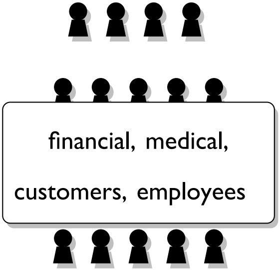
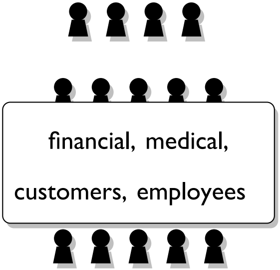
encrypted computation *from* lattices

Hoeteck Wee
ENS, Paris

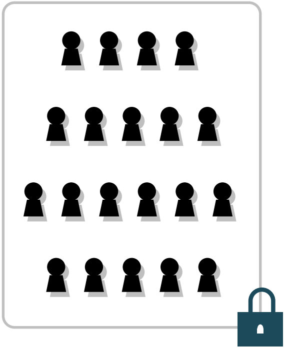


BIG DATA



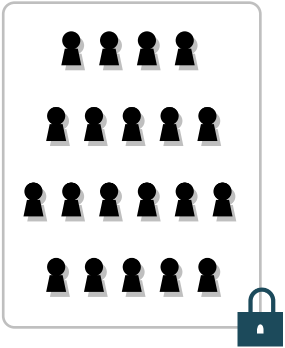
BIG DATA

Q. privacy?



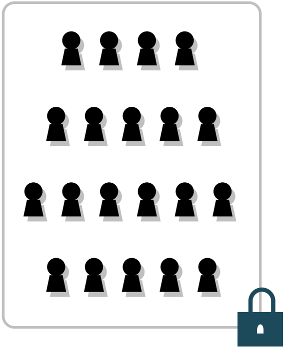
BIG DATA

Q. privacy?



BIG DATA

Q. utility + privacy?

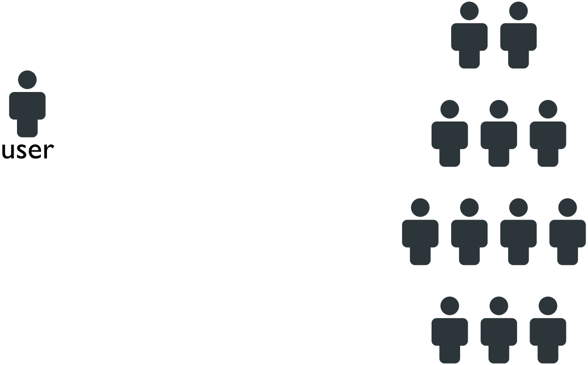


BIG DATA

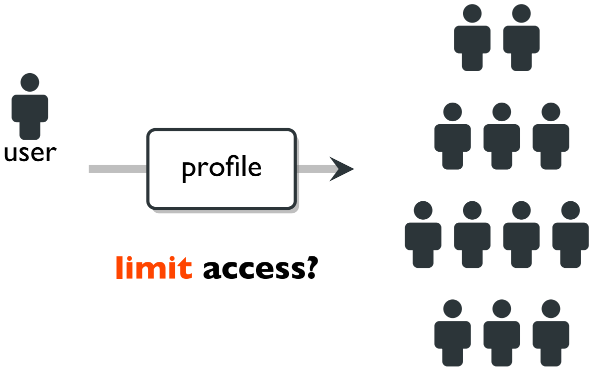
Q. utility + privacy?

encrypted computation

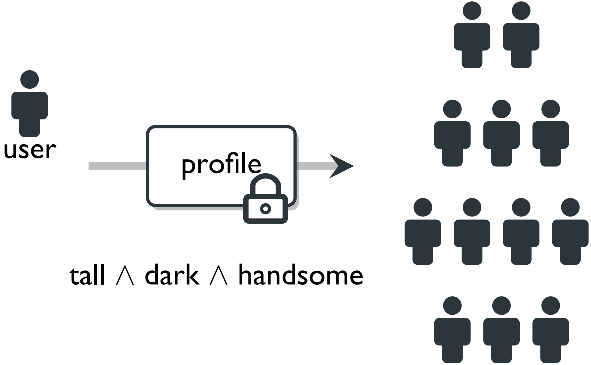
dating + big data



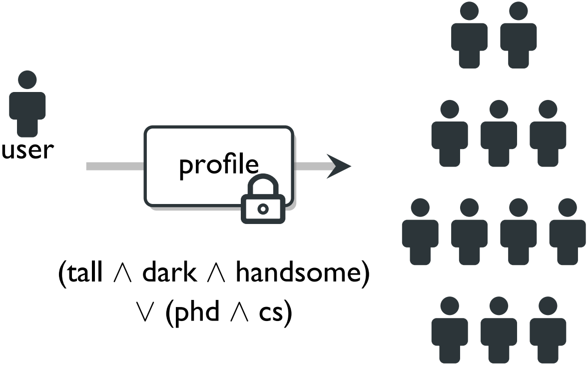
dating + big data



dating + big data

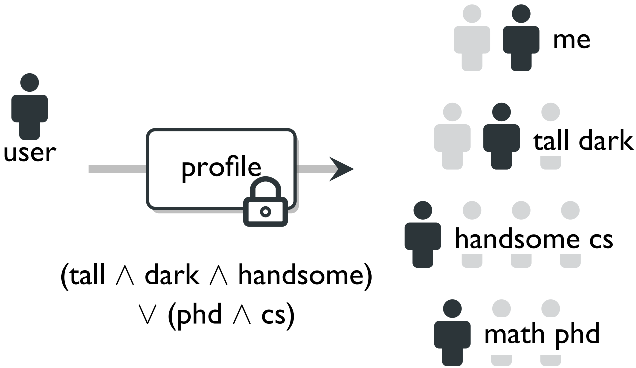


dating + big data



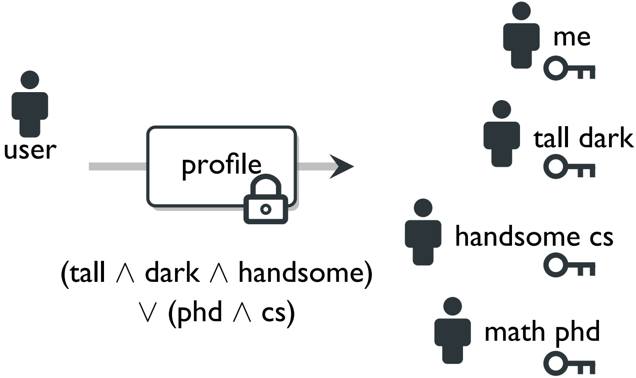
$(\text{tall} \wedge \text{dark} \wedge \text{handsome})$
$\vee\ (\text{phd} \wedge \text{cs})$

dating + big data

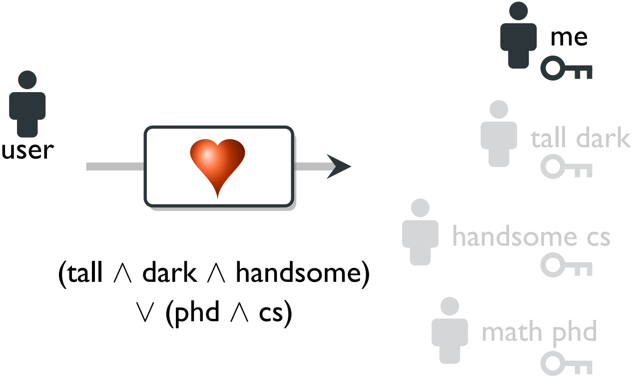


$(\text{tall} \wedge \text{dark} \wedge \text{handsome})$
$\vee\ (\text{phd} \wedge \text{cs})$

