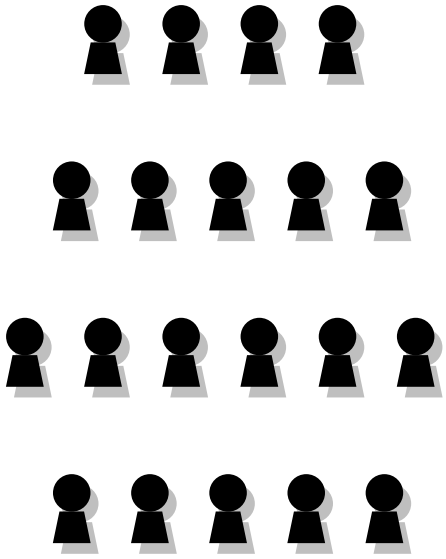
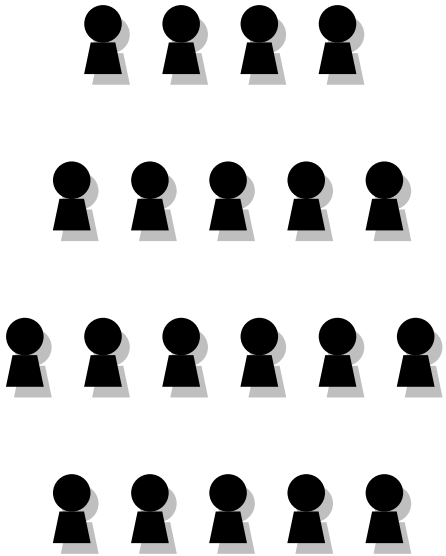
encrypted computation *from* lattices (1/3)

Hoeteck Wee
NTT research

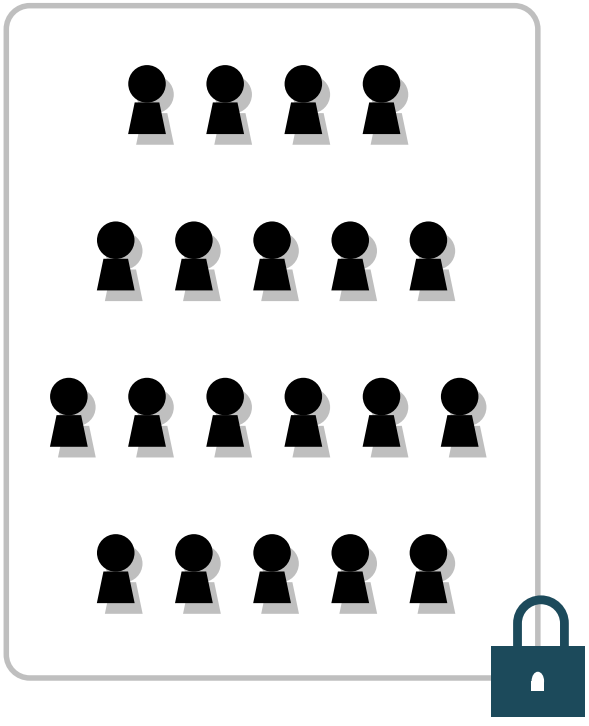


BIG DATA



BIG DATA

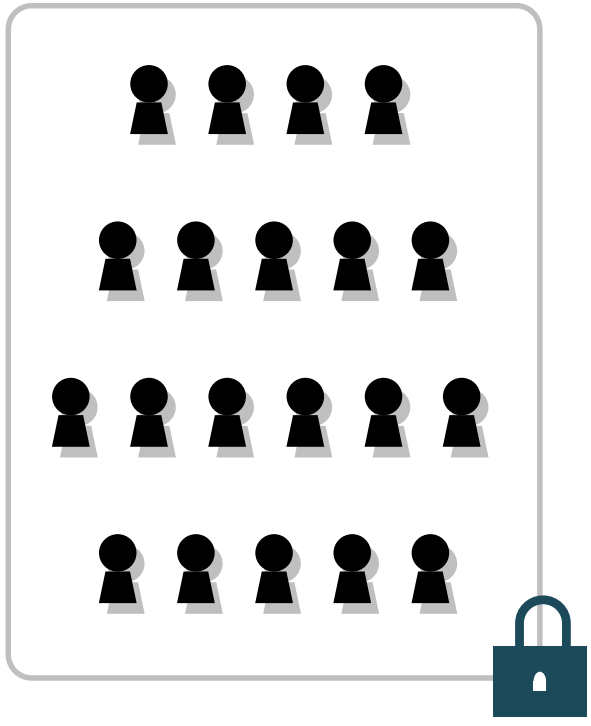
Q. privacy + utility?



BIG DATA

Q. privacy + utility?

encrypted computation

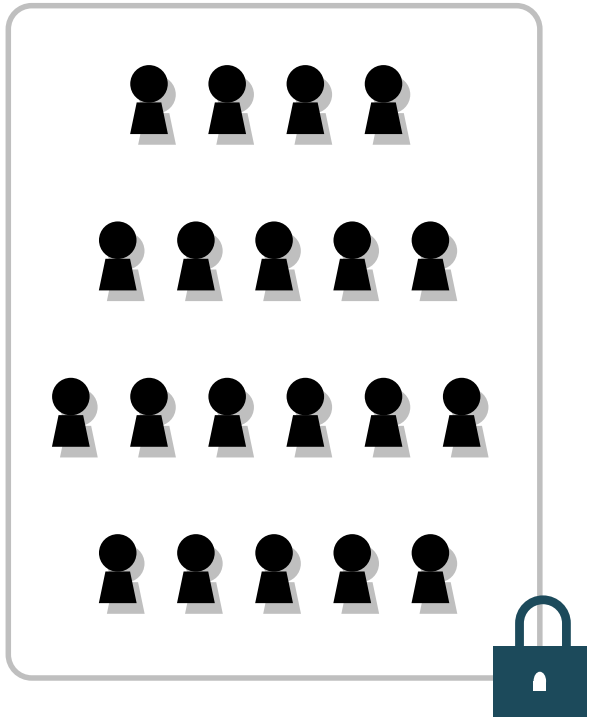


BIG DATA

Q. privacy + utility?

encrypted computation

3 notions

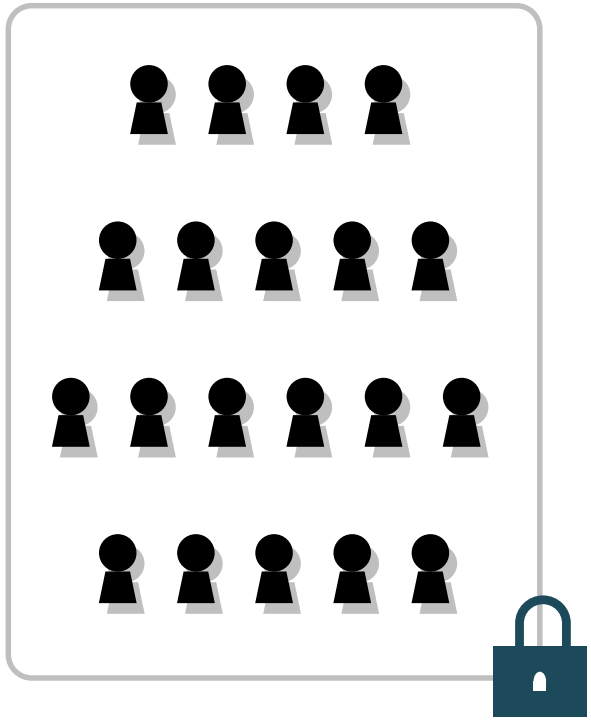


BIG DATA

Q. privacy + utility?

encrypted computation

3 notions *from* **lattices**



BIG DATA

Q. privacy + utility?

encrypted computation

3 notions + **1** equation

fully **homomorphic** encryption

fully homomorphic **encryption**

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

functionality.

fully homomorphic **encryption**

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

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

fully homomorphic **encryption**

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

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

fully **homomorphic** encryption

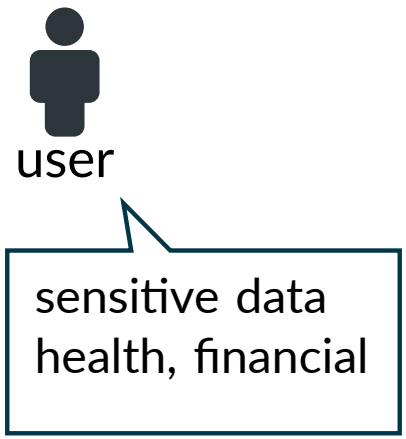
security. $\mathbf{enc}(\mathsf{sk}, x)$ hides x

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

fully **homomorphic** encryption

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

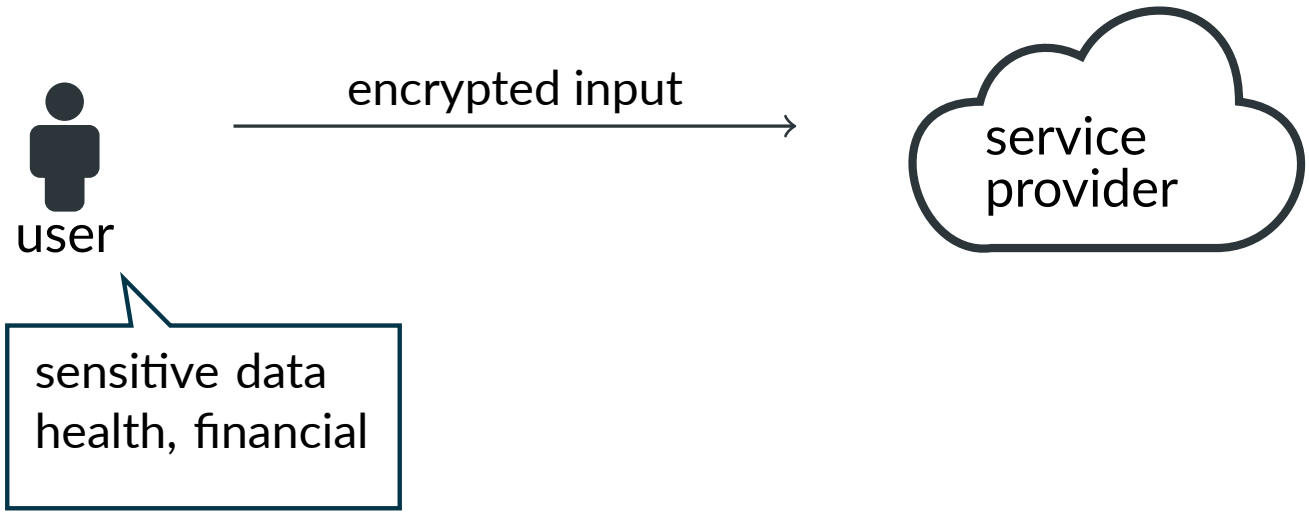
functionality. $\mathbf{enc}(\mathsf{sk}, x) \overset{\mathbf{eval},f}{\mapsto} \mathbf{enc}(\mathsf{sk}, f(x))$



