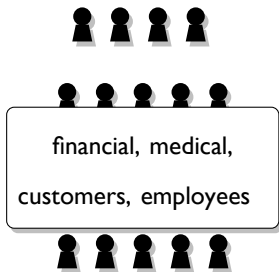


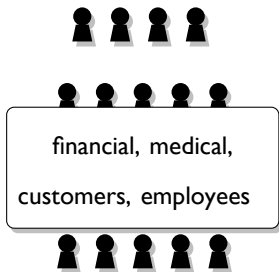
# **encrypted** computation *from* lattices



Hoeteck Wee  
**ENS, Paris**

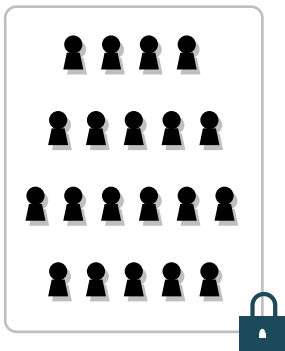


# BIG DATA



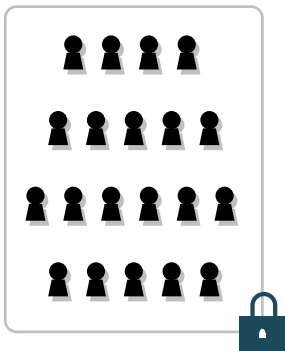
# BIG DATA

Q. privacy?



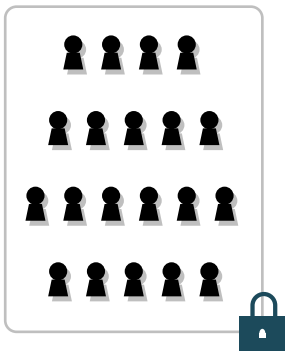
# BIG DATA

Q. privacy?



# BIG DATA

Q. utility + privacy?



# BIG DATA

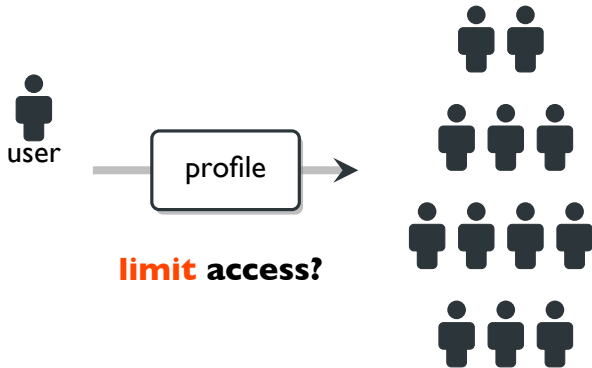
Q. utility + privacy?