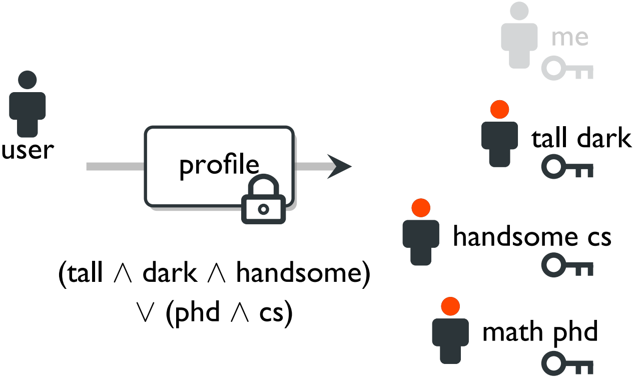
dating + big data



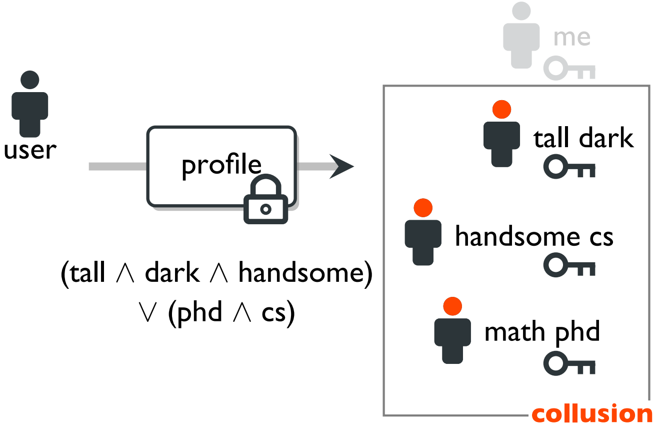
dating + big data



dating + big data



dating + big data



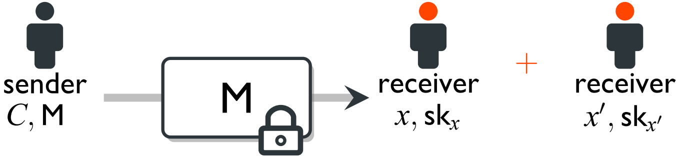
attribute-based encryption

[GPSW06,SW05]

learns M $\Leftrightarrow C(x) = 1$

attribute-based encryption

[GPSW06,SW05]

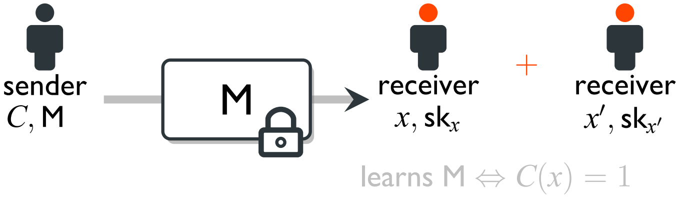


learns M $\Leftrightarrow C(x) = 1$

security against **collusions**

attribute-based encryption

[GPSW06,SW05]

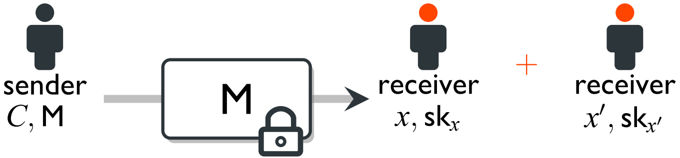


prior works.

[BF01, CHK04, BB04, GPSW06, W09, LW10, LOSTW10, OT10, ...]

attribute-based encryption

[GPSW06,SW05]

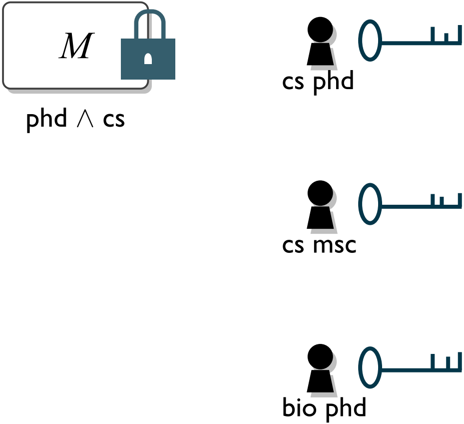


learns M $\Leftrightarrow C(x) = 1$

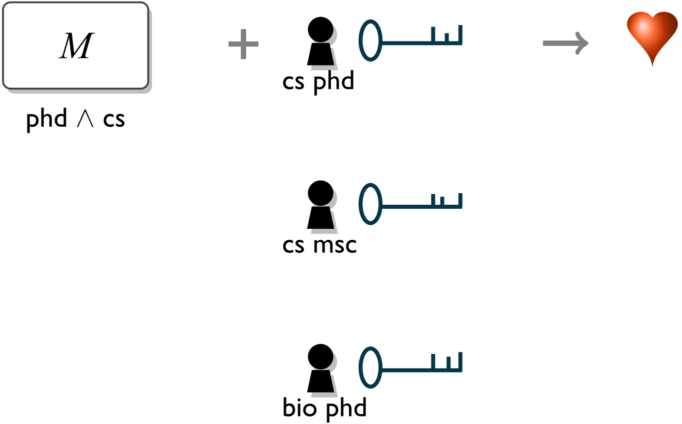
[Gorbunov Vaikuntanathan W 13]