fully **homomorphic** encryption

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

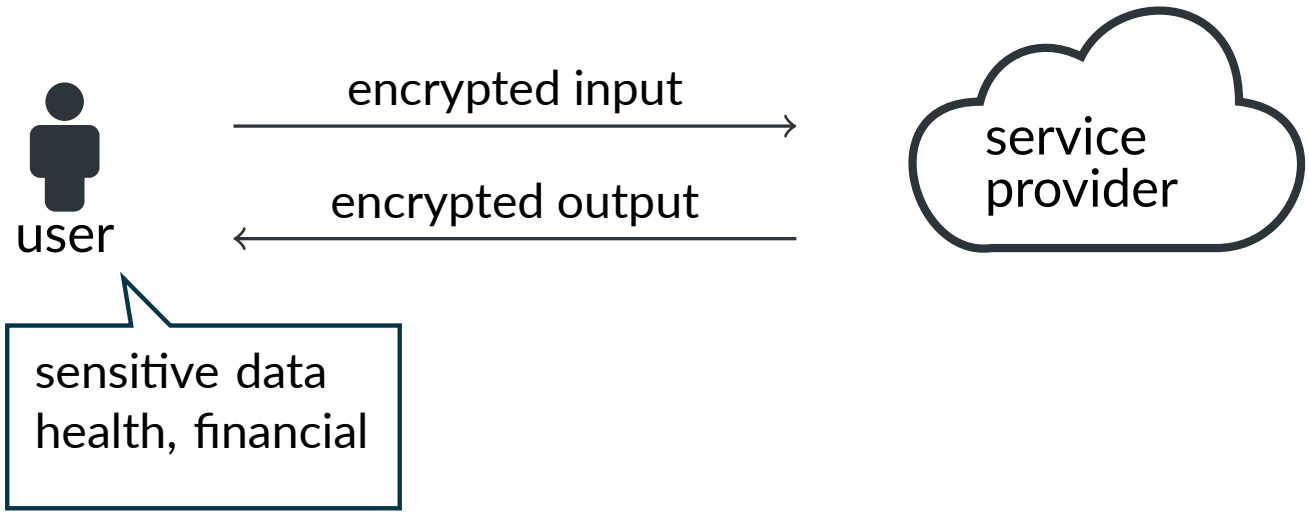
functionality. $\mathbf{enc}(\mathsf{sk}, x) \overset{\mathsf{eval},f}{\mapsto} \mathbf{enc}(\mathsf{sk}, f(x))$



fully **homomorphic** encryption

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

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



fully **homomorphic** encryption

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

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

FHE for **circuits** from lattices

[**Gentry 09, Brakerski Vaikuntanathan 11**]

fully **homomorphic** encryption

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

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

FHE for **circuits** from **LWE**

[Gentry 09, **Brakerski Vaikuntanathan 11**]

$$(\mathbf{B},\ \mathbf{sB} + \mathbf{e}) \approx_c \text{uniform}$$

fully **homomorphic** encryption

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

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

FHE for **circuits** from **LWE**

[Gentry 09, Brakerski Vaikuntanathan 11, **Gentry Sahai Waters 13**]

$$(\mathbf{B},\ \mathbf{sB} + \mathbf{e}) \approx_c \text{uniform}$$

fully **homomorphic** encryption

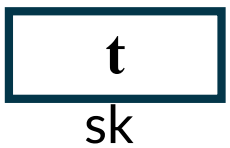
security. $\mathsf{enc}(\mathsf{sk}, x)$ hides x

functionality. $\mathbf{enc}(\mathsf{sk}, x) \mapsto \mathbf{enc}(\mathsf{sk}, f(x))$ 1

fully **homomorphic** encryption

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

functionality. $\mathbf{enc}(\mathsf{sk}, x) \mapsto \mathbf{enc}(\mathsf{sk}, f(x))$ 1

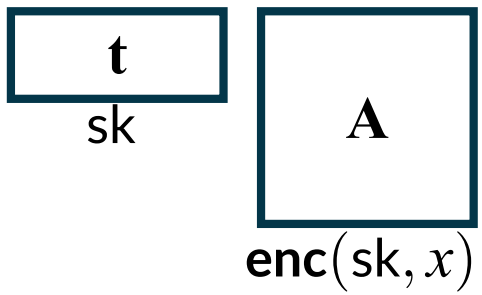


over $\mathbb{Z}_q$

fully **homomorphic** encryption

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

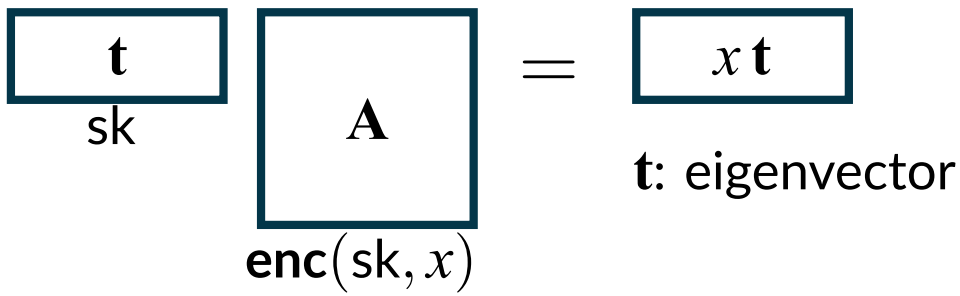
functionality. $\mathsf{enc}(\mathsf{sk}, x) \mapsto \mathsf{enc}(\mathsf{sk}, f(x))$ 1



fully **homomorphic** encryption

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

functionality. $\mathsf{enc}(\mathsf{sk}, x) \mapsto \mathsf{enc}(\mathsf{sk}, f(x))$ 1

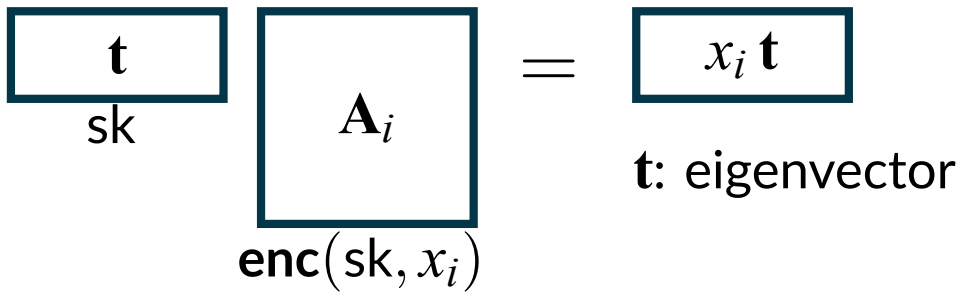


t: eigenvector

fully **homomorphic** encryption

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

functionality. $\mathsf{enc}(\mathsf{sk}, x) \mapsto \mathsf{enc}(\mathsf{sk}, f(x))$ 1



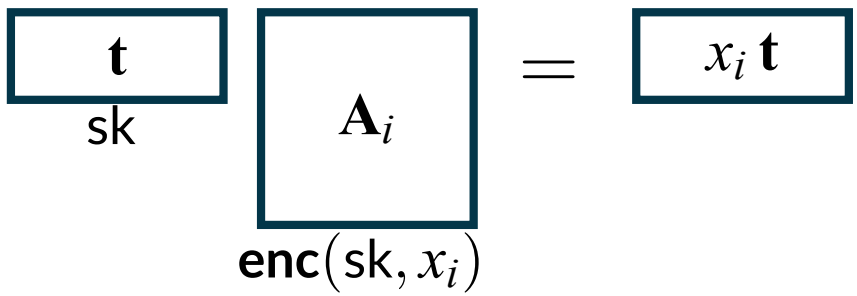
t: eigenvector

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

fully **homomorphic** encryption

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

functionality. $\mathsf{enc}(\mathsf{sk}, x) \mapsto \mathsf{enc}(\mathsf{sk}, f(x))$ 1

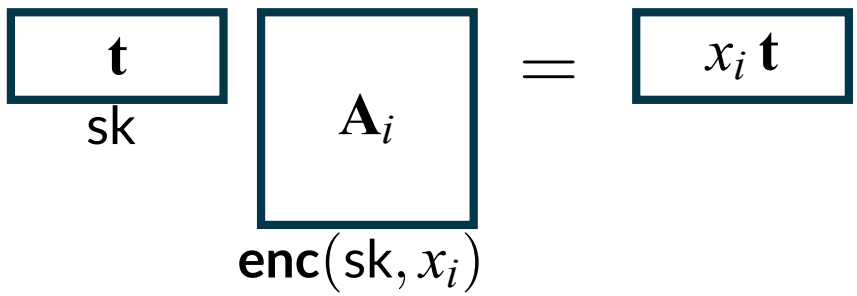


addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) = (x_1 + x_2)\mathbf{t}$

fully **homomorphic** encryption

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

functionality. $\mathsf{enc}(\mathsf{sk}, x) \mapsto \mathsf{enc}(\mathsf{sk}, f(x))$ 1



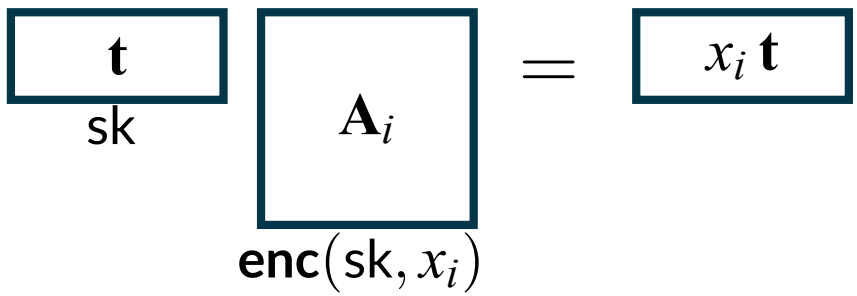
addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) = (x_1 + x_2)\mathbf{t}$

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

fully **homomorphic** encryption

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

functionality. $\mathsf{enc}(\mathsf{sk}, x) \mapsto \mathsf{enc}(\mathsf{sk}, f(x))$ 1



