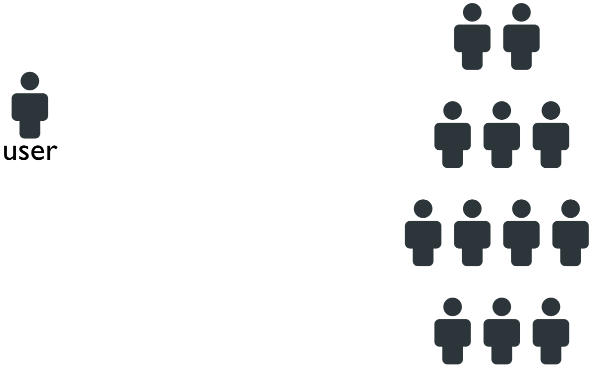
optimal broadcast encryption and CP-ABE from evasive lattice assumptions

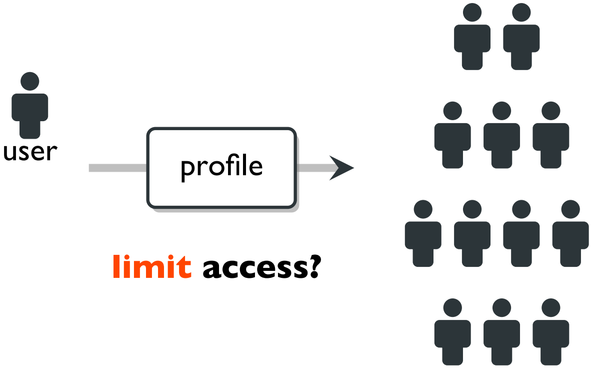
Hoeteck Wee

NTT Research & ENS

dating + big data

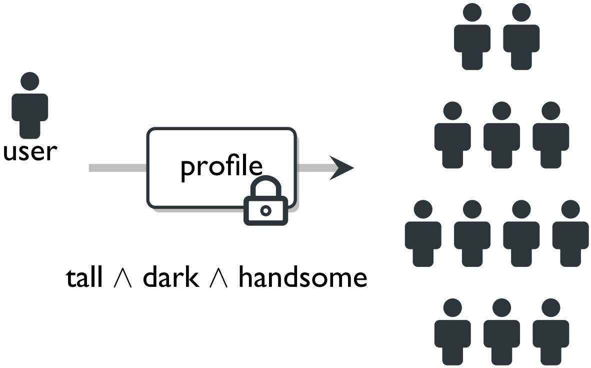


dating + big data

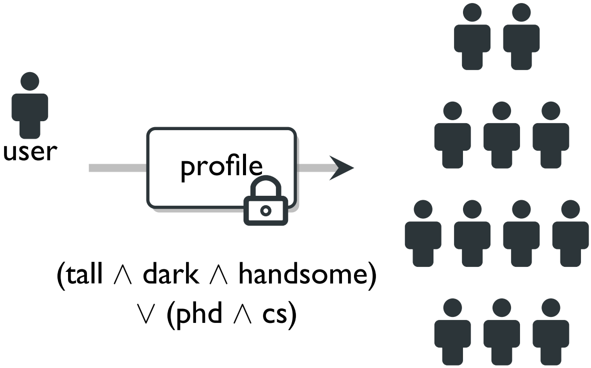


limit access?