attribute-based encryption for **circuits**

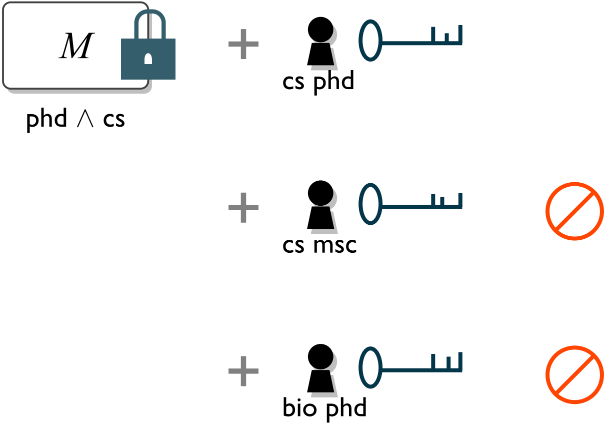
attribute-based encryption



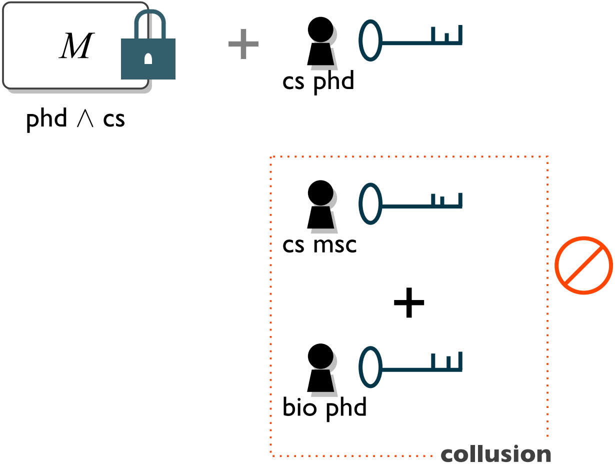
attribute-based encryption



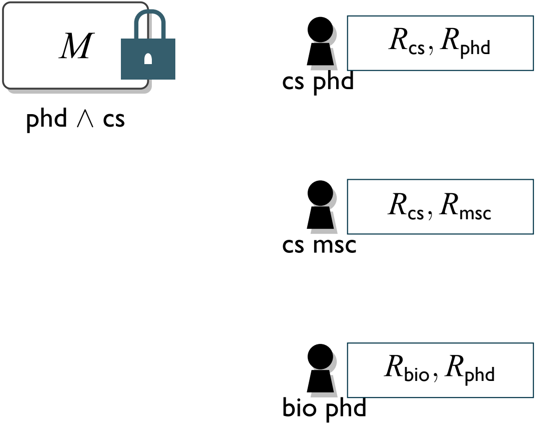
attribute-based encryption



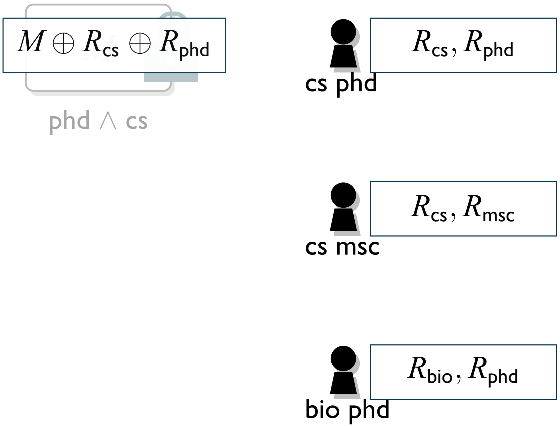
attribute-based encryption



attribute-based encryption



attribute-based encryption



attribute-based encryption

$M \oplus R_{\text{cs}} \oplus R_{\text{phd}}$ + $R_{\text{cs}}, R_{\text{phd}}$ $\rightarrow$ M

phd $\wedge$ cs

cs phd

$R_{\text{cs}}, R_{\text{msc}}$

cs msc

$R_{\text{bio}}, R_{\text{phd}}$

bio phd

attribute-based encryption

$M \oplus R_{\text{cs}} \oplus R_{\text{phd}}$

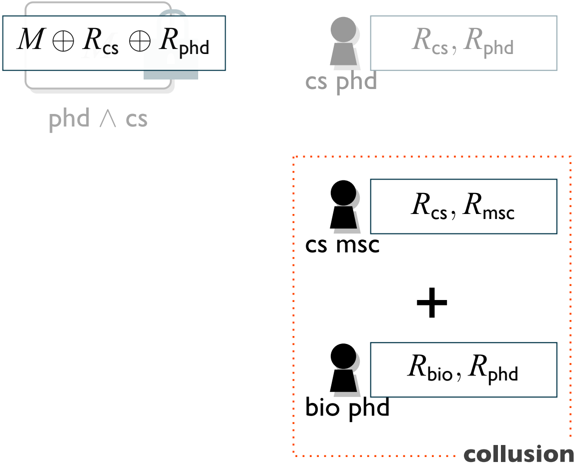
phd ∧ cs

cs phd $R_{\text{cs}}, R_{\text{phd}}$

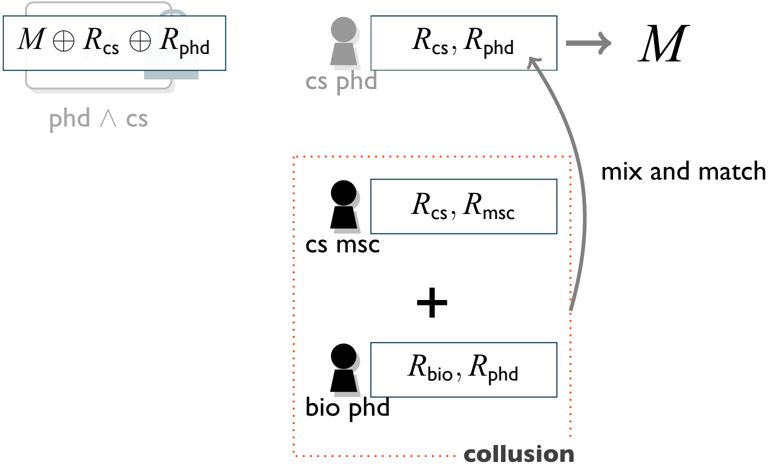
+ cs msc $R_{\text{cs}}, R_{\text{msc}}$