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

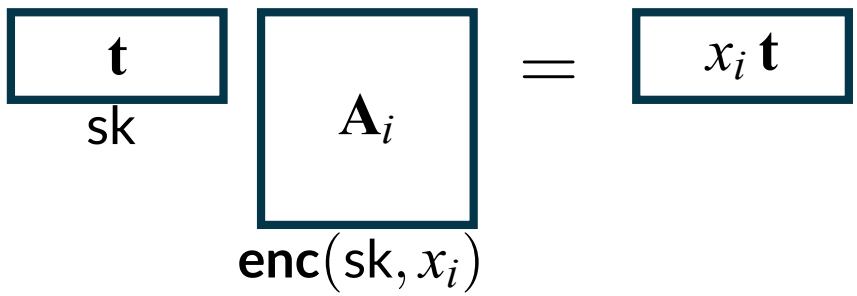
multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 = x_1x_2\mathbf{t}$

$$\text{LHS} = x_1\mathbf{t} \cdot \mathbf{A}_2 = \ldots$$

fully **homomorphic** encryption

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

functionality. $\mathsf{enc}(\mathsf{sk}, x) \mapsto \mathsf{enc}(\mathsf{sk}, f(x))$ 1



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

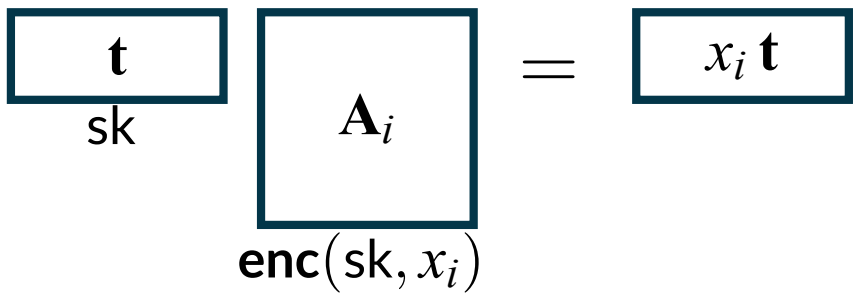
multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 = x_1x_2\mathbf{t}$

polynomials: $\mathbf{t} \cdot (\mathbf{A}_1\mathbf{A}_2 + \mathbf{A}_3\mathbf{A}_4) = (x_1x_2 + x_3x_4)\mathbf{t}$

fully **homomorphic** encryption

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

functionality. $\mathsf{enc}(\mathsf{sk}, x) \mapsto \mathsf{enc}(\mathsf{sk}, f(x))$ 1



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

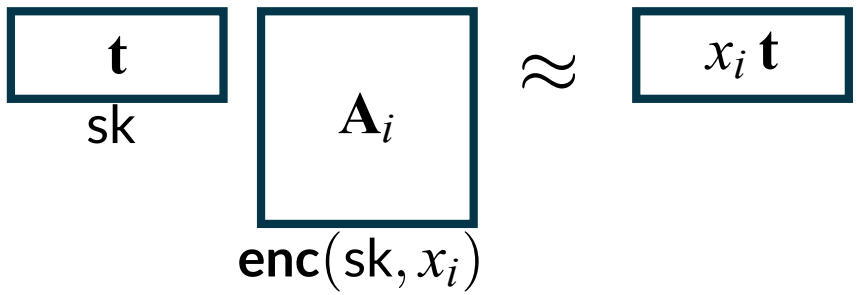
multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 = x_1x_2\mathbf{t}$

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

functionality. $\mathsf{enc}(\mathsf{sk}, x) \mapsto \mathsf{enc}(\mathsf{sk}, f(x))$ 2 + noise



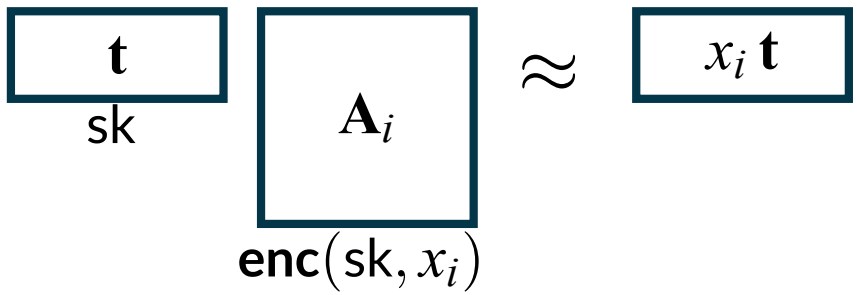
addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) = (x_1 + x_2)\mathbf{t}$

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. $\mathbf{enc}(\mathsf{sk}, x) \mapsto \mathbf{enc}(\mathsf{sk}, f(x))$ 2 + noise



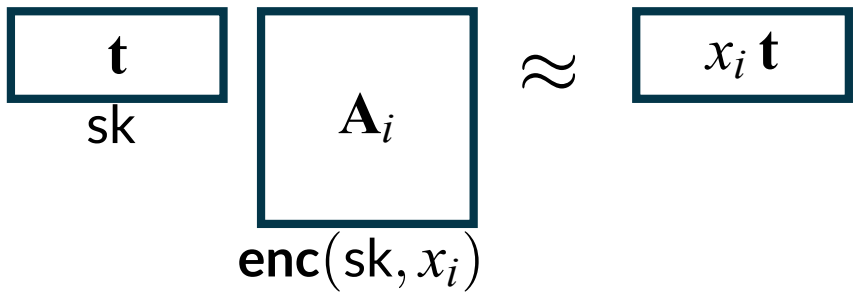
addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) \approx (x_1 + x_2)\mathbf{t}$

– *proof.* small + small = small

fully **homomorphic** encryption

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

functionality. **enc**$(\mathsf{sk}, x) \mapsto$ **enc**$(\mathsf{sk}, f(x))$ 2 + noise



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

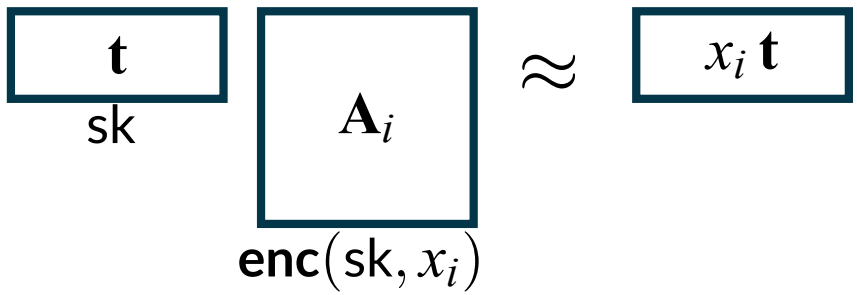
multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 \not\approx x_1x_2\mathbf{t}$

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

fully **homomorphic** encryption

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

functionality. $\mathsf{enc}(\mathsf{sk}, x) \mapsto \mathsf{enc}(\mathsf{sk}, f(x))$ 3 $\mathbf{A}_i$ small



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

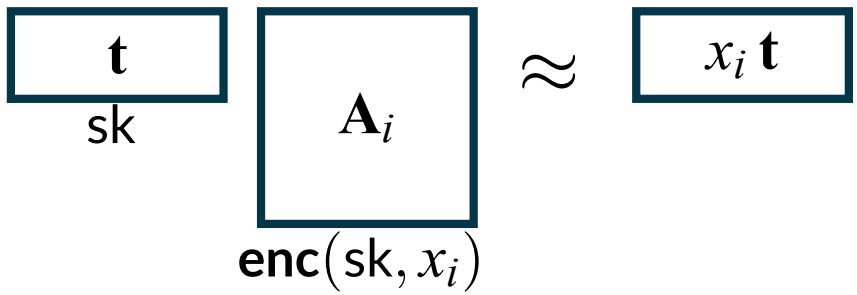
multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 \not\approx x_1x_2\mathbf{t}$

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

fully **homomorphic** encryption

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

functionality. $\mathsf{enc}(\mathsf{sk}, x) \mapsto \mathsf{enc}(\mathsf{sk}, f(x))$ 3 $\mathbf{A}_i$ small



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

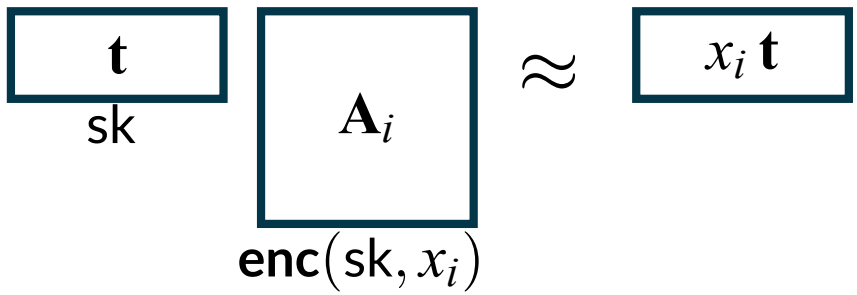
multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 \approx x_1 x_2 \mathbf{t}$

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

fully **homomorphic** encryption

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

functionality. $\mathbf{enc}(\mathsf{sk}, x) \mapsto \mathbf{enc}(\mathsf{sk}, f(x))$ 3 $\mathbf{A}_i$ small

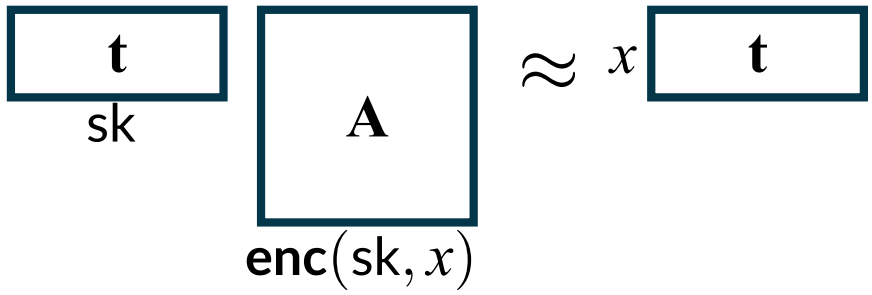


addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) \approx (x_1 + x_2)\mathbf{t}$

