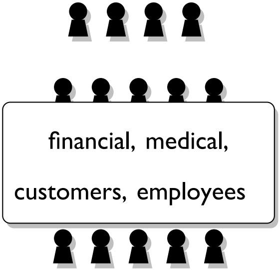
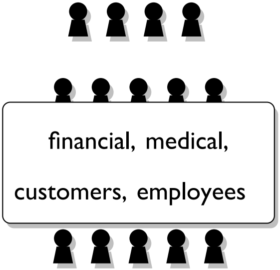
# **encrypted** computation *from* lattices

Hoeteck Wee

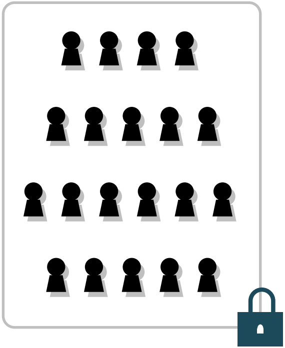



# BIG DATA



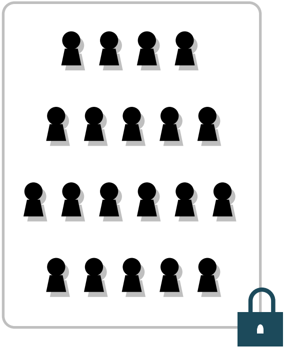

# BIG DATA

**Q.** privacy.



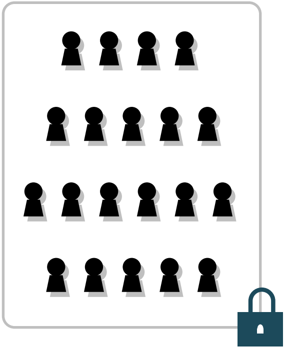
# BIG DATA

Q. privacy.



# BIG DATA

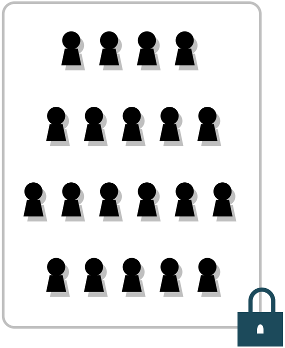
**Q.** privacy. utility?



# BIG DATA

**Q.** privacy + utility

**encrypted computation**

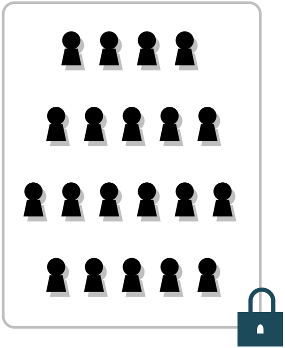


# BIG DATA

Q. privacy + utility

**encrypted computation**

**3** notions

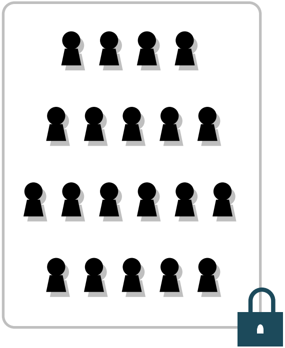


BIG DATA

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

**functionality.**

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

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

# fully **homomorphic** encryption

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

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

# fully **homomorphic** encryption

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

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

**FHE** for **circuits** from lattices

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

# fully **homomorphic** encryption

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

**functionality.** **enc**$(\mathsf{sk}, x) \overset{\textsf{eval}}{\mapsto}$ **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.** $\textbf{enc}(\mathsf{sk}, x)$ hides $x$

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

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

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

# fully **homomorphic** encryption

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

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

# fully **homomorphic** encryption

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

**functionality.** **enc**(sk, $x$) $\mapsto$ **enc**(sk, $f(x)$) 1

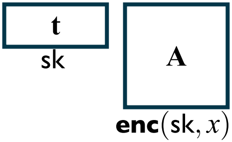
**t**
sk

over $\mathbb{Z}_q$

# fully **homomorphic** encryption

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

**functionality.** **enc**(sk, $x$) $\mapsto$ **enc**(sk, $f(x)$) 1



# fully **homomorphic** encryption

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

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

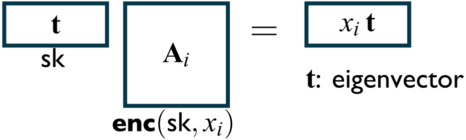
$$\underbrace{\mathbf{t}}_{\mathsf{sk}} \; \underbrace{\mathbf{A}}_{\mathbf{enc}(\mathsf{sk}, x)} = x\,\mathbf{t}$$