**encrypted computation**

# dating + big data

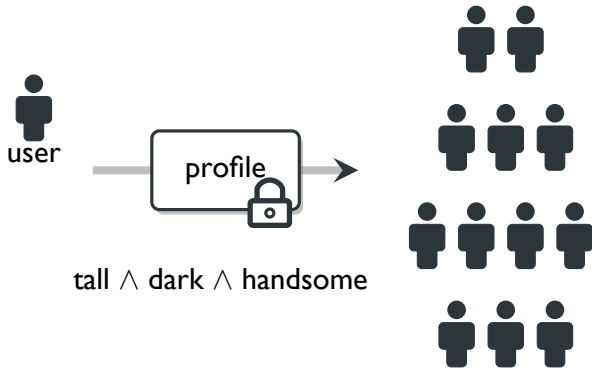


# dating + big data

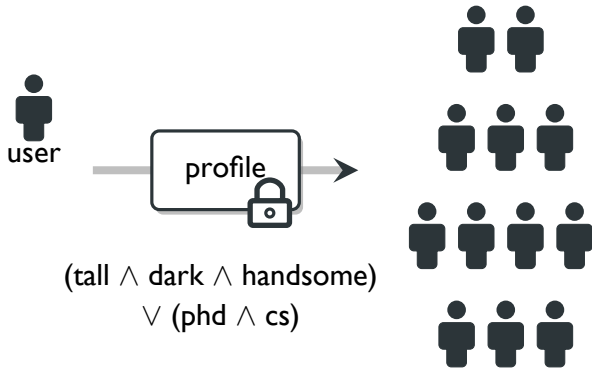




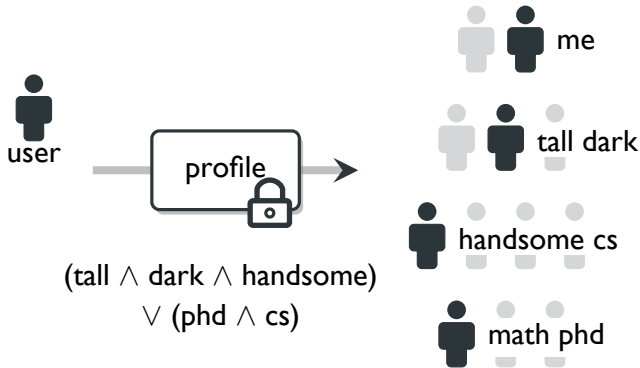
# dating + big data



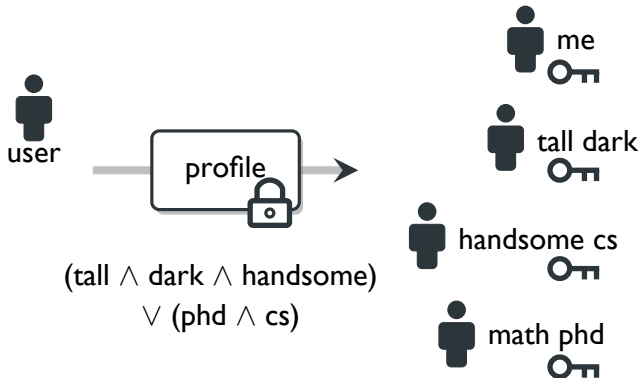
# dating + big data



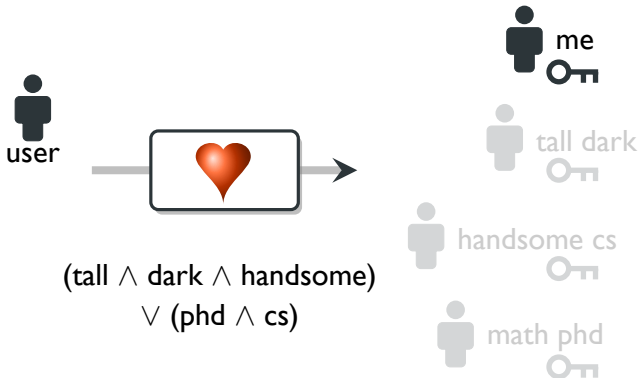
# dating + big data



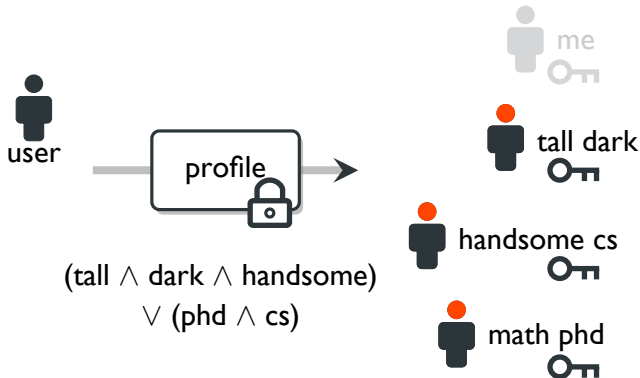
# dating + big data



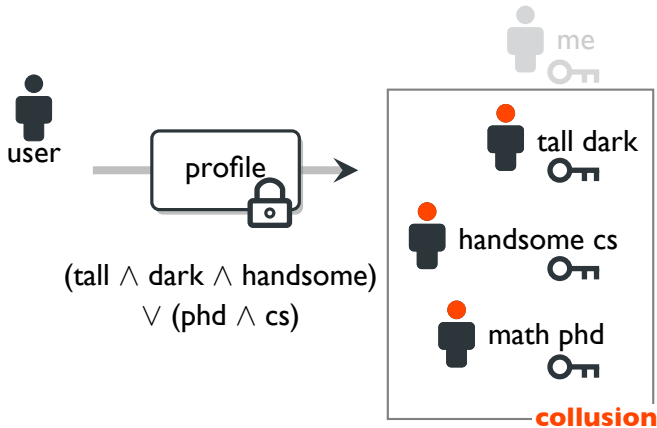
# dating + big data



# dating + big data

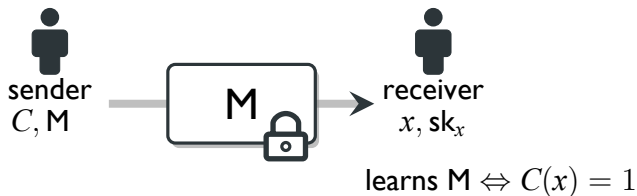


# dating + big data



# attribute-based encryption

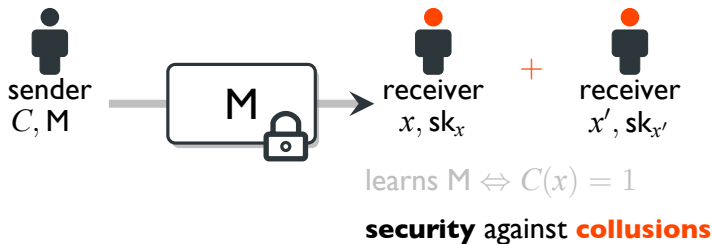
[GPSW06,SW05]





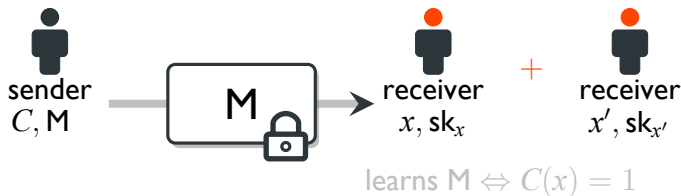
# attribute-based encryption

[GPSW06,SW05]



# attribute-based encryption

[GPSW06,SW05]