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

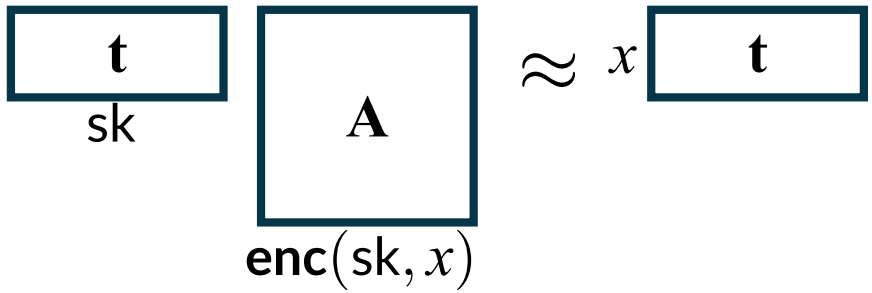
polynomials: $\mathbf{t} \cdot \underbrace{f(\mathbf{A}_1, \ldots, \mathbf{A}_\ell)}_{\mathbf{A}_f} \approx f(x_1, \ldots, x_\ell)\mathbf{t}$

fully **homomorphic** encryption



2. **A** hides x
3. **A** small

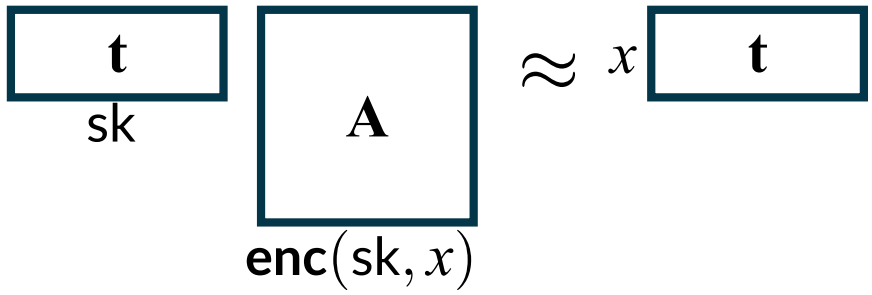
fully **homomorphic** encryption



2. $\mathbf{A}$ hides x
3. $\mathbf{A}$ small

$$\underbrace{(\mathbf{s} \quad -1)}_{\mathbf{t}}$$

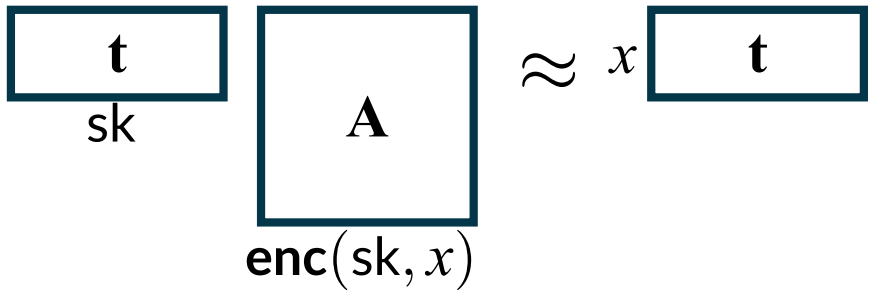
fully **homomorphic** encryption



2. $\mathbf{A}$ hides x
3. $\mathbf{A}$ small

$$\underbrace{(\mathbf{s} \quad -1)}_{\mathbf{t}} \begin{pmatrix} \mathbf{B} \\ \\ \mathbf{sB} + \mathbf{e} \end{pmatrix} \approx \mathbf{0}$$

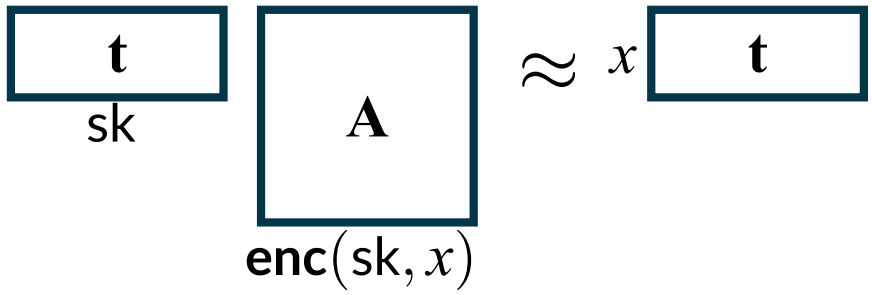
fully **homomorphic** encryption



2. **A** hides x
3. **A** small

$$\underbrace{(\mathbf{s} \quad -1)}_{\mathbf{t}} \left(\begin{pmatrix} \mathbf{B} \\ \\ \mathbf{sB} + \mathbf{e} \end{pmatrix} + x\mathbf{I} \right) \approx x\mathbf{t}$$

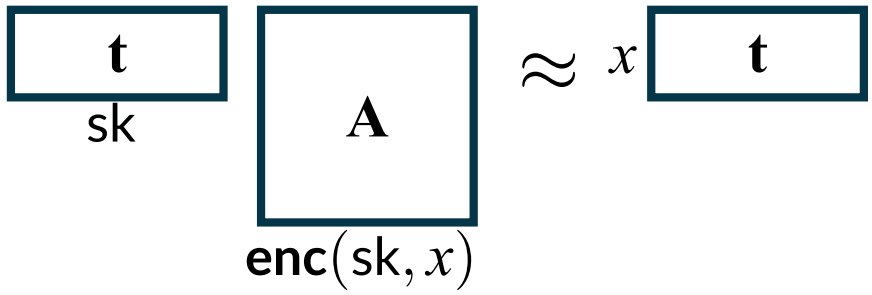
fully **homomorphic** encryption



2. **A** hides x ✓
3. **A** small

$$\underbrace{(\mathbf{s} \quad -1)}_{\mathbf{t}} \left(\begin{pmatrix} \mathbf{B} \\ \mathbf{sB} + \mathbf{e} \end{pmatrix} + x\mathbf{I} \right) \approx x\mathbf{t}$$

fully **homomorphic** encryption



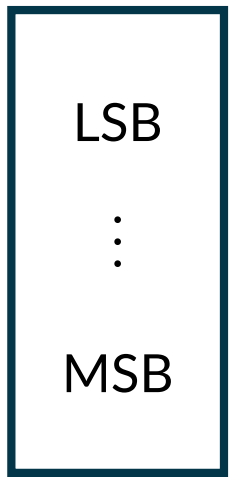
2. **A** hides x ✓
3. **A** small

$$\underbrace{(\mathbf{s} \quad -1)}_{\mathbf{t}} \left(\begin{pmatrix} \mathbf{B} \\ \mathbf{sB} + \mathbf{e} \end{pmatrix} + x\mathbf{I} \right) \approx x\mathbf{t}$$

fully **homomorphic** encryption

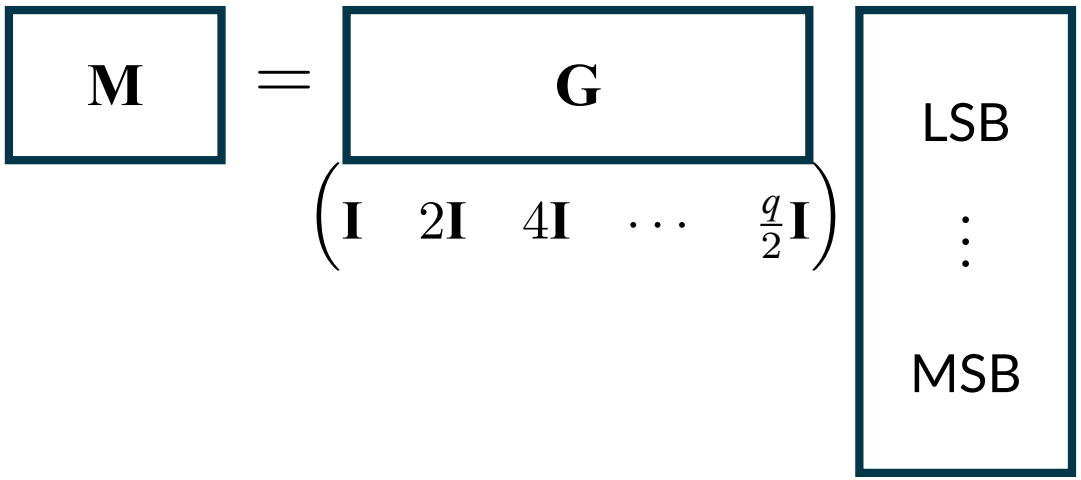
2. $\mathbf{A}$ hides x ✓
3. $\mathbf{A}$ small

