V_M} \in \mathbb{Z}_q^{m \times L}$ low-norm

matrix commitment

$$\mathsf{com}_L^{\mathsf{mx}}(\mathbf{M} \in \mathbb{Z}_q^{n \times L}) \to \mathbf{C_M} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C_M} \overbrace{\mathbf{V}_L}^{\mathsf{ver}^{\mathsf{vc}}(1^L)} = \mathbf{M} - \mathbf{B} \overbrace{\mathbf{Z_M}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{M})}$$

construction. crs: $\mathbf{pp}_{2m^2}$

$\Rightarrow$ vector commitment for $\mathbf{x} \in \{0,1\}^\ell$

matrix commitment

$$\mathsf{com}_L^{\mathsf{mx}}(\mathbf{M} \in \mathbb{Z}_q^{n \times L}) \to \mathbf{C_M} \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C_M} \overbrace{\mathbf{V}_L}^{\mathsf{ver}^{\mathsf{vc}}(1^L)} = \mathbf{M} - \mathbf{B} \overbrace{\mathbf{Z_M}}^{\mathsf{open}^{\mathsf{vc}}(\mathbf{M})}$$

construction. crs: $\mathbf{pp}_{2m^2}$

IDEA. Merkle-style recursion

matrix commitment: $L = 2m$

$\mathsf{com}^{\mathsf{mx}}_{2m}(\mathbf{M})$ where $\mathbf{M} \in \mathbb{Z}_q^{n \times 2m}$

matrix commitment: $L = 2m$

$\mathsf{com}^{\mathsf{mx}}_{2m}(\mathbf{M})$ $\mathsf{bits}(\mathbf{M}) \in \{0,1\}^{2m^2}$

matrix commitment: $L = 2m$

$$\mathsf{com}^{\mathsf{mx}}_{2m}(\mathbf{M}) := \mathsf{com}^{\mathsf{vc}}_{2m^2}(\mathsf{bits}(\mathbf{M}))$$

matrix commitment: $L = 2m$

$$\mathsf{com}^{\mathsf{mx}}_{2m}(\mathbf{M}) := \mathsf{com}^{\mathsf{vc}}_{2m^2}(\mathsf{bits}(\mathbf{M}))$$

$$\mathbf{C}_{\mathsf{bits}(\mathbf{M})} \cdot \mathbf{V}_{2m^2} = \mathsf{bits}(\mathbf{M}) \otimes \mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_{\mathsf{bits}(\mathbf{M})}$$

$$\hookrightarrow \quad \mathbf{C}_{\mathbf{M}} \cdot \mathbf{V}^{\mathsf{mx}}_{2m} = \mathbf{M} - \mathbf{B} \cdot \mathbf{Z}_{\mathbf{M}}$$

matrix commitment: $L = 2m$

$$\mathsf{com}^{\mathsf{mx}}_{2m}(\mathbf{M}) := \mathsf{com}^{\mathsf{vc}}_{2m^2}(\mathsf{bits}(\mathbf{M}))$$

$$\mathbf{C}_{\mathsf{bits}(\mathbf{M})} \cdot \mathbf{V}_{2m^2} = \mathsf{bits}(\mathbf{M}) \otimes \mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_{\mathsf{bits}(\mathbf{M})}$$

$$\hookrightarrow \quad \mathbf{C}_{\mathbf{M}} \cdot \mathbf{V}^{\mathsf{mx}}_{2m} = \mathbf{M} - \mathbf{B} \cdot \mathbf{Z}_{\mathbf{M}}$$

$$(\mathsf{bits}(\mathbf{M}) \otimes \mathbf{G}) \cdot (\underline{\mathbf{I}_{2m^2} \otimes \mathsf{vec}(\mathbf{I}_m)}) = \mathbf{M}$$ [BTVW17]

matrix commitment: $L = 2m$

$$\mathsf{com}^{\mathsf{mx}}_{2m}(\mathbf{M}) := \mathsf{com}^{\mathsf{vc}}_{2m^2}(\mathsf{bits}(\mathbf{M}))$$

$$\mathbf{C}_{\mathsf{bits}(\mathbf{M})} \cdot \mathbf{V}_{2m^2} = \mathsf{bits}(\mathbf{M}) \otimes \mathbf{G} - \mathbf{B} \cdot \mathbf{Z}_{\mathsf{bits}(\mathbf{M})}$$

