Additive-Homomorphic Functional Commitments and Applications to Homomorphic Signatures

Dario Catalano
University of Catania
Italy

Dario Fiore
IMDEA Software Institute
Madrid, Spain

Ida Tucker
Zondax AG

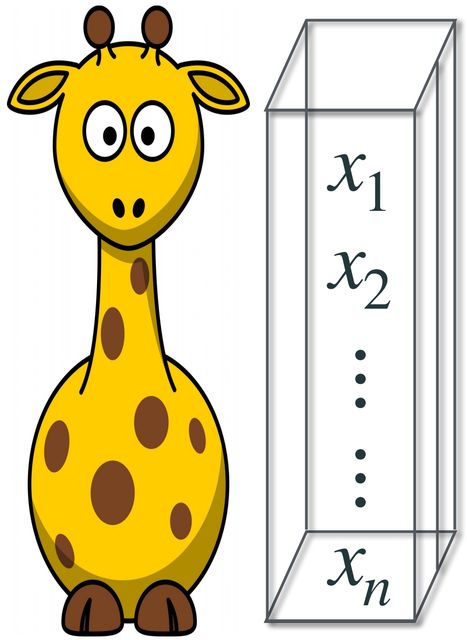
Asiacrypt 2022

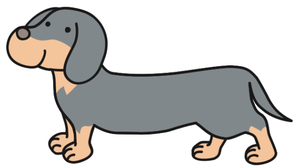
European Research Council
Established by the European Commission

Functional Commitments

[Libert-Ramanna-Yung16]

- Generalization of vector commitments and polynomial commitments

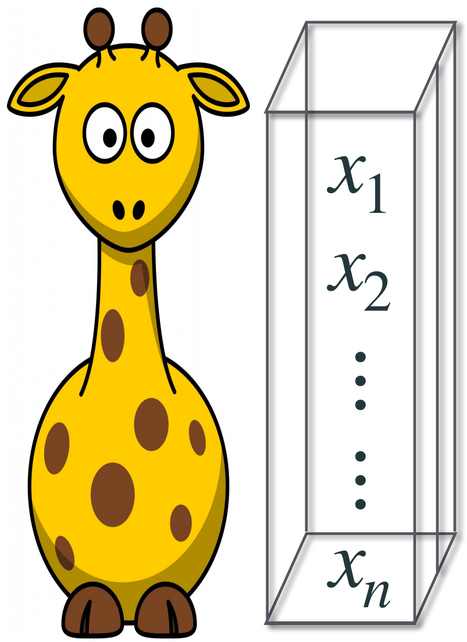




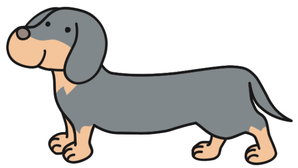
Functional Commitments

[Libert-Ramanna-Yung16]

- Generalization of vector commitments and polynomial commitments



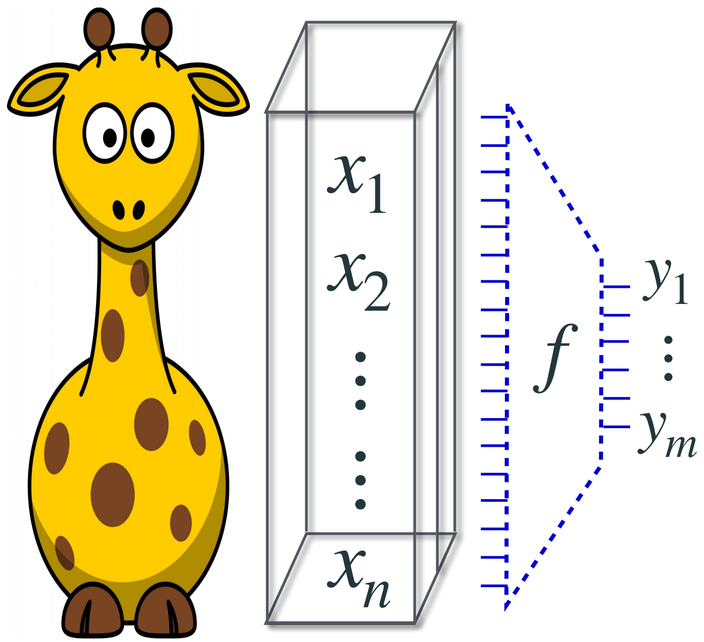
$\mathrm{Com}(\mathbf{x}) \rightarrow$ $C_{\mathbf{x}}$



Functional Commitments

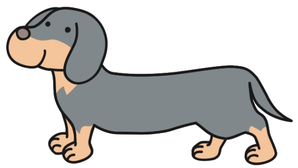
[Libert-Ramanna-Yung16]

- Generalization of vector commitments and polynomial commitments



$\text{Com}(\mathbf{x}) \rightarrow \quad C_{\mathbf{x}}$

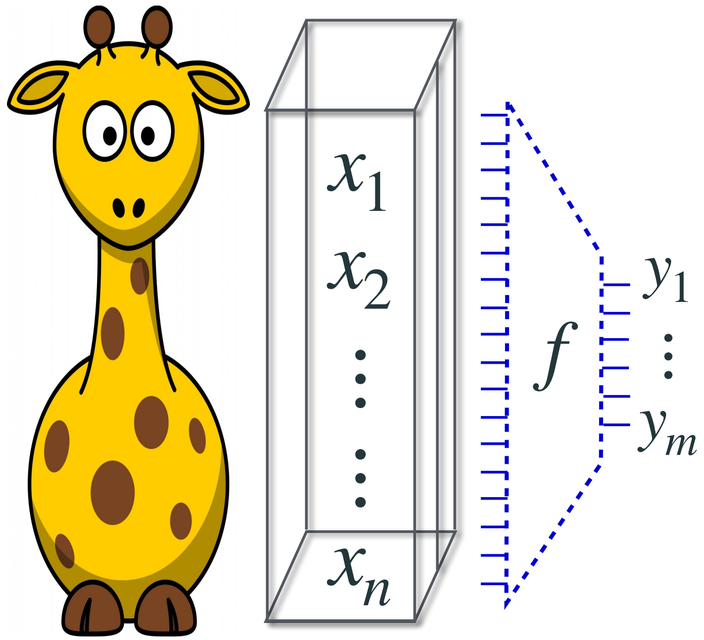
$\mathbf{y} = f(\mathbf{x})$



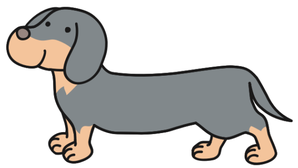
Functional Commitments

[Libert-Ramanna-Yung16]

- Generalization of vector commitments and polynomial commitments



$\mathsf{Com}(\mathbf{x}) \rightarrow$ $\mathsf{C}_{\mathbf{x}}$



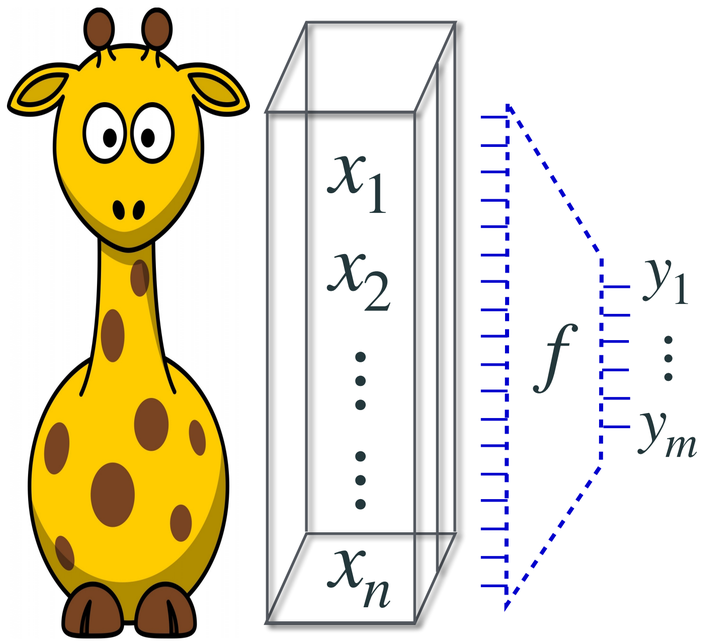
$\mathsf{Open}(f, \mathbf{x}) \rightarrow$ π_f $\mathbf{y} = f(\mathbf{x})$

$\mathsf{Ver}(\mathsf{C}_{\mathbf{x}}, f, \mathbf{y}, \pi_f) \stackrel{?}{=} 1$

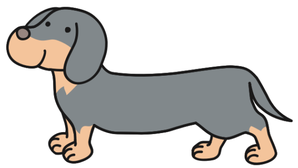
Functional Commitments

[Libert-Ramanna-Yung16]

- Generalization of vector commitments and polynomial commitments



$\text{Com}(\mathbf{x}) \rightarrow \quad C_{\mathbf{x}}$



$\text{Open}(f, \mathbf{x}) \rightarrow \quad \pi_f \quad \mathbf{y} = f(\mathbf{x})$

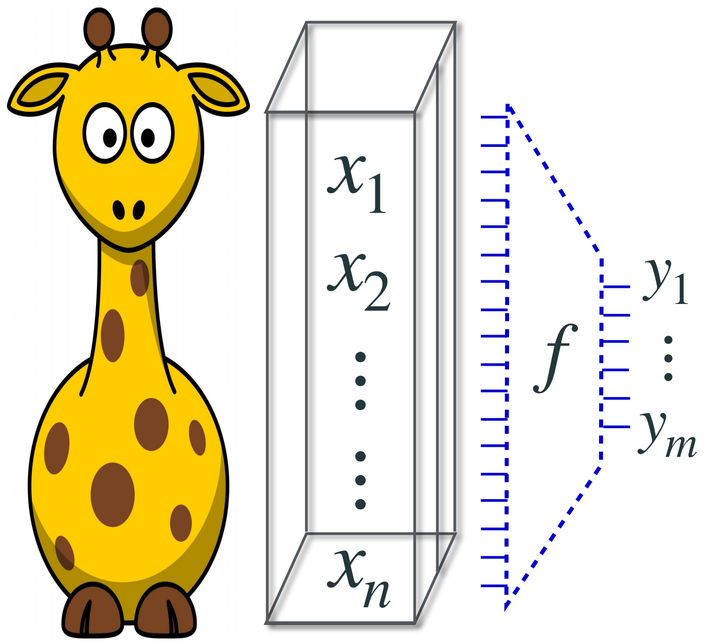
$\text{Ver}(C_{\mathbf{x}}, f, \mathbf{y}, \pi_f) \stackrel{?}{=} 1$

- **Succinctness:** commitments and *openings "short" w.r.t.* $|\mathbf{x}|$: $|C_{\mathbf{x}}| \leq p(\lambda)$ and $|\pi_f| \leq m \cdot p(\lambda)$

Functional Commitments

[Libert-Ramanna-Yung16]

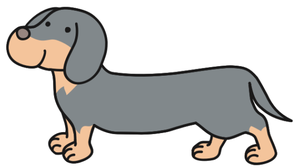
- Generalization of vector commitments and polynomial commitments



$\mathrm{Com}(\mathbf{x}) \rightarrow$ $C_{\mathbf{x}}$

$\mathrm{Open}(f, \mathbf{x}) \rightarrow$ π_f

$\mathbf{y} = f(\mathbf{x})$

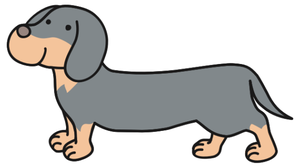


$\mathrm{Ver}(C_{\mathbf{x}}, f, \mathbf{y}, \pi_f) \stackrel{?}{=} 1$

- **Succinctness:** commitments and *openings "short" w.r.t.* $|\mathbf{x}|$: $|C_{\mathbf{x}}| \leq p(\lambda)$ and $|\pi_f| \leq m \cdot p(\lambda)$
- **Compactness** [LM19]: *openings "short" w.r.t.* $|\mathbf{x}|$ *and* $|\mathbf{y}|$ $|C_{\mathbf{x}}|, |\pi_f| \leq p(\lambda)$

