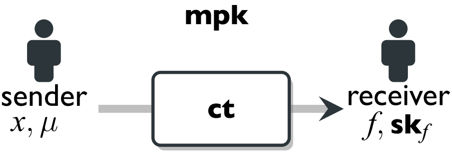
Circuit ABE with poly(depth, λ)-sized Ciphertexts and Keys from Lattices

Hoeteck Wee
NTT Research

attribute-based encryption

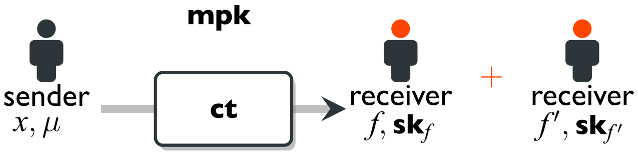
[GPSW06,SW05]



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

attribute-based encryption

[GPSW06,SW05]

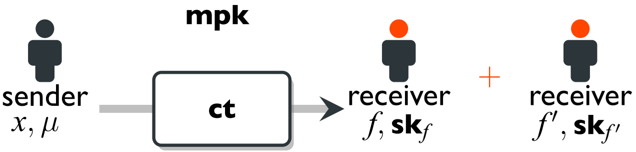


learns $\mu \Leftrightarrow f(x) = 0$

security against **collusions**

attribute-based encryption

[GPSW06,SW05]



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

[BGGHNSVV14,GVW13]

ABE for **circuits** from LWE

attribute-based encryption

[GPSW06,SW05]

[BGGHNSVV14,GVW13]

ABE for **circuits** from LWE

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

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

this work

ABE for **circuits** from evasive LWE [W22,T22]

1. $|\textbf{ct}| = |\textbf{sk}| = O(1)$

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

this work

ABE for **circuits** from evasive LWE **[W22,T22]**

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

$O(\cdot)$ hides $\mathrm{poly}(\mathrm{depth}, \lambda)$ factors

prior. $|\mathbf{ct}| + |\mathbf{sk}| = \Omega(\ell)$

[GVW13, BGGHNSVV14, BV16, BV22, W22, HLL23, CW23, LLL24]

this work

ABE for **circuits** from evasive LWE **[W22,T22]**

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

   $O(\cdot)$ hides $\text{poly}(\text{depth}, \lambda)$ factors

prior. $|\textbf{ct}| + |\textbf{sk}| = \Omega(\ell)$

[GVW13, BGGHNSVV14, BV16, BV22, W22, HLL23, CW23, LLL24]

this work

ABE for **circuits** from evasive LWE **[W22,T22]**

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

prior. $|\textbf{ct}| + |\textbf{sk}| = \Omega(\ell)$

[GVW13, BGGHNSVV14, BV16, BV22, W22, HLL23, CW23, LLL24]

this work

ABE for **circuits** from evasive LWE [W22,T22]

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

prior. $|\mathbf{ct}| + |\mathbf{sk}| = \Omega(\ell)$ & $|\mathbf{mpk}| + |\mathbf{sk}| = \Omega(\ell)$

[GVW13, BGGHNSVV14, BV16, BV22, W22, HLL23, CW23, LLL24]

this work

ABE for **circuits** from ℓ-**succinct LWE** (**falsifiable**)

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

prior. $|\mathsf{ct}| + |\mathsf{sk}| = \Omega(\ell)$ & $|\mathsf{mpk}| + |\mathsf{sk}| = \Omega(\ell)$

[GVW13, BGGHNSVV14, BV16, BV22, W22, HLL23, CW23, LLL24]

this work

ABE for **circuits** from ℓ-**succinct LWE** (**falsifiable**)

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

laconic function evaluation for **circuits** [QWW18]

1. $|\mathbf{ct}| = \ell + O(1)$ — *almost* **optimal**
2. $|\mathbf{ct}| = \ell + O(\ell^{2/3})$, $|\mathbf{crs}| = O(\ell^{2/3})$

this work

ABE for **circuits** from ℓ-**succinct LWE** (**falsifiable**)

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

laconic function evaluation for **circuits** [QWW18]