$$\hookrightarrow \quad \mathbf{C}_{\mathbf{M}} \cdot \mathbf{V}^{\mathsf{mx}}_{2m} = \mathbf{M} - \mathbf{B} \cdot \mathbf{Z}_{\mathbf{M}}$$

$$(\mathsf{bits}(\mathbf{M}) \otimes \mathbf{G}) \cdot (\underline{\mathbf{I}_{2m^2} \otimes \mathrm{vec}(\mathbf{I}_m)}) = \mathbf{M}$$ [BTVW17]

$$\hookrightarrow \mathbf{V}^{\mathsf{mx}}_{2m} := \mathbf{V}_{2m^2}(\mathbf{I}_{2m^2} \otimes \mathrm{vec}(\mathbf{I}_m))$$

$$\hookrightarrow \mathbf{Z}_{\mathbf{M}} := \mathbf{Z}_{\mathsf{bits}(\mathbf{M})}(\mathbf{I}_{2m^2} \otimes \mathrm{vec}(\mathbf{I}_m))$$

matrix commitment: $L/2 \mapsto L$

$\mathsf{com}_L^{\mathsf{mx}}([\mathbf{M}_0 \mid \mathbf{M}_1])$ where $\mathbf{M}_0, \mathbf{M}_1 \in \mathbb{Z}_q^{n \times L/2}$

matrix commitment: $L/2 \mapsto L$

$$\mathsf{com}^{\mathsf{mx}}_{L}([\mathbf{M}_0 \mid \mathbf{M}_1]) \qquad \text{where } \mathbf{M}_0, \mathbf{M}_1 \in \mathbb{Z}_q^{n \times L/2}$$

$$\overbrace{\mathsf{com}^{\mathsf{mx}}_{L/2}(\mathbf{M}_0)}^{\mathbf{C}_0} \; \overbrace{\mathsf{com}^{\mathsf{mx}}_{L/2}(\mathbf{M}_1)}^{\mathbf{C}_1} \qquad \mathbf{C}_0, \mathbf{C}_1 \in \mathbb{Z}_q^{n \times m}$$

matrix commitment: $L/2 \mapsto L$

$$\mathsf{com}^{\mathsf{mx}}_{L}([\mathbf{M}_0 \mid \mathbf{M}_1])$$

$$\mathsf{com}^{\mathsf{mx}}_{2m}([\overbrace{\mathsf{com}^{\mathsf{mx}}_{L/2}(\mathbf{M}_0)}^{\mathbf{C}_0} \mid \overbrace{\mathsf{com}^{\mathsf{mx}}_{L/2}(\mathbf{M}_1)}^{\mathbf{C}_1}]) \quad \mathbf{C}_0, \mathbf{C}_1 \in \mathbb{Z}_q^{n \times m}$$

matrix commitment: $L/2 \mapsto L$

$$\mathsf{com}^{\mathsf{mx}}_{L}([\mathbf{M}_0 \mid \mathbf{M}_1]) :=$$

$$\underbrace{\mathsf{com}^{\mathsf{mx}}_{2m}([\overbrace{\mathsf{com}^{\mathsf{mx}}_{L/2}(\mathbf{M}_0)}^{\mathbf{C}_0} \mid \overbrace{\mathsf{com}^{\mathsf{mx}}_{L/2}(\mathbf{M}_1)}^{\mathbf{C}_1}])}_{\mathbf{C}} \qquad \mathbf{C} \in \mathbb{Z}_q^{n \times m}$$

matrix commitment: $L/2 \mapsto L$

$$\mathsf{com}^{\mathsf{mx}}_{L}([\mathbf{M}_0 \mid \mathbf{M}_1]) :=$$

$$\underbrace{\mathsf{com}^{\mathsf{mx}}_{2m}([\overbrace{\mathsf{com}^{\mathsf{mx}}_{L/2}(\mathbf{M}_0)}^{\mathbf{C}_0} \mid \overbrace{\mathsf{com}^{\mathsf{mx}}_{L/2}(\mathbf{M}_1)}^{\mathbf{C}_1}])}_{\mathbf{C}} \qquad \mathbf{C} \in \mathbb{Z}_q^{n \times m}$$

