Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption

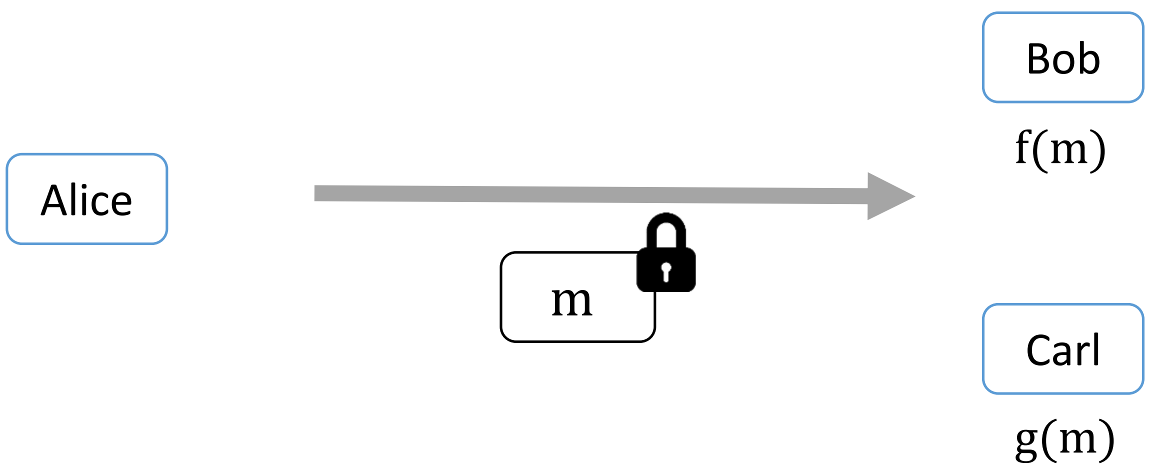
Carmen Elisabetta Zaira Baltico, Università di Catania