$\times \log q$ ⟶



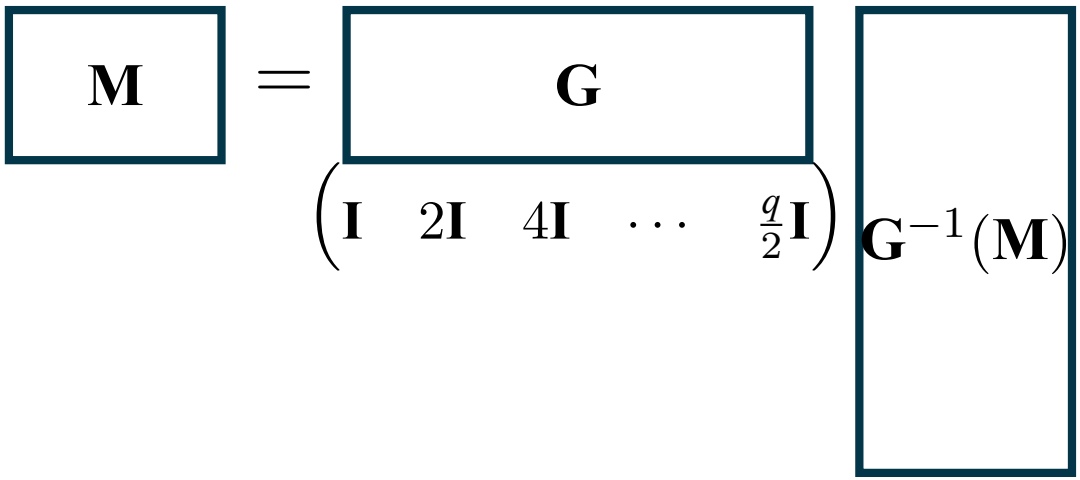
fully **homomorphic** encryption

2. $\mathbf{A}$ hides x ✓
3. $\mathbf{A}$ small

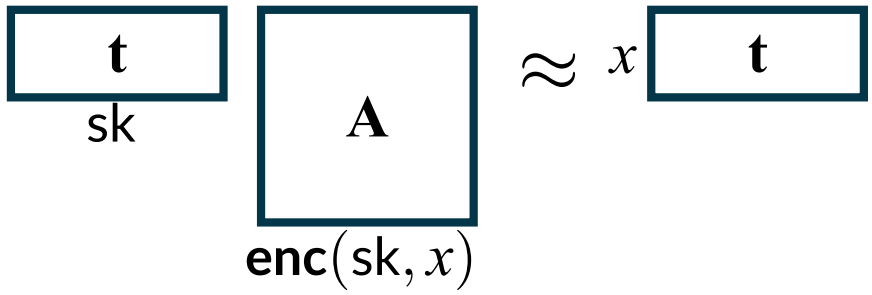


fully **homomorphic** encryption

2. **A** hides x ✓
3. **A** small



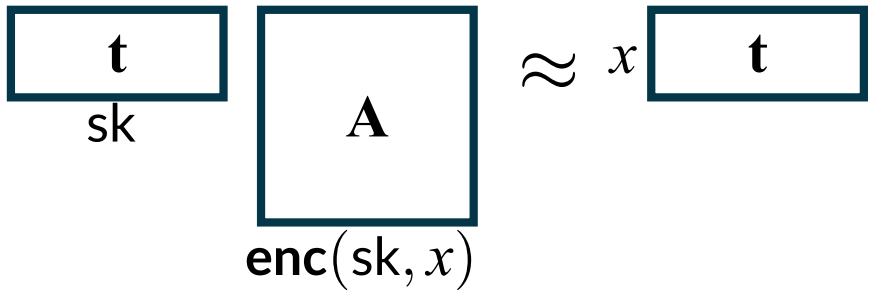
fully **homomorphic** encryption



2. **A** hides x ✓
3. **A** small

$$\underbrace{(\mathbf{s} \quad -1)}_{\mathbf{t}} \qquad \left(\begin{pmatrix} \mathbf{B} \\ \mathbf{sB} + \mathbf{e} \end{pmatrix} + x\,\mathbf{I} \right) \approx x\,\mathbf{t}$$

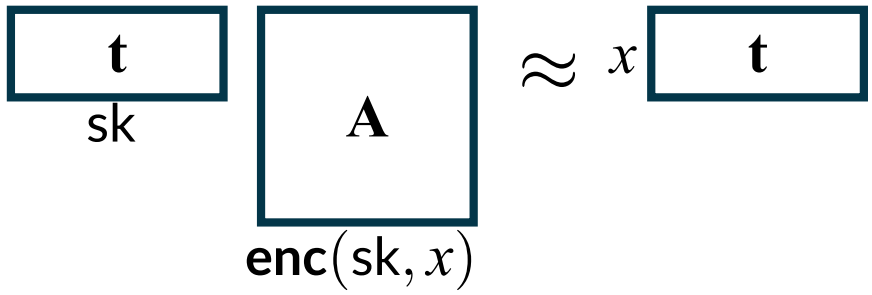
fully **homomorphic** encryption



2. **A** hides x ✓
3. **A** small ✓

$$\underbrace{(\mathbf{s} \quad -1)}_{\mathbf{t}}\mathbf{G} \cdot \underbrace{\mathbf{G}^{-1}\left(\begin{pmatrix}\mathbf{B}\\ \mathbf{sB}+\mathbf{e}\end{pmatrix} + x\,\mathbf{I}\right)}_{\mathbf{A}} \approx x\,\mathbf{t}$$

fully **homomorphic** encryption

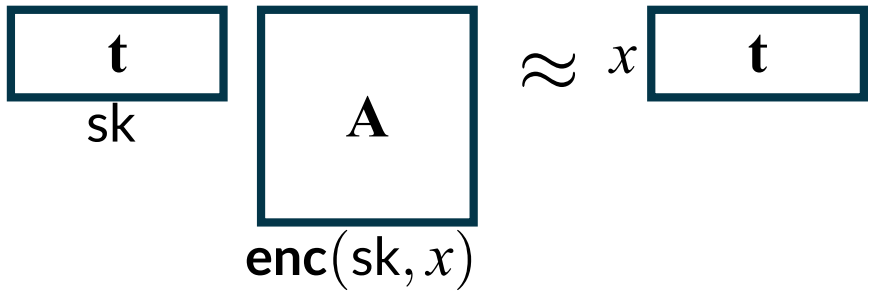


2. **A** hides x ✓
3. **A** small ✓

$$\overbrace{(\mathbf{s} \quad -1)\,\mathbf{G}}^{\text{new } \mathbf{t}} \cdot \underbrace{\mathbf{G}^{-1}\left(\begin{pmatrix} \mathbf{B} \\ \mathbf{sB}+\mathbf{e} \end{pmatrix} + x\,\mathbf{I}\right)}_{\mathbf{A}} \approx x\,\mathbf{t}$$

$\mathbf{t}$

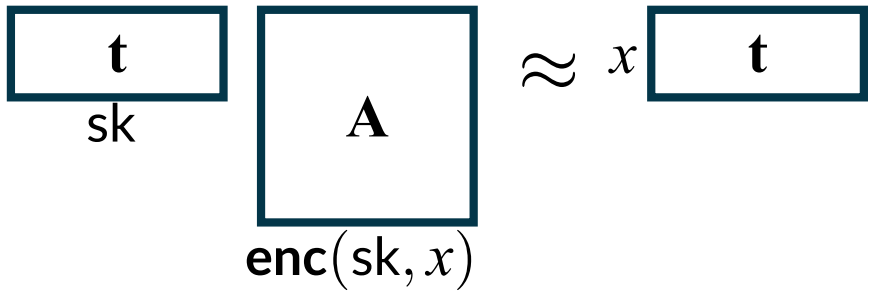
fully **homomorphic** encryption



2. **A** hides x ✓
3. **A** small ✓

$$\underbrace{\overbrace{\begin{pmatrix}\mathbf{s} & -1\end{pmatrix}}^{\text{new } \mathbf{t}}\mathbf{G}}_{\mathbf{t}} \cdot \underbrace{\mathbf{G}^{-1}\left(\begin{pmatrix}\mathbf{B} \\ \mathbf{sB}+\mathbf{e}\end{pmatrix} + x\mathbf{G}\right)}_{\mathbf{A}} \approx x\overbrace{\mathbf{tG}}^{\text{new } \mathbf{t}}$$

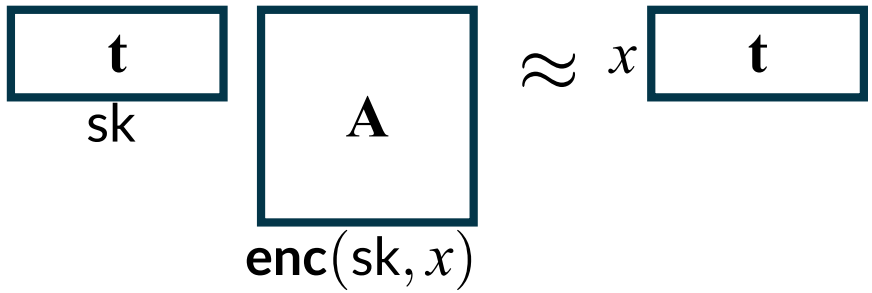
fully **homomorphic** encryption



2. **A** hides x ✓
3. **A** small ✓

$$\underbrace{(\mathbf{s} \quad -1)}_{\mathbf{t}} \cdot \underbrace{\begin{pmatrix} \mathbf{B} \\ \mathbf{sB} + \mathbf{e} \end{pmatrix} + x\mathbf{G}}_{\mathbf{A}} \approx x\,\mathbf{tG}$$

fully **homomorphic** encryption

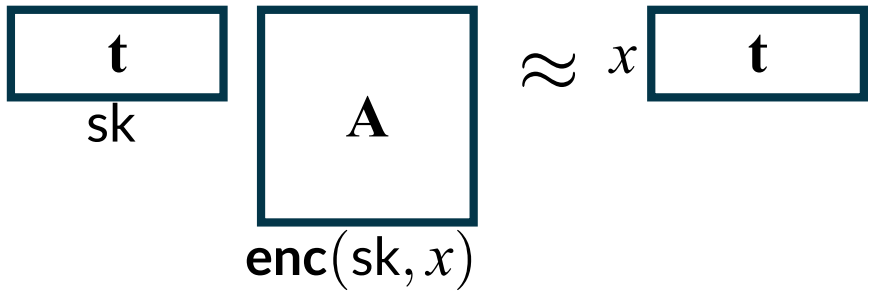


2. $\mathbf{A}$ hides x ✓
3. $\mathbf{A}$ small ✓

alternatively. $\mathbf{t} \cdot \mathbf{A} \approx x \cdot \mathbf{tG}$

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

fully **homomorphic** encryption



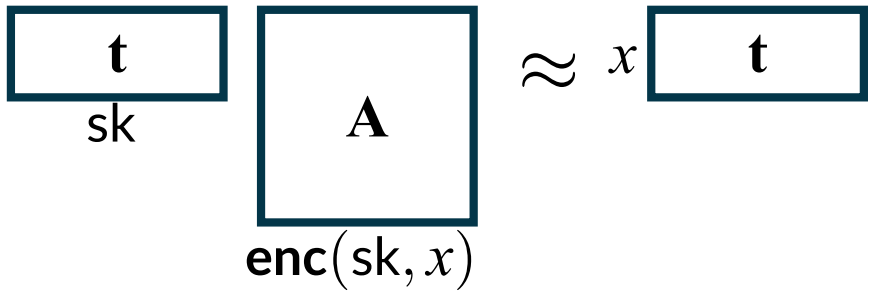
2. $\mathbf{A}$ hides x ✓
3. $\mathbf{A}$ small ✓

alternatively. $\mathbf{t} \cdot \mathbf{A} \approx x \cdot \mathbf{tG}$

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

multiplication: $\mathbf{t} \cdot (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{A}_2)) \approx x_1 x_2 \cdot \mathbf{tG}$

fully **homomorphic** encryption



2. $\mathbf{A}$ hides x ✓
3. $\mathbf{A}$ small ✓

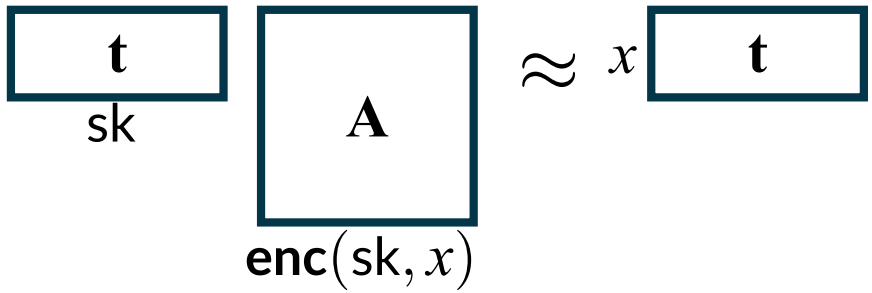
alternatively. $\mathbf{t} \cdot \mathbf{A} \approx x \cdot \mathbf{tG}$