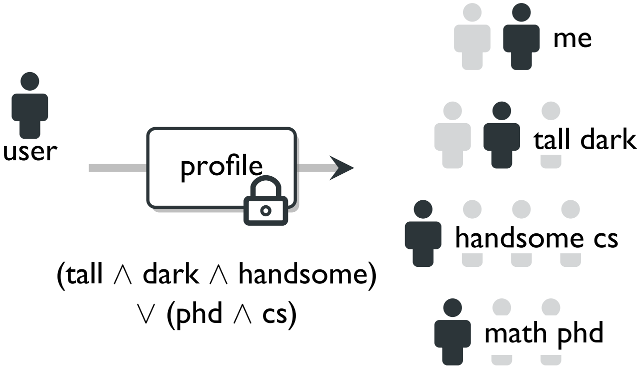
dating + big data



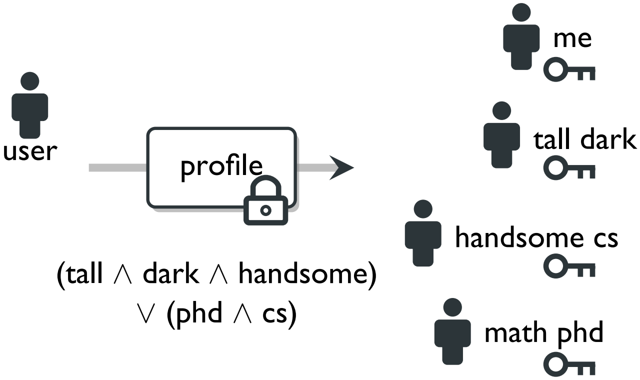
dating + big data



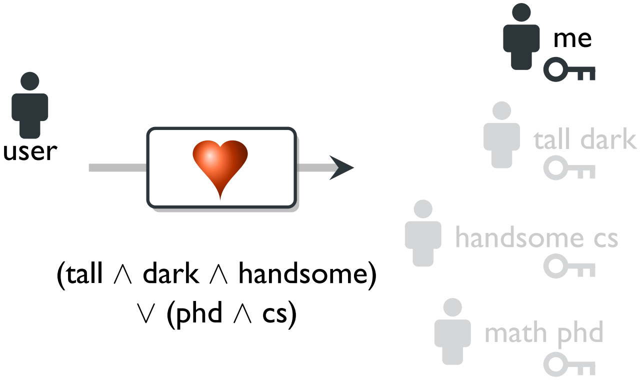
dating + big data



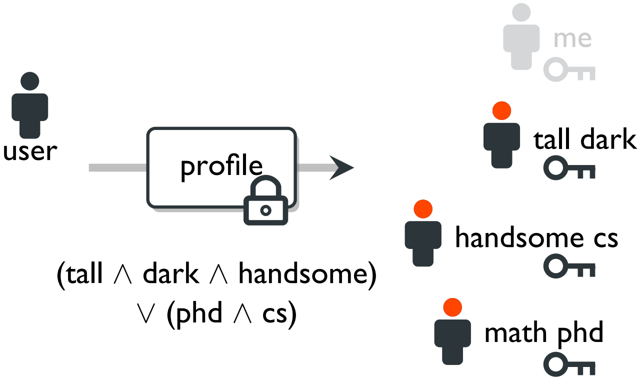
dating + big data



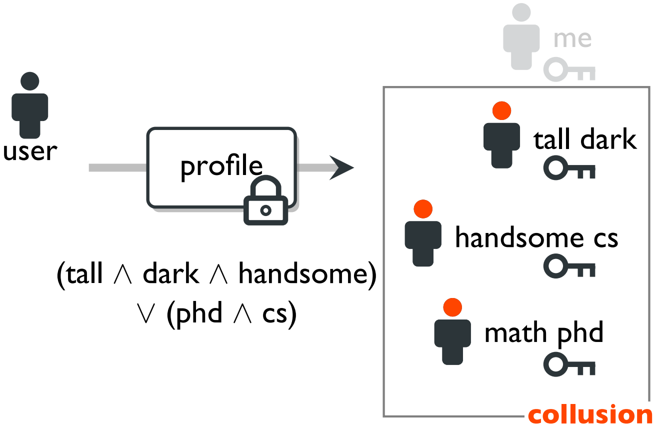
dating + big data



dating + big data



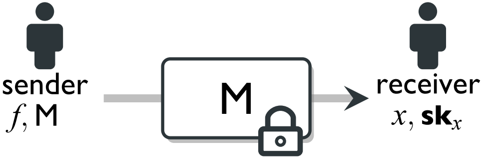
dating + big data



attribute-based encryption

ciphertext-policy

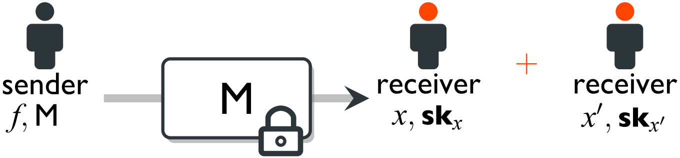
[GPSW06,SW05]



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

attribute-based encryption
ciphertext-policy

[GPSW06,SW05]

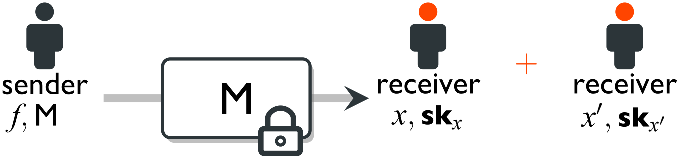


learns M $\Leftrightarrow f(x) = 0$

security against **collusions**

attribute-based encryption
ciphertext-policy

[GPSW06,SW05]



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

[GVW13, BGGHNSVV14]