Dario Catalano, Università di Catania

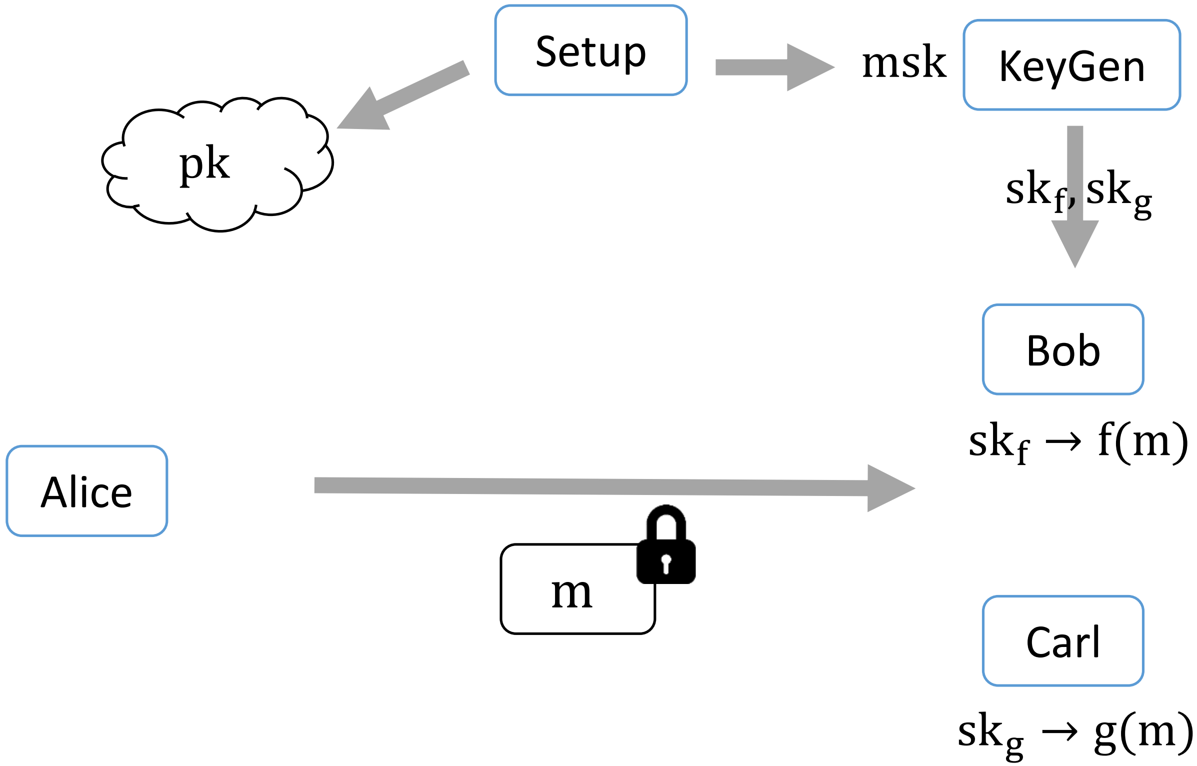
Dario Fiore, IMDEA

Romain Gay, ENS

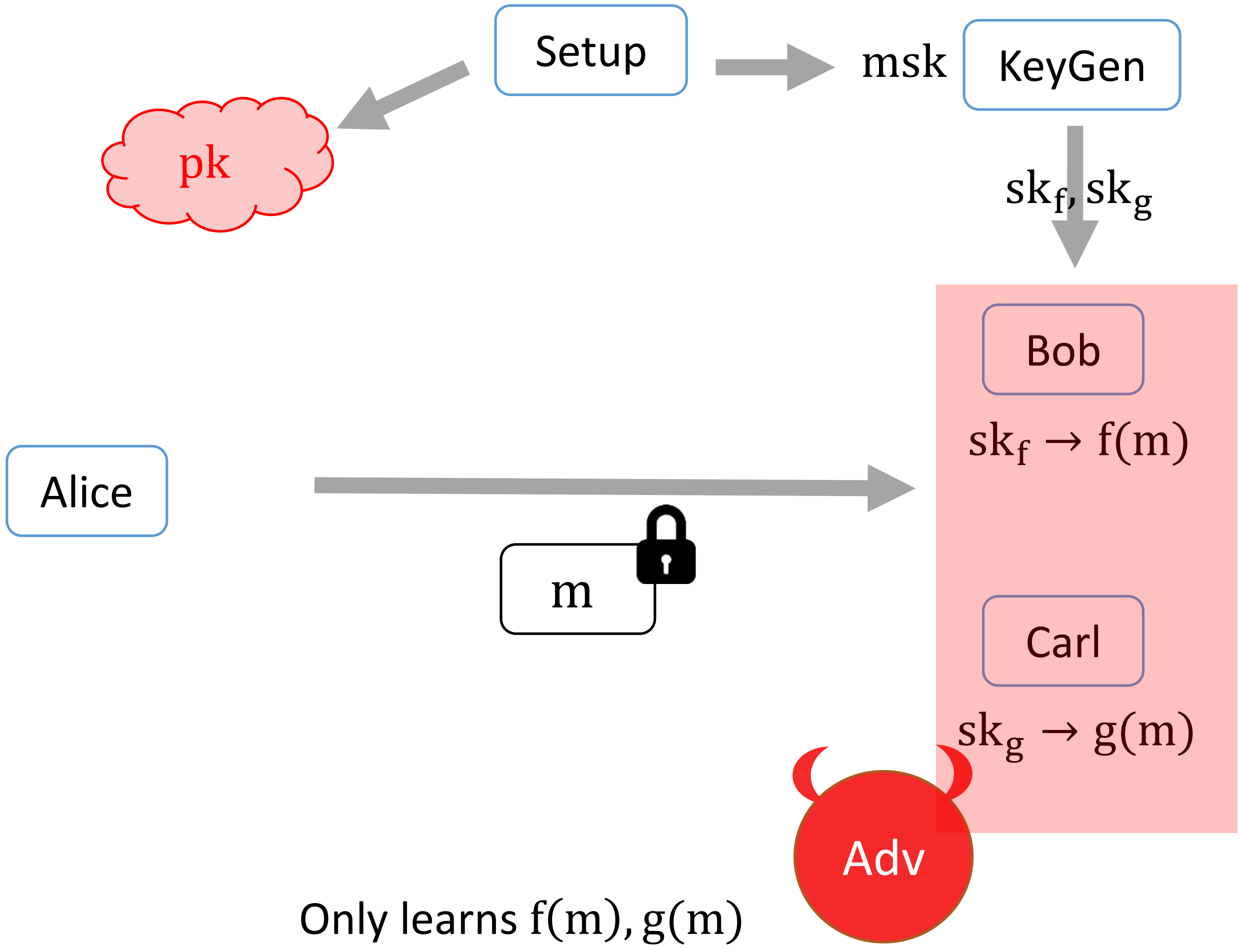
FE [Boneh, Sahai, Waters 11]