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

multiplication: $\mathbf{t} \cdot (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{A}_2)) \approx x_1 x_2 \cdot \mathbf{tG}$

$x_1 x_2 x_3 = (x_1 x_2) x_3$: $\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{A}_2) \cdot \mathbf{G}^{-1}(\mathbf{A}_3)$

fully **homomorphic** encryption



2. $\mathbf{A}$ hides x ✓
3. $\mathbf{A}$ small ✓

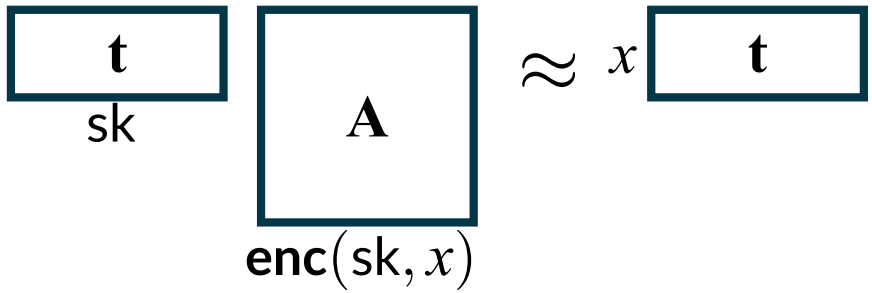
alternatively. $\mathbf{t} \cdot \mathbf{A} \approx x \cdot \mathbf{tG}$

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

multiplication: $\mathbf{t} \cdot (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{A}_2)) \approx x_1 x_2 \cdot \mathbf{tG}$

$x_1 x_2 x_3 = x_1(x_2 x_3)$: $\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{A}_2 \cdot \mathbf{G}^{-1}(\mathbf{A}_3))$

fully **homomorphic** encryption



2. $\mathbf{A}$ hides x ✓
3. $\mathbf{A}$ small ✓

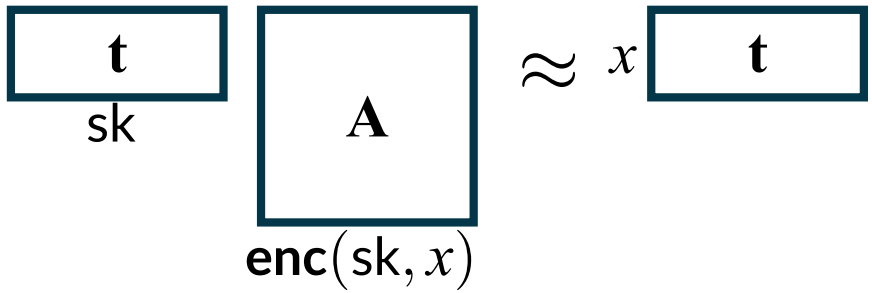
alternatively. $\mathbf{t} \cdot \mathbf{A} \approx x \cdot \mathbf{tG}$

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

multiplication: $\mathbf{t} \cdot (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{A}_2)) \approx x_1 x_2 \cdot \mathbf{tG}$

polynomials: $\mathbf{t} \cdot \mathbf{A}_f \approx f(x_1, \ldots, x_\ell) \cdot \mathbf{tG}$ error: degree $\cdot$ poly(λ)

fully **homomorphic** encryption



2. $\mathbf{A}$ hides x ✓
3. $\mathbf{A}$ small ✓

alternatively. $\mathbf{t} \cdot \mathbf{A} \approx x \cdot \mathbf{tG}$

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

multiplication: $\mathbf{t} \cdot (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{A}_2)) \approx x_1 x_2 \cdot \mathbf{tG}$

circuits: $\mathbf{t} \cdot \mathbf{A}_f \approx f(x_1, \ldots, x_\ell) \cdot \mathbf{tG}$ error: $\lambda^{O(\text{depth})}$

eigenvectors, revisited

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

eigenvectors, revisited

lemma I. $\mathbf{t} \cdot (\mathbf{A}_i - x_i \mathbf{I}) = \mathbf{0} \;\Rightarrow\; \mathbf{t} \cdot (\mathbf{A}_f - f(x)\mathbf{I}) = \mathbf{0}$

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

eigenvectors, revisited

lemma I. $\mathbf{t} \cdot (\mathbf{A}_i - x_i \mathbf{I}) = \mathbf{0} \;\Rightarrow\; \mathbf{t} \cdot (\mathbf{A}_f - f(x)\mathbf{I}) = \mathbf{0}$

lemma II. $\forall \mathbf{A}_i$

$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \cdots \mid \mathbf{A}_\ell - x_\ell \mathbf{I}] \qquad \mathbf{A}_f - f(x)\mathbf{I}$$

[GSW13, BGGHNSVV14, GVW15, ...]

eigenvectors, revisited

lemma I. $\mathbf{t} \cdot (\mathbf{A}_i - x_i \mathbf{I}) = \mathbf{0} \;\Rightarrow\; \mathbf{t} \cdot (\mathbf{A}_f - f(x)\mathbf{I}) = \mathbf{0}$

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

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

[GSW13, BGGHNSVV14, GVW15, ...]

eigenvectors, revisited

lemma I. $\mathbf{t} \cdot (\mathbf{A}_i - x_i \mathbf{I}) = \mathbf{0} \;\Rightarrow\; \mathbf{t} \cdot (\mathbf{A}_f - f(x)\mathbf{I}) = \mathbf{0}$

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

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

[GSW13, BGGHNSVV14, GVW15, ...]

claim. **lemma II** $\Rightarrow$ **lemma I**

proof. multiply both sides by $\mathbf{t}$: observe $\mathbf{0} \cdot \mathbf{H}_{f,x} = \mathbf{0}$

eigenvectors, revisited

lemma I. $\mathbf{t} \cdot (\mathbf{A}_i - x_i \mathbf{I}) = \mathbf{0} \;\Rightarrow\; \mathbf{t} \cdot (\mathbf{A}_f - f(x)\mathbf{I}) = \mathbf{0}$

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

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

proof. handle $+$ and $\times$

eigenvectors, revisited

lemma I. $\mathbf{t} \cdot (\mathbf{A}_i - x_i\mathbf{I}) = \mathbf{0} \;\Rightarrow\; \mathbf{t} \cdot (\mathbf{A}_f - f(x)\mathbf{I}) = \mathbf{0}$

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

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

proof. handle $+$ and $\times$

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

eigenvectors, revisited

lemma I. $\mathbf{t} \cdot (\mathbf{A}_i - x_i\mathbf{I}) = \mathbf{0} \;\Rightarrow\; \mathbf{t} \cdot (\mathbf{A}_f - f(x)\mathbf{I}) = \mathbf{0}$

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

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

proof. handle $+$ and $\times$

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

eigenvectors, revisited

lemma I. $\mathbf{t} \cdot (\mathbf{A}_i - x_i\mathbf{I}) = \mathbf{0} \;\Rightarrow\; \mathbf{t} \cdot (\mathbf{A}_f - f(x)\mathbf{I}) = \mathbf{0}$

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

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

proof. handle $+$ and $\times$

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

eigenvectors, revisited

lemma I. $\mathbf{t} \cdot (\mathbf{A}_i - x_i\mathbf{I}) = \mathbf{0} \;\Rightarrow\; \mathbf{t} \cdot (\mathbf{A}_f - f(x)\mathbf{I}) = \mathbf{0}$

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

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

proof. handle $+$ and $\times$

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

eigenvectors, revisited

lemma I. $\mathbf{t} \cdot (\mathbf{A}_i - x_i\mathbf{I}) = \mathbf{0} \;\Rightarrow\; \mathbf{t} \cdot (\mathbf{A}_f - f(x)\mathbf{I}) = \mathbf{0}$

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

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

proof. handle $+$ and $\times$

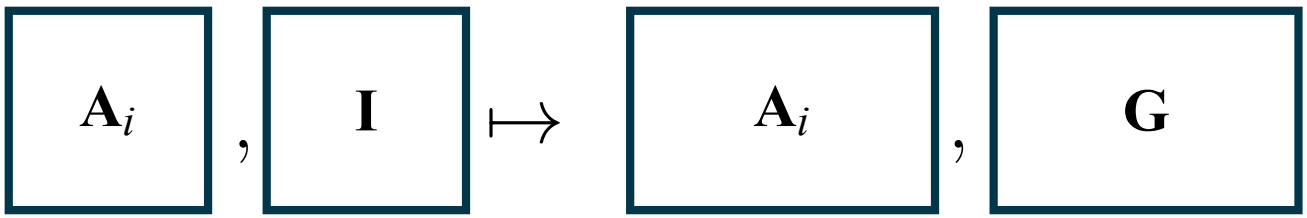
$$[\mathbf{A}_1 - x_1\mathbf{I} \mid \mathbf{A}_2 - x_2\mathbf{I}] \underbrace{\begin{pmatrix} \mathbf{A}_2 \\ \\ x_1\mathbf{I} \end{pmatrix}}_{\mathbf{H}_{\times,x_1,x_2}} = \underbrace{\mathbf{A}_1\mathbf{A}_2}_{\mathbf{A}_\times} - x_1x_2\mathbf{I}$$

eigenvectors, revisited*

lemma I. $\mathbf{t} \cdot \mathbf{A}_i = x_i \mathbf{t} \;\Rightarrow\; \mathbf{t} \cdot \mathbf{A}_f = f(x)\mathbf{t}$

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

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

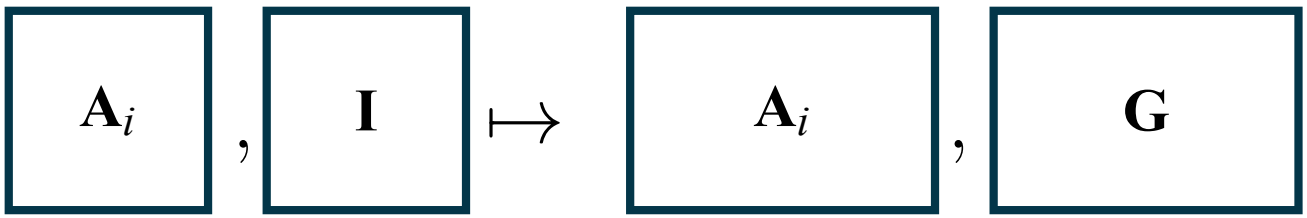


eigenvectors, revisited*

lemma I. $\mathbf{t} \cdot \mathbf{A}_i = x_i \mathbf{t} \;\Rightarrow\; \mathbf{t} \cdot \mathbf{A}_f = f(x)\mathbf{t}$