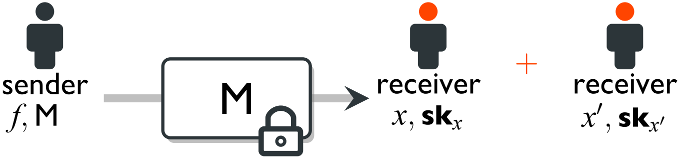
ABE for **circuits** from LWE

$$(\mathbf{A}, \mathbf{s}^\top\mathbf{A}) \approx_c \text{random}$$

attribute-based encryption

ciphertext-policy

[GPSW06,SW05]



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

[GVW13, BGGHNSVV14]

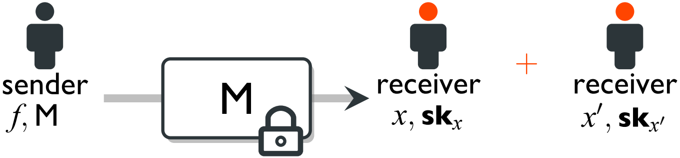
CP-ABE for **circuits** with $|\mathbf{ct}| \approx \text{size}(f)$

$(\mathbf{A}, \mathbf{s}^{\top}\mathbf{A}) \approx_c$ random

attribute-based encryption

ciphertext-policy

[GPSW06,SW05]



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

[AY20, AWY20, BV22]

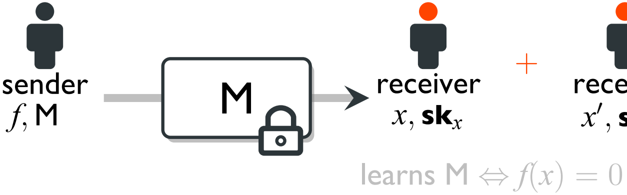
CP-ABE for **circuits** with $|\mathbf{ct}| = \text{poly(depth)} \cdot |x|$

from LWE + ...

attribute-based encryption

ciphertext-policy

[GPSW06,SW05]



[AY20, AWY20, BV22]

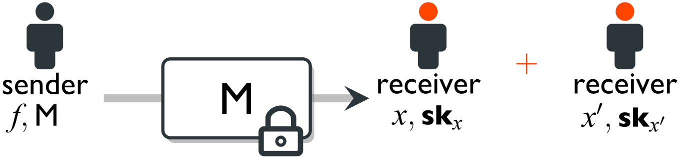
CP-ABE for **circuits** with $|\mathbf{ct}| =$ poly(depth) $\cdot\ |x|$

$\Rightarrow$ **optimal** broadcast enc // size poly$(\log N)$

attribute-based encryption

ciphertext-policy

[GPSW06,SW05]



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

[AY20, AWY20, BV22]

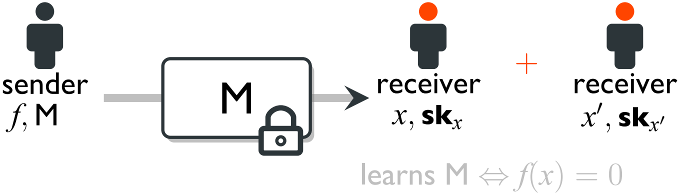
CP-ABE for **circuits** with $|\mathbf{ct}| = \text{poly(depth)} \cdot |x|$

from LWE + pairings (NC^1)

attribute-based encryption

ciphertext-policy

[GPSW06,SW05]



[AY20, AWY20, **BV22**]

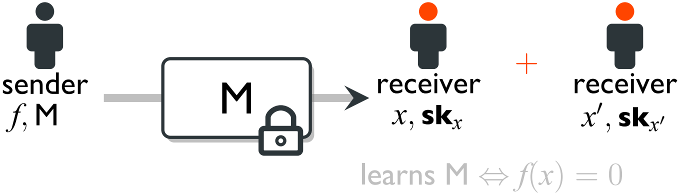
CP-ABE for **circuits** with $|\mathbf{ct}| = \text{poly(depth)} \cdot |x|$

from lattice heuristics

attribute-based encryption

ciphertext-policy

[GPSW06,SW05]



our results **[W22]**

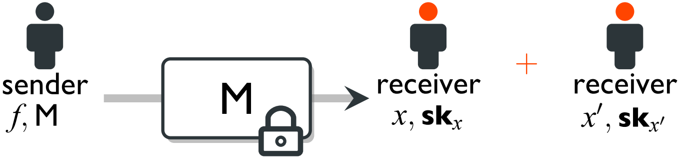
CP-ABE for **circuits** with $|\mathbf{ct}| = $ poly(depth)

from **new** lattice assumptions

attribute-based encryption

ciphertext-policy

[GPSW06,SW05]