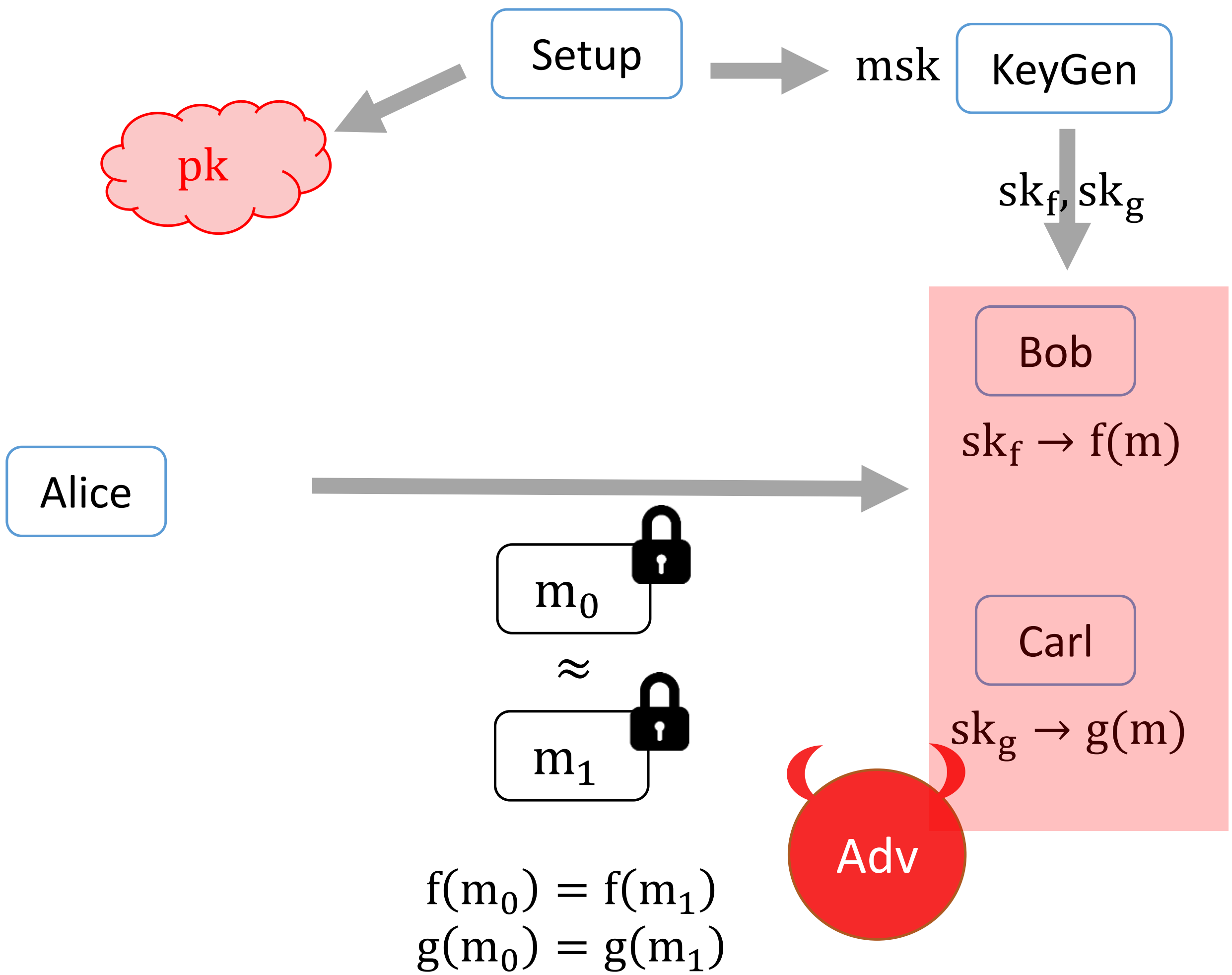
FE [Boneh, Sahai, Waters 11]