+ bio phd $R_{\text{bio}}, R_{\text{phd}}$

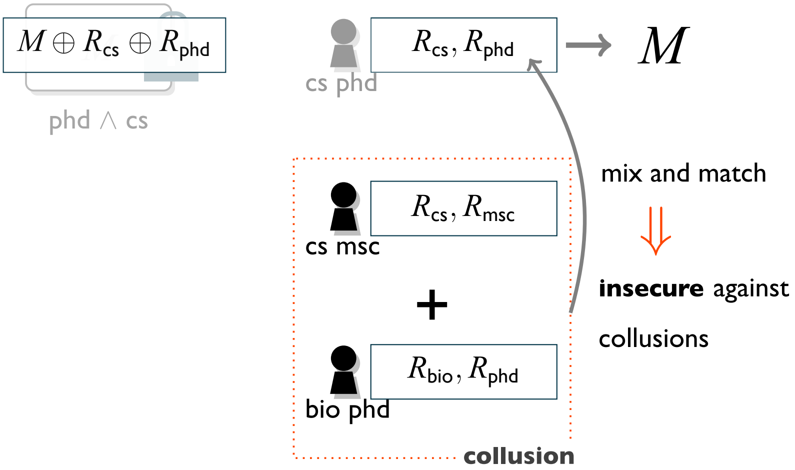
attribute-based encryption



attribute-based encryption



attribute-based encryption



attribute-based encryption

Key Idea. [GVW13]

strings $R \rightarrow$ functions $\phi(\cdot)$

one-use $\rightarrow$ many-use

$R_{\text{cs}}, R_{\text{phd}}$

$R_{\text{cs}}, R_{\text{msc}}$

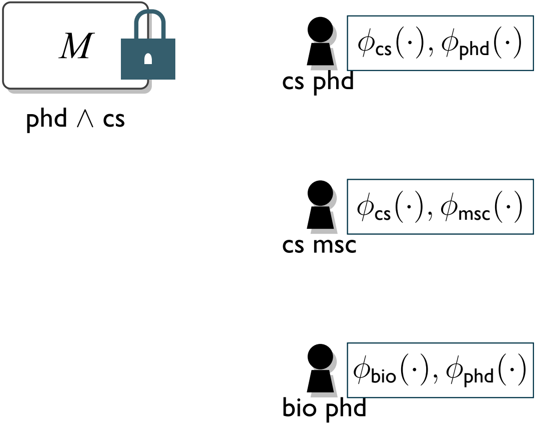
cs msc

$R_{\text{bio}}, R_{\text{phd}}$

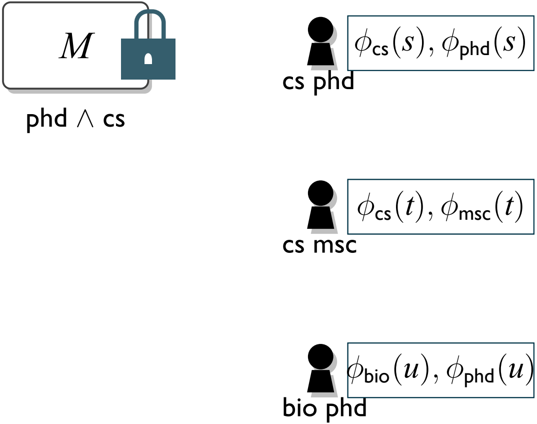
bio phd

mix and match

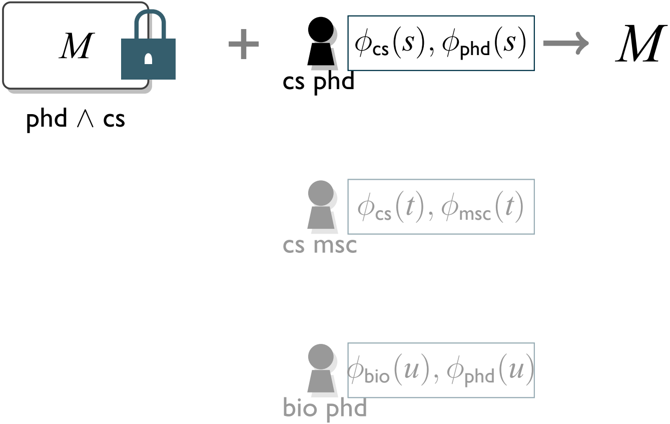
attribute-based encryption



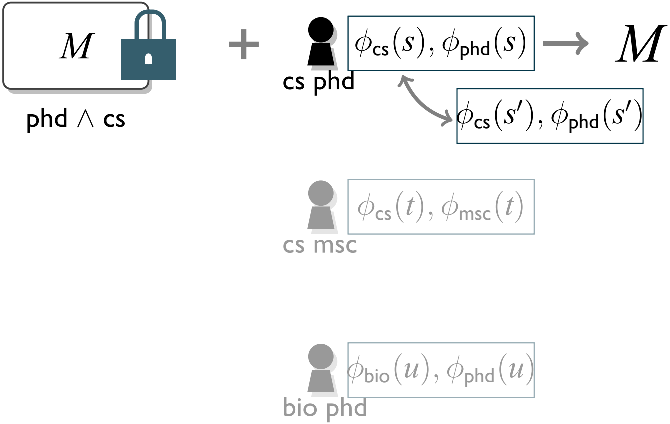
attribute-based encryption



attribute-based encryption



attribute-based encryption



attribute-based encryption

M

phd $\wedge$ cs

$\phi_{\text{cs}}(s), \phi_{\text{phd}}(s)$

cs phd

$\phi_{\text{cs}}(t), \phi_{\text{msc}}(t)$

cs msc

+

$\phi_{\text{bio}}(u), \phi_{\text{phd}}(u)$

bio phd

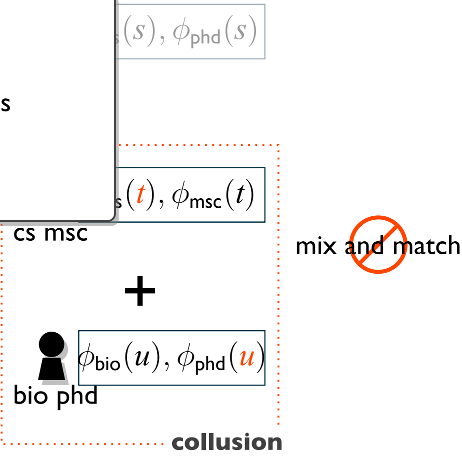
collusion

mix and match

attribute-based encryption

theorem. [GVW13]

secure against collusions

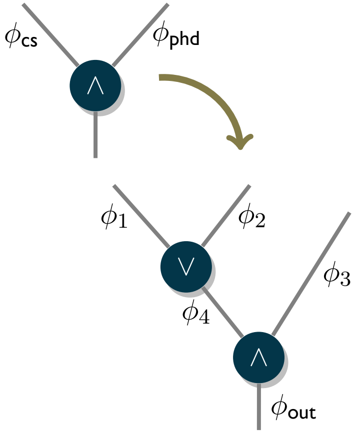


attribute-based encryption

theorem. [GVW13]

secure against collusions

works for general **circuits**

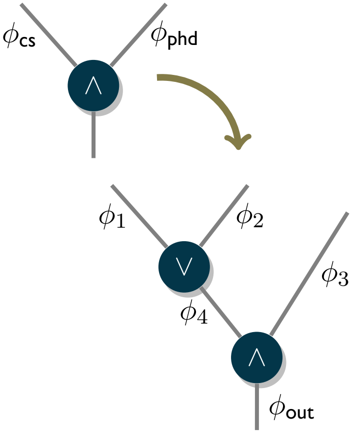


attribute-based encryption

theorem. **[GVW13]**

secure against collusions

works for general **circuits**



prior. shallow circuits

[GPSW06, OT10, B13, ...]