$$\begin{aligned}
\mathbf{C} \cdot \mathbf{V}^{\mathsf{mx}}_{2m} &= [\mathbf{C}_0 \mid \mathbf{C}_1] - \mathbf{B} \cdot \mathbf{Z}_{[\mathbf{C}_0|\mathbf{C}_1]} \\
\mathbf{C}_0 \cdot \mathbf{V}^{\mathsf{mx}}_{L/2} &= \mathbf{M}_0 - \mathbf{B} \cdot \mathbf{Z}_{\mathbf{M}_0} \\
\mathbf{C}_1 \cdot \mathbf{V}^{\mathsf{mx}}_{L/2} &= \mathbf{M}_1 - \mathbf{B} \cdot \mathbf{Z}_{\mathbf{M}_1}
\end{aligned}$$

matrix commitment: $L/2 \mapsto L$

$$\mathsf{com}^{\mathsf{mx}}_{L}([\mathbf{M}_0 \mid \mathbf{M}_1]) :=$$

$$\underbrace{\mathsf{com}^{\mathsf{mx}}_{2m}([\overbrace{\mathsf{com}^{\mathsf{mx}}_{L/2}(\mathbf{M}_0)}^{\mathbf{C}_0} \mid \overbrace{\mathsf{com}^{\mathsf{mx}}_{L/2}(\mathbf{M}_1)}^{\mathbf{C}_1}])}_{\mathbf{C}} \qquad \mathbf{C} \in \mathbb{Z}_q^{n \times m}$$

$$\begin{aligned} \mathbf{V}^{\mathsf{mx}}_{L} &:= \mathbf{V}^{\mathsf{mx}}_{2m}(\mathbf{I}_2 \otimes \mathbf{V}^{\mathsf{mx}}_{L/2}) \\ \mathbf{Z}_{[\mathbf{M}_0|\mathbf{M}_1]} &:= \mathbf{Z}_{[\mathbf{C}_0|\mathbf{C}_1]}(\mathbf{I}_2 \otimes \mathbf{V}^{\mathsf{mx}}_{L/2}) + [\mathbf{Z}_{\mathbf{M}_0} \mid \mathbf{Z}_{\mathbf{M}_1}]) \end{aligned}$$

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \to \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \rightarrow \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_f \qquad\qquad f(\mathbf{x}) \qquad\qquad \overbrace{\mathbf{Z}_{f,\mathbf{x}}}^{\mathsf{open}^{\mathsf{c}}(f,\mathbf{x})}$$

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \to \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_f \overbrace{\mathbf{V}_{\mathbf{x}}}^{\mathsf{ver}^{\mathsf{c}}(\mathbf{x})} = f(\mathbf{x})\mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{f,\mathbf{x}}}^{\mathsf{open}^{\mathsf{c}}(f,\mathbf{x})}$$

where $\mathbf{Z}_{f,\mathbf{x}}, \mathbf{V}_{\mathbf{x}} \in \mathbb{Z}_q^{m \times m}$ low-norm

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \to \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_f \overbrace{\mathbf{V}_{\mathbf{x}}}^{\mathsf{ver}^{\mathsf{c}}(\mathbf{x})} = f(\mathbf{x})\mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{f,\mathbf{x}}}^{\mathsf{open}^{\mathsf{c}}(f,\mathbf{x})}$$

$\Rightarrow$ *almost* **optimal** **CP-ABE** for circuits

$$|\mathbf{mpk}| = |\mathbf{pp}_{2m^2}| = O(1)$$

$$|\mathbf{ct}| \approx |\mathbf{C}_f| = O(1)$$

$$|\mathbf{sk}| \approx |\mathbf{V}_{\mathbf{x}}| = O(1)$$

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \rightarrow \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_f \overbrace{\mathbf{V}_{\mathbf{x}}}^{\mathsf{ver}^{\mathsf{c}}(\mathbf{x})} = f(\mathbf{x})\mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{f,\mathbf{x}}}^{\mathsf{open}^{\mathsf{c}}(f,\mathbf{x})}$$

input.

addition.

multiplication.

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \to \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_f \overbrace{\mathbf{V}_{\mathbf{x}}}^{\mathsf{ver}^{\mathsf{c}}(\mathbf{x})} = f(\mathbf{x})\mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{f,\mathbf{x}}}^{\mathsf{open}^{\mathsf{c}}(f,\mathbf{x})}$$

input. $\mathsf{com}^{\mathsf{vc}}$ & linear homomorphism

addition. $\mathbf{C}_{f_0+f_1} = \mathbf{C}_{f_0} + \mathbf{C}_{f_1}$

multiplication. $\mathbf{C}_{f_0}, \mathbf{C}_{f_1} \mapsto \mathbf{C}_{f_0 \cdot f_1}$?