FE [Boneh, Sahai, Waters 11]



FE [Boneh, Sahai, Waters 11]



Prior works on FE

Construction:	Functions:	Assumption:	Practical:
[GGHRSW 13,…]	any circuit	iO	✗
[ABCP 15]	Inner Product	DDH	✓

$m = \vec{x} \in \mathbb{Z}_p^n$

$f = \vec{y} \in \mathbb{Z}_p^n$

$f(m) = \vec{x}^T \vec{y} \in \mathbb{Z}_p$

ct size $= O(\mathrm{n})$

Prior works on FE

Construction:	Functions:	Assumption:	Practical:
[GGHRSW 13,…]	any circuit	iO	✗
[ABCP 15]	Inner Product	DDH	✓
Our work	Quadratic functions	pairings	✓

$$m = (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m$$

$$f = \left(f_{i,j}\right)_{i \in [n], j \in [m]} \in \mathbb{Z}_p^{n \times m}$$

$$f(m) = \vec{x}^T f \vec{y} = \sum_{i \in [n], j \in [m]} x_i f_{i,j} y_j \in \mathbb{Z}_p$$

$\text{ct size} = O(\text{n} + \text{m})$

vs

$\text{ct size} = O(\text{n} \cdot \text{m})$

Prior works on FE

Construction:	Functions:	Assumption:	Practical:
[GGHRSW 13,...]	any circuit	iO	✗
[ABCP 15]	Inner Product	DDH	✓
Our work	Quadratic functions	pairings	✓

Quadratic FE:	Security:	Assumption:	Private/public key:	Function-hiding:
[AS 17]	SEL-IND	GGM	private	✓
[Lin 17]	SEL-IND	SXDH	private	✓
Our work	SEL-IND	SXDH & 3-PDDH	public	-
Our work	AD-IND	GGM	public	-

Prior works on Predicate Encryption

$$\mathrm{m} = (\mathrm{plaintext}, \mathrm{attribute})$$

$$\mathrm{f(m)} = \mathrm{plaintext\ iff\ P(attribute)} = 1$$

Construction:	Predicate P:	Assumption:
[BW 06]	Anonymous IBE	pairings

$$\mathrm{attribute} = id \in \{0,1\}^n$$

$$\forall id' \in \{0,1\}^n\!: \mathrm{sk}_{id'} \rightarrow \mathrm{P}(id) = 1 \ \text{ iff } \ id = id'$$

Prior works on Predicate Encryption

$$\mathrm{m} = (\mathrm{plaintext}, \mathrm{attribute})$$

$$\mathrm{f(m)} = \mathrm{plaintext\ iff\ P(attribute)} = 1$$

Construction:	Predicate P:	Assumption:
[BW 06]	Anonymous IBE	pairings
[KSW 08]	Inner Product	pairings

$\mathrm{attribute} = \vec{x} \in \mathbb{Z}_p^n$

$\mathrm{ct\ size} = O(\mathrm{n})$

$\forall \vec{y} \in \mathbb{Z}_p^n \colon \mathrm{sk}_{\vec{y}} \rightarrow \mathrm{P}(\vec{x}) = 1 \ \text{ iff } \ \vec{x}^T\vec{y} = 0$

Prior works on Predicate Encryption

$$\text{m} = (\text{plaintext}, \text{attribute})$$

$$\text{f}(\text{m}) = \text{plaintext iff P}(\text{attribute}) = 1$$

Construction:	Predicate P:	Assumption:
[BW 06]	Anonymous IBE	pairings
[KSW 08]	Inner Product	pairings
Our work	Bilinear	pairings