Evaluation binding

$C_{\mathbf{x}}$ $\quad f, \quad \pi_f, \mathbf{y}, \quad \pi'_f, \mathbf{y}'$



$$\mathrm{Ver}(C_{\mathbf{x}}, f, \mathbf{y}, \pi_f) = 1$$

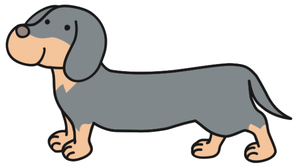
$$\mathrm{Ver}(C_{\mathbf{x}}, f, \mathbf{y}', \pi'_f) = 1$$

$$\mathbf{y} \neq \mathbf{y}'$$

Open to two different outputs for the same function

Evaluation binding

$C_{\mathbf{x}}$ $f,$ $\pi_f, \mathbf{y},$ $\pi'_f, \mathbf{y}'$



$\mathsf{Ver}(C_{\mathbf{x}}, f, \mathbf{y}, \pi_f) = 1$

$\mathsf{Ver}(C_{\mathbf{x}}, f, \mathbf{y}', \pi'_f) = 1$

$\mathbf{y} \neq \mathbf{y}'$

Open to two different outputs for the same function

- **FCs** can be seen as **weaker version of (commit-and-prove) SNARGs** (Eval. binding vs. Soundness)

  Potentially, a replacement for SNARGs in some applications

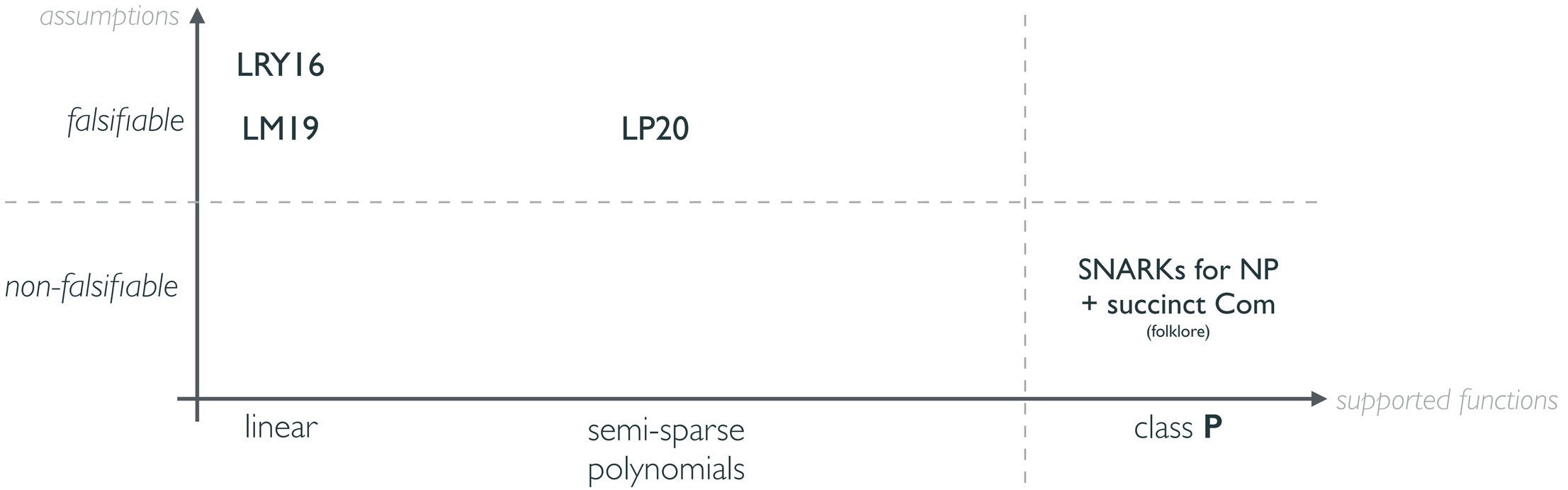
- **Other properties: hiding, zero-knowledge openings** (see paper, not focus in this talk)

State of the art (prior to our work)

State of the art (prior to our work)

State of the art (prior to our work)

State of the art (prior to our work)



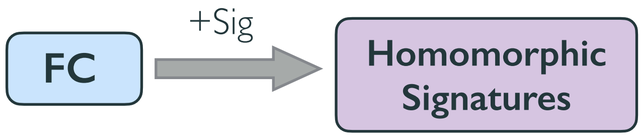
This work

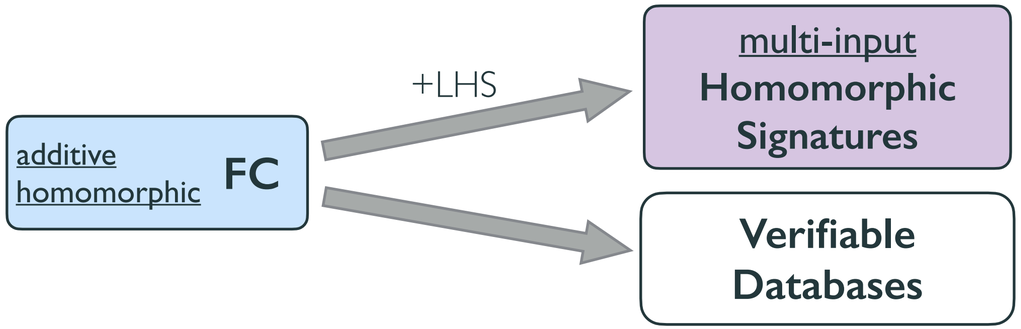
- *In which applications evaluation-binding is sufficient?*

This work

- *In which applications evaluation-binding is sufficient?*

➡ **Motivating Result:**

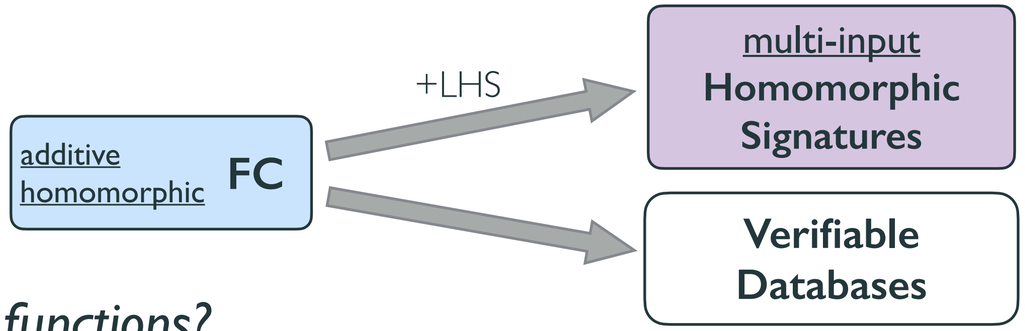




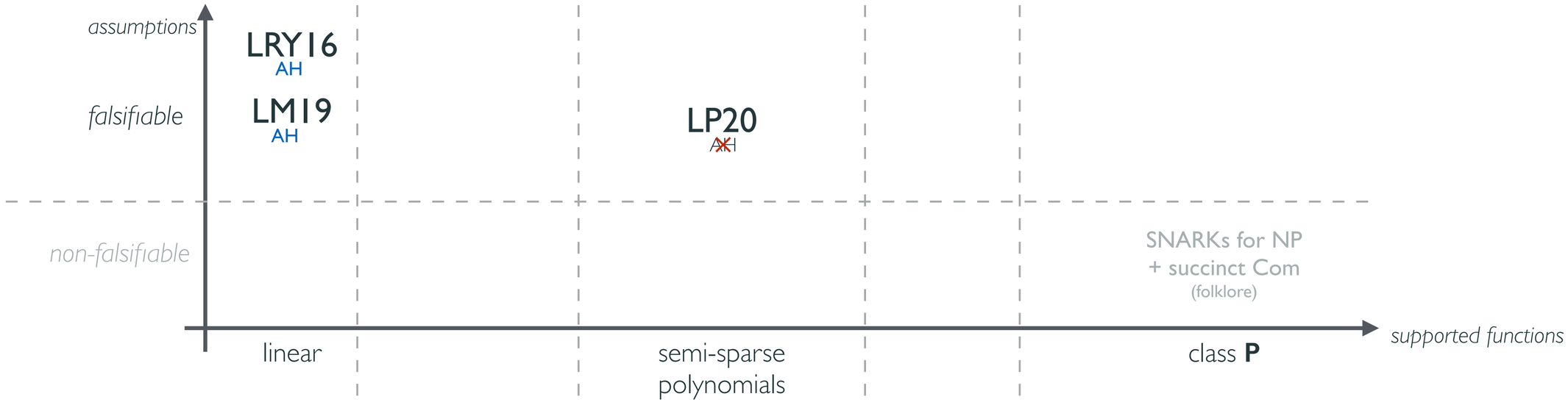
This work

- *In which applications evaluation-binding is sufficient?*

➡ **Motivating Result:** **FC** —+Sig→ **Homomorphic Signatures**



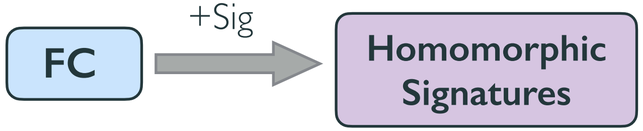
- *Can we construct additive-homomorphic FCs for expressive functions?*