attribute-based encryption

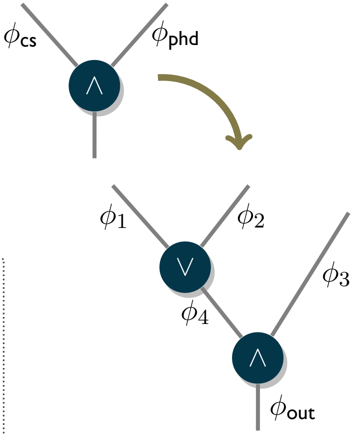
theorem. [GVW13]

secure against collusions

works for general **circuits**

$$\mathbf{A}\,\mathbf{s} + \mathbf{e} \approx_c \mathbf{u}$$

learning with errors [**R05**]



fully **homomorphic** encryption
& **lattice** tool-kit

fully **homomorphic** encryption

fully **homomorphic** encryption

syntax. $\textbf{enc}(\mathsf{sk}, \cdot), \textbf{dec}(\mathsf{sk}, \cdot)$

functionality. $\textbf{dec}(\mathsf{sk}, \textbf{enc}(\mathsf{sk}, x)) = x$

fully **homomorphic** encryption

security. $\textbf{enc}(\mathrm{sk}, x)$ hides x

functionality. $\textbf{dec}(\mathrm{sk}, \textbf{enc}(\mathrm{sk}, x)) = x$

fully **homomorphic** encryption

security. $\textbf{enc}(\mathsf{sk}, x)$ hides x

functionality. $\textbf{enc}(\mathsf{sk}, x) \mapsto \textbf{enc}(\mathsf{sk}, f(x))$

fully **homomorphic** encryption

security. $\mathbf{enc}(\mathsf{sk}, x)$ hides x

functionality. $\mathbf{enc}(\mathsf{sk}, x) \mapsto \mathbf{enc}(\mathsf{sk}, f(x))$

fully **homomorphic** encryption

security. **enc**(sk, x) hides x

functionality. **enc**$(\mathsf{sk}, x) \mapsto$ **enc**$(\mathsf{sk}, f(x))$

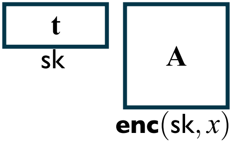
$\underset{\mathsf{sk}}{\boxed{\;\mathbf{t}\;}}$

[Gentry Sahai Waters 13]

fully **homomorphic** encryption

security. **enc**(sk, x) hides x

functionality. **enc**$(\mathsf{sk}, x) \mapsto$ **enc**$(\mathsf{sk}, f(x))$



[Gentry Sahai Waters 13]

fully **homomorphic** encryption

security. **enc**(sk, x) hides x

functionality. **enc**$(\mathsf{sk}, x) \mapsto$ **enc**$(\mathsf{sk}, f(x))$

$$\underbrace{\boxed{\mathbf{t}}}_{\mathsf{sk}} \; \underbrace{\boxed{\mathbf{A}}}_{\mathbf{enc}(\mathsf{sk},x)} = \boxed{x\,\mathbf{t}}$$

$\mathbf{t}$: eigenvector

[Gentry Sahai Waters 13]

fully **homomorphic** encryption

security. **enc**(sk, x) hides x

functionality. **enc**$(\mathsf{sk}, x) \mapsto$ **enc**$(\mathsf{sk}, f(x))$

$$\underbrace{\boxed{\mathbf{t}}}_{\mathsf{sk}} \; \underbrace{\boxed{\mathbf{A}_i}}_{\mathbf{enc}(\mathsf{sk}, x_i)} = \boxed{x_i\,\mathbf{t}}$$

$\mathbf{t}$: eigenvector

[Gentry Sahai Waters 13]

$$\mathbf{enc}(\mathsf{sk}, x_1), \mathbf{enc}(\mathsf{sk}, x_2) \overset{?}{\mapsto} \mathbf{enc}(\mathsf{sk}, x_1 + x_2), \mathbf{enc}(\mathsf{sk}, x_1 x_2)$$

fully **homomorphic** encryption

security. **enc**(sk, x) hides x

functionality. **enc**(sk, x) $\mapsto$ **enc**(sk, $f(x)$)

$$\underbrace{\boxed{\;\mathbf{t}\;}}_{\text{sk}}\;\underbrace{\boxed{\;\mathbf{A}_i\;}}_{\textbf{enc}(\text{sk},\,x_i)} = \boxed{\;x_i\,\mathbf{t}\;}$$

addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) = (x_1 + x_2)\mathbf{t}$

fully **homomorphic** encryption

security. **enc**(sk, x) hides x

functionality. **enc**(sk, x) $\mapsto$ **enc**(sk, $f(x)$)

$$\underset{\mathsf{sk}}{\boxed{\mathbf{t}}}\ \underset{\mathbf{enc}(\mathsf{sk},\, x_i)}{\boxed{\mathbf{A}_i}} = \boxed{x_i\,\mathbf{t}}$$

addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) = (x_1 + x_2)\mathbf{t}$

multiplication: $\mathbf{t} \cdot \qquad\qquad = x_1 x_2 \mathbf{t}$

fully **homomorphic** encryption

security. **enc**(sk, x) hides x

functionality. **enc**(sk, x) $\mapsto$ **enc**(sk, $f(x)$)

$$\underbrace{\boxed{\mathbf{t}}}_{\mathsf{sk}} \; \underbrace{\boxed{\mathbf{A}_i}}_{\mathbf{enc}(\mathsf{sk},\, x_i)} = \boxed{x_i \, \mathbf{t}}$$

addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) = (x_1 + x_2)\mathbf{t}$

multiplication: $\mathbf{t} \cdot \mathbf{A}_1 \mathbf{A}_2 = x_1 x_2 \mathbf{t}$

fully **homomorphic** encryption

security. **enc**(sk, x) hides x

functionality. **enc**$(\mathsf{sk}, x) \mapsto$ **enc**$(\mathsf{sk}, f(x))$

$$\underbrace{\boxed{\mathbf{t}}}_{\mathsf{sk}}\ \underbrace{\boxed{\mathbf{A}_i}}_{\mathbf{enc}(\mathsf{sk},\, x_i)} = \boxed{x_i\, \mathbf{t}}$$

addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) = (x_1 + x_2)\mathbf{t}$

multiplication: $\mathbf{t} \cdot \mathbf{A}_1 \mathbf{A}_2 = x_1 x_2 \mathbf{t}$

polynomials: $\mathbf{t} \cdot (\mathbf{A}_1\mathbf{A}_2 + \mathbf{A}_3\mathbf{A}_4) = (x_1 x_2 + x_3 x_4)\mathbf{t}$

fully **homomorphic** encryption

security. **enc**(sk, x) hides x

functionality. **enc**$(\mathsf{sk}, x) \mapsto$ **enc**$(\mathsf{sk}, f(x))$

$$\underset{\mathsf{sk}}{\boxed{\mathbf{t}}}\ \underset{\mathbf{enc}(\mathsf{sk}, x_i)}{\boxed{\mathbf{A}_i}} = \boxed{x_i\,\mathbf{t}}$$

addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) = (x_1 + x_2)\mathbf{t}$