$\text{attribute} = (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m$

$\forall f \in \mathbb{Z}_p^{n \times m}: \text{sk}_f \to \text{P}(\vec{x}) = 1 \text{ iff } \vec{x}^T f \vec{y} = 0$

$\text{ct size} = O(\text{n} + \text{m})$

vs

$\text{ct size} = O(\text{n} \cdot \text{m})$

Prior works on Predicate Encryption

$$\mathrm{m} = (\mathrm{plaintext}, \mathrm{attribute})$$

$$\mathrm{f(m)} = \mathrm{plaintext\ iff\ P(attribute)} = 1$$

Construction:	Predicate P:	Assumption:	Hiding:
[BW 06]	Anonymous IBE	pairings	fully
[KSW 08]	Inner Product	pairings	fully
Our work	Bilinear	pairings	fully
[GVW 15]	Any circuit	LWE	weakly

Outline

1 FE $f: (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m \rightarrow \vec{x}^T f \vec{y} \in \mathbb{Z}_p$

Outline

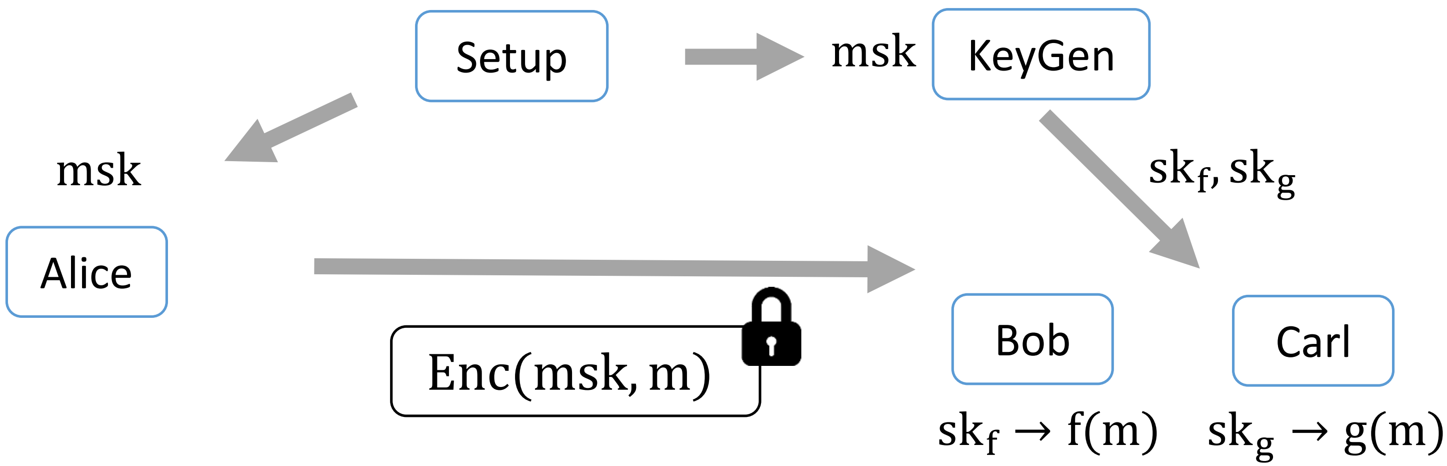
1 FE $f: (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m \rightarrow \vec{x}^T f \vec{y} \in \mathbb{Z}_p$