**t**: eigenvector

# fully **homomorphic** encryption

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

**functionality.** **enc**(sk, $x$) $\mapsto$ **enc**(sk, $f(x)$) 1

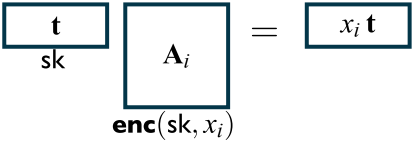



**enc**(sk, $x_1$), **enc**(sk, $x_2$) $\overset{?}{\mapsto}$ **enc**(sk, $x_1 + x_2$), **enc**(sk, $x_1 x_2$)

# fully **homomorphic** encryption

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

**functionality.** **enc**(sk, $x$) $\mapsto$ **enc**(sk, $f(x)$) 1

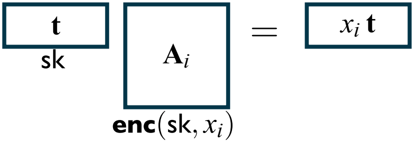



addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) = (x_1 + x_2)\mathbf{t}$

# fully **homomorphic** encryption

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

**functionality.** **enc**(sk, $x$) $\mapsto$ **enc**(sk, $f(x)$) 1



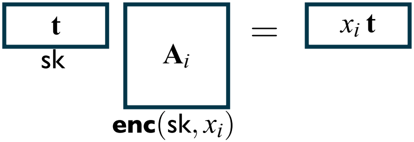

addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) = (x_1 + x_2)\mathbf{t}$

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

# fully **homomorphic** encryption

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

**functionality.** **enc**(sk, $x$) $\mapsto$ **enc**(sk, $f(x)$) 1




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

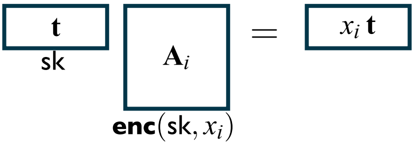
multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 = x_1 x_2 \mathbf{t}$

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

# fully **homomorphic** encryption

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

**functionality.** **enc**(sk, $x$) $\mapsto$ **enc**(sk, $f(x)$) 1




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

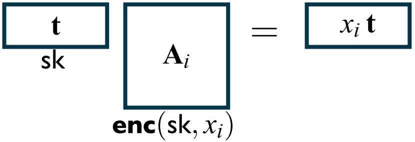
multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 = x_1 x_2 \mathbf{t}$

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

**functionality.** **enc**(sk, $x$) $\mapsto$ **enc**(sk, $f(x)$) 1




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

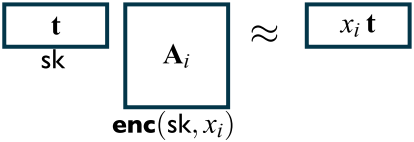
multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 = x_1 x_2 \mathbf{t}$

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

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



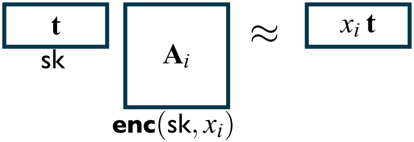

addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) = (x_1 + x_2)\mathbf{t}$

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

# fully **homomorphic** encryption

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

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



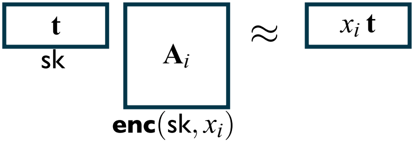

addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) \approx (x_1 + x_2)\mathbf{t}$

– *proof.* small + small = small

# fully **homomorphic** encryption

**security.** **enc**$(\mathsf{sk}, x)$ 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: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 \not\approx x_1 x_2 \mathbf{t}$

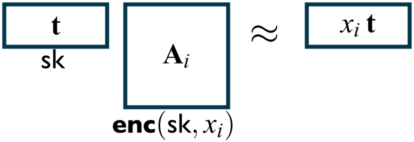
– *proof.* small $\cdot \mathbf{A}_2$ = big

# fully **homomorphic** encryption

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

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

3 $\mathbf{A}_i$ small




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

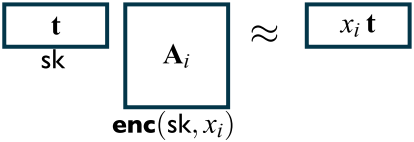
multiplication: $\mathbf{t} \cdot \mathbf{A}_1\mathbf{A}_2 \not\approx x_1 x_2 \mathbf{t}$

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

# fully **homomorphic** encryption

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

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




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

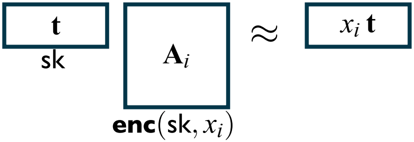
multiplication: $\mathbf{t} \cdot \mathbf{A}_1 \mathbf{A}_2 \approx x_1 x_2 \mathbf{t}$

