functional encryption for **quadratic** functions from k-LIN, revisited

Hoeteck Wee

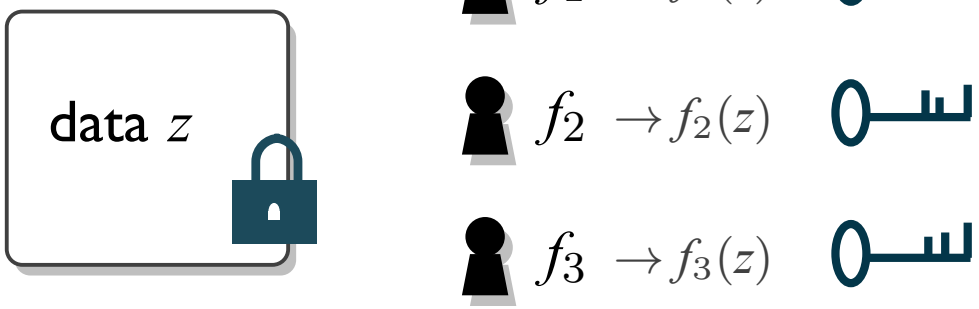
NTT Research

functional encryption

[SW05, GPSW06, BSW11]

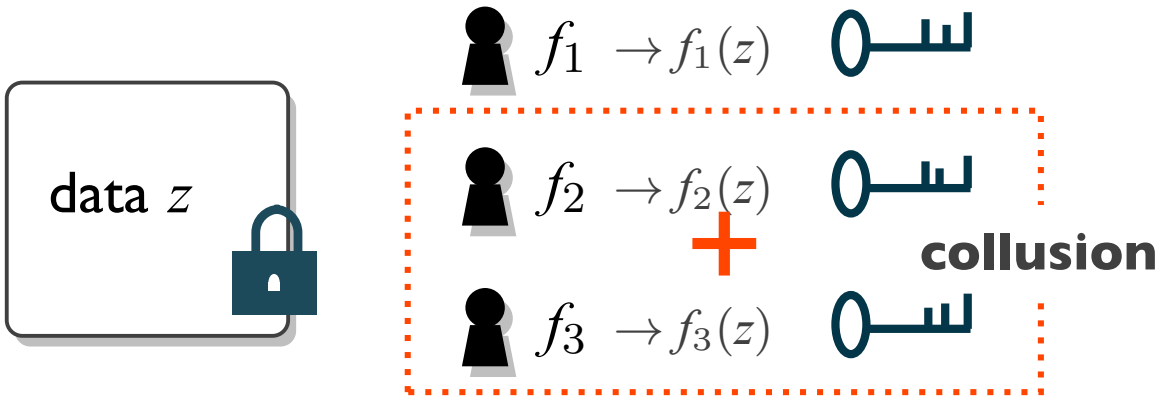
functional encryption

[SW05, GPSW06, BSW11]



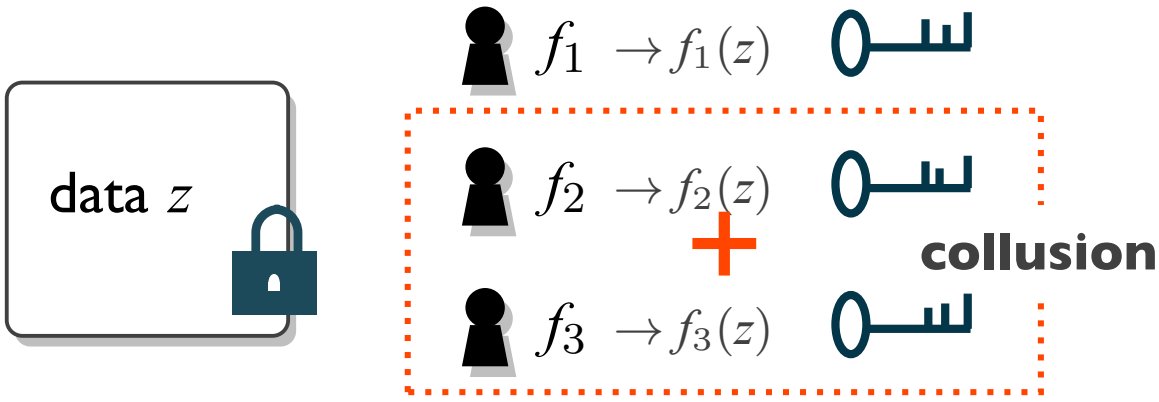
functional encryption

[SW05, GPSW06, BSW11]