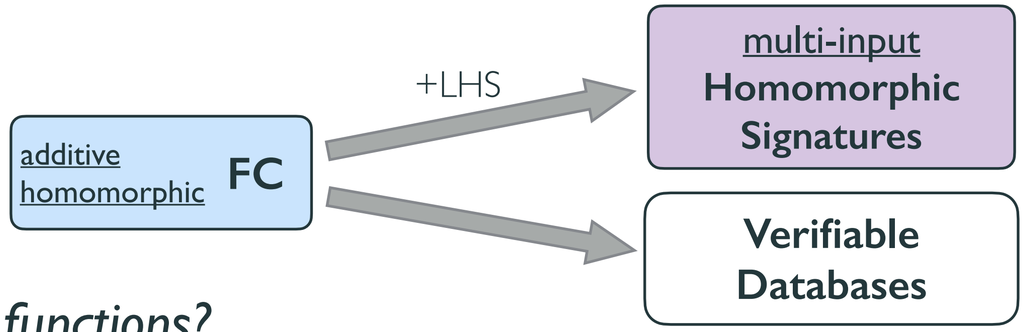


This work

- *In which applications evaluation-binding is sufficient?*

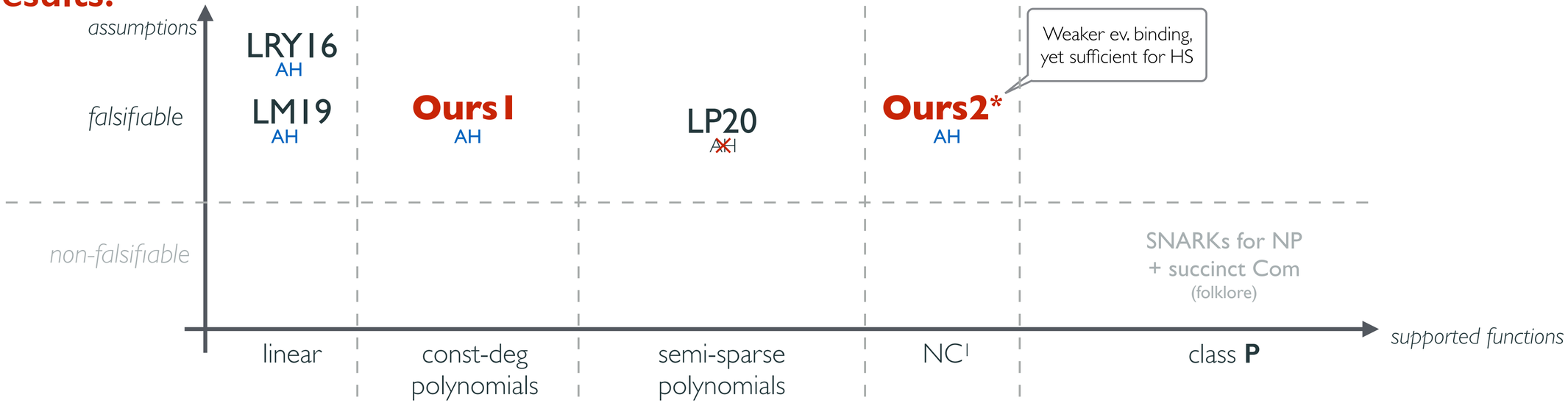
➡ **Motivating Result:**





- *Can we construct additive-homomorphic FCs for expressive functions?*

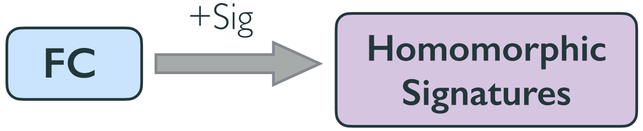
➡ **Main results:**

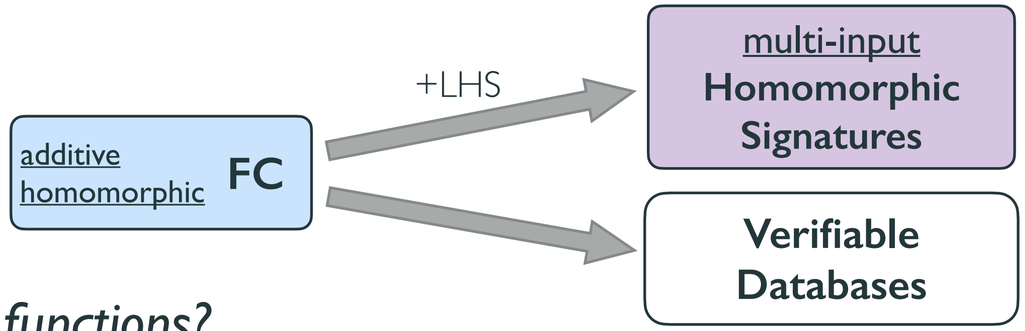


This work

- *In which applications evaluation-binding is sufficient?*

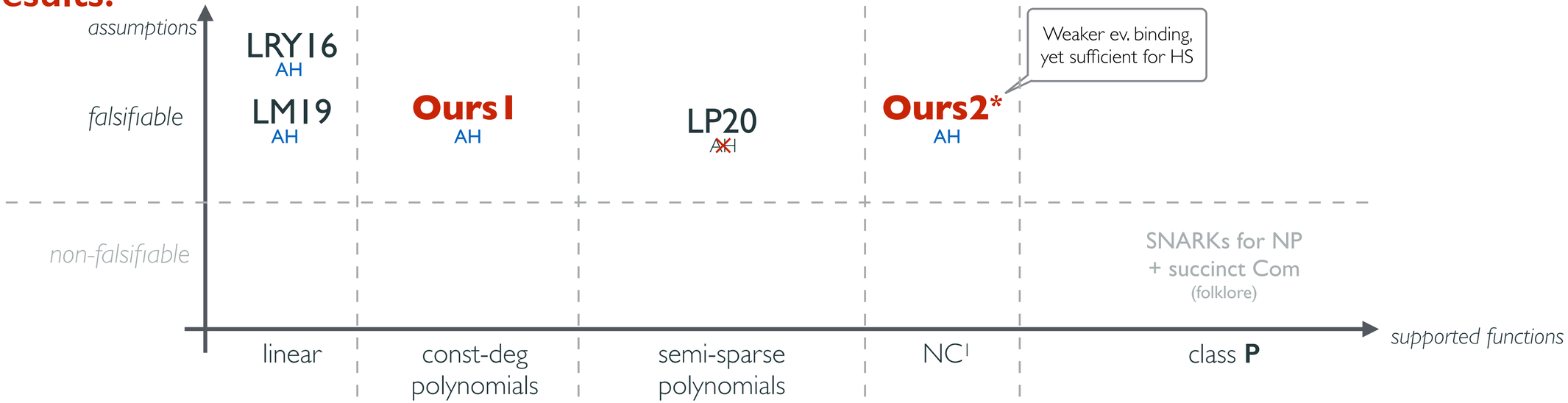
➡ **Motivating Result:**





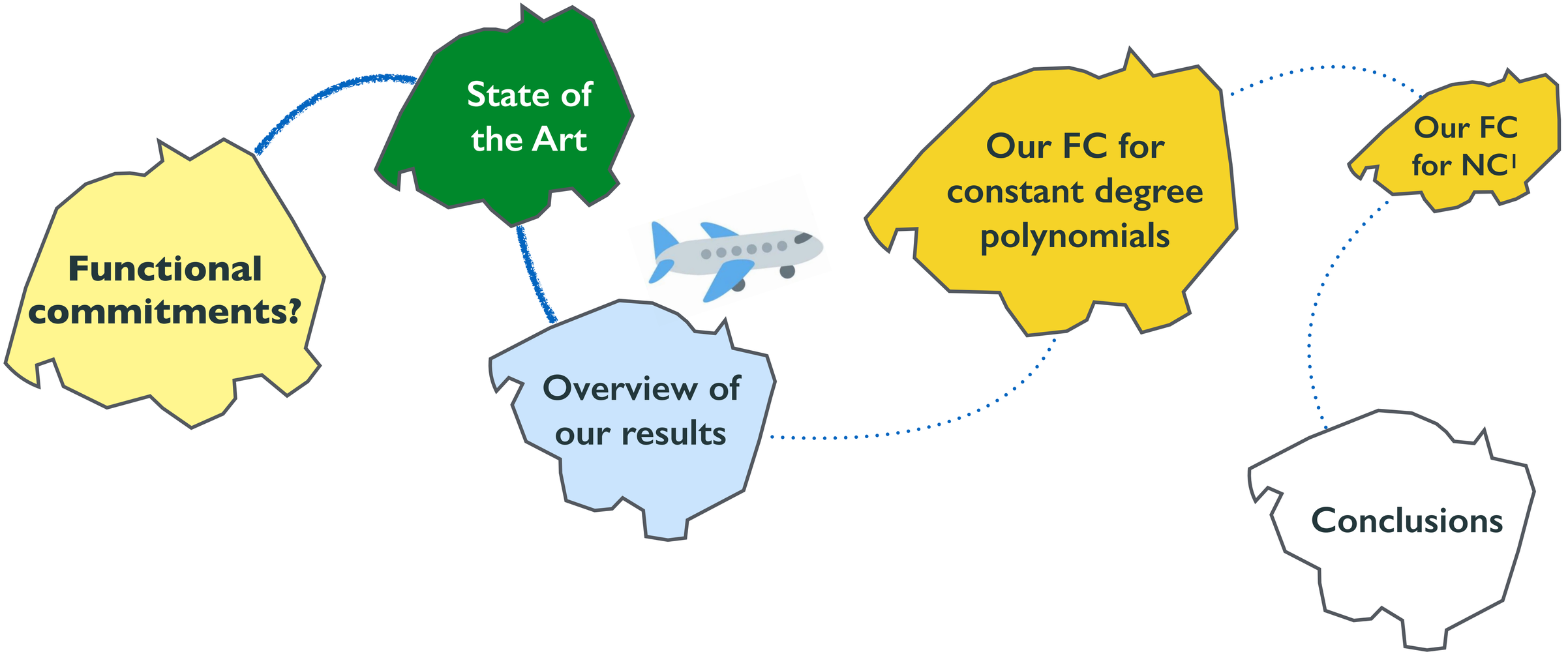
- *Can we construct additive-homomorphic FCs for expressive functions?*

➡ **Main results:**



➡ **Implications:** new pairing-based homomorphic signatures

Roadmap of the talk



Warmup: FC for O(1)-deg polynomials via linearization

- Homogeneous polynomials of degree d

Warmup: FC for O(1)-deg polynomials via linearization

- Homogeneous polynomials of degree d

$$f : \mathbb{F}^n \to \mathbb{F} \qquad f(\mathbf{x}) = \sum_{\ell} f_\ell \cdot x_1^{d_{\ell,1}} \cdots x_n^{d_{\ell,n}} \quad \text{s.t.} \quad \sum_j d_{\ell,j} = d$$

Warmup: FC for O(1)-deg polynomials via linearization

- Homogeneous polynomials of degree d

$$f : \mathbb{F}^n \to \mathbb{F} \qquad f(\mathbf{x}) = \sum_{\ell} f_\ell \cdot x_1^{d_{\ell,1}} \cdots x_n^{d_{\ell,n}} \quad \text{s.t.} \quad \sum_j d_{\ell,j} = d$$

$$\exists \hat{\mathbf{f}} \in \mathbb{F}^{n^d} : f(\mathbf{x}) = \langle \hat{\mathbf{f}}, \mathbf{x}^{(\delta)} \rangle \quad \text{where, for } \delta = \log d, \quad \mathbf{x}^{(\delta)} = \begin{cases} \mathbf{x} & \delta = 0 \\ \mathbf{x}^{(\delta-1)} \otimes \mathbf{x}^{(\delta-1)} & \delta \geq 1 \end{cases}$$

Warmup: FC for O(1)-deg polynomials via linearization

- Homogeneous polynomials of degree d

$$f : \mathbb{F}^n \to \mathbb{F} \qquad f(\mathbf{x}) = \sum_{\ell} f_\ell \cdot x_1^{d_{\ell,1}} \cdots x_n^{d_{\ell,n}} \quad \text{s.t.} \quad \sum_j d_{\ell,j} = d$$

$$\exists \hat{\mathbf{f}} \in \mathbb{F}^{n^d} : f(\mathbf{x}) = \langle \hat{\mathbf{f}}, \mathbf{x}^{(\delta)} \rangle \quad \text{where, for } \delta = \log d, \quad \mathbf{x}^{(\delta)} = \begin{cases} \mathbf{x} & \delta = 0 \\ \mathbf{x}^{(\delta-1)} \otimes \mathbf{x}^{(\delta-1)} & \delta \geq 1 \end{cases}$$

- $\overline{\text{FC}}$ for linear forms $\Rightarrow$ FC for deg-d polynomials, d=O(1)

$$\text{Com}(\mathbf{x}) = \overline{\text{Com}}(\mathbf{x}^{(\delta)}) \qquad \pi_f = \pi_{\hat{\mathbf{f}}} = \overline{\text{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(\delta)})$$