1. $|\mathbf{ct}| = \ell + O(1)$
2. $|\mathbf{ct}| = \ell + O(\ell^{2/3})$, $|\mathbf{crs}| = O(\ell^{2/3})$

technical overview

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

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

technical overview

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

$\{\mathbf{T}_i\}_{i\in[\ell]}, \underline{\mathbf{T}}$ small

technical overview

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

compress $\mathbf{s}(\mathbf{A} - \mathbf{x} \otimes \mathbf{G}) + \mathbf{e}$

technical overview

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

compress $\mathbf{s}(\mathbf{A} - \mathbf{x} \otimes \mathbf{G}) + \mathbf{e}$

[W Wu23]: **i.** $\mathbf{W}_i = \mathbf{V}_i^{-1}\mathbf{G},\ \mathbf{V}_i \leftarrow \mathbb{Z}_q^{n \times n}$

technical overview

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

compress $\mathbf{s}(\mathbf{A} - \mathbf{x} \otimes \mathbf{G}) + \mathbf{e}$

[W Wu23]: **ii.** compress $\mathbf{A} - \mathbf{x} \otimes \mathbf{G}$

technical overview

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

compress $\mathbf{s}(\mathbf{A} - \mathbf{x} \otimes \mathbf{G}) + \mathbf{e}$

[W Wu23]: **ii.** compress $\mathbf{A} - \mathbf{x} \otimes \mathbf{G} \mapsto \underline{\mathbf{T}}(\mathbf{x}^\top \otimes \mathbf{I})$

$\curvearrowleft$ *left*-multiplies by *large* matrices

technical overview

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

compress $\mathbf{s}(\mathbf{A} - \mathbf{x} \otimes \mathbf{G}) \mapsto \mathbf{s}[\mathbf{B} \mid \sum x_i \mathbf{W}_i]$

[W Wu23]: **ii.** compress $\mathbf{A} - \mathbf{x} \otimes \mathbf{G} \mapsto \underline{\mathbf{T}}(\mathbf{x}^\top \otimes \mathbf{I})$

↶ *right*-multiplies by *small* matrices

technical overview

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

compress $\mathbf{s}(\mathbf{A} - \mathbf{x} \otimes \mathbf{G}) \mapsto \mathbf{s}[\mathbf{B} \mid \mathbf{B}_1 + \sum x_i \mathbf{W}_i]$

$\mathbf{B}_1 \leftarrow \mathbb{Z}_q^{n \times m}$

↶ *right*-multiplies by *small* matrices

technical overview

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

compress $\mathbf{s}(\mathbf{A} - \mathbf{x} \otimes \mathbf{G}) \mapsto \mathbf{s}[\mathbf{B} \mid \mathbf{B}_1 + \sum x_i \mathbf{W}_i]$

$$[\mathbf{B} \mid \quad \sum x_i \mathbf{W}_i] \begin{pmatrix} \sum x_i \mathbf{T}_i \\ \underline{\mathbf{T}} \end{pmatrix} = \quad \mathbf{x} \otimes \mathbf{G}$$

technical overview

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

compress $\mathbf{s}(\mathbf{A} - \mathbf{x} \otimes \mathbf{G}) \mapsto \mathbf{s}[\mathbf{B} \mid \mathbf{B}_1 + \sum x_i \mathbf{W}_i]$

$$[\mathbf{B} \mid \mathbf{B}_1 + \sum x_i \mathbf{W}_i] \begin{pmatrix} -\sum x_i \mathbf{T}_i \\ -\underline{\mathbf{T}} \end{pmatrix} = \overbrace{-\mathbf{B}_1 \underline{\mathbf{T}}}^{\mathbf{A}} - \mathbf{x} \otimes \mathbf{G}$$

ℓ-succinct LWE

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

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

ℓ-succinct LWE

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

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

FALSIFIABLE

ℓ-succinct LWE

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

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

claim. LWE $= 1$-succinct LWE

ℓ-succinct LWE

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

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

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

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

ℓ-succinct LWE

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

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

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

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

ABE overview

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

mpk: $\mathbf{B}, \mathbf{A}, \mathbf{p}$ $\quad O(\ell)$

ct: $\mathbf{s}[\mathbf{B} \mid \mathbf{A} - \mathbf{x} \otimes \mathbf{G}] + \mathbf{e}, \mathbf{s}\mathbf{p}^\top + \mu \cdot q/2$ $\quad O(\ell)$

sk: $[\mathbf{B} \mid \mathbf{A}_f]^{-1}(\mathbf{p}^\top)$ $\quad O(1)$

ABE overview

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

mpk: $\mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}, \mathbf{B}_1, \mathbf{p}$ $\quad O(\ell^2)$

ct: $\mathbf{s}[\mathbf{B} \mid \mathbf{A} - \mathbf{x} \otimes \mathbf{G}] + \mathbf{e}, \mathbf{s}\mathbf{p}^\top + \mu \cdot q/2$ $\quad O(\ell)$

sk: $[\mathbf{B} \mid \mathbf{A}_f]^{-1}(\mathbf{p}^\top), \mathbf{A} := -\mathbf{B}_1 \underline{\mathbf{T}}$ $\quad O(1)$