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

our results [w22]

optimal broadcast enc // size $\mathrm{poly}(\log N)$

from **new** lattice assumptions

warm-up

fact. $[\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}] \cdot \mathbf{H}_{f,\mathbf{x}} = \mathbf{A}_f - f(\mathbf{x})\mathbf{G}$ **[BGGHNSVV14]**

warm-up

fact. $[\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}] \cdot \mathbf{H}_{f,\mathbf{x}} = \mathbf{A}_f - f(\mathbf{x})\mathbf{G}$ **[BGGHNSVV14]**

$$\mathbf{mpk} = \mathbf{A}$$

$$\overbrace{\mathbf{s}^\top \mathbf{A}_f}^{\mathbf{kem}} \quad \overbrace{\mathbf{s}^\top(\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G})}^{\mathbf{ct} \cdot \mathbf{sk}}$$

warm-up

fact. $[\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}] \cdot \mathbf{H}_{f,\mathbf{x}} = \mathbf{A}_f - f(\mathbf{x})\mathbf{G}$ **[BGGHNSVV14]**

$$\textbf{mpk} = \mathbf{A}, \mathbf{B}$$

$$\overbrace{\mathbf{s}^\top \mathbf{A}_f}^{\textbf{kem}} \quad \overbrace{\mathbf{s}^\top \mathbf{B}}^{\textbf{ct}} \cdot \overbrace{\mathbf{B}^{-1}(\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G})}^{\textbf{sk}}$$

warm-up

fact. $[\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}] \cdot \mathbf{H}_{f,\mathbf{x}} = \mathbf{A}_f - f(\mathbf{x})\mathbf{G}$ [BGGHNSVV14]

$$\textbf{mpk} = \mathbf{A}, \mathbf{B}$$

$$\overbrace{\underset{\sim}{\mathbf{s}^\top \mathbf{A}_f}}^{\textbf{kem}} \approx \overbrace{\underset{\sim}{\mathbf{s}^\top \mathbf{B}}}^{\textbf{ct}} \cdot \overbrace{\mathbf{B}^{-1}(\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G})}^{\textbf{sk}} \cdot \mathbf{H}_{f,\mathbf{x}} \quad \text{if } f(\mathbf{x}) = 0$$

warm-up

fact. $[\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}] \cdot \mathbf{H}_{f,\mathbf{x}} = \mathbf{A}_f - f(\mathbf{x})\mathbf{G}$ [BGGHNSVV14]

$$\textbf{mpk} = \mathbf{A}, \mathbf{B}$$

$$\overbrace{\mathbf{s}^\top \mathbf{A}_f}^{\textbf{kem}} \quad \overbrace{\mathbf{s}^\top \mathbf{B}}^{\textbf{ct}} \quad \overbrace{\mathbf{B}^{-1}(\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G})}^{\textbf{sk}}$$

secure for **one** key **[AY20, BV22, BK20]**

warm-up

fact. $[\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}] \cdot \mathbf{H}_{f,\mathbf{x}} = \mathbf{A}_f - f(\mathbf{x})\mathbf{G}$ [BGGHNSVV14]

$\mathsf{mpk} = \mathbf{A}, \mathbf{B}$

$$\overbrace{\mathbf{s}^\top \mathbf{A}_f}^{\mathsf{kem}} \quad \overbrace{\mathbf{s}^\top \mathbf{B}}^{\mathsf{ct}} \quad \overbrace{\mathbf{B}^{-1}(\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G})}^{\mathsf{sk}}$$

insecure for **two** keys:

$$\mathsf{ct} \cdot \mathsf{sk}_i = \boxed{\mathbf{s}^\top}(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{G}),\ i=1,2 \ \mapsto\ \mathbf{s}^\top \mathbf{G}$$

warm-up

fact. $[\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}] \cdot \mathbf{H}_{f,\mathbf{x}} = \mathbf{A}_f - f(\mathbf{x})\mathbf{G}$ [BGGHNSVV14]