Warmup: FC for O(1)-deg polynomials via linearization

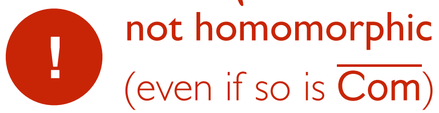
- Homogeneous polynomials of degree d

$$f : \mathbb{F}^n \to \mathbb{F} \qquad f(\mathbf{x}) = \sum_{\ell} f_\ell \cdot x_1^{d_{\ell,1}} \cdots x_n^{d_{\ell,n}} \quad \text{s.t.} \quad \sum_j d_{\ell,j} = d$$

$$\exists \hat{\mathbf{f}} \in \mathbb{F}^{n^d} : f(\mathbf{x}) = \langle \hat{\mathbf{f}}, \mathbf{x}^{(\delta)} \rangle \quad \text{where, for } \delta = \log d, \quad \mathbf{x}^{(\delta)} = \begin{cases} \mathbf{x} & \delta = 0 \\ \mathbf{x}^{(\delta-1)} \otimes \mathbf{x}^{(\delta-1)} & \delta \geq 1 \end{cases}$$

- $\overline{\text{FC}}$ for linear forms ⇒ FC for deg-d polynomials, d=O(1)

$$\text{Com}(\mathbf{x}) = \overline{\text{Com}}(\mathbf{x}^{(\delta)}) \qquad \pi_f = \pi_{\hat{\mathbf{f}}} = \overline{\text{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(\delta)})$$



Warmup: FC for O(1)-deg polynomials via linearization

- Homogeneous polynomials of degree d

$$f : \mathbb{F}^n \to \mathbb{F} \qquad f(\mathbf{x}) = \sum_{\ell} f_\ell \cdot x_1^{d_{\ell,1}} \cdots x_n^{d_{\ell,n}} \quad \text{s.t.} \quad \sum_j d_{\ell,j} = d$$

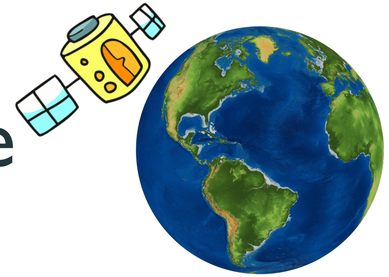
$$\exists \hat{\mathbf{f}} \in \mathbb{F}^{n^d} : f(\mathbf{x}) = \langle \hat{\mathbf{f}}, \mathbf{x}^{(\delta)} \rangle \quad \text{where, for } \delta = \log d, \quad \mathbf{x}^{(\delta)} = \begin{cases} \mathbf{x} & \delta = 0 \\ \mathbf{x}^{(\delta-1)} \otimes \mathbf{x}^{(\delta-1)} & \delta \geq 1 \end{cases}$$

- $\overline{\text{FC}}$ for linear forms ⇒ FC for deg-d polynomials, d=O(1)

$$\text{Com}(\mathbf{x}) = \overline{\text{Com}}(\mathbf{x}^{(\delta)}) \qquad \pi_f = \pi_{\hat{\mathbf{f}}} = \overline{\text{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(\delta)})$$

! not homomorphic (even if so is $\overline{\text{Com}}$) e.g., $\overline{\text{Com}}(\cdots, x_i \cdot x_j, x_i \cdot x_{j+1}, \cdots)$

Our FC for polynomials …seen from the space



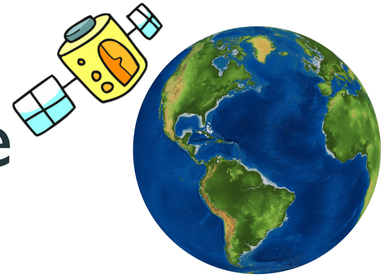
- **Our approach**

  Additive-homomorphic $\overline{\mathsf{FC}} = (\overline{\mathsf{Com}}, \overline{\mathsf{Open}}, \overline{\mathsf{Ver}})$ for linear maps over $\mathbb{F}^{n^d}$

$$\mathsf{Com}(\mathbf{x}) = \overline{\mathsf{Com}}(\mathbf{x})$$

✔ $\overline{\mathsf{Com}}$ hom. ⇒ Com hom.

Our FC for polynomials …seen from the space



- **Our approach**

Additive-homomorphic $\overline{\mathsf{FC}} = (\overline{\mathsf{Com}}, \overline{\mathsf{Open}}, \overline{\mathsf{Ver}})$ for linear maps over $\mathbb{F}^{n^d}$

$\mathsf{Com}(\mathbf{x}) = \overline{\mathsf{Com}}(\mathbf{x})$

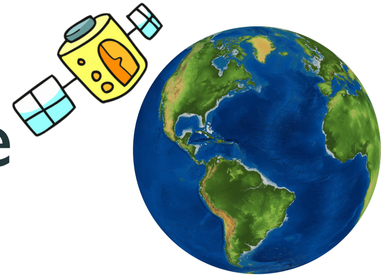
✔ $\overline{\mathsf{Com}}$ hom. ⇒ Com hom.

$\pi_f = \mathsf{Open}(f, \mathbf{x})$

$X_\delta = \overline{\mathsf{Com}}(\mathbf{x}^{(\delta)})$

$\pi_{\hat{\mathbf{f}}} = \overline{\mathsf{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(\delta)})$ w.r.t. X_δ

Our FC for polynomials …seen from the space



- **Our approach**

  Additive-homomorphic $\overline{\mathsf{FC}} = (\overline{\mathsf{Com}}, \overline{\mathsf{Open}}, \overline{\mathsf{Ver}})$ for linear maps over $\mathbb{F}^{n^d}$

$\mathsf{Com}(\mathbf{x}) = \overline{\mathsf{Com}}(\mathbf{x})$

✔ $\overline{\mathsf{Com}}$ hom. ⇒ Com hom.

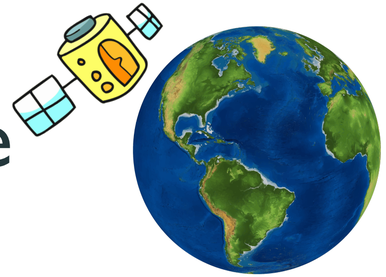
$\pi_f = \mathsf{Open}(f, \mathbf{x})$

$X_\delta = \overline{\mathsf{Com}}(\mathbf{x}^{(\delta)})$

$\pi_{\hat{\mathbf{f}}} = \overline{\mathsf{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(\delta)})$ w.r.t. X_δ

π_δ = proof that $X_\delta = \overline{\mathsf{Com}}(\mathbf{x} \otimes \cdots \otimes \mathbf{x})$ w.r.t. $\mathbf{x}$ in $\mathsf{C}_{\mathbf{x}}$

Our FC for polynomials …seen from the space



- **Our approach**

  Additive-homomorphic $\overline{\mathsf{FC}} = (\overline{\mathsf{Com}}, \overline{\mathsf{Open}}, \overline{\mathsf{Ver}})$ for linear maps over $\mathbb{F}^{n^d}$

$\mathsf{Com}(\mathbf{x}) = \overline{\mathsf{Com}}(\mathbf{x})$

✔ $\overline{\mathsf{Com}}$ hom. ⇒ Com hom.

$\pi_f = \mathsf{Open}(f, \mathbf{x})$

$X_\delta = \overline{\mathsf{Com}}(\mathbf{x}^{(\delta)})$

$\pi_{\hat{\mathbf{f}}} = \overline{\mathsf{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(\delta)})$ w.r.t. X_δ

π_δ = proof that $X_\delta = \overline{\mathsf{Com}}(\mathbf{x} \otimes \cdots \otimes \mathbf{x})$ w.r.t. $\mathbf{x}$ in $\mathsf{C}_{\mathbf{x}}$

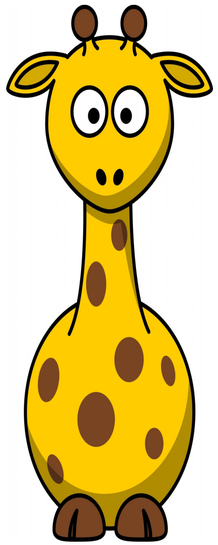
- **Our construction:** *we "open the box" of the FC for linear maps of* [Lai-Malavolta19]

Our FC for polynomials

…from 10Km

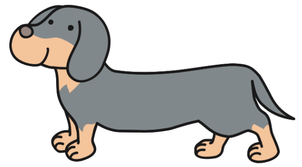
Let's start with f of degree 2

- Bilinear pairings $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, Notation: $[\alpha]_i = g_1^{\alpha} \in \mathbb{G}_i$



$\mathsf{Setup}(1^{\lambda}) \to \mathsf{ck} = [\alpha^1, \ldots, \alpha^{n^d}]_{1,2}$ …*and more elements*

Verification:

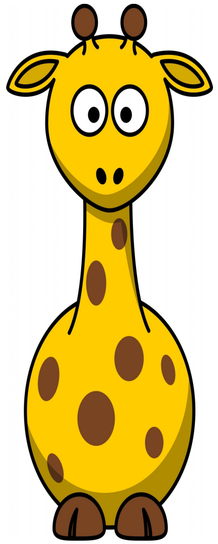


Our FC for polynomials …from 10Km

Let's start with f of degree 2

- Bilinear pairings $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, Notation: $[\alpha]_i = g_1^{\alpha} \in \mathbb{G}_i$

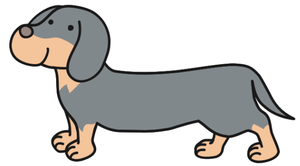
Setup$(1^{\lambda}) \to$ ck = $[\alpha^1, \ldots, \alpha^{n^d}]_{1,2}$ *…and more elements*



$\text{Com}(\mathbf{x}) \to \text{C}_{\mathbf{x}} =$

$$X_0 = [\sum_{j=1}^{n} x_j \cdot \alpha^j] = [p_{\mathbf{x}}^{(0)}(\alpha)]_1$$

Verification:

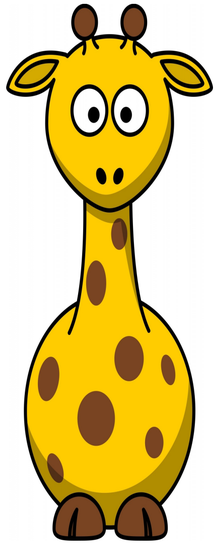


Our FC for polynomials

…from 10Km

Let's start with f of degree 2

- Bilinear pairings $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, Notation: $[\alpha]_i = g_1^{\alpha} \in \mathbb{G}_i$



$\mathsf{Setup}(1^{\lambda}) \to \mathsf{ck} = [\alpha^1, \ldots, \alpha^{n^d}]_{1,2}$ …*and more elements*

$\mathsf{Com}(\mathbf{x}) \to \mathsf{C}_{\mathbf{x}} =$

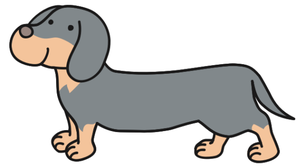
$$X_0 = [\sum_{j=1}^{n} x_j \cdot \alpha^j] = [p_{\mathbf{x}}^{(0)}(\alpha)]_1$$

$\mathsf{Open}(f, \mathbf{x}) \to \pi_f =$

$$X_1 = \overline{\mathsf{Com}}(\mathbf{x} \otimes \mathbf{x}) = [\sum_{k=1}^{n^2} x_k^{(1)} \cdot \alpha^k]_1 = [p_{\mathbf{x}}^{(1)}(\alpha)]_1$$

$$\pi_{\hat{\mathbf{f}}} = \overline{\mathsf{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(1)}) \text{ w.r.t. } X_1$$

Verification:



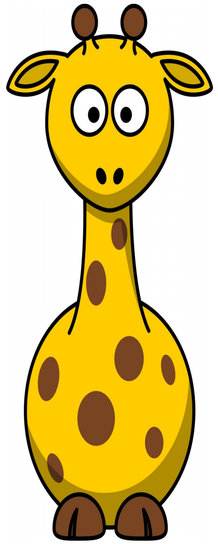
- $\underbrace{\overline{\mathsf{Ver}}(X_1, \hat{\mathbf{f}}, \mathbf{y}, \pi_{\hat{\mathbf{f}}}) \stackrel{?}{=} 1}_{\Rightarrow \quad \mathbf{y}=\langle \hat{\mathbf{f}}, \mathbf{x}^{(1)} \rangle}$