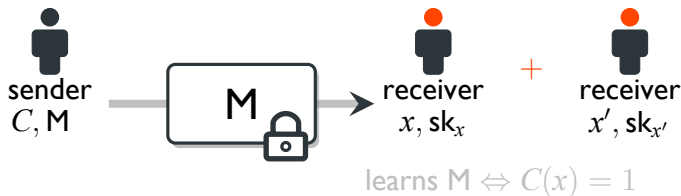


**prior works.**

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

# attribute-based encryption

[GPSW06,SW05]



[Gorbunov Vaikuntanathan W 13]

attribute-based encryption for **circuits**

# attribute-based encryption



$\text{phd} \wedge \text{cs}$



cs phd



cs msc



bio phd

# attribute-based encryption



# attribute-based encryption



$\text{phd} \wedge \text{cs}$

+



$\text{cs phd}$



+



$\text{cs msc}$



+



$\text{bio phd}$



# attribute-based encryption

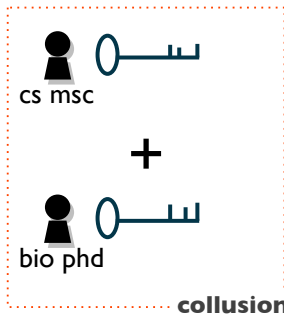


$\text{phd} \wedge \text{cs}$

+



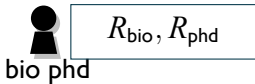
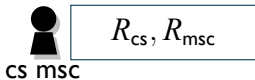
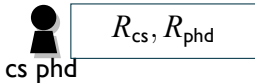
$\text{cs phd}$