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

# fully **homomorphic** encryption

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

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

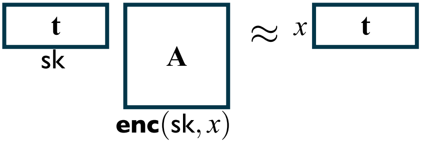



addition: $\mathbf{t} \cdot (\mathbf{A}_1 + \mathbf{A}_2) \approx (x_1 + x_2)\mathbf{t}$

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

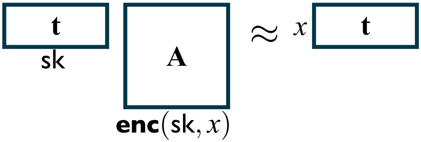
polynomials: $\mathbf{t} \cdot \underbrace{f(\mathbf{A}_1, \ldots, \mathbf{A}_n)}_{\mathbf{A}_f} \approx f(x_1, \ldots, x_n)\mathbf{t}$

# fully **homomorphic** encryption




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

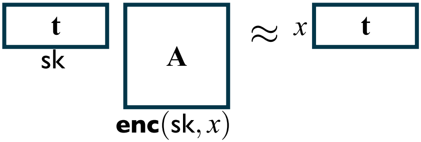
# fully **homomorphic** encryption




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

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

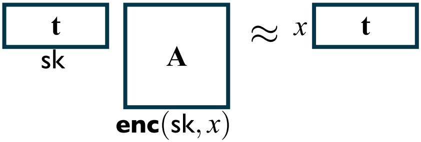
# fully **homomorphic** encryption




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

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

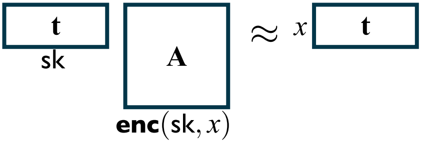
# fully **homomorphic** encryption




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

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

# fully **homomorphic** encryption




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

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

# fully **homomorphic** encryption

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

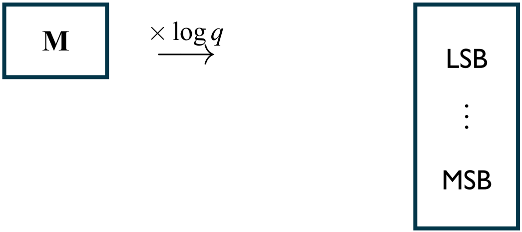
2. $\mathbf{A}$ hides $x$
3. $\mathbf{A}$ small

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

# fully **homomorphic** encryption



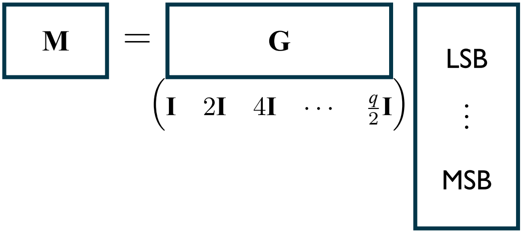

2. A hides $x$
3. A small



# fully **homomorphic** encryption




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



# fully **homomorphic** encryption

$\mathbf{t}$ (sk) $\cdot$ $\mathbf{A}$ (**enc**(sk, $x$)) $\approx x\,\mathbf{t}$

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

$$\mathbf{M} = \mathbf{G}\;\mathbf{G}^{-1}(\mathbf{M})$$

$$\mathbf{G} = \begin{pmatrix} \mathbf{I} & 2\mathbf{I} & 4\mathbf{I} & \cdots & \frac{q}{2}\mathbf{I} \end{pmatrix}$$

# fully **homomorphic** encryption

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

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

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

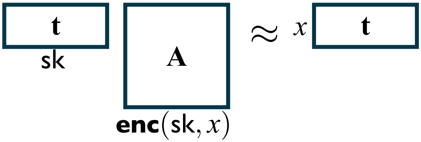
# fully **homomorphic** encryption

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

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

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

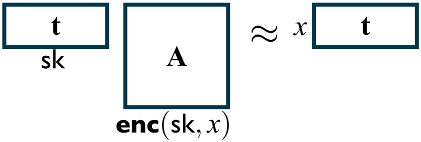
# fully **homomorphic** encryption




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

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

# fully **homomorphic** encryption




- ② **A** hides $x$
- ③ **A** small

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

# fully **homomorphic** encryption

$$\underbrace{\boxed{\;\mathbf{t}\;}}_{\text{sk}} \; \underbrace{\boxed{\;\mathbf{A}\;}}_{\textbf{enc}(\text{sk},\, x)} \approx x \, \boxed{\;\mathbf{t}\;}$$