functional encryption

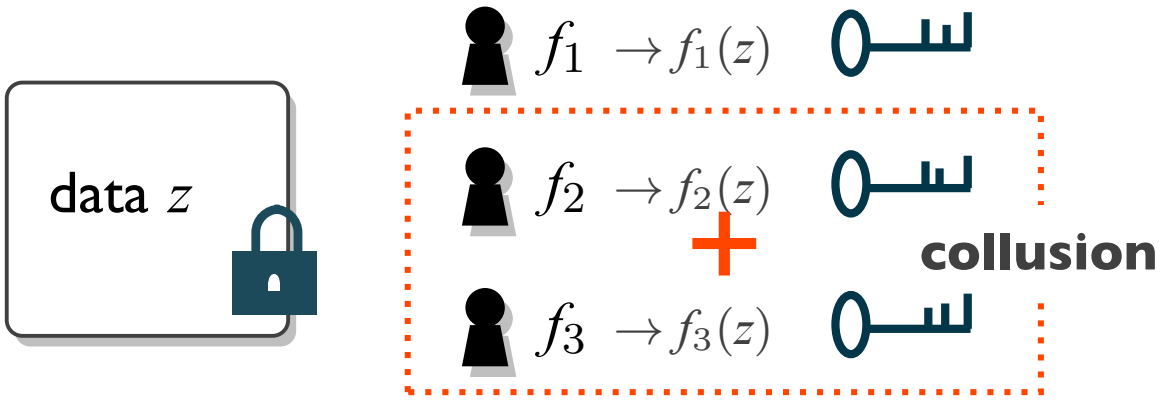
[SW05, GPSW06, BSW11]



this talk. quadratic functions **[BCFG17,LI7,RPBDG19,G20]**

functional encryption

[SW05, GPSW06, BSW11]



this talk. quadratic functions **[BCFG17,LI7,RPBDG19,G20]**

- traitor tracing **[BW06,BSW06,GKSW10,GKW19]**
- obfuscation **[AJLMS19,JLMS19,JLS19,GJLS20,JLS20]**
- privacy-preserving machine learning **[RPBDG19]**

our **results** [W20]

functional encryption for **quadratic** functions

– simpler & improved [BCFG17, L17, G20, RDGBP19]

our **results** [w20]

functional encryption for **quadratic** functions

- $|\mathbf{ct}| = O(n), |\mathbf{sk}| = O(1)$

our **results** [w20]

functional encryption for **quadratic** functions

- $|\mathbf{ct}| = O(n), |\mathbf{sk}| = O(1)$
- **simulation**-security against collusions
- **prime**-order bilinear groups, bilateral k-Lin

our **results** [w20]

functional encryption for **quadratic** functions

– $|\mathbf{ct}| = O(n), |\mathbf{sk}| = O(1)$

– **simulation**-security against collusions

– **prime**-order bilinear groups, bilateral k-Lin

$$([\mathbf{A}], [\mathbf{sA}]) \approx_c ([\mathbf{A}], [\mathbf{c}]), \mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$$

our **results** [w20]

functional encryption for **quadratic** functions

- $|\mathbf{ct}| = O(n), |\mathbf{sk}| = O(1)$
- **simulation**-security against collusions
- **prime**-order bilinear groups, bilateral k-Lin

$$([\mathbf{A}]_b, [\mathbf{sA}]_b)_{b=1,2} \approx_c ([\mathbf{A}]_b, [\mathbf{c}]_b)_{b=1,2},\ \mathbf{A} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$$

our **results** [w20]