# attribute-based encryption



$\text{phd} \wedge \text{cs}$







# attribute-based encryption

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


$phd \wedge cs$


$$R_{cs}, R_{phd}$$

cs phd


$$R_{cs}, R_{msc}$$

cs msc


$$R_{bio}, R_{phd}$$

bio phd

# attribute-based encryption

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

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



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



# attribute-based encryption

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

$phd \wedge cs$

  $R_{cs}, R_{phd}$   
cs phd

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

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

# attribute-based encryption

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

$phd \wedge cs$



cs phd

$R_{cs}, R_{phd}$



cs msc

$R_{cs}, R_{msc}$

+



bio phd

$R_{bio}, R_{phd}$

**collusion**

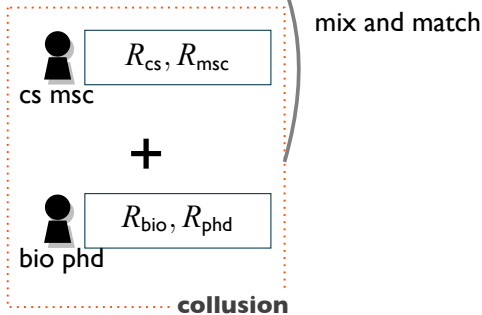
# attribute-based encryption

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

phd  $\wedge$  cs

cs phd

$$R_{cs}, R_{phd} \rightarrow M$$



# attribute-based encryption

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

phd  $\wedge$  cs

cs phd

$$R_{cs}, R_{phd} \rightarrow M$$

cs msc

$$R_{cs}, R_{msc}$$

+

bio phd

$$R_{bio}, R_{phd}$$

**collusion**

mix and match



**insecure** against  
collusions

# attribute-based encryption

**Key Idea.** [GVW13]

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

one-use  $\rightarrow$  many-use

$R_{cs}, R_{phd}$

$R_{cs}, R_{msc}$

cs msc

mix and match

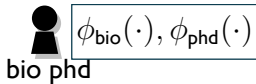
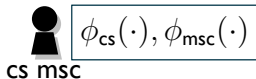
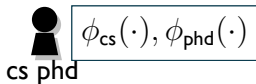
$R_{bio}, R_{phd}$

bio phd

# attribute-based encryption



$\text{phd} \wedge \text{cs}$

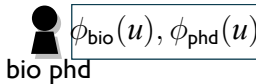
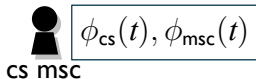
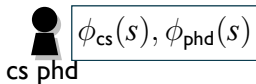




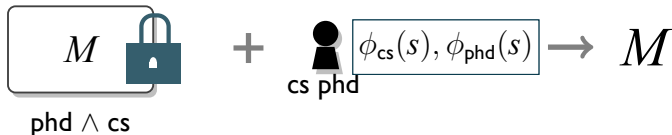
# attribute-based encryption



$\text{phd} \wedge \text{cs}$



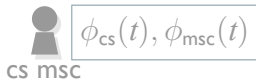
# attribute-based encryption



The diagram illustrates the decryption process in attribute-based encryption. On the left, a message  $M$  is shown inside a box with a blue padlock icon, representing an encrypted message. Below this box is the attribute set  $\text{phd} \wedge \text{cs}$ . This is followed by a plus sign and a user icon (a black silhouette of a person). Below the user icon is the attribute set  $\text{cs phd}$ . To the right of the user icon is a box containing the decryption keys  $\phi_{\text{cs}}(s), \phi_{\text{phd}}(s)$ . An arrow points from this box to the final message  $M$ .

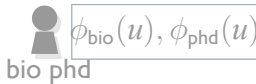
$$\boxed{M} \text{ (with lock)} + \text{cs phd} \left[ \phi_{\text{cs}}(s), \phi_{\text{phd}}(s) \right] \rightarrow M$$

$\text{phd} \wedge \text{cs}$



A user icon (grey silhouette of a person) is shown next to a box containing the decryption keys  $\phi_{\text{cs}}(t), \phi_{\text{msc}}(t)$ . Below the user icon is the attribute set  $\text{cs msc}$ .