ABE overview

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

mpk: $\mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}, \mathbf{B}_1, \mathbf{p}$ $\quad O(\ell^2)$

ct: $\mathbf{s}[\mathbf{B} \mid \mathbf{B}_1 + \sum x_i \mathbf{W}_i] + \mathbf{e}, \mathbf{s}\mathbf{p}^\top + \mu \cdot q/2$ $\quad O(1)$

sk: $[\mathbf{B} \mid \mathbf{A}_f]^{-1}(\mathbf{p}^\top), \mathbf{A} := -\mathbf{B}_1 \underline{\mathbf{T}}$ $\quad O(1)$

ABE overview

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

mpk: $\mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}, \mathbf{B}_1, \mathbf{p}$ $\qquad O(\ell^2)$

ct: $\mathbf{s}[\mathbf{B} \mid \mathbf{B}_1 + \sum x_i \mathbf{W}_i] + \mathbf{e}, \mathbf{s}\mathbf{p}^\top + \mu \cdot q/2$ $\qquad O(1)$

sk: $[\mathbf{B} \mid \mathbf{A}_f]^{-1}(\mathbf{p}^\top), \mathbf{A} := -\mathbf{B}_1 \underline{\mathbf{T}}$ $\qquad O(1)$

ABE overview

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

mpk: $\mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}, \mathbf{B}_1, \mathbf{p}$ $\qquad O(\ell^2)$

ct: $\mathbf{s}[\mathbf{B} \mid \mathbf{B}_1 + \sum x_i \mathbf{W}_i] + \mathbf{e}, \mathbf{s}\mathbf{p}^\top + \mu \cdot q/2$

proof. $\mathbf{B}_1 + \sum x_i \mathbf{W}_i = \mathbf{B}\mathbf{U} \Rightarrow \mathbf{A}_f = \mathbf{B}\mathbf{U}' - f(x)\mathbf{G}$

ABE : $|\textsf{mpk}| = |\textsf{ct}| = O(\ell^{2/3})$

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

mpk: $\mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell]}, \underline{\mathbf{T}}, \mathbf{B}_1, \mathbf{p}$ $\qquad O(\ell^2)$

ABE : $|\textbf{mpk}| = |\textbf{ct}| = O(\ell^{2/3})$

$$\begin{pmatrix} \mathbf{B} & & & \mathbf{W}_1 \\ & \ddots & & \vdots \\ & & \mathbf{B} & \mathbf{W}_{\ell^{1/3}} \end{pmatrix} \begin{pmatrix} \mathbf{T}_1 \\ \vdots \\ \mathbf{T}_{\ell^{1/3}} \\ \underline{\mathbf{T}} \end{pmatrix} = \begin{pmatrix} \mathbf{G} & & \\ & \ddots & \\ & & \mathbf{G} \end{pmatrix}$$

mpk: $\mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell^{1/3}]}, \underline{\mathbf{T}}, \mathbf{B}_1, \mathbf{p}$ $\qquad O(\ell^{2/3})$

ABE : $|\textsf{mpk}| = |\textsf{ct}| = O(\ell^{2/3})$

$$\begin{pmatrix} \mathbf{B} & & & \mathbf{W}_1 \\ & \ddots & & \vdots \\ & & \mathbf{B} & \mathbf{W}_{\ell^{1/3}} \end{pmatrix} \begin{pmatrix} \mathbf{T}_1 \\ \vdots \\ \mathbf{T}_{\ell^{1/3}} \\ \underline{\mathbf{T}} \end{pmatrix} = \begin{pmatrix} \mathbf{G} & & \\ & \ddots & \\ & & \mathbf{G} \end{pmatrix}$$

mpk: $\mathbf{B}, \{\mathbf{W}_i, \mathbf{T}_i\}_{i \in [\ell^{1/3}]}, \underline{\mathbf{T}}, \mathbf{B}_1, \mathbf{p}$ $\qquad O(\ell^{2/3})$

$$\mathbf{B}_1 \leftarrow \mathbb{Z}_q^{n \times \ell^{2/3} m}$$

$$\mathbf{A} := -\mathbf{B}_1 (\mathbf{I}_{\ell^{2/3}} \otimes \underline{\mathbf{T}})$$

conclusion

ABE for **circuits** from **ℓ-succinct LWE**

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

conclusion

ABE for **circuits** from **ℓ-succinct LWE**

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

open.

– poly(~~depth~~, λ)? cryptanalysis? $o(\ell^{2/3})$?

conclusion

ABE for **circuits** from ℓ-**succinct LWE**

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

open.

– poly(~~depth~~, λ)? cryptanalysis? $o(\ell^{2/3})$?

– **falsifiable** lattice assumptions

conclusion

ABE for **circuits** from **ℓ-succinct LWE**

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

open.

– poly(~~depth~~, λ)? cryptanalysis? $o(\ell^{2/3})$?

– **falsifiable** lattice assumptions

// merci !

Luca Trevisan (1971 – 2024)