Our FC for polynomials

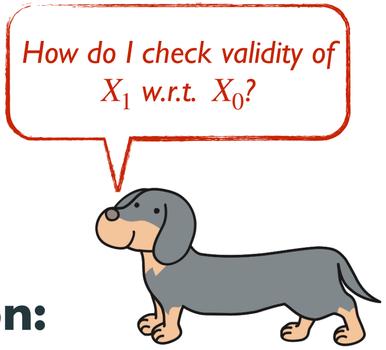
…from 10Km

Let's start with f of degree 2

- Bilinear pairings $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, Notation: $[\alpha]_i = g_1^{\alpha} \in \mathbb{G}_i$



$\mathsf{Setup}(1^{\lambda}) \to \mathsf{ck} = [\alpha^1, \ldots, \alpha^{n^d}]_{1,2}$ …*and more elements*



$\mathsf{Com}(\mathbf{x}) \to \mathsf{C}_{\mathbf{x}} =$

$$X_0 = [\sum_{j=1}^{n} x_j \cdot \alpha^j] = [p_{\mathbf{x}}^{(0)}(\alpha)]_1$$

$\mathsf{Open}(f, \mathbf{x}) \to \pi_f =$

$$X_1 = \overline{\mathsf{Com}}(\mathbf{x} \otimes \mathbf{x}) = [\sum_{k=1}^{n^2} x_k^{(1)} \cdot \alpha^k]_1 = [p_{\mathbf{x}}^{(1)}(\alpha)]_1$$

$$\pi_{\hat{\mathbf{f}}} = \overline{\mathsf{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(1)}) \text{ w.r.t. } X_1$$

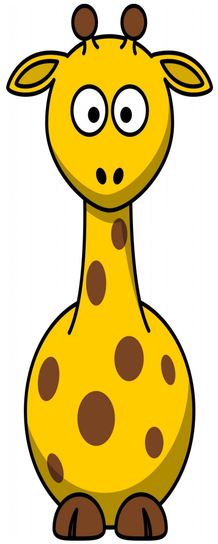
Verification:

- $\underbrace{\overline{\mathsf{Ver}}(X_1, \hat{\mathbf{f}}, \mathbf{y}, \pi_{\hat{\mathbf{f}}}) \stackrel{?}{=} 1}_{\Rightarrow \quad \mathbf{y}=\langle \hat{\mathbf{f}}, \mathbf{x}^{(1)} \rangle}$

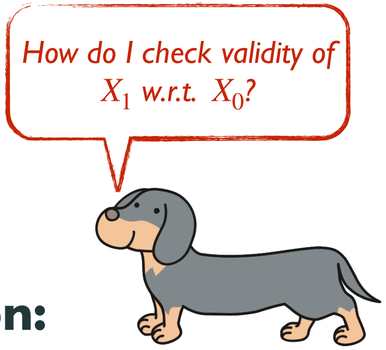
Our FC for polynomials …from 10Km

Let's start with f of degree 2

- Bilinear pairings $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, Notation: $[\alpha]_i = g_1^{\alpha} \in \mathbb{G}_i$



$\mathsf{Setup}(1^\lambda) \to \mathsf{ck} = [\alpha^1, \ldots, \alpha^{n^d}]_{1,2}$ …*and more elements*



$\mathsf{Com}(\mathbf{x}) \to \mathsf{C}_\mathbf{x} =$

$$X_0 = [\sum_{j=1}^{n} x_j \cdot \alpha^j] = [p_\mathbf{x}^{(0)}(\alpha)]_1$$

$\mathsf{Open}(f, \mathbf{x}) \to \pi_f =$

$$X_1 = \overline{\mathsf{Com}}(\mathbf{x} \otimes \mathbf{x}) = [\sum_{k=1}^{n^2} x_k^{(1)} \cdot \alpha^k]_1 = [p_\mathbf{x}^{(1)}(\alpha)]_1$$

$$\pi_{\hat{\mathbf{f}}} = \overline{\mathsf{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(1)}) \text{ w.r.t. } X_1$$

Verification:

- $\underbrace{\overline{\mathsf{Ver}}(X_1, \hat{\mathbf{f}}, \mathbf{y}, \pi_{\hat{\mathbf{f}}}) \stackrel{?}{=} 1}_{\Rightarrow \quad \mathbf{y}=\langle \hat{\mathbf{f}}, \mathbf{x}^{(1)} \rangle}$

$p_\mathbf{x}^{(1)}(\alpha)$ factors in two polynomials *linear in* $\mathbf{x}$.

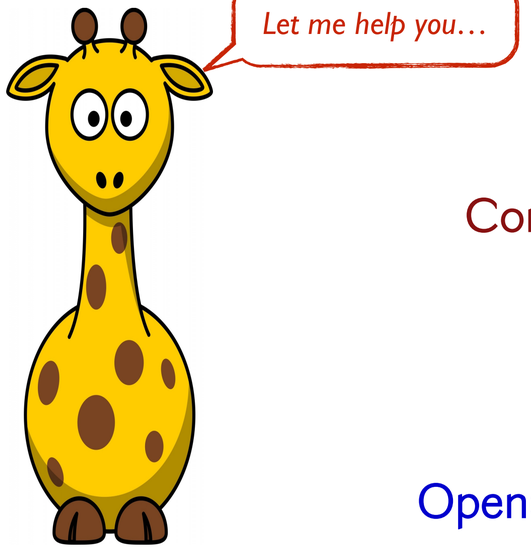
$\Rightarrow \mathsf{C}_\mathbf{x}$ *additive homomorphic*

$$p_\mathbf{x}^{(1)}(\alpha) = \sum_{k=1}^{n^2} x_k^{(1)} \cdot \alpha^k = \sum_{i,j=1}^{n} x_i^{(0)} x_j^{(0)} \cdot \alpha^{i+n(j-1)} = (\sum_{i=1}^{n} x_i^{(0)} \cdot \alpha^i)(\sum_{j=1}^{n} x_j^{(0)} \cdot \alpha^{n(j-1)}) = p_\mathbf{x}^{(0)}(\alpha) \cdot (p_\mathbf{x}^{(0)}(\alpha^n)/\alpha^n)$$

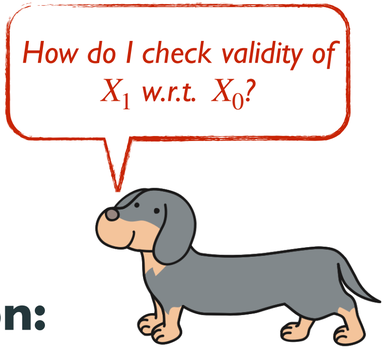
Our FC for polynomials …from 10Km

Let's start with f of degree 2

- Bilinear pairings $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, Notation: $[\alpha]_i = g_1^{\alpha} \in \mathbb{G}_i$



$\mathsf{Setup}(1^\lambda) \to \mathsf{ck} = [\alpha^1, \ldots, \alpha^{n^d}]_{1,2}$ …*and more elements*



$\mathsf{Com}(\mathbf{x}) \to \mathsf{C}_\mathbf{x} =$

$$X_0 = [\sum_{j=1}^{n} x_j \cdot \alpha^j] = [p_\mathbf{x}^{(0)}(\alpha)]_1$$

$$\hat{X}_0 = [\sum_{j=1}^{n} x_j \cdot \alpha^{n(j-1)}]_2 = [p_\mathbf{x}^{(0)}(\alpha^n)/\alpha^n]_2 = [\hat{p}_\mathbf{x}^{(0)}(\alpha)]_2$$

$\mathsf{Open}(f, \mathbf{x}) \to \pi_f =$

$$X_1 = \overline{\mathsf{Com}}(\mathbf{x} \otimes \mathbf{x}) = [\sum_{k=1}^{n^2} x_k^{(1)} \cdot \alpha^k]_1 = [p_\mathbf{x}^{(1)}(\alpha)]_1$$

$$\pi_{\hat{\mathbf{f}}} = \overline{\mathsf{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(1)}) \text{ w.r.t. } X_1$$

Verification:

- $\underbrace{\overline{\mathsf{Ver}}(X_1, \hat{\mathbf{f}}, \mathbf{y}, \pi_{\hat{\mathbf{f}}}) \stackrel{?}{=} 1}_{\Rightarrow \quad \mathbf{y}=\langle \hat{\mathbf{f}}, \mathbf{x}^{(1)} \rangle}$

$p_\mathbf{x}^{(1)}(\alpha)$ factors in two polynomials *linear in* $\mathbf{x}$.

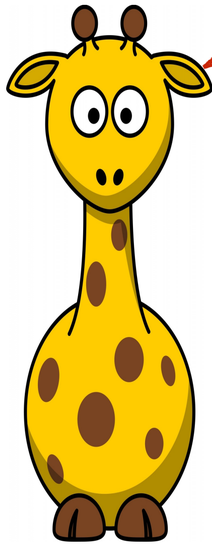
$\Rightarrow \mathsf{C}_\mathbf{x}$ *additive homomorphic*

$$p_\mathbf{x}^{(1)}(\alpha) = \sum_{k=1}^{n^2} x_k^{(1)} \cdot \alpha^k = \sum_{i,j=1}^{n} x_i^{(0)} x_j^{(0)} \cdot \alpha^{i+n(j-1)} = (\sum_{i=1}^{n} x_i^{(0)} \cdot \alpha^i)(\sum_{j=1}^{n} x_j^{(0)} \cdot \alpha^{n(j-1)}) = p_\mathbf{x}^{(0)}(\alpha) \cdot (p_\mathbf{x}^{(0)}(\alpha^n)/\alpha^n)$$

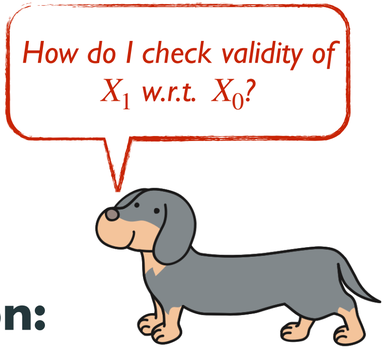
Our FC for polynomials …from 10Km

Let's start with f of degree 2

- Bilinear pairings $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, Notation: $[\alpha]_i = g_1^{\alpha} \in \mathbb{G}_i$



$\mathsf{Setup}(1^\lambda) \to \mathsf{ck} = [\alpha^1, \ldots, \alpha^{n^d}]_{1,2}$ …*and more elements*



$\mathsf{Com}(\mathbf{x}) \to \mathsf{C}_\mathbf{x} =$

$$X_0 = [\sum_{j=1}^{n} x_j \cdot \alpha^j] = [p_\mathbf{x}^{(0)}(\alpha)]_1$$

$$\hat{X}_0 = [\sum_{j=1}^{n} x_j \cdot \alpha^{n(j-1)}]_2 = [p_\mathbf{x}^{(0)}(\alpha^n)/\alpha^n]_2 = [\hat{p}_\mathbf{x}^{(0)}(\alpha)]_2$$

$\mathsf{Open}(f, \mathbf{x}) \to \pi_f =$

$$X_1 = \overline{\mathsf{Com}}(\mathbf{x} \otimes \mathbf{x}) = [\sum_{k=1}^{n^2} x_k^{(1)} \cdot \alpha^k]_1 = [p_\mathbf{x}^{(1)}(\alpha)]_1$$

$$\pi_{\hat{\mathbf{f}}} = \overline{\mathsf{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(1)}) \text{ w.r.t. } X_1$$

Verification:

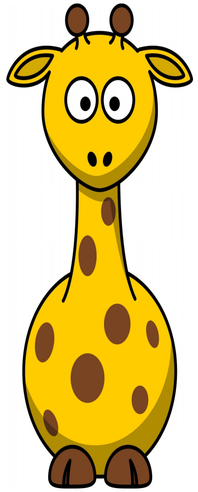
- $\underbrace{\overline{\mathsf{Ver}}(X_1, \hat{\mathbf{f}}, \mathbf{y}, \pi_{\hat{\mathbf{f}}}) \stackrel{?}{=} 1}_{\Rightarrow \quad \mathbf{y}=\langle \hat{\mathbf{f}}, \mathbf{x}^{(1)} \rangle}$
- $\underbrace{e(X_0, \hat{X}_0) \stackrel{?}{=} e(X_1, [1]_2)}_{\Rightarrow \quad X_1 = \overline{\mathsf{Com}}(\mathbf{x}^{(1)} = \mathbf{x}^{(0)} \otimes \mathbf{x}^{(0)})}$

$p_\mathbf{x}^{(1)}(\alpha)$ factors in two polynomials *linear in* $\mathbf{x}$.