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

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

# **small**, small, ...

# **small**, small, ...

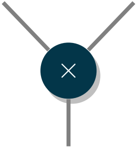
– $\mathbf{G}^{-1}(\mathbf{M}_1)\mathbf{G}^{-1}(\mathbf{M}_2) \Rightarrow \text{small} \approx \text{small}^{\text{deg}(f)}$

# **small**, small, ...

- $\mathbf{G}^{-1}(\mathbf{M}_1)\mathbf{G}^{-1}(\mathbf{M}_2) \Rightarrow \text{small} \approx \text{small}^{\text{deg}(f)}$
- $\mathbf{G}^{-1}(\mathbf{M}_1\mathbf{G}^{-1}(\mathbf{M}_2)) \Rightarrow \text{small} \approx \text{small}^{\log \text{deg}(f)}$

# **small**, small, ...

**circuit**

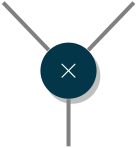



intermediate × intermediate

$$\text{small}_{\text{output}} = n^{\text{depth}} \cdot \text{small}_{\text{input}}$$

# **small**, small, ...

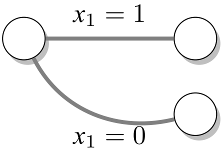
**circuit**




intermediate $\times$ intermediate

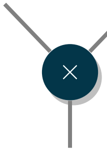
$\text{small}_{\text{output}} = n^{\text{depth}} \cdot \text{small}_{\text{input}}$

**branching program**



# **small**, small, ...

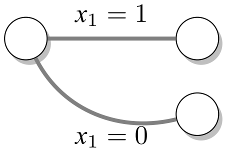
**circuit**



intermediate $\times$ intermediate

$\text{small}_{\text{output}} = n^{\text{depth}} \cdot \text{small}_{\text{input}}$

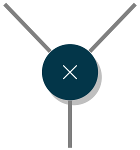
**branching program**




intermediate $\times$ input

# **small**, small, ...

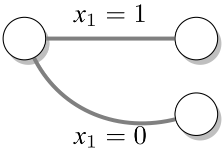
**circuit**



intermediate $\times$ intermediate

$\text{small}_{\text{output}} = n^{\text{depth}} \cdot \text{small}_{\text{input}}$

**branching program**



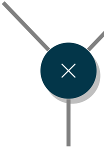

intermediate $\times$ input

$\text{small}_{\text{output}} = n \cdot \text{length} \cdot \text{small}_{\text{input}}$

# **small**, small, ...

**circuit**

depth $O(\log n)$



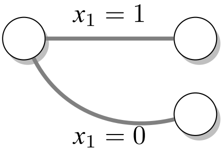
intermediate $\times$ intermediate

$\text{small}_{\text{output}} = n^{\text{depth}} \cdot \text{small}_{\text{input}}$

$\subseteq$

**branching program**

length $\text{poly}(n)$

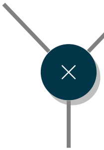



intermediate $\times$ input

$\text{small}_{\text{output}} = n \cdot \text{length} \cdot \text{small}_{\text{input}}$

# **small**, small, ...

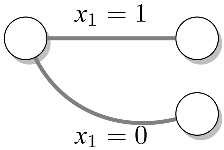
**circuit**
depth $O(\log n)$



$n^{O(\log n)}$ blow-up

$\subseteq$

**branching program**
length poly$(n)$

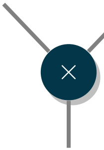



poly$(n)$ blow-up

# **small**, small, ...

**circuit**

depth $O(\log n)$

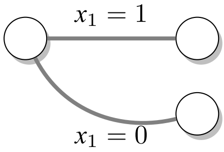


$n^{O(\log n)}$ blow-up

$\subseteq$

**branching program**

length poly$(n)$




poly$(n)$ blow-up

log-depth circuits with **polynomial** hardness **[BV14, AP14, GVW13]**

# **eigenvectors**, revisited

**lemma 1.** $\mathbf{t} \cdot \mathbf{A}_i = x_i \mathbf{t} \ \Rightarrow \ \mathbf{t} \cdot \underbrace{\mathbf{A}_f}_{f(\mathbf{A}_1,\ldots,\mathbf{A}_n)} = f(x)\mathbf{t}$

# **eigenvectors**, revisited

**lemma 1.** $\mathbf{t} \cdot (\mathbf{A}_i - x_i \mathbf{I}) = \mathbf{0} \;\Rightarrow\; \mathbf{t} \cdot (\mathbf{A}_f - f(x)\mathbf{I}) = \mathbf{0}$