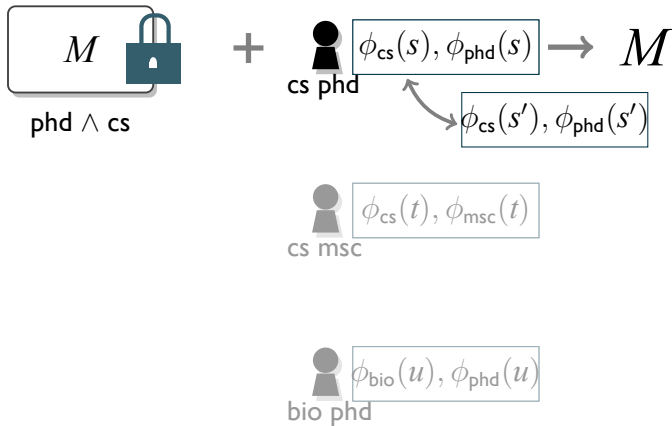
$$\text{cs msc} \left[ \phi_{\text{cs}}(t), \phi_{\text{msc}}(t) \right]$$



A user icon (grey silhouette of a person) is shown next to a box containing the decryption keys  $\phi_{\text{bio}}(u), \phi_{\text{phd}}(u)$ . Below the user icon is the attribute set  $\text{bio phd}$ .

$$\text{bio phd} \left[ \phi_{\text{bio}}(u), \phi_{\text{phd}}(u) \right]$$

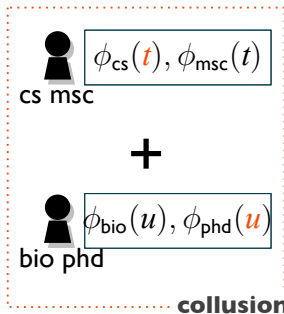
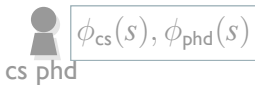
# attribute-based encryption



# attribute-based encryption



$\text{phd} \wedge \text{cs}$



mix and match

# attribute-based encryption

**theorem.** [GVW13]

**secure** against collusions

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

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

cs msc

+



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

bio phd

**collusion**

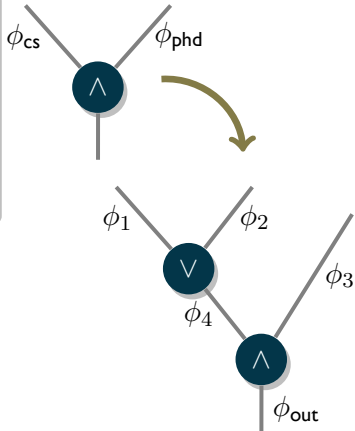
mix and match

# attribute-based encryption

**theorem.** [GVW13]

**secure** against collusions

works for general **circuits**



# attribute-based encryption

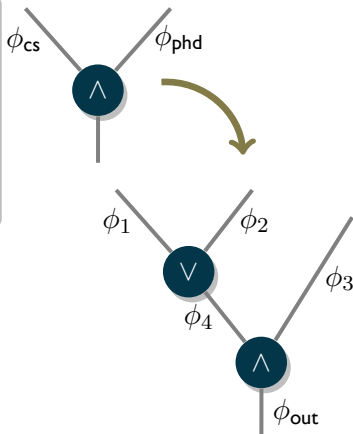
**theorem.** [GVW13]

**secure** against collusions

works for general **circuits**

**prior.** shallow circuits

[GPSW06, OT10, BI3, ...]



# attribute-based encryption

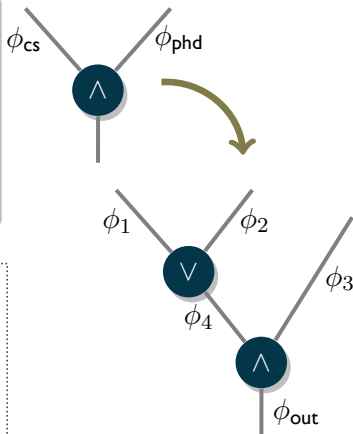
**theorem.** [GVW13]

**secure** against collusions

works for general **circuits**

$$\begin{array}{|c|} \hline \mathbf{A} \\ \hline \end{array} \begin{array}{|c|} \hline \mathbf{s} \\ \hline \end{array} + \begin{array}{|c|} \hline \mathbf{e} \\ \hline \end{array} \approx_c \begin{array}{|c|} \hline \mathbf{u} \\ \hline \end{array}$$

learning with errors [R05]