$\Rightarrow \mathsf{C}_\mathbf{x}$ *additive homomorphic*

$$p_\mathbf{x}^{(1)}(\alpha) = \sum_{k=1}^{n^2} x_k^{(1)} \cdot \alpha^k = \sum_{i,j=1}^{n} x_i^{(0)} x_j^{(0)} \cdot \alpha^{i+n(j-1)} = (\sum_{i=1}^{n} x_i^{(0)} \cdot \alpha^i)(\sum_{j=1}^{n} x_j^{(0)} \cdot \alpha^{n(j-1)}) = p_\mathbf{x}^{(0)}(\alpha) \cdot (p_\mathbf{x}^{(0)}(\alpha^n)/\alpha^n)$$

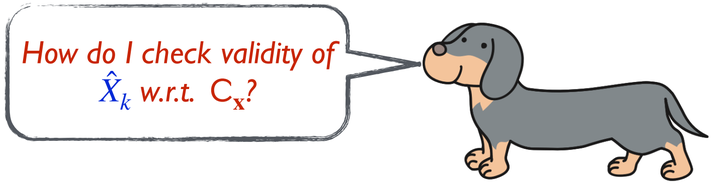
Our FC for polynomials ..almost down to earth



f of degree $d = 2^\delta$

$$\mathsf{Com}(\mathbf{x}) \to \mathsf{C}_\mathbf{x} = \quad X_0 = [\sum_{j=1}^{n} x_j \cdot \alpha^j] = [p_\mathbf{x}^{(0)}(\alpha)]_1 \qquad \hat{X}_0 = [\hat{p}_\mathbf{x}^{(0)}(\alpha)]_2 = [p_\mathbf{x}^{(0)}(\alpha^n)/\alpha^n]_2$$

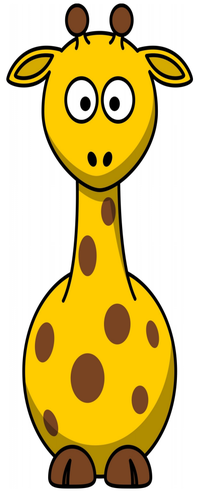
$$\mathsf{Open}(f, \mathbf{x}) \to \pi_f = \quad X_\delta = [p_\mathbf{x}^{(\delta)}(\alpha)]_1 \qquad \pi_{\hat{\mathbf{f}}} = \overline{\mathsf{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(\delta)}) \text{ w.r.t. } X_\delta$$
$$\{\ X_k = [p_\mathbf{x}^{(k)}(\alpha)]_1, \qquad \hat{X}_k = [\hat{p}_\mathbf{x}^{(k)}(\alpha)]_2\ \}_{k=1}^{\delta-1}$$



Verification:

- $\underbrace{\overline{\mathsf{Ver}}(X_\delta, \hat{\mathbf{f}}, \mathbf{y}, \pi_{\hat{\mathbf{f}}}) \stackrel{?}{=} 1}_{\Rightarrow \quad \mathbf{y}=\langle \hat{\mathbf{f}}, \mathbf{x}^{(\delta)} \rangle}$
- $\underbrace{e(X_0, \hat{X}_0) \stackrel{?}{=} e(X_1, [1]_2)}_{\Rightarrow \quad X_1=\overline{\mathsf{Com}}(\mathbf{x}^{(1)}=\mathbf{x}^{(0)} \otimes \mathbf{x}^{(0)})}$
- $\forall k \geq 1 : \underbrace{e(X_k, \hat{X}_k) \stackrel{?}{=} e(X_{k+1}, [1]_2)}_{\Rightarrow\ ? \quad X_{k+1}=\overline{\mathsf{Com}}(\mathbf{x}^{(k)} \otimes \mathbf{x}^{(k)})}$

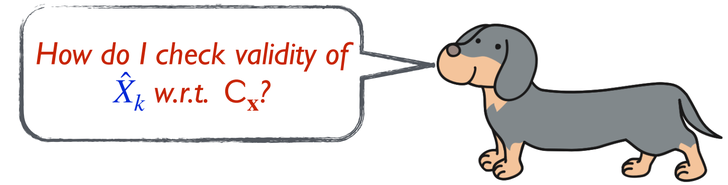
Our FC for polynomials ..almost down to earth



f of degree $d = 2^\delta$

$$\mathrm{Com}(\mathbf{x}) \to \mathsf{C}_\mathbf{x} = \quad X_0 = [\sum_{j=1}^{n} x_j \cdot \alpha^j] = [p_\mathbf{x}^{(0)}(\alpha)]_1 \qquad \hat{X}_0 = [\hat{p}_\mathbf{x}^{(0)}(\alpha)]_2 = [p_\mathbf{x}^{(0)}(\alpha^n)/\alpha^n]_2$$

$$\mathrm{Open}(f, \mathbf{x}) \to \pi_f = \quad X_\delta = [p_\mathbf{x}^{(\delta)}(\alpha)]_1 \qquad \pi_{\hat{\mathbf{f}}} = \overline{\mathsf{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(\delta)}) \text{ w.r.t. } X_\delta$$
$$\{\ X_k = [p_\mathbf{x}^{(k)}(\alpha)]_1, \quad \hat{X}_k = [\hat{p}_\mathbf{x}^{(k)}(\alpha)]_2\ \}_{k=1}^{\delta-1}$$



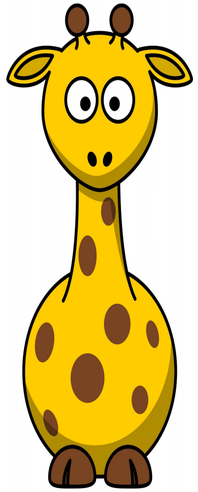
Verification:

- $\underbrace{\overline{\mathsf{Ver}}(X_\delta, \hat{\mathbf{f}}, \mathbf{y}, \pi_{\hat{\mathbf{f}}}) \stackrel{?}{=} 1}_{\Rightarrow \quad \mathbf{y}=\langle \hat{\mathbf{f}}, \mathbf{x}^{(\delta)} \rangle}$
- $\underbrace{e(X_0, \hat{X}_0) \stackrel{?}{=} e(X_1, [1]_2)}_{\Rightarrow \quad X_1 = \overline{\mathsf{Com}}(\mathbf{x}^{(1)} = \mathbf{x}^{(0)} \otimes \mathbf{x}^{(0)})}$
- $\forall k \geq 1 : \underbrace{e(X_k, \hat{X}_k) \stackrel{?}{=} e(X_{k+1}, [1]_2)}_{\Rightarrow\ ? \quad X_{k+1} = \overline{\mathsf{Com}}(\mathbf{x}^{(k)} \otimes \mathbf{x}^{(k)})}$

Generalization: $\hat{p}_\mathbf{x}^{(k)}(\alpha)$ *factors in* 2^k *polynomials linear in* $\mathbf{x}$**:**

$$\hat{p}_\mathbf{x}^{(k)}(\alpha) = \prod_{\ell=2^k}^{2^{k+1}-1} \phi_\mathbf{x}^{(\ell)}(\alpha)$$

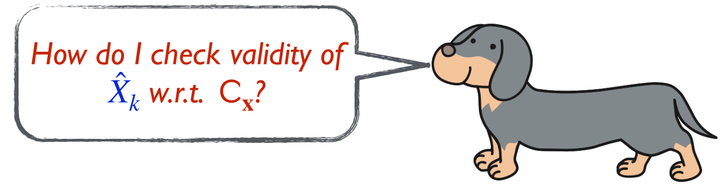
Our FC for polynomials ..almost down to earth



f of degree $d = 2^\delta$

$$\mathsf{Com}(\mathbf{x}) \to \mathsf{C}_\mathbf{x} = \begin{array}{l} X_0 = [\sum_{j=1}^{n} x_j \cdot \alpha^j] = [p_\mathbf{x}^{(0)}(\alpha)]_1 \quad \hat{X}_0 = [\hat{p}_\mathbf{x}^{(0)}(\alpha)]_2 = [p_\mathbf{x}^{(0)}(\alpha^n)/\alpha^n]_2 \\ \Phi_\ell = [\sum_{j=1}^{n} x_j \cdot \alpha^{n^\ell(j-1)})]_b = [\phi_\mathbf{x}^{(\ell)}(\alpha)]_b, l = 2,\ldots,d-1 \end{array}$$

$$\mathsf{Open}(f, \mathbf{x}) \to \pi_f = \begin{array}{l} X_\delta = [p_\mathbf{x}^{(\delta)}(\alpha)]_1 \quad \pi_{\hat{\mathbf{f}}} = \overline{\mathsf{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(\delta)}) \text{ w.r.t. } X_\delta \\ \{\ X_k = [p_\mathbf{x}^{(k)}(\alpha)]_1, \quad \hat{X}_k = [\hat{p}_\mathbf{x}^{(k)}(\alpha)]_2\ \}_{k=1}^{\delta-1} \end{array}$$



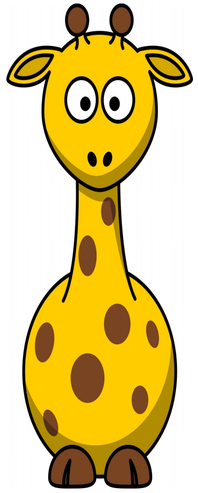
Verification:

- $\underbrace{\overline{\mathsf{Ver}}(X_\delta, \hat{\mathbf{f}}, \mathbf{y}, \pi_{\hat{\mathbf{f}}}) \stackrel{?}{=} 1}_{\Rightarrow \quad \mathbf{y}=\langle \hat{\mathbf{f}}, \mathbf{x}^{(\delta)} \rangle}$
- $\underbrace{e(X_0, \hat{X}_0) \stackrel{?}{=} e(X_1, [1]_2)}_{\Rightarrow \quad X_1=\overline{\mathsf{Com}}(\mathbf{x}^{(1)}=\mathbf{x}^{(0)} \otimes \mathbf{x}^{(0)})}$
- $\forall k \geq 1 : \underbrace{e(X_k, \hat{X}_k) \stackrel{?}{=} e(X_{k+1}, [1]_2)}_{\Rightarrow\ ? \quad X_{k+1}=\overline{\mathsf{Com}}(\mathbf{x}^{(k)} \otimes \mathbf{x}^{(k)})}$