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

# **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.** $\forall \mathbf{A}_i$

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

**[GSW13, BGG+14, GVW15, BCTW16, MP12]**

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

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

**[GSW13, BGG+14, GVW15, BCTW16, MP12]**

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

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

**[GSW13, BGG+14, GVW15, BCTW16, MP12]**

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

*proof.* multiply both sides by $\mathbf{t}$

# **eigenvectors**, revisited

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

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

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

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

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

**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

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

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

**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

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

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

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

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

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

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

**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

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

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

**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*

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

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

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

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

# **eigenvectors**, revisited*

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

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

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

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

# **eigenvectors**, revisited*

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

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

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

*corollary.* small $\mathbf{H}_{f,x} \Rightarrow$ robust to noise

# eigenvectors, revisited*

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

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

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

*corollary.* small $\mathbf{H}_{f,x} \Rightarrow$ robust to noise

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

# **eigenvectors**, revisited*

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

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

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

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

# **eigenvectors**, revisited*

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

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

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

**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*

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

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

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

**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*

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

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

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

**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*

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

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

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

**proof.** handle + and ×

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

# **eigenvectors**, revisited*

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

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

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

**applications.**

fully homomorphic enc **[GSW]**

attribute-based enc **[BGGHNSVV]**

fully homomorphic sig **[GVW]**

# **eigenvectors**, revisited*

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

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

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

| **applications.** | $\mathbf{A}_f$ | $\mathbf{H}_{f,x}$ |
|---|---|---|
| fully homomorphic enc [**GSW**] | eval output | correctness |
| attribute-based enc [**BGGHNSVV**] | | |
| fully homomorphic sig [**GVW**] | | |

# eigenvectors, revisited*

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

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

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

| **applications.** | $\mathbf{A}_f$ | $\mathbf{H}_{f,x}$ |
|---|---|---|
| fully homomorphic enc [**GSW**] | eval output | correctness |
| attribute-based enc [**BGGHNSVV**] | keygen | decryption |
| fully homomorphic sig [**GVW**] | verification | homomorphic sign |

# conclusion

**today.** lattices $\Rightarrow$ **encrypted computation**

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

# conclusion

**today.** lattices $\Rightarrow$ **encrypted computation**

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

# conclusion

**today.** lattices $\Rightarrow$ **encrypted computation**

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

**today.** lattices $\Rightarrow$ **FHE** for circuits with **dec** $\approx \langle \text{sk}, \text{ct} \rangle$

# conclusion

**today.** lattices $\Rightarrow$ **encrypted computation**

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

**today.** lattices $\Rightarrow$ **FHE** for circuits with **dec** $\approx \langle$sk, ct$\rangle$

" XXX for fhe.dec $\Rightarrow$ XXX for circuits " **[GVW12,GKPVZ13,GVW15]**

# conclusion

**today.** lattices $\Rightarrow$ **encrypted computation**

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

**today.** lattices $\Rightarrow$ **FHE** for circuits with **dec** $\approx \langle$sk, ct$\rangle$

"XXX for $\approx$ lin $\Rightarrow$ XXX for circuits" [GVW12,GKPVZ13,**GVW15**]

# conclusion

**today.** lattices $\Rightarrow$ **encrypted computation**

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

**today.** lattices $\Rightarrow$ **FHE** for circuits with **dec** $\approx \langle$sk, ct$\rangle$

" XXX for $\approx$ lin $\Rightarrow$ XXX for circuits " [GVW12,GKPVZ13,**GVW15**]

starting point for **obfuscation** – **tomorrow**

# conclusion

**today.** lattices $\Rightarrow$ **encrypted computation**

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

**tue.** obfuscation

**wed.** another way to encode computation into lattices

**[GGH15, KW16, CC17, GKW17, WZ17, GKW18, CVW18, ...]**

# conclusion

**today.** lattices $\Rightarrow$ **encrypted computation**

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

**tue.** obfuscation

**wed.** another way to encode computation into lattices

**thu.** MPC, LWE, FHE

# conclusion

**today.** lattices $\Rightarrow$ **encrypted computation**

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

**tue.** obfuscation

**wed.** another way to encode computation into lattices

**thu.** MPC, LWE, FHE

**fri.** quantum crypto

# conclusion

**today.** lattices $\Rightarrow$ **encrypted computation**

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

**tue.** obfuscation

**wed.** another way to encode computation into lattices

**thu.** MPC, LWE, FHE

**fri.** quantum crypto

**// thank you & enjoy!**