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

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



eigenvectors, revisited*

lemma I*. $\mathbf{t} \cdot \mathbf{A}_i \approx x_i \cdot \mathbf{tG} \;\Rightarrow\; \mathbf{t} \cdot \mathbf{A}_f \approx f(x) \cdot \mathbf{tG}$

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

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

claim. **lemma II*** $\Rightarrow$ **lemma I***

eigenvectors, revisited*

lemma I*. $\mathbf{t} \cdot \mathbf{A}_i \approx x_i \cdot \mathbf{tG} \;\Rightarrow\; \mathbf{t} \cdot \mathbf{A}_f \approx f(x) \cdot \mathbf{tG}$

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

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

claim. **lemma II*** $\Rightarrow$ **lemma I***

proof. multiply both sides by $\mathbf{t}$: observe small $\cdot\, \mathbf{H}_{f,x} \approx \mathbf{0}$

eigenvectors, revisited*

lemma I*. $\mathbf{t} \cdot \mathbf{A}_i \approx x_i \cdot \mathbf{tG} \;\Rightarrow\; \mathbf{t} \cdot \mathbf{A}_f \approx f(x) \cdot \mathbf{tG}$

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

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

proof. handle $+$ and $\times$

eigenvectors, revisited*

lemma I*. $\mathbf{t} \cdot \mathbf{A}_i \approx x_i \cdot \mathbf{tG} \;\Rightarrow\; \mathbf{t} \cdot \mathbf{A}_f \approx f(x) \cdot \mathbf{tG}$

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

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

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*

lemma I*. $\mathbf{t} \cdot \mathbf{A}_i \approx x_i \cdot \mathbf{tG} \;\Rightarrow\; \mathbf{t} \cdot \mathbf{A}_f \approx f(x) \cdot \mathbf{tG}$

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

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

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*

lemma I*. $\mathbf{t} \cdot \mathbf{A}_i \approx x_i \cdot \mathbf{tG} \;\Rightarrow\; \mathbf{t} \cdot \mathbf{A}_f \approx f(x) \cdot \mathbf{tG}$

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

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

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*

lemma I*. $\mathbf{t} \cdot \mathbf{A}_i \approx x_i \cdot \mathbf{tG} \;\Rightarrow\; \mathbf{t} \cdot \mathbf{A}_f \approx f(x) \cdot \mathbf{tG}$

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

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

proof. handle $+$ and $\times$

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

eigenvectors, revisited*

lemma I*. $\mathbf{t} \cdot \mathbf{A}_i \approx x_i \cdot \mathbf{tG} \;\Rightarrow\; \mathbf{t} \cdot \mathbf{A}_f \approx f(x) \cdot \mathbf{tG}$

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

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

insight. $\mathbf{A}_i, \mathbf{A}_f \in \mathbb{Z}_q^{n \times O(n \log q)}$

eigenvectors, revisited*

lemma I*. $\mathbf{t} \cdot \mathbf{A}_i \approx x_i \cdot \mathbf{tG} \Rightarrow \mathbf{t} \cdot \mathbf{A}_f \approx f(x) \cdot \mathbf{tG}$

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

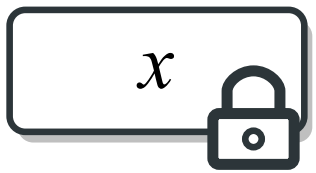
$$[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}] \cdot \mathbf{H}_{f,x} = \mathbf{A}_f - f(x)\mathbf{G}$$

insight. $\mathbf{A}_i, \mathbf{A}_f \in \mathbb{Z}_q^{n \times O(n \log q)}$ where $n, \log q = \text{poly}(\lambda, \text{depth})$

functional commitment

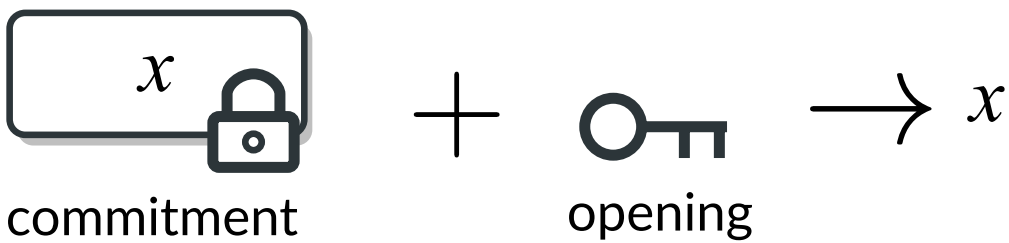
functional **commitment**

functional **commitment**



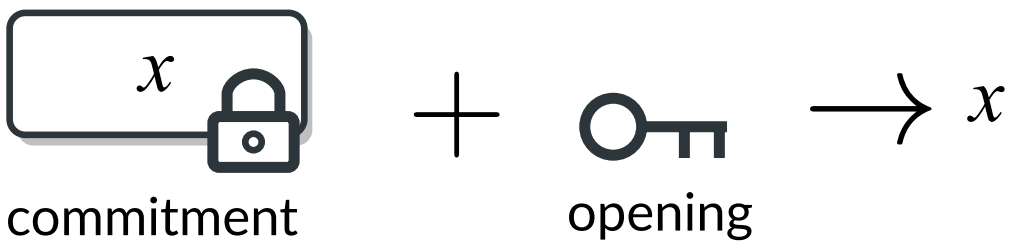
commitment

functional **commitment**



functional **commitment**

commit$(\mathsf{crs}, x) \mapsto (\sigma, \mathsf{st})$ commitment, state



functional **commitment**

commit$(\mathsf{crs}, x) \mapsto (\sigma, \mathsf{st})$ commitment, state

open$(\mathsf{st}) \mapsto \pi$ opening

verify$(\mathsf{crs}, \sigma, y, \pi) \mapsto 0/1$

functional **commitment**

commit$(\mathsf{crs}, x) \mapsto (\sigma, \mathsf{st})$ commitment, state

open$(\mathsf{st}) \mapsto \pi$ opening

verify$(\mathsf{crs}, \sigma, y, \pi) \mapsto 0/1$

---

correctness. **verify**$(\mathsf{crs}, \sigma, x, \pi) = 1$

functional **commitment**

commit$(\mathsf{crs}, x) \mapsto (\sigma, \mathsf{st})$ commitment, state

open$(\mathsf{st}) \mapsto \pi$ opening

verify$(\mathsf{crs}, \sigma, y, \pi) \mapsto 0/1$

---

correctness. **verify**$(\mathsf{crs}, \sigma, x, \pi) = 1$

binding. cannot produce σ with openings π_0, π_1 to $y_0 \neq y_1$

hiding. σ hides x

functional **commitment**

commit$(\mathsf{crs}, x) \mapsto (\sigma, \mathsf{st})$ commitment, state

open$(\mathsf{st}) \mapsto \pi$ opening

verify$(\mathsf{crs}, \sigma, y, \pi) \mapsto 0/1$

---

correctness. **verify**$(\mathsf{crs}, \sigma, x, \pi) = 1$

binding. cannot produce σ with openings π_0, π_1 to $y_0 \neq y_1$

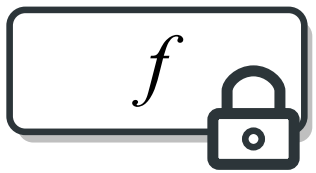
succinctness. $|\sigma| \ll |x|$

functional commitment

commit$(\mathsf{crs}, f) \mapsto (\sigma, \mathsf{st})$

open$(\mathsf{st}) \mapsto \pi$

verify$(\mathsf{crs}, \sigma, y, \pi) \mapsto 0/1$



commitment

functional commitment

commit$(\mathsf{crs}, f) \mapsto (\sigma, \mathsf{st})$

open$(\mathsf{st}) \mapsto \pi$

verify$(\mathsf{crs}, \sigma, y, \pi) \mapsto 0/1$

functional commitment

commit$(\mathsf{crs}, f) \mapsto (\sigma, \mathsf{st})$

open$(\mathsf{st}, x) \mapsto \pi$

verify$(\mathsf{crs}, \sigma, (x, y), \pi) \mapsto 0/1$

commitment opening

functional commitment

commit$(\mathsf{crs}, f) \mapsto (\sigma, \mathsf{st})$

open$(\mathsf{st}, x) \mapsto \pi$

verify$(\mathsf{crs}, \sigma, (x, y), \pi) \mapsto 0/1$

---

correctness. **verify**$(\mathsf{crs}, \sigma, (x, f(x)), \pi) = 1$

functional commitment

commit$(\mathsf{crs}, f) \mapsto (\sigma, \mathsf{st})$

open$(\mathsf{st}, x) \mapsto \pi$

verify$(\mathsf{crs}, \sigma, (x, y), \pi) \mapsto 0/1$

---

correctness. **verify**$(\mathsf{crs}, \sigma, (x, f(x)), \pi) = 1$

binding. cannot produce σ with openings x, π_0, π_1 to $y_0 \neq y_1$

functional commitment

commit$(\mathsf{crs}, f) \mapsto (\sigma, \mathsf{st})$

open$(\mathsf{st}, x) \mapsto \pi$

verify$(\mathsf{crs}, \sigma, (x, y), \pi) \mapsto 0/1$

---

correctness. **verify**$(\mathsf{crs}, \sigma, (x, f(x)), \pi) = 1$

binding. cannot produce σ with openings x, π_0, π_1 to $y_0 \neq y_1$

succinctness. $|\sigma|, |\pi| \ll |f|$

functional commitment

commit$(\mathsf{crs}, f) \mapsto (\sigma, \mathsf{st})$

open$(\mathsf{st}, x) \mapsto \pi$

verify$(\mathsf{crs}, \sigma, (x, y), \pi) \mapsto 0/1$

[**de Castro Peikert 23**] functional commitments for circuits from SIS

functional commitment

commit$(\mathsf{crs}, f) \mapsto (\sigma, \mathsf{st})$

open$(\mathsf{st}, x) \mapsto \pi$

verify$(\mathsf{crs}, \sigma, (x, y), \pi) \mapsto 0/1$

[**de Castro Peikert 23**] functional commitments for circuits from SIS

crs: $\mathbf{A}_1, \ldots, \mathbf{A}_\ell$

here, $x = (x_1, \ldots, x_\ell) \in \{0,1\}^\ell$, $f \colon \{0,1\}^\ell \to \{0,1\}$