- Private-Key, one-ct secure FE
- Public-Key FE

Outline

1 FE $f: (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m \rightarrow \vec{x}^T f \vec{y} \in \mathbb{Z}_p$

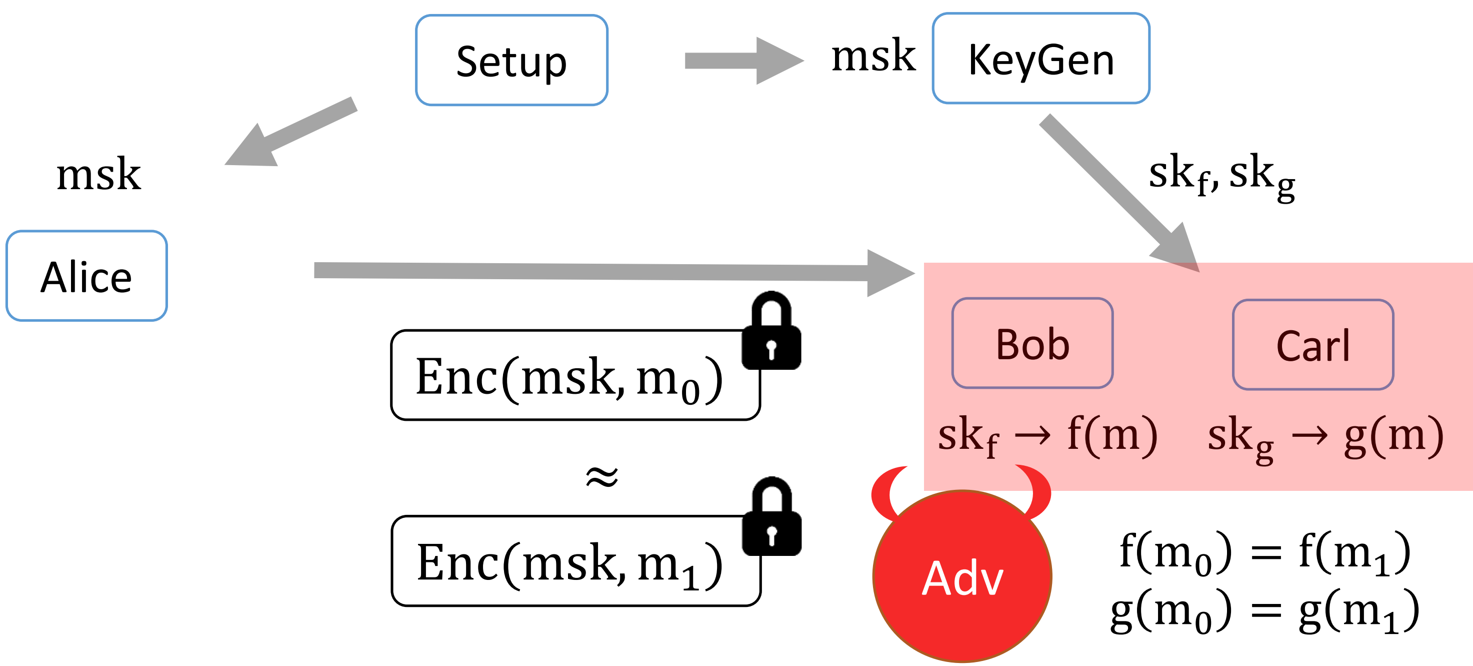
- Private-Key, one-ct secure FE
- Public-Key FE