Generalization: $\hat{p}_\mathbf{x}^{(k)}(\alpha)$ *factors in* 2^k *polynomials linear in* $\mathbf{x}$**:**

$$\hat{p}_\mathbf{x}^{(k)}(\alpha) = \prod_{\ell=2^k}^{2^{k+1}-1} \phi_\mathbf{x}^{(\ell)}(\alpha)$$

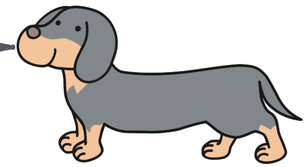
Our FC for polynomials ..almost down to earth



f of degree $d = 2^\delta$

$$\text{Com}(\mathbf{x}) \to C_{\mathbf{x}} = \left[X_0 = [\sum_{j=1}^{n} x_j \cdot \alpha^j] = [p_{\mathbf{x}}^{(0)}(\alpha)]_1 \quad \hat{X}_0 = [\hat{p}_{\mathbf{x}}^{(0)}(\alpha)]_2 = [p_{\mathbf{x}}^{(0)}(\alpha^n)/\alpha^n]_2 \right.$$
$$\left. \Phi_\ell = [\sum_{j=1}^{n} x_j \cdot \alpha^{n^\ell (j-1)})]_b = [\phi_{\mathbf{x}}^{(\ell)}(\alpha)]_b, l = 2, \ldots, d-1 \right]$$

How do I check validity of $\hat{X}_k$ *w.r.t.* $C_{\mathbf{x}}$*?*



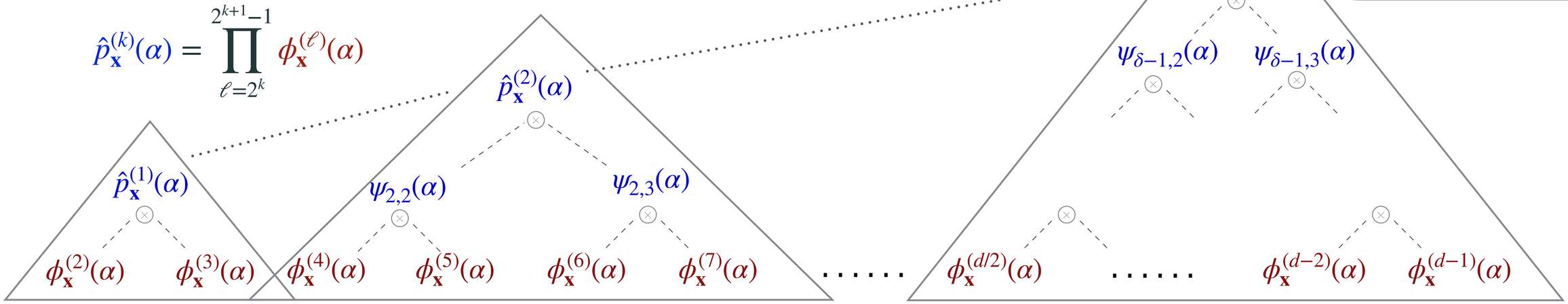
$$\text{Open}(f, \mathbf{x}) \to \pi_f = \left[X_\delta = [p_{\mathbf{x}}^{(\delta)}(\alpha)]_1 \quad \pi_{\hat{\mathbf{f}}} = \overline{\text{Open}}(\hat{\mathbf{f}}, \mathbf{x}^{(\delta)}) \text{ w.r.t. } X_\delta \right.$$
$$\left. \{ X_k = [p_{\mathbf{x}}^{(k)}(\alpha)]_1, \quad \hat{X}_k = [\hat{p}_{\mathbf{x}}^{(k)}(\alpha)]_2 \}_{k=1}^{\delta-1} \quad \{\Psi_{k,\mu} = [\psi_{k,\mu}(\alpha)]\}_{\mu=2^k}^{2^{k+1}-1} \right]$$

Main ideas

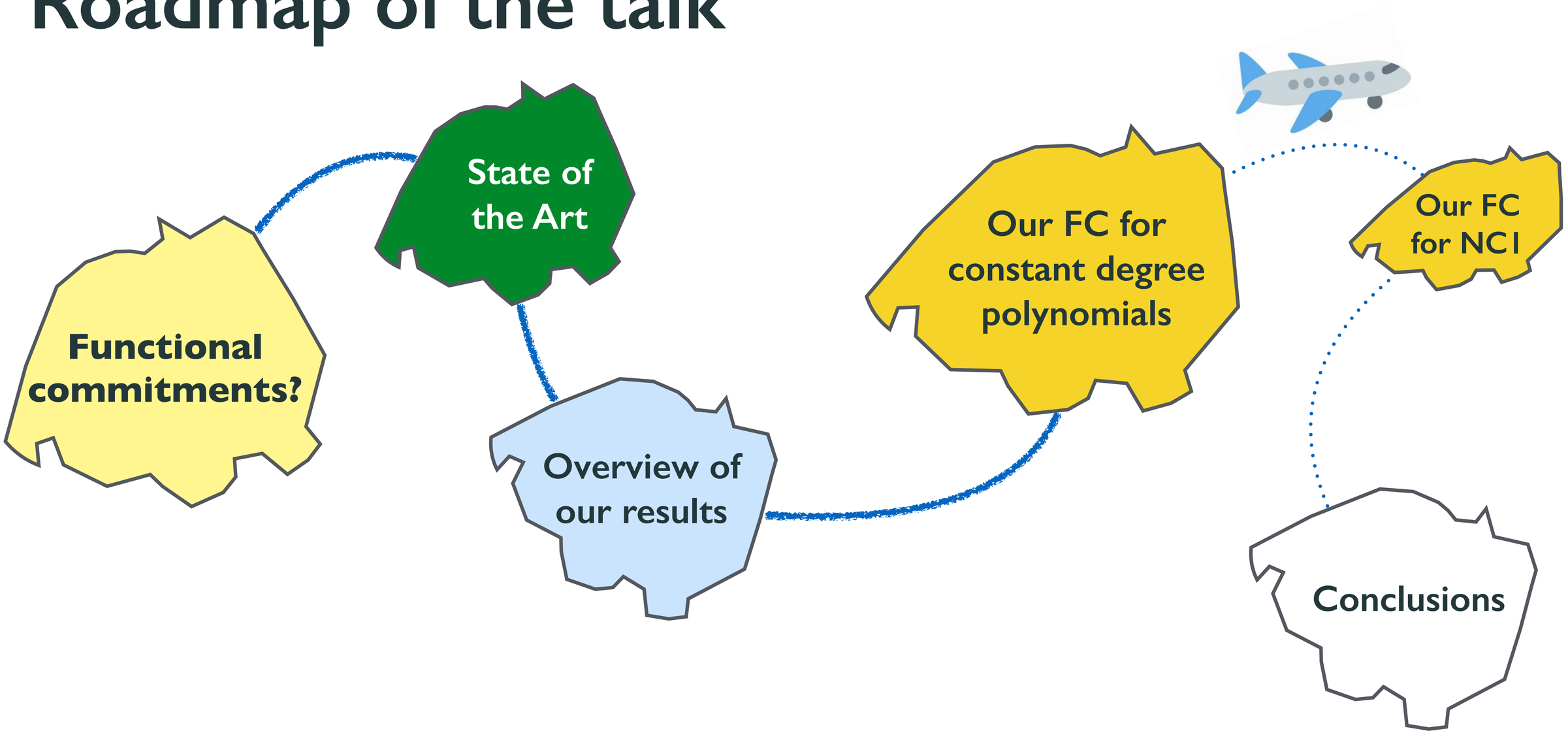
- *Prover gives all the internal nodes of the tree*
- *Verifier checks their consistency bottom-up via quadratic checks (using a pairing)*
  - *Cost* $O(2^\delta) = O(d) = O(1)$

Generalization: $\hat{p}_{\mathbf{x}}^{(k)}(\alpha)$ *factors in* 2^k *polynomials linear in* $\mathbf{x}$*:*

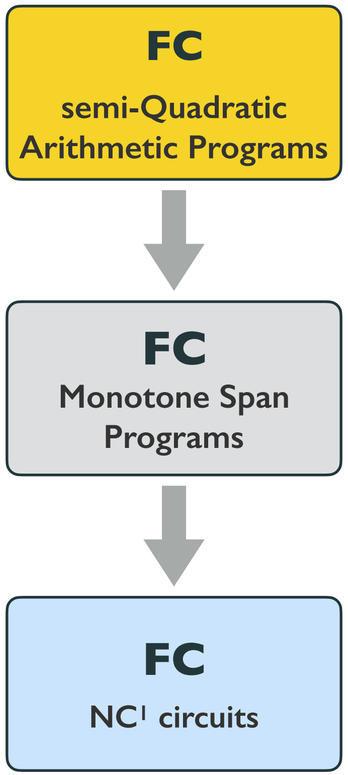
$$\hat{p}_{\mathbf{x}}^{(k)}(\alpha) = \prod_{\ell=2^k}^{2^{k+1}-1} \phi_{\mathbf{x}}^{(\ell)}(\alpha)$$



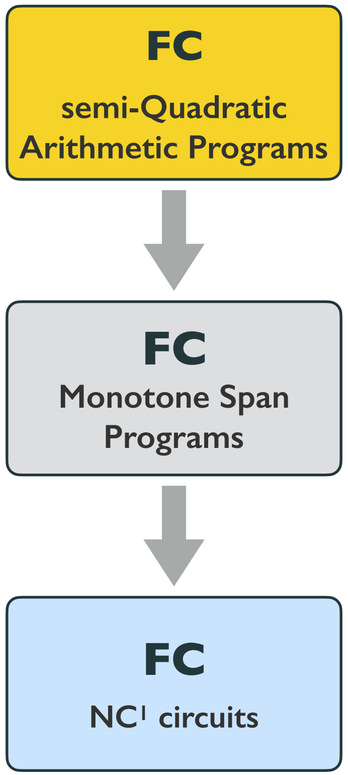
Roadmap of the talk



Our FC for NC^1



Our FC for NC^1

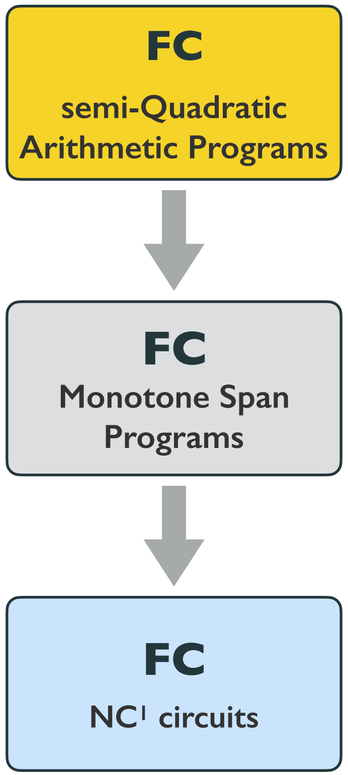


sQAP: semi-Quadratic Arithmetic Programs

$$f : \mathbb{F}^n \times \mathbb{F}^m \to \{\text{true}, \text{false}\} \text{ defined by matrix } \mathbf{F} \in \mathbb{F}^{n \times m}$$

$$f(\mathbf{z}, \mathbf{y}) = \text{true} \iff \exists \mathbf{w} : \mathbf{F} \cdot (\mathbf{w} \circ \mathbf{z}) = \mathbf{y}$$

Our FC for NC^1



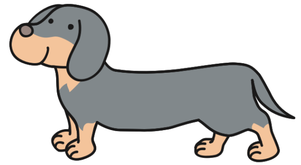
sQAP: semi-Quadratic Arithmetic Programs

$$f : \mathbb{F}^n \times \mathbb{F}^m \to \{\text{true}, \text{false}\} \text{ defined by matrix } \mathbf{F} \in \mathbb{F}^{n \times m}$$