functional commitment

commit$(\mathsf{crs}, f) \mapsto (\sigma, \mathsf{st})$

open$(\mathsf{st}, x) \mapsto \pi$

verify$(\mathsf{crs}, \sigma, (x, y), \pi) \mapsto 0/1$

[**de Castro Peikert 23**] functional commitments for circuits from SIS

crs: $\mathbf{A}_1, \ldots, \mathbf{A}_\ell$

commit: $\sigma := \mathbf{A}_f$ i.e., $|\sigma| = \mathsf{poly}(\lambda, \mathsf{depth})$

functional commitment

commit$(\mathsf{crs}, f) \mapsto (\sigma, \mathsf{st})$

open$(\mathsf{st}, x) \mapsto \pi$

verify$(\mathsf{crs}, \sigma, (x, y), \pi) \mapsto 0/1$

[**de Castro Peikert 23**] functional commitments for circuits from SIS

crs: $\mathbf{A}_1, \ldots, \mathbf{A}_\ell$

commit: $\sigma := \mathbf{A}_f$ **open** : $\pi := \mathbf{H}_{f,x}$

functional commitment

commit$(\mathsf{crs}, f) \mapsto (\sigma, \mathsf{st})$

open$(\mathsf{st}, x) \mapsto \pi$

verify$(\mathsf{crs}, \sigma, (x, y), \pi) \mapsto 0/1$

[**de Castro Peikert 23**] functional commitments for circuits from SIS

crs: $\mathbf{A}_1, \ldots, \mathbf{A}_\ell$

commit: $\sigma := \mathbf{A}_f$ **open** : $\pi := \mathbf{H}_{f,x}$

verify: π is small and $[\mathbf{A}_1 - x_1\mathbf{G} \mid \cdots \mid \mathbf{A}_\ell - x_\ell\mathbf{G}] \cdot \pi = \mathbf{A}_f - y\mathbf{G}$

laconic function evaluation

[Quach W Wichs 18, CDGGMP17]

alice

x

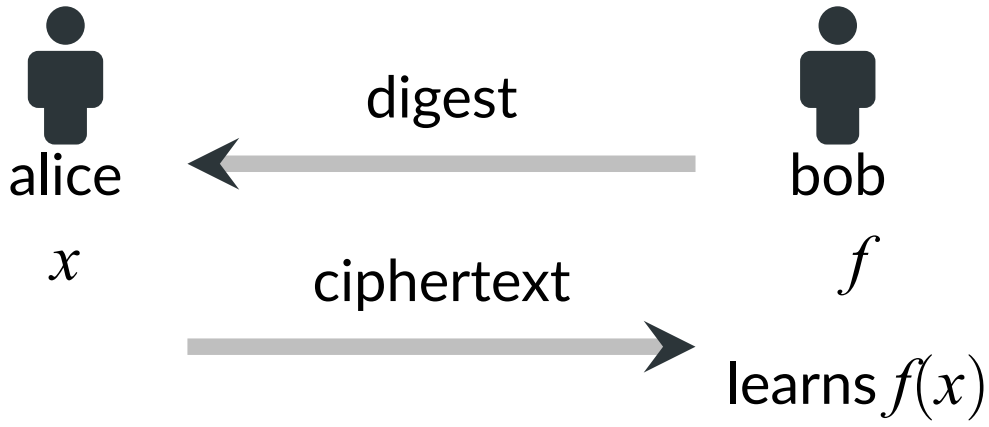
bob

f

learns $f(x)$

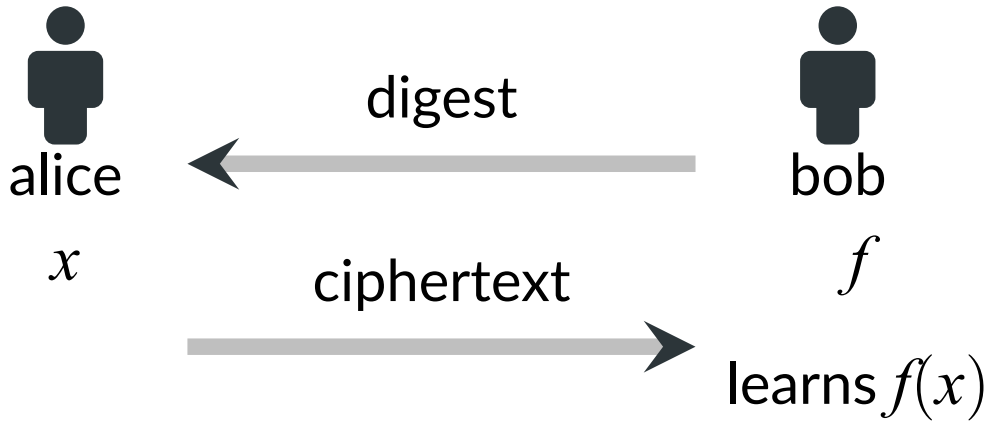
laconic function evaluation

[Quach W Wichs 18, CDGGMP17]



laconic function evaluation

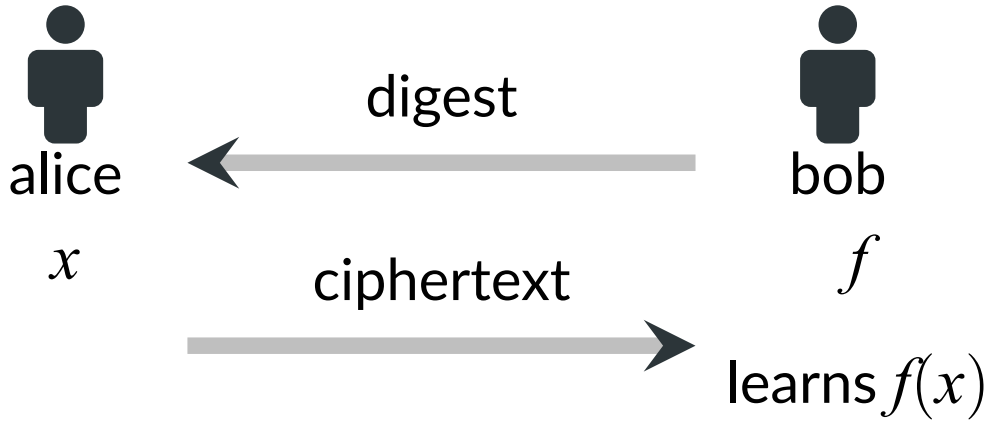
[**Quach W Wichs 18, CDGGMP17**]



security. ciphertext leaks only $f(x)$ (nothing else about x)

laconic function evaluation

[Quach W Wichs 18, CDGGMP17]

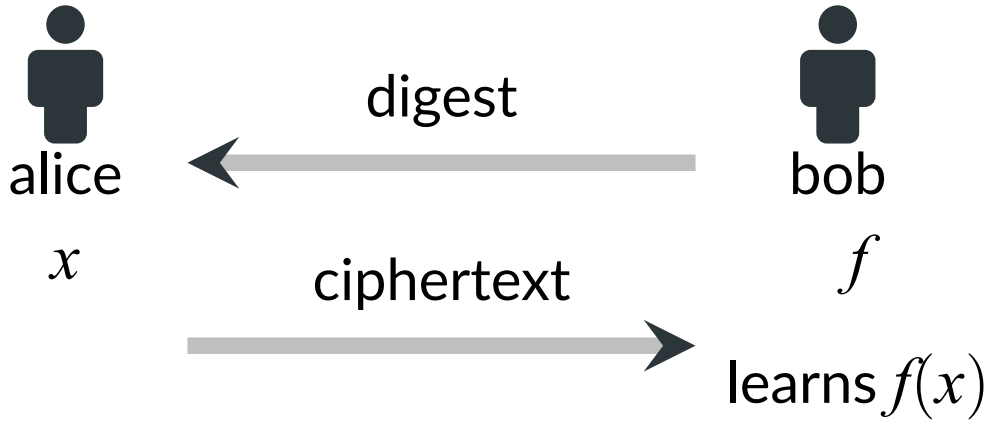


security. ciphertext leaks only $f(x)$ (nothing else about x)

efficiency. $\approx$ alice sends x (faster than computing f)

laconic function evaluation

[Quach W Wichs 18, CDGGMP17]



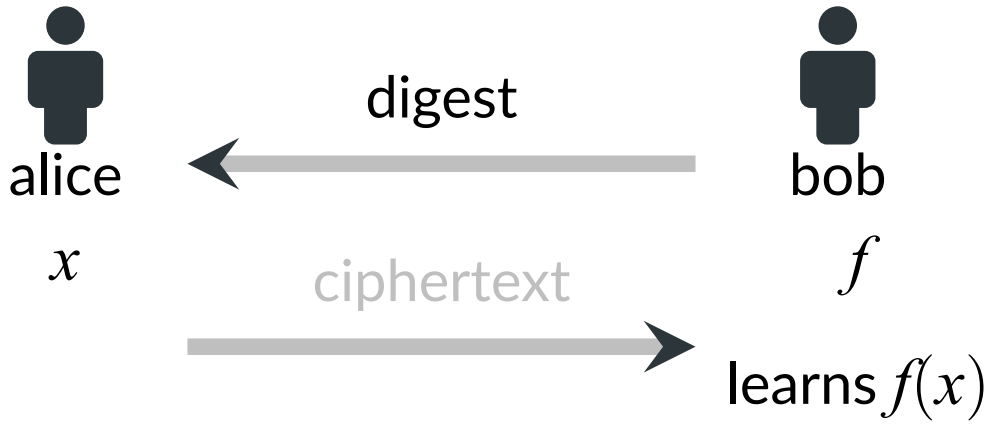
security. ciphertext leaks only $f(x)$ (nothing else about x)

efficiency. $\approx$ alice sends x (faster than computing f)

NOTE. FHE requires more interaction

laconic function evaluation

[Quach W Wichs 18, CDGGMP17]



security. ciphertext leaks only $f(x)$ (nothing else about x)

efficiency. $\approx$ alice sends x (faster than computing f)

construction. digest = $\mathbf{A}_1, \ldots, \mathbf{A}_\ell, \mathbf{A}_f$

conclusion

1/3. lattices $\Rightarrow$ **encrypted computation**

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

conclusion

1/3. lattices $\Rightarrow$ **encrypted computation**

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

2/3 & 3/3. lattice trapdoors & attribute-based encryption

conclusion

1/3. lattices $\Rightarrow$ **encrypted computation**

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

2/3 & 3/3. lattice trapdoors & attribute-based encryption

// thank you & enjoy!