functional encryption for **quadratic** functions

- $|\mathbf{ct}| = O(n), |\mathbf{sk}| = O(1)$ $(= \text{[RDGBP19]} + 1)$
- **simulation**-security against collusions
- **prime**-order bilinear groups, bilateral k-Lin

our **results** [w20]

functional encryption for **quadratic** functions

- $|\mathbf{ct}| = O(n), |\mathbf{sk}| = O(1)$
- **simulation**-security against collusions
- **prime**-order bilinear groups, bilateral k-Lin

extension. partially hiding FE

$$f(\overbrace{x}^{\text{NC1 public}}, \overbrace{z}^{\text{deg 2 private}})$$

[JLS19,GJLS20,GVW12,GVW15,W17,...]

our **results** [W20]

functional encryption for **quadratic** functions

- $|\mathbf{ct}| = O(n), |\mathbf{sk}| = O(1)$
- **simulation**-security against collusions
- **prime**-order bilinear groups, bilateral k-Lin

compiler: linear FE $\mapsto$ quadratic FE

[ABDP15,ALS16,W17]

our **results** [w20]

functional encryption for **quadratic** functions

- $|\mathbf{ct}| = O(n), |\mathbf{sk}| = O(1)$
- **simulation**-security against collusions
- **prime**-order bilinear groups, bilateral k-Lin

compiler: linear FE $\mapsto$ quadratic FE

$$\mathbf{z} \mapsto \mathbf{z} \cdot \mathbf{f}^\intercal$$

our **results** [w20]

functional encryption for **quadratic** functions

- $|\mathbf{ct}| = O(n), |\mathbf{sk}| = O(1)$
- **simulation**-security against collusions
- **prime**-order bilinear groups, bilateral k-Lin

compiler: linear FE $\mapsto$ quadratic FE

$$\mathbf{z} \mapsto \mathbf{z} \cdot \mathbf{f}^\intercal \qquad \mathbf{z}_1, \mathbf{z}_2 \mapsto (\mathbf{z}_1 \otimes \mathbf{z}_2) \cdot \mathbf{f}^\intercal$$

our **results** [W20]

functional encryption for **quadratic** functions

- $|\mathbf{ct}| = O(n), |\mathbf{sk}| = O(1)O(n)$
- **simulation**-security against collusions
- **prime**-order bilinear groups, bilateral k-Lin

compiler: linear FE $\mapsto$ quadratic FE

function-hiding [L17, G20]

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk}^1$

(2) $\mathbf{enc}^1(\mathbf{z})$

(3) $\mathbf{kg}^1(\mathbf{f})$

compiler: linear $\mapsto$ quadratic

(1) **mpk**

(2) **enc**$(\mathbf{z}_1, \mathbf{z}_2)$

(3) **kg**$(\mathbf{f})$

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk} := \mathbf{mpk}^1$

(2) $\mathbf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $\mathbf{enc}^1(\mathbf{z}_1 \otimes \mathbf{z}_2)$

(3) $\mathbf{kg}(\mathbf{f})$: $\mathbf{kg}^1(\mathbf{f})$

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk} := \mathbf{mpk}^1$

(2) $\mathbf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $\mathbf{enc}^1(\mathbf{z}_1 \otimes \mathbf{z}_2)$

(3) $\mathbf{kg}(\mathbf{f})$: $\mathbf{kg}^1(\mathbf{f})$

problem: $|\mathbf{ct}| = O(n^2)$

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk} := \mathbf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathbf{A}_1, \mathbf{A}_2 \leftarrow \mathbb{Z}_p^{k \times n}$

(2) $\mathbf{enc}(\mathbf{z}_1, \mathbf{z}_2)$:

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk} := \mathbf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathbf{A}_1, \mathbf{A}_2 \leftarrow \mathbb{Z}_p^{k \times n}$

(2) $\mathbf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $[\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1]_1, [\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2]_2, \ldots$

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk} := \mathbf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathbf{A}_1, \mathbf{A}_2 \leftarrow \mathbb{Z}_p^{k \times n}$

(2) $\mathbf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $[\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2}_{\mathbf{y}_2}]_2, \ldots$