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \to \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_f \overbrace{\mathbf{V}_{\mathbf{x}}}^{\mathsf{ver}^{\mathsf{c}}(\mathbf{x})} = f(\mathbf{x})\mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{f,\mathbf{x}}}^{\mathsf{open}^{\mathsf{c}}(f,\mathbf{x})}$$

input. $\mathsf{com}^{\mathsf{vc}}$ & linear homomorphism

addition. $\mathbf{C}_{f_0+f_1} = \mathbf{C}_{f_0} + \mathbf{C}_{f_1}$

multiplication. $\mathbf{C}_{f_0}, \mathbf{C}_{f_1} \mapsto \mathbf{C}_{f_0 \cdot f_1}$? **CHALLENGE**

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \to \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_f \overbrace{\mathbf{V}_{\mathbf{x}}}^{\mathsf{ver}^{\mathsf{c}}(\mathbf{x})} = f(\mathbf{x})\mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{f,\mathbf{x}}}^{\mathsf{open}^{\mathsf{c}}(f,\mathbf{x})}$$

multiplication. $\mathbf{C}_{f_0}, \mathbf{C}_{f_1} \mapsto \mathbf{C}_{f_0 \cdot f_1}$**?**

✗ $\mathbf{C}_{f_0} \cdot \mathbf{G}^{-1}(\mathbf{C}_{f_1})$ **[BGGHNSVV14,GSW13]**

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \to \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_f \overbrace{\mathbf{V}_{\mathbf{x}}}^{\mathsf{ver}^{\mathsf{c}}(\mathbf{x})} = f(\mathbf{x})\mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{f,\mathbf{x}}}^{\mathsf{open}^{\mathsf{c}}(f,\mathbf{x})}$$

multiplication. $\mathbf{C}_{f_0}, \mathbf{C}_{f_1} \mapsto \mathbf{C}_{f_0 \cdot f_1}$**?**

✗ $\mathbf{C}_{f_0} \cdot \mathbf{G}^{-1}(\mathbf{C}_{f_1})$ **[BGGHNSVV14,GSW13]**

$$(\mathbf{C}_{f_0}\mathbf{V}_{\mathbf{x}}) \cdot \mathbf{G}^{-1}(\mathbf{C}_{f_1}\mathbf{V}_{\mathbf{x}}) = f_0(\mathbf{x}) f_1(\mathbf{x})\mathbf{G} - \mathbf{B} \cdot (\cdots)$$

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \to \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_f \overbrace{\mathbf{V}_{\mathbf{x}}}^{\mathsf{ver}^{\mathsf{c}}(\mathbf{x})} = f(\mathbf{x})\mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{f,\mathbf{x}}}^{\mathsf{open}^{\mathsf{c}}(f,\mathbf{x})}$$

multiplication. $\mathbf{C}_{f_0}, \mathbf{C}_{f_1} \mapsto \mathbf{C}_{f_0 \cdot f_1}$**?**

✗ $\mathbf{C}_{f_0} \cdot \mathbf{G}^{-1}(\mathbf{C}_{f_1})$ **[BGGHNSVV14,GSW13]**

$$(\mathbf{C}_{f_0}\mathbf{V}_{\mathbf{x}}) \cdot \mathbf{G}^{-1}(\mathbf{C}_{f_1}\mathbf{V}_{\mathbf{x}}) = f_0(\mathbf{x}) f_1(\mathbf{x})\mathbf{G} - \mathbf{B} \cdot (\cdots)$$

$$\neq \mathbf{C}_f \cdot \mathbf{V}_{\mathbf{x}}$$

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \to \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_f \overbrace{\mathbf{V}_{\mathbf{x}}}^{\mathsf{ver}^{\mathsf{c}}(\mathbf{x})} = f(\mathbf{x})\mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{f,\mathbf{x}}}^{\mathsf{open}^{\mathsf{c}}(f,\mathbf{x})}$$

multiplication. $\mathbf{C}_{f_0}, \mathbf{C}_{f_1} \mapsto \mathbf{C}_{f_0 \cdot f_1}$**?**