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

# fully **homomorphic** encryption

# fully **homomorphic** encryption

**syntax.**  $\text{enc}(\text{sk}, \cdot), \text{dec}(\text{sk}, \cdot)$

**functionality.**  $\text{dec}(\text{sk}, \text{enc}(\text{sk}, x)) = x$

# fully **homomorphic** encryption

**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

**functionality.**  $\text{dec}(\text{sk}, \text{enc}(\text{sk}, x)) = x$

# fully **homomorphic** encryption

**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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

# fully **homomorphic** encryption

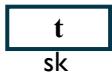
**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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

# fully **homomorphic** encryption

**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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

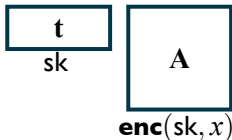


[Gentry Sahai Waters 13]

# fully **homomorphic** encryption

**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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



[Gentry Sahai Waters 13]



# fully **homomorphic** encryption

**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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

$$\begin{array}{c} \boxed{t} \\ \text{sk} \end{array} \begin{array}{c} \boxed{A} \\ \text{enc}(\text{sk}, x) \end{array} = \begin{array}{c} \boxed{x t} \\ t: \text{eigenvector} \end{array}$$

[Gentry Sahai Waters 13]

# fully **homomorphic** encryption

**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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

$$\begin{array}{c} \boxed{\text{t}} \\ \text{sk} \end{array} \begin{array}{c} \boxed{A_i} \\ \text{enc}(\text{sk}, x_i) \end{array} = \begin{array}{c} \boxed{x_i \text{t}} \\ \text{t: eigenvector} \end{array}$$

[Gentry Sahai Waters 13]

$$\text{enc}(\text{sk}, x_1), \text{enc}(\text{sk}, x_2) \stackrel{?}{\mapsto} \text{enc}(\text{sk}, x_1 + x_2), \text{enc}(\text{sk}, x_1 x_2)$$

# fully **homomorphic** encryption

**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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

$$\boxed{\begin{matrix} \mathbf{t} \\ \text{sk} \end{matrix}} \quad \boxed{\begin{matrix} \mathbf{A}_i \\ \text{enc}(\text{sk}, x_i) \end{matrix}} = \boxed{x_i \mathbf{t}}$$

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

# fully **homomorphic** encryption

**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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

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

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

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

# fully **homomorphic** encryption

**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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

$$\boxed{\underset{\text{sk}}{t}} \quad \boxed{\underset{\text{enc}(\text{sk}, x_i)}{A_i}} = \boxed{x_i t}$$

addition:  $t \cdot (A_1 + A_2) = (x_1 + x_2)t$

multiplication:  $t \cdot A_1 A_2 = x_1 x_2 t$

# fully **homomorphic** encryption

**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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

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

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

# fully **homomorphic** encryption

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

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

$$\boxed{\begin{array}{c} \mathbf{t} \\ \mathbf{sk} \end{array}} \quad \boxed{\begin{array}{c} \mathbf{A}_i \\ \mathbf{enc}(\mathbf{sk}, x_i) \end{array}} = \boxed{\begin{array}{c} x_i \mathbf{t} \end{array}}$$

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

# fully **homomorphic** encryption

**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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

$$\begin{array}{c} \boxed{\mathbf{t}} \\ \text{sk} \end{array} \quad \begin{array}{c} \boxed{\mathbf{A}_i} \\ \text{enc}(\text{sk}, x_i) \end{array} \approx \boxed{x_i \mathbf{t}}$$

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.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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

$$\boxed{\begin{array}{c} \mathbf{t} \\ \text{sk} \end{array}} \quad \boxed{\begin{array}{c} \mathbf{A}_i \\ \text{enc}(\text{sk}, x_i) \end{array}} \approx \boxed{x_i \mathbf{t}}$$

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

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

$$\boxed{\begin{array}{c} \mathbf{t} \\ \mathbf{sk} \end{array}} \quad \boxed{\begin{array}{c} \mathbf{A}_i \\ \mathbf{enc}(\mathbf{sk}, x_i) \end{array}} \approx \boxed{\begin{array}{c} x_i \mathbf{t} \end{array}}$$

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

multiplication:  $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 \not\approx x_1x_2\mathbf{t}$

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

# fully **homomorphic** encryption

**security.**  $\text{enc}(\text{sk}, x)$  hides  $x$

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

$$\begin{array}{c} \boxed{\text{t}} \\ \text{sk} \end{array} \quad \boxed{\text{A}_i} \quad \approx \quad \boxed{x_i \text{t}} \quad \boxed{\text{I}}$$