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk} := \mathbf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathbf{A}_1, \mathbf{A}_2 \leftarrow \mathbb{Z}_p^{k \times n}$

(2) $\mathbf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $[\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2}_{\mathbf{y}_2}]_2, \ldots$

$$(\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1) \otimes (\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2) \cdot \mathbf{f}$$

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk} := \mathbf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathbf{A}_1, \mathbf{A}_2 \leftarrow \mathbb{Z}_p^{k \times n}$

(2) $\mathbf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $[\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2}_{\mathbf{y}_2}]_2, \ldots$

$$(\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1) \otimes (\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2) \cdot \mathbf{f}$$

$$= \mathbf{z}_1 \otimes \mathbf{z}_2 \cdot \mathbf{f} + \cdots$$

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk} := \mathbf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathbf{A}_1, \mathbf{A}_2 \leftarrow \mathbb{Z}_p^{k \times n}$

(2) $\mathbf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $[\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2}_{\mathbf{y}_2}]_2, \ldots$

$$(\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1) \otimes (\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2) \cdot \mathbf{f}$$

$$= \mathbf{z}_1 \otimes \mathbf{z}_2 \cdot \mathbf{f} + (\mathbf{s}_1\mathbf{A}_1 \otimes \mathbf{z}_2) \cdot \mathbf{f} + \cdots$$

compiler: linear $\mapsto$ quadratic

(1) $\mathsf{mpk} := \mathsf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathbf{A}_1, \mathbf{A}_2 \leftarrow \mathbb{Z}_p^{k \times n}$

(2) $\mathsf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $[\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2}_{\mathbf{y}_2}]_2, \ldots$

$$(\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1) \otimes (\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2) \cdot \mathbf{f}$$

$$= \mathbf{z}_1 \otimes \mathbf{z}_2 \cdot \mathbf{f} + (\mathbf{s}_1\mathbf{A}_1 \otimes \mathbf{z}_2) \cdot \mathbf{f} + \cdots$$

fact. $\mathbf{AC} \otimes \mathbf{BD} = (\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D})$

compiler: linear $\mapsto$ quadratic

(1) $\mathsf{mpk} := \mathsf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathbf{A}_1, \mathbf{A}_2 \leftarrow \mathbb{Z}_p^{k \times n}$

(2) $\mathsf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $[\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2}_{\mathbf{y}_2}]_2, \ldots$

$$(\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1) \otimes (\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2) \cdot \mathbf{f}$$

$$= \mathbf{z}_1 \otimes \mathbf{z}_2 \cdot \mathbf{f} + (\mathbf{s}_1 \otimes \mathbf{z}_2)(\mathbf{A}_1 \otimes \mathbf{I}) \cdot \mathbf{f} + \cdots$$

fact. $\mathbf{AC} \otimes \mathbf{BD} = (\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D})$

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk} := \mathbf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathbf{A}_1, \mathbf{A}_2 \leftarrow \mathbb{Z}_p^{k \times n}$

(2) $\mathbf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $[\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2}_{\mathbf{y}_2}]_2, \ldots$

$$(\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1) \otimes (\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2) \cdot \mathbf{f}$$

$$= \mathbf{z}_1 \otimes \mathbf{z}_2 \cdot \mathbf{f} + (\mathbf{s}_1 \otimes \mathbf{z}_2)(\mathbf{A}_1 \otimes \mathbf{I}) \cdot \mathbf{f} + \cdots$$

$$\mathbf{enc}^1(\underbrace{\mathbf{s}_1 \otimes \mathbf{z}_2}_{\text{length } kn}), \mathbf{kg}^1((\mathbf{A}_1 \otimes \mathbf{I}) \cdot \mathbf{f})$$

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk} := \mathbf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_1]_2, [\mathbf{A}_2]_2,$