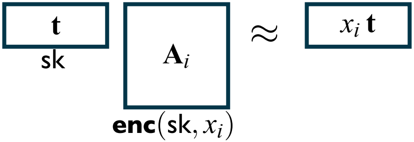
multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 = x_1 x_2 \mathbf{t}$

polynomials: $\mathbf{t} \cdot \underbrace{f(\mathbf{A}_1, \ldots, \mathbf{A}_n)}_{\mathbf{A}_f} = f(x_1, \ldots, x_n)\mathbf{t}$

fully **homomorphic** encryption

security. $\textbf{enc}(\mathsf{sk}, x)$ hides x

functionality. $\textbf{enc}(\mathsf{sk}, x) \mapsto \textbf{enc}(\mathsf{sk}, f(x))$



addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) = (x_1 + x_2)\mathbf{t}$

multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 = x_1 x_2 \mathbf{t}$

fully **homomorphic** encryption

security. $\mathbf{enc}(\mathsf{sk}, x)$ hides x

functionality. $\mathbf{enc}(\mathsf{sk}, x) \mapsto \mathbf{enc}(\mathsf{sk}, f(x))$

$$\underset{\mathsf{sk}}{\boxed{\;\mathbf{t}\;}} \;\; \underset{\mathbf{enc}(\mathsf{sk}, x_i)}{\boxed{\;\mathbf{A}_i\;}} \approx \boxed{\;x_i\,\mathbf{t}\;}$$

addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) \approx (x_1 + x_2)\mathbf{t}$

– *proof.* small + small = small

fully **homomorphic** encryption

security. $\mathbf{enc}(\mathsf{sk}, x)$ hides x

functionality. $\mathbf{enc}(\mathsf{sk}, x) \mapsto \mathbf{enc}(\mathsf{sk}, f(x))$

$$\underbrace{\boxed{\mathbf{t}}}_{\mathsf{sk}} \; \underbrace{\boxed{\mathbf{A}_i}}_{\mathbf{enc}(\mathsf{sk}, x_i)} \approx \boxed{x_i \, \mathbf{t}}$$

addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) \approx (x_1 + x_2)\mathbf{t}$

multiplication: $\mathbf{t} \cdot \mathbf{A}_1 \mathbf{A}_2 \not\approx x_1 x_2 \mathbf{t}$

– *proof.* small $\cdot \mathbf{A}_2$ = big

fully **homomorphic** encryption

security. **enc**(sk, x) hides x

functionality. **enc**(sk, x) $\mapsto$ **enc**(sk, $f(x)$)

$$\underset{\mathsf{sk}}{\boxed{\mathbf{t}}}\ \underset{\mathbf{enc}(\mathsf{sk},\,x_i)}{\boxed{\mathbf{A}_i}} \approx \boxed{x_i\,\mathbf{t}}\ \boxed{\mathbf{I}}$$

addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) \approx (x_1 + x_2)\mathbf{t}$

multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 \not\approx x_1 x_2 \mathbf{t}$

– *proof.* small $\cdot \mathbf{A}_2$ = big

fully **homomorphic** encryption

security. $\mathbf{enc}(\mathsf{sk}, x)$ hides x

functionality. $\mathbf{enc}(\mathsf{sk}, x) \mapsto \mathbf{enc}(\mathsf{sk}, f(x))$

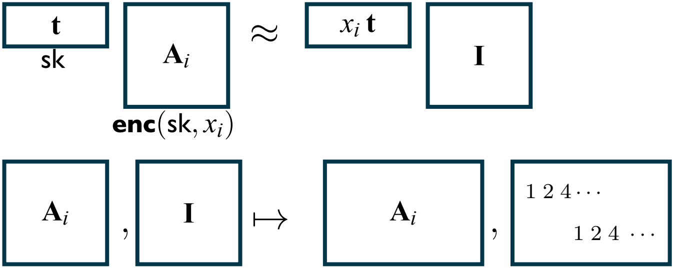
$$\underset{\mathsf{sk}}{\boxed{\mathbf{t}}}\ \underset{\mathbf{enc}(\mathsf{sk},\, x_i)}{\boxed{\mathbf{A}_i}} \approx \boxed{x_i\,\mathbf{t}}\ \boxed{\mathbf{I}}$$

$$\boxed{\mathbf{A}_i},\ \boxed{\mathbf{I}} \mapsto \boxed{\mathbf{A}_i},\ \boxed{\mathbf{G}}$$

fully **homomorphic** encryption

security. **enc**(sk, x) hides x

functionality. **enc**$(\mathsf{sk}, x) \mapsto$ **enc**$(\mathsf{sk}, f(x))$



eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i = x_i \mathbf{t} \;\Rightarrow\; \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} = f(x)\mathbf{t}$$

for any polynomial f, $x = (x_1, \ldots, x_n)$

eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i = x_i \mathbf{t} \;\Rightarrow\; \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} = f(x)\mathbf{t}$$

strengthening. $\forall \mathbf{A}_i, \forall x, \exists\ \mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{I}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{I}$$

[GSW13,BGG+14,GVW15,BCTW16]

eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i = x_i \mathbf{t} \ \Rightarrow \ \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} = f(x)\mathbf{t}$$

strengthening. $\forall \mathbf{A}_i, \forall x, \exists\ \mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{I}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{I}$$

proof. handle $+$ and $\times$

eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i = x_i \mathbf{t} \;\Rightarrow\; \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} = f(x)\mathbf{t}$$

strengthening. $\forall \mathbf{A}_i, \forall x, \exists\, \mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{I}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{I}$$

proof. handle $+$ and $\times$

$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \mathbf{A}_2 - x_2\mathbf{I}] \underbrace{\begin{pmatrix} \\ \\ \\ \end{pmatrix}}_{\mathbf{H}_{+,x_1,x_2}} = (\mathbf{A}_1 + \mathbf{A}_2) - (x_1 + x_2)\mathbf{I}$$

eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i = x_i \mathbf{t} \;\Rightarrow\; \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} = f(x)\mathbf{t}$$

strengthening. $\forall \mathbf{A}_i, \forall x, \exists\, \mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{I}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{I}$$