✗ $\mathbf{C}_{f_0} \cdot \mathbf{G}^{-1}(\mathbf{C}_{f_1})$ **[BGGHNSVV14,GSW13]**

$$(\mathbf{C}_{f_0}\mathbf{V}_{\mathbf{x}}) \cdot \mathbf{G}^{-1}(\mathbf{C}_{f_1})\mathbf{V}_{\mathbf{x}} = \underbrace{(\mathsf{bits}(\mathbf{C}_{f_1}) \otimes \mathbf{C}_{f_0})}_{\in \mathbb{Z}_q^{n \times m^3}} \cdot \underbrace{(\mathbf{I}_m \otimes \mathrm{vec}(\mathbf{V}_{\mathbf{x}}))\mathbf{V}_{\mathbf{x}}}_{\text{new } \mathbf{V}_{\mathbf{x}}?}$$

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \to \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_f \overbrace{\mathbf{V}_{\mathbf{x}}}^{\mathsf{ver}^{\mathsf{c}}(\mathbf{x})} = f(\mathbf{x})\mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{f,\mathbf{x}}}^{\mathsf{open}^{\mathsf{c}}(f,\mathbf{x})}$$

multiplication. $\mathbf{C}_{f_0}, \mathbf{C}_{f_1} \mapsto \mathbf{C}_{f_0 \cdot f_1}$**?**

✓ $\mathsf{com}_{m^3}^{\mathsf{mx}}(\mathsf{bits}(\mathbf{C}_{f_1}) \otimes \mathbf{C}_{f_0})$

$$(\mathbf{C}_{f_0}\mathbf{V}_{\mathbf{x}}) \cdot \mathbf{G}^{-1}(\mathbf{C}_{f_1})\mathbf{V}_{\mathbf{x}} = \underbrace{(\mathsf{bits}(\mathbf{C}_{f_1}) \otimes \mathbf{C}_{f_0})}_{\in \mathbb{Z}_q^{n \times m^3}} \cdot \underbrace{(\mathbf{I}_m \otimes \mathrm{vec}(\mathbf{V}_{\mathbf{x}}))\mathbf{V}_{\mathbf{x}}}_{\text{new } \mathbf{V}_{\mathbf{x}}?}$$

commitment to **circuits**

$$\mathsf{com}^{\mathsf{c}}(f) \to \mathbf{C}_f \in \mathbb{Z}_q^{n \times m}$$

$$\mathbf{C}_f \overbrace{\mathbf{V}_{\mathbf{x}}}^{\mathsf{ver}^{\mathsf{c}}(\mathbf{x})} = f(\mathbf{x})\mathbf{G} - \mathbf{B} \overbrace{\mathbf{Z}_{f,\mathbf{x}}}^{\mathsf{open}^{\mathsf{c}}(f,\mathbf{x})}$$

multiplication. $\mathbf{C}_{f_0}, \mathbf{C}_{f_1} \mapsto \mathbf{C}_{f_0 \cdot f_1}$**?**

✓ $\mathsf{com}^{\mathsf{mx}}_{m^3 \log m}((\mathsf{bits}(\mathbf{C}_{f_1}) \otimes \mathbf{C}_{f_0}) \cdot \mathbf{G}_{m^3})$

conclusion

KP & CP-ABE for **circuits** from $2m^2$-succinct LWE

$$|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(1)$$

conclusion

KP & CP-ABE for **circuits** from $2m^2$-succinct LWE

$$|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(1)$$

corollaries.

- optimal broadcast encryption
- $2m^2$-succinct LWE $\Rightarrow$ ℓ-succinct LWE

conclusion

KP & CP-ABE for **circuits** from $2m^2$-succinct LWE

$$|\mathbf{mpk}| = |\mathbf{ct}| = |\mathbf{sk}| = O(1)$$

corollaries.

- optimal broadcast encryption
- $2m^2$-succinct LWE $\Rightarrow$ ℓ-succinct LWE

concurrent. *almost* optimal

laconic function evaluation from LWE [AMR25]

final thought

What's your secret to teaching well?

years ago

final thought

What's your secret to teaching well?

Dress well ...

a few secs later

final thought

What's your secret to teaching well?

Dress well ...

"that's the complexity-theorist's approach: take a hard problem, reduce it to an even harder problem."

— Luca Trevisan

final thought

What's your secret to teaching well?

Dress well ...

"that's the complexity-theorist's approach: take a hard problem, reduce it to an even harder problem."

— Luca Trevisan (1971 – 2024)