(2) $\mathbf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $[\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2}_{\mathbf{y}_2}]_2, \ldots$

$$(\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1) \otimes (\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2) \cdot \mathbf{f}$$

$$= \mathbf{z}_1 \otimes \mathbf{z}_2 \cdot \mathbf{f} + (\mathbf{s}_1 \otimes \mathbf{z}_2)(\mathbf{A}_1 \otimes \mathbf{I}) \cdot \mathbf{f} + \cdots$$

$$\mathbf{enc}^1(\underbrace{\mathbf{s}_1 \otimes \mathbf{z}_2}_{\text{length } kn}), \mathbf{kg}^1(\underbrace{[(\mathbf{A}_1 \otimes \mathbf{I}) \cdot \mathbf{f}]_2}_{\text{public}})$$

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk} := \mathbf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_1]_2, [\mathbf{A}_2]_2,$

(2) $\mathbf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $[\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2}_{\mathbf{y}_2}]_2, \ldots$

$$(\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1) \otimes (\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2) \cdot \mathbf{f}$$

$$= \mathbf{z}_1 \otimes \mathbf{z}_2 \cdot \mathbf{f} + (\mathbf{s}_1 \otimes \mathbf{z}_2)(\mathbf{A}_1 \otimes \mathbf{I})\mathbf{f} + (\mathbf{y}_1 \otimes \mathbf{s}_2)(\mathbf{I} \otimes \mathbf{A}_2)\mathbf{f}$$

$$\mathbf{enc}^1(\underbrace{\mathbf{s}_1 \otimes \mathbf{z}_2}_{\text{length } kn}), \mathbf{kg}^1(\underbrace{[(\mathbf{A}_1 \otimes \mathbf{I}) \cdot \mathbf{f}]_2}_{\text{public}})$$

compiler: linear $\mapsto$ quadratic

(1) $\mathbf{mpk} := \mathbf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_1]_2, [\mathbf{A}_2]_2,$

(2) $\mathbf{enc}(\mathbf{z}_1, \mathbf{z}_2)$: $[\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2}_{\mathbf{y}_2}]_2, \ldots$

$$(\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1) \otimes (\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2) \cdot \mathbf{f}$$

$$= \mathbf{z}_1 \otimes \mathbf{z}_2 \cdot \mathbf{f} + (\mathbf{s}_1 \otimes \mathbf{z}_2)(\mathbf{A}_1 \otimes \mathbf{I})\mathbf{f} + (\mathbf{y}_1 \otimes \mathbf{s}_2)(\mathbf{I} \otimes \mathbf{A}_2)\mathbf{f}$$

$$\mathbf{enc}^1(\mathbf{s}_1 \otimes \mathbf{z}_2 \| \mathbf{y}_1 \otimes \mathbf{s}_2), \mathbf{kg}^1([\binom{(\mathbf{A}_1 \otimes \mathbf{I})\mathbf{f}}{(\mathbf{I} \otimes \mathbf{A}_2)\mathbf{f}}]_2)$$

compiler: linear $\mapsto$ quadratic

(1) $\mathsf{mpk} := \mathsf{mpk}^1, [\mathbf{A}_1]_1, [\mathbf{A}_1]_2, [\mathbf{A}_2]_2$

(2) $\mathsf{enc}(\mathbf{z}_1, \mathbf{z}_2)$:

$$[\underbrace{\mathbf{s}_1\mathbf{A}_1 + \mathbf{z}_1}_{\mathbf{y}_1}]_1, [\underbrace{\mathbf{s}_2\mathbf{A}_2 + \mathbf{z}_2}_{\mathbf{y}_2}]_2, \mathsf{enc}^1(\mathbf{s}_1 \otimes \mathbf{z}_2 \| \mathbf{y}_1 \otimes \mathbf{s}_2)$$

(3) $\mathsf{kg}(\mathbf{f})$: $\mathsf{kg}^1([\binom{(\mathbf{A}_1 \otimes \mathbf{I})\mathbf{f}}{(\mathbf{I} \otimes \mathbf{A}_2)\mathbf{f}}]_2)$

conclusion

new constructions & techniques for **quadratic** FE

conclusion

new constructions & techniques for **quadratic** FE

open problems.

- constructions from (standard) k-Lin
- adaptive security
- lattice-based analogue

conclusion

new constructions & techniques for **quadratic** FE

open problems.

- constructions from (standard) k-Lin
- adaptive security
- lattice-based analogue

// merci !