proof. handle $+$ and $\times$

$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \mathbf{A}_2 - x_2\mathbf{I}] \underbrace{\begin{pmatrix} \mathbf{I} \\ \mathbf{I} \end{pmatrix}}_{\mathbf{H}_{+,x_1,x_2}} = (\mathbf{A}_1 + \mathbf{A}_2) - (x_1 + x_2)\mathbf{I}$$

eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i = x_i \mathbf{t} \;\Rightarrow\; \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} = f(x)\mathbf{t}$$

strengthening. $\forall \mathbf{A}_i, \forall x, \exists\ \mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{I}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{I}$$

proof. handle $+$ and $\times$

$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \mathbf{A}_2 - x_2\mathbf{I}] \underbrace{\begin{pmatrix} \mathbf{A}_2 \\ \\ \\ \end{pmatrix}}_{\mathbf{H}_{\times,x_1,x_2}} = \mathbf{A}_1\mathbf{A}_2 - x_1x_2\mathbf{I}$$

eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i = x_i \mathbf{t} \;\Rightarrow\; \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} = f(x)\mathbf{t}$$

strengthening. $\forall \mathbf{A}_i, \forall x, \exists\, \mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{I}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{I}$$

proof. handle $+$ and $\times$

$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \mathbf{A}_2 - x_2\mathbf{I}] \underbrace{\begin{pmatrix} \mathbf{A}_2 \\ x_1\mathbf{I} \end{pmatrix}}_{\mathbf{H}_{\times,x_1,x_2}} = \mathbf{A}_1\mathbf{A}_2 - x_1x_2\mathbf{I}$$

eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i = x_i \mathbf{t} \;\Rightarrow\; \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} = f(x)\mathbf{t}$$

strengthening. $\forall \mathbf{A}_i, \exists\, \mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{I}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{I}$$

$$\boxed{\mathbf{A}_i}\,,\ \boxed{\mathbf{I}} \mapsto \boxed{\quad\mathbf{A}_i\quad}\,,\ \boxed{\quad\mathbf{G}\quad}$$

eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i = x_i \mathbf{t} \;\Rightarrow\; \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} = f(x)\mathbf{t}$$

"magic". $\forall \mathbf{A}_i, \forall x, \exists$ <u>**small**</u> $\mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{G}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{G}$$

$$\boxed{\mathbf{A}_i}\,,\ \boxed{\mathbf{I}} \mapsto \boxed{\mathbf{A}_i}\,,\ \boxed{\mathbf{G}}$$

eigenvectors, revisited

$$\mathbf{t}\cdot\mathbf{A}_i \approx x_i \mathbf{t}\cdot\mathbf{G} \;\Rightarrow\; \mathbf{t}\cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} \approx f(x)\mathbf{t}\cdot\mathbf{G}$$

"magic". $\forall \mathbf{A}_i, \forall x, \exists$ **small** $\mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{G}]\cdot\mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{G}$$

eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i \approx x_i \mathbf{t} \cdot \mathbf{G} \;\Rightarrow\; \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} \approx f(x)\mathbf{t} \cdot \mathbf{G}$$

"magic". $\forall \mathbf{A}_i, \forall x, \exists$ **small** $\mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{G}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{G}$$

proof. handle $+$ and $\times$

eigenvectors, revisited

$$\mathbf{t}\cdot\mathbf{A}_i \approx x_i\mathbf{t}\cdot\mathbf{G} \;\Rightarrow\; \mathbf{t}\cdot\underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} \approx f(x)\mathbf{t}\cdot\mathbf{G}$$

"magic". $\forall \mathbf{A}_i, \forall x, \exists$ **small** $\mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{G}]\cdot\mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{G}$$

proof. handle $+$ and $\times$

$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \mathbf{A}_2 - x_2\mathbf{G}]\underbrace{\begin{pmatrix}\mathbf{I}\\ \mathbf{I}\end{pmatrix}}_{\text{small}} = (\mathbf{A}_1+\mathbf{A}_2) - (x_1+x_2)\mathbf{G}$$

eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i \approx x_i \mathbf{t} \cdot \mathbf{G} \;\Rightarrow\; \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} \approx f(x)\mathbf{t} \cdot \mathbf{G}$$

"magic". $\forall \mathbf{A}_i, \forall x, \exists$ **small** $\mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{G}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{G}$$

proof. handle $+$ and $\times$

$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \mathbf{A}_2 - x_2\mathbf{G}] \underbrace{\begin{pmatrix} \mathbf{A}_2 \\ x_1\mathbf{I} \end{pmatrix}}_{\text{small?}} = \mathbf{A}_1\mathbf{A}_2 - x_1x_2\mathbf{G}$$

eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i \approx x_i \mathbf{t} \cdot \mathbf{G} \;\Rightarrow\; \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} \approx f(x)\mathbf{t} \cdot \mathbf{G}$$

"magic". $\forall \mathbf{A}_i, \forall x, \exists$ **small** $\mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{G}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{G}$$

proof. handle $+$ and $\times$

$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \mathbf{A}_2 - x_2\mathbf{G}] \underbrace{\begin{pmatrix} \mathbf{G}^{-1}(\mathbf{A}_2) \\ x_1\mathbf{I} \end{pmatrix}}_{\text{small}} = \mathbf{A}_1\mathbf{G}^{-1}(\mathbf{A}_2) - x_1x_2\mathbf{G}$$

eigenvectors, revisited

$$\mathbf{t} \cdot \mathbf{A}_i \approx x_i \mathbf{t} \cdot \mathbf{G} \Rightarrow \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} \approx f(x)\mathbf{t} \cdot \mathbf{G}$$

"magic". $\forall \mathbf{A}_i, \forall x, \exists$ **small** $\mathbf{H}_{f,x}$

$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{G}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{G}$$

applications.	$\mathbf{A}_f$	$\mathbf{H}_{f,x}$
attribute-based enc **[BGGHNSVV]**	keygen	decryption
fully homomorphic sig **[GVW]**	verification	homomorphic sign
constrained PRFs **[BV]**	normal eval	constrained eval

laconic function evaluation

[Quach W Wichs 18, CDGGMP17]

alice

x

bob

f

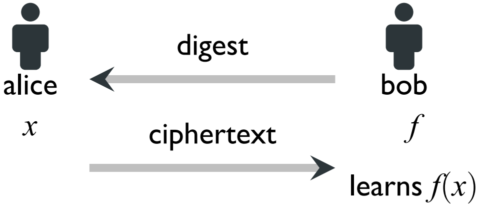
learns $f(x)$

laconic function evaluation

[Quach W Wichs 18, CDGGMP17]