$\mathsf{mpk} = \mathbf{A}, \mathbf{B}$

$$\underbrace{\mathbf{s}^\top \mathbf{A}_f}_{\text{kem}} \quad \underbrace{\mathbf{s}^\top \mathbf{B}}_{\text{ct}} \quad \underbrace{\mathbf{B}^{-1}(\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G})}_{\text{sk}}$$

insecure for **two** keys:

$$\mathsf{ct} \cdot \mathsf{sk}_i = \boxed{\mathbf{s}_i^\top}(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{G}),\ i=1,2 \ \mapsto\ \mathbf{s}^\top \mathbf{G}$$

fix. [AY20, BV22] $\mathbf{s}^\top \mapsto \mathbf{s}_i^\top$

warm-up

fact. $[\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}] \cdot \mathbf{H}_{f,\mathbf{x}} = \mathbf{A}_f - f(\mathbf{x})\mathbf{G}$ [BGGHNSVV14]

mpk $= \mathbf{A}, \mathbf{B}$

$$\overbrace{\mathbf{s}^\top \mathbf{A}_f}^{\textbf{kem}} \quad \overbrace{\mathbf{s}^\top \mathbf{B}}^{\textbf{ct}} \quad \overbrace{\mathbf{B}^{-1}(\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G})}^{\textbf{sk}}$$

insecure for **two** keys:

$$\textbf{ct} \cdot \textbf{sk}_i = \boxed{\mathbf{s}_i^\top}(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{G}),\ i=1,2 \ \mapsto\ \mathbf{s}^\top \mathbf{G}$$

fix. [AY20, **BV22**] $\mathbf{s}^\top \mapsto \mathbf{s}_i^\top \mapsto \overbrace{\mathbf{r}_i^\top}^{\textbf{sk}} \cdot \overbrace{\mathbf{S}}^{\textbf{ct}}$

candidate cp-abe for circuits

want ct $\cdot$ **sk** $= \overbrace{\mathbf{r}^\top}^{\textbf{sk}} \cdot \overbrace{\mathbf{S}}^{\textbf{ct}} \cdot (\mathbf{A} - \overbrace{\mathbf{x}^\top}^{\textbf{sk}} \otimes \mathbf{G})$

candidate cp-abe for circuits

want $\mathbf{ct} \cdot \mathbf{sk} = \overbrace{\mathbf{r}^\top}^{\mathbf{sk}} \cdot \overbrace{\mathbf{S}}^{\mathbf{ct}} \cdot (\mathbf{A} - \overbrace{\mathbf{x}^\top}^{\mathbf{sk}} \otimes \mathbf{G})$

[BV22] $\mathbf{r}$ IBE key for $\mathbf{x}$

candidate cp-abe for circuits

$$\textbf{want ct} \cdot \textbf{sk} = \overbrace{\mathbf{r}^{\top}}^{\textbf{sk}} \cdot \overbrace{\mathbf{S}}^{\textbf{ct}} \cdot (\mathbf{A} - \overbrace{\mathbf{x}^{\top}}^{\textbf{sk}} \otimes \mathbf{G})$$

$$= \mathsf{flat}(\mathbf{S})((\mathbf{A} - \mathbf{x}^{\top} \otimes \mathbf{G}) \otimes \mathbf{r})$$

$$\mathbf{S} \mapsto \mathsf{flat}(\mathbf{S})$$

candidate cp-abe for circuits

want $\mathbf{ct} \cdot \mathbf{sk} = \overbrace{\mathbf{r}^\top}^{\textsf{sk}} \cdot \overbrace{\mathbf{S}}^{\textsf{ct}} \cdot (\mathbf{A} - \overbrace{\mathbf{x}^\top}^{\textsf{sk}} \otimes \mathbf{G})$

$$\approx \overbrace{\underset{\sim}{\mathsf{flat}(\mathbf{S})\mathbf{B}}}^{\textsf{ct}} \cdot \overbrace{\mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{r})}^{\textsf{sk}}$$

candidate cp-abe for circuits

want ct · sk $= \overbrace{\mathbf{r}^\top}^{\textsf{sk}} \cdot \overbrace{\mathbf{S}}^{\textsf{ct}} \cdot (\mathbf{A} - \overbrace{\mathbf{x}^\top}^{\textsf{sk}} \otimes \mathbf{G})$

$$\approx \overbrace{\underset{\sim}{\mathsf{flat}(\mathbf{S})\mathbf{B}}}^{\textsf{ct}} \cdot \overbrace{\mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{r})}^{\textsf{sk}}$$

candidate CP-ABE for circuits

$$\textbf{ct} = \mathsf{flat}(\mathbf{S})\mathbf{B}, \quad \textbf{kem} = \mathbf{S}\mathbf{A}_f$$

$$\textbf{sk} = \mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{r}), \mathbf{r} \qquad \text{// } \mathbf{r} \text{ Gaussian}$$

candidate cp-abe for circuits

want ct · sk $= \overbrace{\mathbf{r}^\top}^{\textbf{sk}} \cdot \overbrace{\mathbf{S}}^{\textbf{ct}} \cdot (\mathbf{A} - \overbrace{\mathbf{x}^\top}^{\textbf{sk}} \otimes \mathbf{G})$

$$\approx \overbrace{\underset{\sim}{\mathsf{flat}(\mathbf{S})\mathbf{B}}}^{\textbf{ct}} \cdot \overbrace{\mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{r})}^{\textbf{sk}}$$

candidate CP-ABE for circuits *proof?*

$\textbf{ct} = \underset{\sim}{\mathsf{flat}(\mathbf{S})\mathbf{B}}, \quad \textbf{kem} = \underset{\sim}{\mathbf{S}\mathbf{A}_f}$