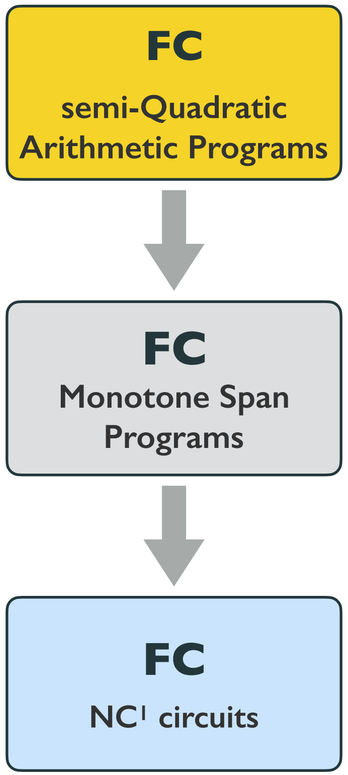
$$f(\mathbf{z}, \mathbf{y}) = \text{true} \iff \exists \mathbf{w} : \mathbf{F} \cdot (\mathbf{w} \circ \mathbf{z}) = \mathbf{y}$$

High-level ideas of our approach

(1) linearize the system of equations $\mathbf{F} \cdot (\mathbf{w} \circ \mathbf{z}) = \underbrace{\left(\mathbf{F} \circ \begin{bmatrix} \mathbf{z}^\top \\ \vdots \\ \mathbf{z}^\top \end{bmatrix} \right)}_{\mathbf{F}_\mathbf{z}} \cdot \mathbf{w} = \mathbf{y}$



Our FC for NC^1



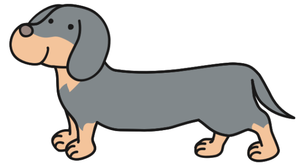
sQAP: semi-Quadratic Arithmetic Programs

$$f : \mathbb{F}^n \times \mathbb{F}^m \to \{\text{true}, \text{false}\} \text{ defined by matrix } \mathbf{F} \in \mathbb{F}^{n \times m}$$

$$f(\mathbf{z}, \mathbf{y}) = \text{true} \iff \exists \mathbf{w} : \mathbf{F} \cdot (\mathbf{w} \circ \mathbf{z}) = \mathbf{y}$$

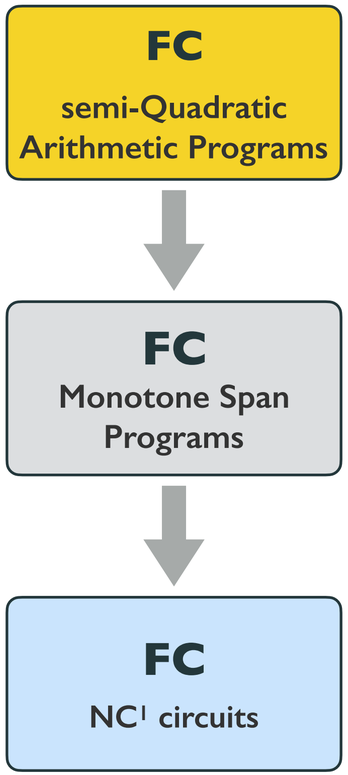
High-level ideas of our approach

(1) linearize the system of equations $\mathbf{F} \cdot (\mathbf{w} \circ \mathbf{z}) = \underbrace{\left(\mathbf{F} \circ \begin{bmatrix} \mathbf{z}^\top \\ \vdots \\ \mathbf{z}^\top \end{bmatrix} \right)}_{\mathbf{F}_\mathbf{z}} \cdot \mathbf{w} = \mathbf{y}$



(2) Adapt the linear-map FC of LM19 to prove satisfiability of $(\mathbf{F}_\mathbf{z} \,|\, \mathbf{y})$ for *committed* $\mathbf{z}$ and $\mathbf{y}$

Our FC for NC^1



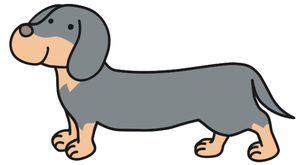
sQAP: semi-Quadratic Arithmetic Programs

$$f : \mathbb{F}^n \times \mathbb{F}^m \to \{\text{true}, \text{false}\} \text{ defined by matrix } \mathbf{F} \in \mathbb{F}^{n \times m}$$

$$f(\mathbf{z}, \mathbf{y}) = \text{true} \iff \exists \mathbf{w} : \mathbf{F} \cdot (\mathbf{w} \circ \mathbf{z}) = \mathbf{y}$$

High-level ideas of our approach

(1) linearize the system of equations $\mathbf{F} \cdot (\mathbf{w} \circ \mathbf{z}) = \underbrace{\left(\mathbf{F} \circ \begin{bmatrix} \mathbf{z}^\top \\ \vdots \\ \mathbf{z}^\top \end{bmatrix} \right)}_{\mathbf{F}_\mathbf{z}} \cdot \mathbf{w} = \mathbf{y}$



(2) Adapt the linear-map FC of LM19 to prove satisfiability of $(\mathbf{F}_\mathbf{z} \,|\, \mathbf{y})$ for *committed* $\mathbf{z}$ and $\mathbf{y}$

(*) Prove *strong evaluation binding* of LM19 from a falsifiable assumption (LM19 proved it in the GGM); this implies a falsifiable SNARG for linear systems (of independent interest).

Summary of our results

FC scheme	Functions $f : \mathbb{Z}_q^n \to \mathbb{Z}_q^m$	|pp|	|C|	|π|	Add Hom	Assumption
[LM19]	linear maps	$O(mn)$	$1\ \|\mathbb{G}\|$	$1\ \|\mathbb{G}\|$	yes	n-DHE
[LP20]	semi-sparse polynomials	$O(\mu)$	$O(m)$	$O(1)$	no	
Ours (FC_{poly})	polynomials of deg d=O(1)	$O(mn^d)$	$d/2\|\mathbb{G}_1\|+d/2\|\mathbb{G}_2\|$	$d/2\|\mathbb{G}_1\|+d/2\|\mathbb{G}_2\|$	yes	n^d-DHE
Ours (FC_{sQAP})	sQAP	$O(mn^2)$	$2\ \|\mathbb{G}_1\|$	$2\|\mathbb{G}_1\|+ 1\|\mathbb{G}_2\|$	yes	(n,m)-DP-BDHE

Weak ev. binding, yet sufficient to build HS

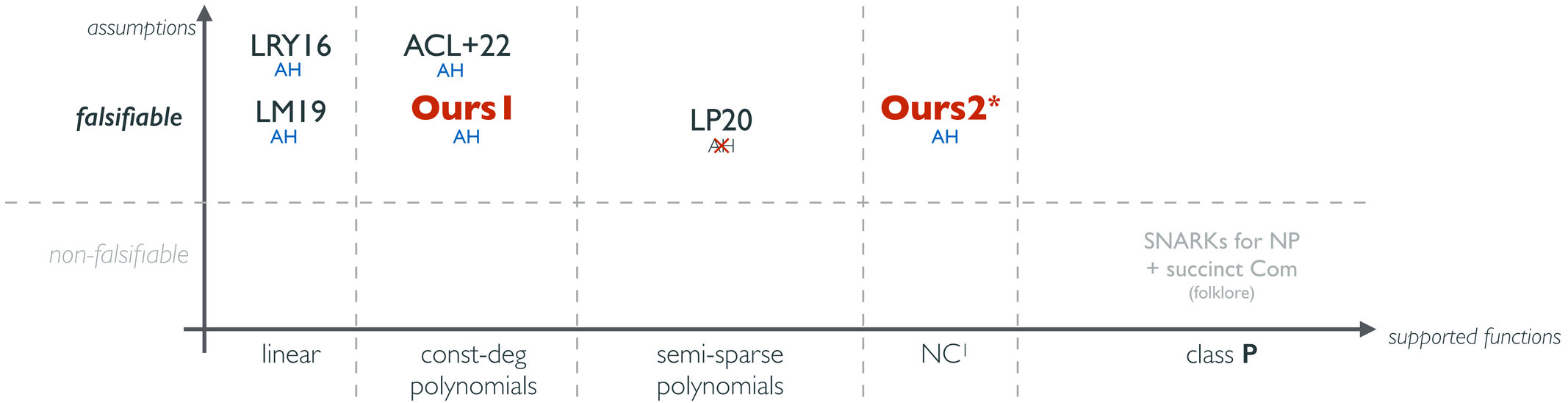
Homomorphic Signatures highlights:

- First HS with *compact* signatures (size constant in number of outputs)
- First *multi-input* HS for NC^1 based on pairings (prior HS for NC1 [KNYY19] only single-input)

Conclusions

Main results: First additive-homomorphic FCs for functions beyond linear

New pairing-based homomorphic signatures

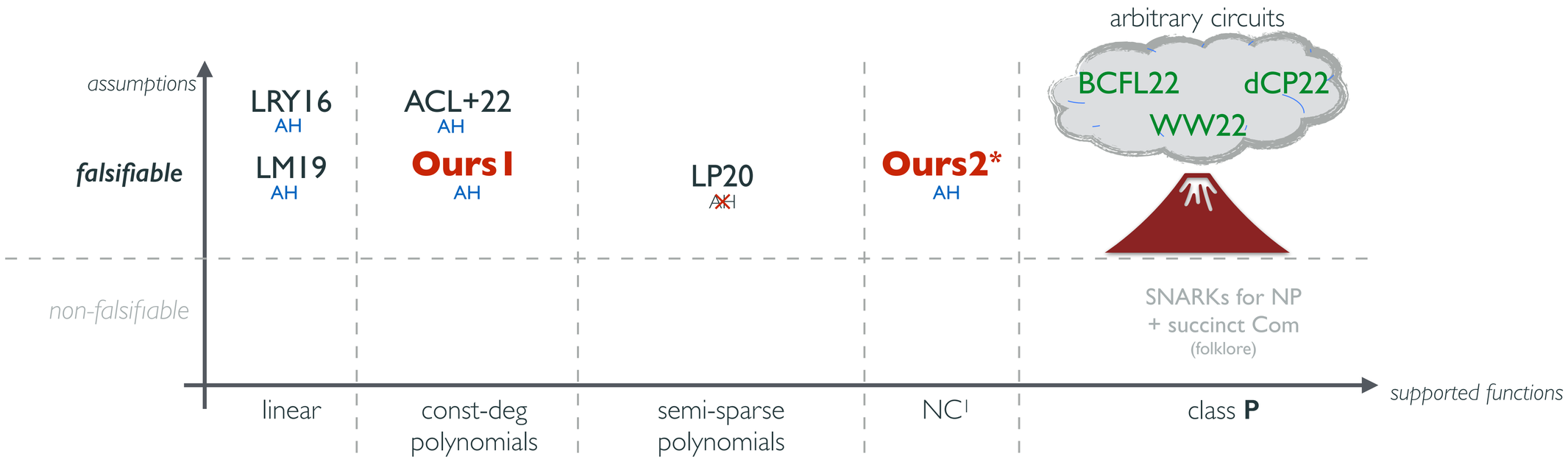


Conclusions

Main results: First additive-homomorphic FCs for functions beyond linear

New pairing-based homomorphic signatures

Recent works: First FC for circuits from falsifiable assumptions!



Conclusions

Main results: First additive-homomorphic FCs for functions beyond linear

New pairing-based homomorphic signatures

Recent works: First FC for circuits from falsifiable assumptions!

Open problems: Compact&constant-size FC for NC^1? FC for circuits with shorter openings?

More applications?