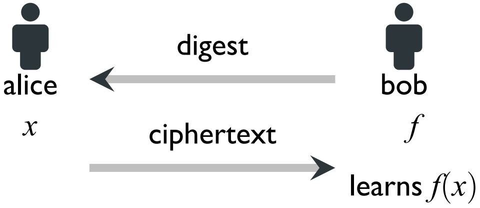
laconic function evaluation

[Quach W Wichs 18, CDGGMP17]



laconic function evaluation

[Quach W Wichs 18, CDGGMP17]

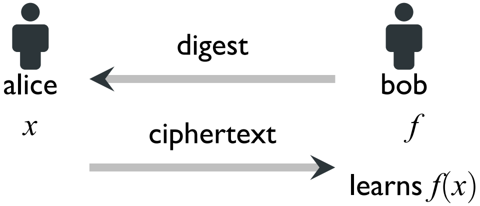


security. hides x

efficiency. $\approx$ Alice sends x

laconic function evaluation

[Quach W Wichs 18, CDGGMP17]

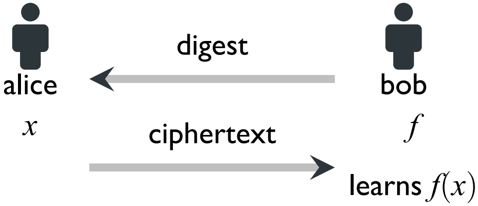


security. semi-honest Bob learns $f(x)$ and nothing else about x

efficiency. $\approx$ Alice sends x

laconic function evaluation

[**Quach W Wichs 18, CDGGMP17**]

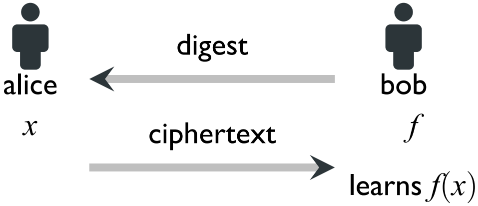


security. semi-honest Bob learns $f(x)$ and nothing else about x

efficiency. Alice's computation independent of f

laconic function evaluation

[Quach W Wichs 18, CDGGMP17]



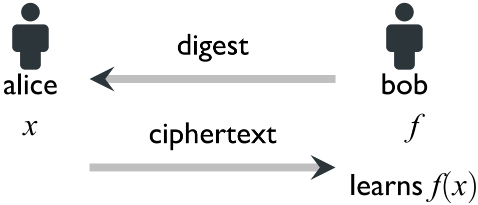
security. semi-honest Bob learns $f(x)$ and nothing else about x

efficiency. Alice's computation independent of f

NOTE. naive solution with FHE requires additional interaction

laconic function evaluation

[Quach W Wichs 18, CDGGMP17]

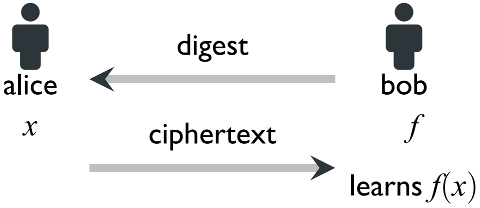


construction.

digest = $\mathbf{A}_1, \ldots, \mathbf{A}_n, \mathbf{A}_f$

laconic function evaluation

[Quach W Wichs 18, CDGGMP17]



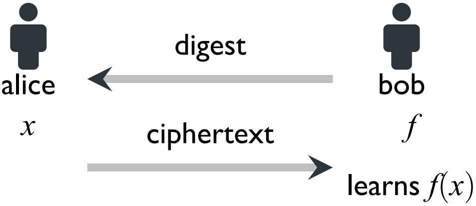
construction.

digest = $\mathbf{A}_1, \ldots, \mathbf{A}_n, \mathbf{A}_f$

ciphertext $\approx \mathbf{s}[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_n - x_n\mathbf{G}], \mathbf{s}\mathbf{A}_f$

laconic function evaluation

[Quach W Wichs 18, CDGGMP17]

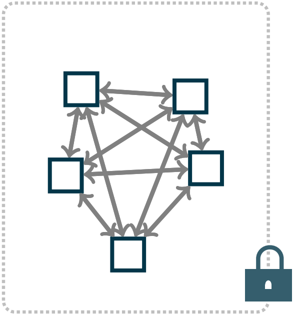


construction.

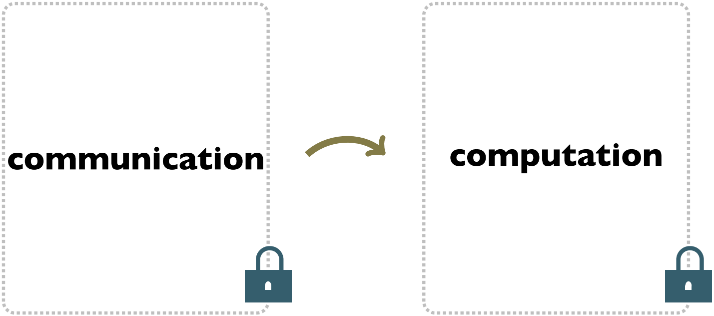
digest = $\mathbf{A}_1, \ldots, \mathbf{A}_n, \mathbf{A}_{\hat{f}}$

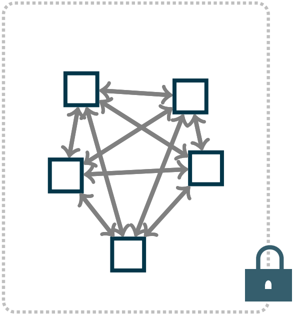
where $\hat{f}$ = fhe.eval$(f, \cdot)$ **[GKPVZ13, GVW12, GVW15, ...]**

communication

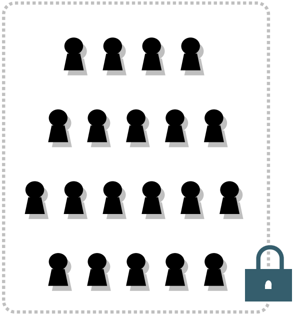


internet

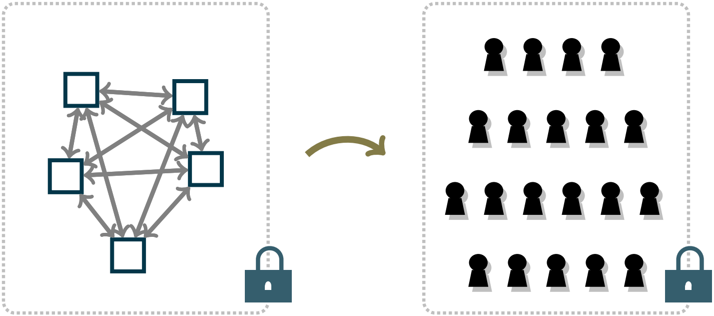

communication
computation



internet



big data



internet **big data**

// thank you