$\textbf{sk} = \mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{r}), \mathbf{r}$ // $\mathbf{r}$ Gaussian

candidate cp-abe for circuits

want ct · sk = $\overbrace{\mathbf{r}_i^\top \cdot \mathbf{S} \cdot (\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{G})}^{\mathbf{ct}\cdot\mathbf{sk}_i}$

$$\approx \overbrace{\underset{\sim}{\text{flat}(\mathbf{S})\mathbf{B}}}^{\mathbf{ct}} \cdot \overbrace{\mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{r})}^{\mathbf{sk}}$$

candidate CP-ABE **step 1.** $\mathbf{ct} \cdot \mathbf{sk}_i \approx_c$ random

ct $= \text{flat}(\mathbf{S})\mathbf{B}$, **kem** $= \mathbf{S}\mathbf{A}_f$

sk $= \mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{r}), \mathbf{r}$ // $\mathbf{r}$ Gaussian

proof (attempt)

fact 1. by LWE

$$\underset{\sim}{\mathbf{r}_i^\top \mathbf{S}} \qquad \approx_c \mathbf{s}_i^\top$$

proof (attempt)

fact 1. by LWE, if $\mathbf{A}$ has low-norm:

$$\mathbf{r}_i^\top \mathbf{S}(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I}) \approx_c \mathbf{s}_i^\top (\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I})$$

proof (attempt)

fact 1. by LWE, if $\mathbf{A}$ has low-norm:

$$\underset{\sim}{\mathbf{r}_i^\top \mathbf{S}(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I})} \approx_c \underset{\sim}{\mathbf{s}_i^\top (\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I})} \approx_c \text{random}$$

proof (attempt)

fact 1. by LWE, if $\mathbf{A}$ has low-norm:

$$\mathbf{r}_i^\top \mathbf{S}(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I}) \approx_c \mathbf{s}_i^\top(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I}) \approx_c \text{random}$$

fact 2. $[\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{I}] \cdot \mathbf{H}_{f,\mathbf{x}} = \mathbf{A}_f - f(\mathbf{x})\mathbf{I}$

$$|\mathbf{H}_{f,\mathbf{x}}| = \lambda^{O(2^{\text{depth}})} \cdot \text{size}, |\textbf{ct}|, |\textbf{sk}| \approx 2^{\text{depth}}$$

proof (attempt)

fact 1. by LWE, if $\mathbf{A}$ has low-norm:

$$\mathbf{r}_i^\top \mathbf{S}(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I}) \approx_c \mathbf{s}_i^\top (\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I}) \approx_c \text{random}$$

fact 2. $[\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{I}] \cdot \mathbf{H}_{f,\mathbf{x}} = \mathbf{A}_f - f(\mathbf{x})\mathbf{I}$

$|\mathbf{H}_{f,\mathbf{x}}| = \lambda^{O(2^{\text{depth}})} \cdot \text{size}, |\mathbf{ct}|, |\mathbf{sk}| \approx 2^{\text{depth}}$

$\times$ circuits : $2^{\text{depth}} \approx$ size

✓ broadcast : depth = $O(\log \log N)$, size = $O(N)$

proof (attempt)

fact 1. by LWE, if $\mathbf{A}$ has low-norm:

$$\underbrace{\mathbf{r}_i^\top \mathbf{S}(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I})}_{\mathbf{ct}\cdot\mathbf{sk}_i} \approx_c \mathbf{s}_i^\top(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I}) \approx_c \text{random}$$

$$\overbrace{\text{flat}(\mathbf{S})\mathbf{B}}^{\mathbf{ct}}, \overbrace{\mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I}) \otimes \mathbf{r}_i)}^{\mathbf{sk}_i}$$

proof (attempt)

fact 1. by LWE, if $\mathbf{A}$ has low-norm:

$$\underbrace{\mathbf{r}_i^\top \mathrm{S}(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I})}_{\mathbf{ct}\cdot\mathbf{sk}_i} \approx_c \mathbf{s}_i^\top(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I}) \approx_c \text{random}$$