$\text{enc}(\text{sk}, x_i)$

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

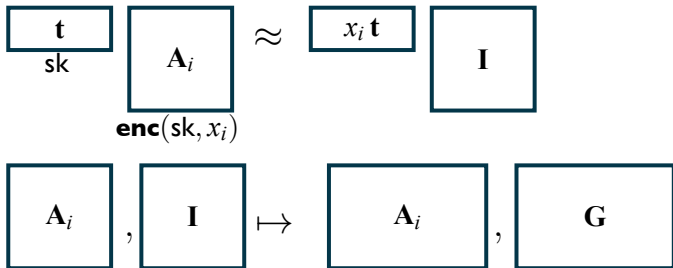
multiplication:  $\text{t} \cdot \text{A}_1\text{A}_2 \not\approx x_1x_2\text{t}$

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

# fully **homomorphic** encryption

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

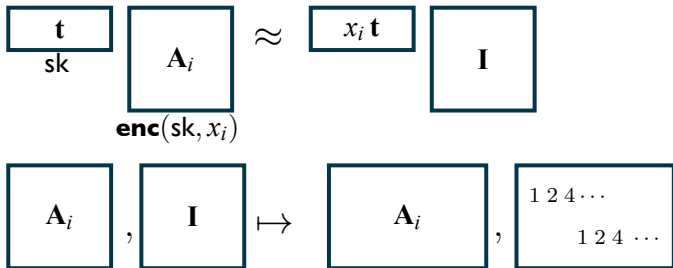
**functionality.**  $\mathbf{enc}(\mathbf{sk}, x) \mapsto \mathbf{enc}(\mathbf{sk}, f(x))$



# fully **homomorphic** encryption

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

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



# eigenvectors, revisited

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

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

# eigenvectors, revisited

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

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

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

[GSW13,BGG+14,GVW15,BCTW16]