step 2. $(\mathbf{ct}, \mathbf{sk}_i) \approx_c (\text{random}, \mathbf{sk}_i)$

$$\overbrace{\mathrm{flat}(\mathrm{S})\mathbf{B}}^{\mathbf{ct}}, \overbrace{\mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I}) \otimes \mathbf{r}_i)}^{\mathbf{sk}_i}$$

proof (attempt)

fact 1. by LWE, if $\mathbf{A}$ has low-norm:

$$\underbrace{\mathbf{r}_i^\top \mathbf{S}(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I})}_{\mathbf{ct}\cdot\mathbf{sk}_i} \approx_c \mathbf{s}_i^\top(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I}) \approx_c \text{random}$$

step 2. $(\mathbf{ct}, \mathbf{sk}_i) \approx_c (\text{random}, \mathbf{sk}_i)$

$$\overbrace{\text{flat}(\mathbf{S})\mathbf{B}}^{\mathbf{ct}},\ \overbrace{\mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{I}) \otimes \mathbf{r}_i)}^{\mathbf{sk}_i}$$

intuition. $\mathbf{s}^\top\mathbf{B}, \mathbf{B}^{-1}(\mathbf{P})$ only "leaks" $\mathbf{s}^\top\mathbf{P}$

evasive LWE [W22, T22]

evasive LWE [W22, T22]

assumption. fix distribution $\mathbf{P}$

if $\mathbf{s}^{\top}[\mathbf{B} \mid \mathbf{P} \quad] \approx_c$ random

then $\mathbf{s}^{\top}[\mathbf{B} \quad] \approx_c$ random given $\mathbf{B}^{-1}(\mathbf{P})$

evasive LWE [W22, T22]

assumption. fix distribution $\mathbf{P}$

if $\mathbf{s}^\top[\mathbf{B} \mid \mathbf{P} \quad\quad] \approx_c$ random given $\mathbf{B}, \mathbf{P}$

then $\mathbf{s}^\top[\mathbf{B} \quad\quad] \approx_c$ random given $\mathbf{B}^{-1}(\mathbf{P}), \mathbf{B}$

evasive LWE [W22, T22]

assumption. fix distribution $\mathbf{P}$

if $\mathbf{s}^\top[\mathbf{B} \mid \mathbf{P} \quad] \approx_c$ random given $\mathbf{B}, \mathbf{P}$

then $\mathbf{s}^\top[\mathbf{B} \quad] \approx_c$ random given $\mathbf{B}^{-1}(\mathbf{P}), \mathbf{B}$

examples. $\mathbf{P}$ uniform (both true via LWE)

evasive LWE [W22, T22]

assumption. fix distribution $\mathbf{P}$

if $\mathbf{s}^\top[\mathbf{B} \mid \mathbf{P} \quad] \approx_c$ random given $\mathbf{B}, \mathbf{P}$

then $\mathbf{s}^\top[\mathbf{B} \quad] \approx_c$ random given $\mathbf{B}^{-1}(\mathbf{P}), \mathbf{B}$

examples. $\mathbf{P} = \mathbf{G}$ (both false)

evasive LWE [W22, T22]

assumption. fix distribution $\mathbf{P}$

if $\mathbf{s}^\top[\mathbf{B} \mid \mathbf{P} \quad\quad] \approx_c$ random given $\mathbf{B}, \mathbf{P}$

then $\mathbf{s}^\top[\mathbf{B} \quad\quad] \approx_c$ random given $\mathbf{B}^{-1}(\mathbf{P}), \mathbf{B}$

avoids zeroizing attacks [CHLRS15, CLLT16, MSZ16, ...]

evasive LWE [W22, T22]

assumption. fix distributions $\mathbf{P}, \mathbf{A}'$

if $\mathbf{s}^\top[\mathbf{B} \mid \mathbf{P} \mid \mathbf{A}'] \approx_c$ random given $\mathbf{B}, \mathbf{P}, \mathbf{A}'$

then $\mathbf{s}^\top[\mathbf{B} \mid \mathbf{A}'] \approx_c$ random given $\mathbf{B}^{-1}(\mathbf{P}), \mathbf{B}, \mathbf{A}'$

proof (almost)

$$\textbf{mpk} = \mathbf{A}, \mathbf{B}$$

$$\textbf{ct} = \underbrace{\mathrm{flat}(\mathbf{S})\mathbf{B}}, \qquad \textbf{kem} = \underbrace{\mathbf{S}\mathbf{A}_f}$$

$$\textbf{sk} = \mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{I}) \otimes \mathbf{r}), \mathbf{r}$$

summary. $(\textbf{ct}, \textbf{sk}_i) \approx_c (\text{random}, \textbf{sk}_i)$

proof (almost)

$\textbf{mpk} = \mathbf{A}, \mathbf{B}$

$\textbf{ct} = \underbrace{\text{flat}(\mathbf{S})\mathbf{B}}, \qquad \textbf{kem} = \underbrace{\mathbf{S}\mathbf{A}_f}$

$\textbf{sk} = \mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{I}) \otimes \mathbf{r}), \mathbf{r}$

summary. $(\textbf{ct}, \textbf{sk}_i) \not\approx_c (\text{random}, \textbf{sk}_i)$ given **kem**

proof (almost)

$$\textbf{mpk} = \mathbf{A}, \mathbf{B}$$

$$\textbf{ct} = \mathrm{flat}(\mathbf{S})\mathbf{B}, \qquad \textbf{kem} = \mathbf{S}\mathbf{A}_f + \mathbf{S}_0\mathbf{A}_0$$

$$\textbf{sk} = \mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{I}) \otimes \mathbf{r}), \mathbf{r}$$

fix. **kem** leaks $\mathbf{r}_i\mathbf{S}\mathbf{A}_f$ instead of $\mathbf{S}\mathbf{A}_f$.

proof (final)

$\textbf{mpk} = \mathbf{A}, \mathbf{B}, \mathbf{A}_0, \mathbf{B}_0$

$\textbf{ct} = \underbrace{\mathsf{flat}(\mathbf{S})\mathbf{B}}, \underbrace{\mathsf{flat}(\mathbf{S}_0)\mathbf{B}_0}, \quad \textbf{kem} = \underbrace{\mathbf{S}\mathbf{A}_f + \mathbf{S}_0\mathbf{A}_0}$

$\textbf{sk} = \mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{I}) \otimes \mathbf{r}), \mathbf{r}, \mathbf{B}_0^{-1}(\mathbf{A}_0 \otimes \mathbf{r})$

proof (final)

$$\textbf{mpk} = \mathbf{A}, \mathbf{B}, \mathbf{A}_0, \mathbf{B}_0$$

$$\textbf{ct} = \text{flat}(\mathbf{S})\mathbf{B},\ \text{flat}(\mathbf{S}_0)\mathbf{B}_0, \qquad \textbf{kem} = \mathbf{S}\mathbf{A}_f + \mathbf{S}_0\mathbf{A}_0$$

$$\textbf{sk} = \mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{I}) \otimes \mathbf{r}), \mathbf{r}, \mathbf{B}_0^{-1}(\mathbf{A}_0 \otimes \mathbf{r})$$

thm. assuming sub-exp evasive LWE (+ LWE)

1 **optimal** broadcast enc // size poly$(\log N)$

proof (final)

$$\textbf{mpk} = \mathbf{A}, \mathbf{B}, \mathbf{A}_0, \mathbf{B}_0$$

$$\textbf{ct} = \underset{\sim}{\text{flat}(\mathbf{S})\mathbf{B}},\ \underset{\sim}{\text{flat}(\mathbf{S}_0)\mathbf{B}_0}, \quad \textbf{kem} = \underset{\sim}{\mathbf{S}\mathbf{A}_f + \mathbf{S}_0\mathbf{A}_0}$$

$$\textbf{sk} = \mathbf{B}^{-1}((\mathbf{A} - \mathbf{x}^\top \otimes \mathbf{G}) \otimes \mathbf{r}), \mathbf{r}, \mathbf{B}_0^{-1}(\mathbf{A}_0 \otimes \mathbf{r})$$

thm. assuming sub-exp evasive LWE (+ LWE)

1. **optimal** broadcast enc // size poly$(\log N)$
2. **compact** CP-ABE for circuits, assuming

$$\mathbf{A}, \mathbf{r}_i, \underset{\sim}{\mathbf{r}_i\mathbf{S}(\mathbf{A} - \mathbf{x}_i^\top \otimes \mathbf{G})} \approx_c \text{random}$$

conclusion

this. broadcast enc, CP-ABE, evasive LWE

conclusion

this. broadcast enc, CP-ABE, evasive LWE

open.

– evasive LWE: crypt-analysis? reductions?

– applications? witness encryption [**T22, VWW22**]

– CP-ABE for circuits from *just* evasive LWE

conclusion

this. broadcast enc, CP-ABE, evasive LWE

open.

– evasive LWE: crypt-analysis? reductions?

– applications? witness encryption [**T22, VWW22**]

– CP-ABE for circuits from *just* evasive LWE

// merci !