# eigenvectors, revisited

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

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

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

**proof.** handle  $+$  and  $\times$



# eigenvectors, revisited

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

**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  $\times$

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

# eigenvectors, revisited

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

**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

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

**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  $\times$

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

# eigenvectors, revisited

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

**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  $\times$

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

# eigenvectors, revisited

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

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

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

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

# eigenvectors, revisited

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

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

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

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

# eigenvectors, revisited

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

**“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

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

**“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

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

**“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

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

**“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  $\times$

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

# eigenvectors, revisited

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

**“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  $\times$

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

# eigenvectors, revisited

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

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

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

**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

$x$



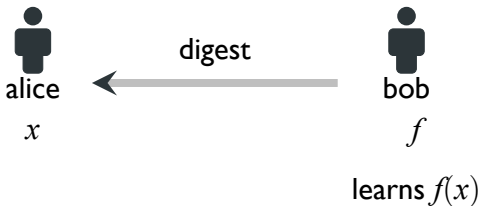
bob

$f$

learns  $f(x)$

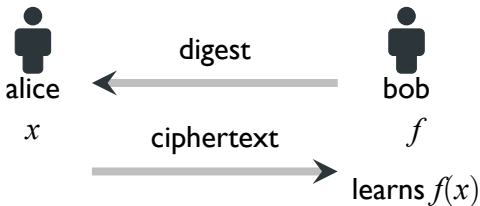
# laconic function evaluation

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



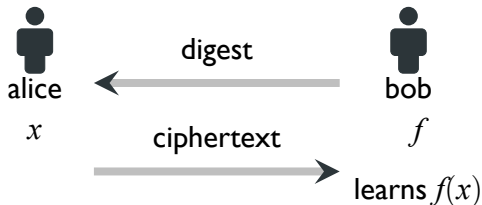
# laconic function evaluation

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



# laconic function evaluation

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



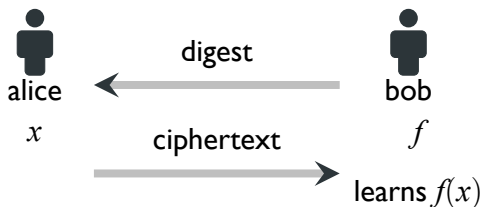
**security.** hides  $x$

**efficiency.**  $\approx$  Alice sends  $x$



# laconic function evaluation

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

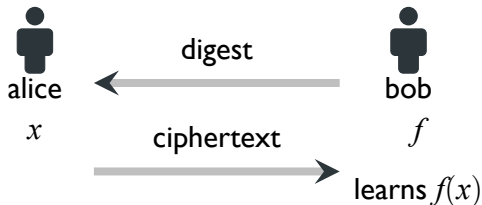


**security.** semi-honest Bob learns  $f(x)$  and nothing else about  $x$

**efficiency.**  $\approx$  Alice sends  $x$

# laconic function evaluation

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

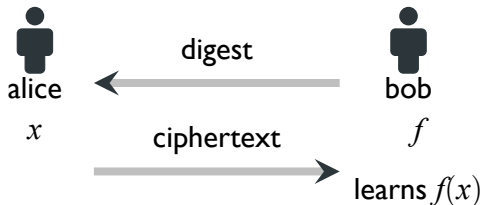


**security.** semi-honest Bob learns  $f(x)$  and nothing else about  $x$

**efficiency.** Alice's computation independent of  $f$

# laconic function evaluation

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



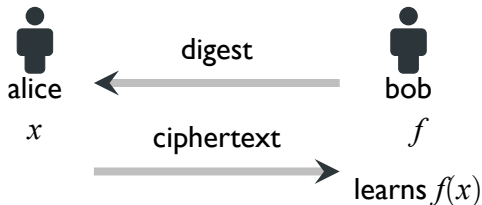
**security.** semi-honest Bob learns  $f(x)$  and nothing else about  $x$

**efficiency.** Alice's computation independent of  $f$

**NOTE.** naive solution with FHE requires additional interaction

# laconic function evaluation

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

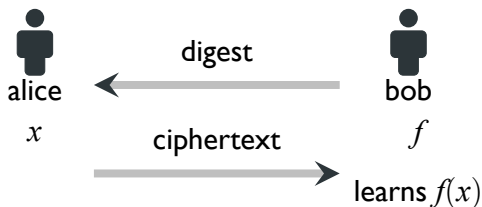


**construction.**

$$\text{digest} = A_1, \dots, A_n, A_f$$

# laconic function evaluation

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



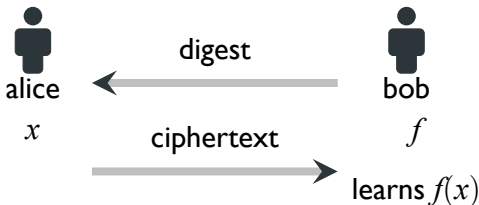
**construction.**

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

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

# laconic function evaluation

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



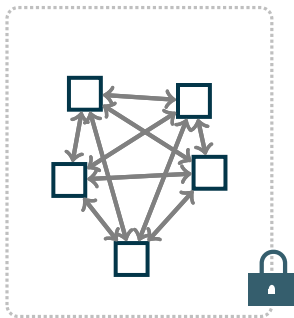
**construction.**

$$\text{digest} = A_1, \dots, A_n, A_{\hat{f}}$$

where  $\hat{f} = \text{fhe.eval}(f, \cdot)$  [GKPVZ13, GV**W**12, GV**W**15, ...]

**communication**





**internet**

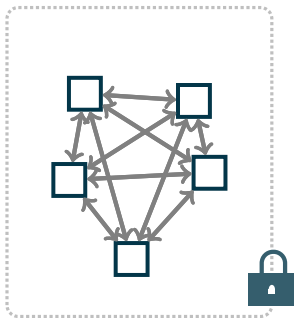


**communication**



**computation**

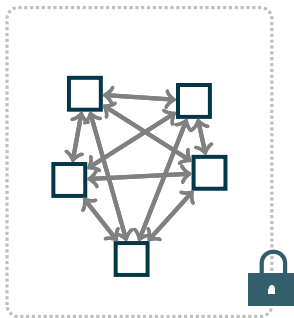




**internet**



**big data**



**internet**



**big data**

**// thank you**