Outline

1 FE $f: (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m \rightarrow \vec{x}^T f \vec{y} \in \mathbb{Z}_p$

- Private-Key, one-ct secure FE
- Public-Key FE



Outline

1 FE $f: (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m \rightarrow \vec{x}^T f \vec{y} \in \mathbb{Z}_p$

- Private-Key, one-ct secure FE

- Public-Key FE

Outline

1 FE $f\colon (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m \to \vec{x}^T f \vec{y} \in \mathbb{Z}_p$

- Private-Key, one-ct secure FE
- Public-Key FE

2 PE $sk_f \to P(\vec{x}, \vec{y}) = 1 \text{ iff } \vec{x}^T f \vec{y} = 1$

Private-Key, one-ct secure FE

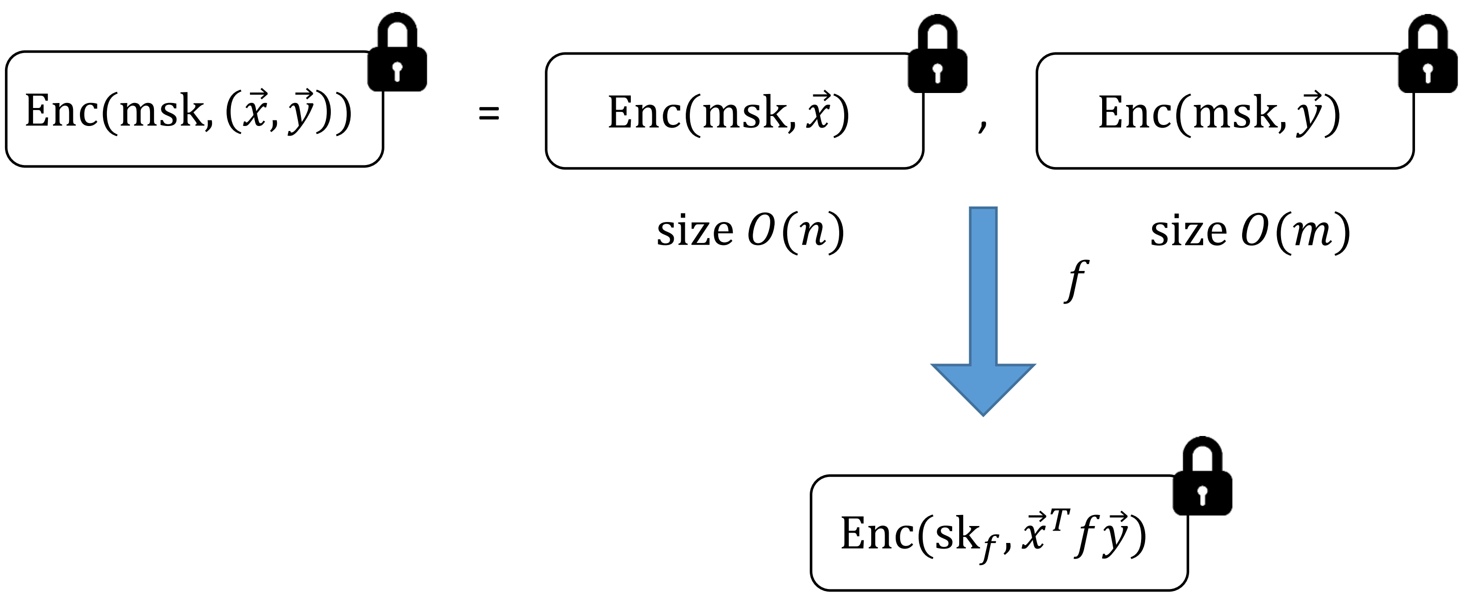
FE $f: (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m \to \vec{x}^T f \vec{y} \in \mathbb{Z}_p$

$\text{Enc}(\text{msk}, (\vec{x}, \vec{y}))$ = $\text{Enc}(\text{msk}, \vec{x})$, $\text{Enc}(\text{msk}, \vec{y})$

size $O(n)$ size $O(m)$

Private-Key, one-ct secure FE

FE $\quad f\colon (\vec{x},\vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m \rightarrow \vec{x}^T f \vec{y} \in \mathbb{Z}_p$



Private-Key, one-ct secure FE

FE $f: (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m \to \vec{x}^T f \vec{y} \in \mathbb{Z}_p$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ of order p, generator P_1, P_2, P_T

$\forall a, b \in \mathbb{Z}_p, aP_1 + bP_1 = (a+b)P_1$

$\mathbb{G}_1 \quad \times \quad \mathbb{G}_2$

$\mathrm{Enc}(\mathrm{msk}, (\vec{x}, \vec{y}))$ = $\mathrm{Enc}(\mathrm{msk}, \vec{x})$, $\mathrm{Enc}(\mathrm{msk}, \vec{y})$

size $O(n)$ size $O(m)$

f

$\mathrm{Enc}(\mathrm{sk}_f, \vec{x}^T f \vec{y})$ $\in \mathbb{G}_T$

Private-Key, one-ct secure FE

FE $f\colon (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m \to \vec{x}^T f \vec{y} \in \mathbb{Z}_p$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ of order p, generator P_1, P_2, P_T

$\forall a, b \in \mathbb{Z}_p, aP_1 + bP_1 = (a+b)P_1$

$\mathbb{G}_1 \times \mathbb{G}_2$

$\text{Enc}(\text{msk}, (\vec{x}, \vec{y}))$ = $\text{Enc}(\text{msk}, \vec{x})$, $\text{Enc}(\text{msk}, \vec{y})$

size $O(n)$ size $O(m)$

f

$e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

$\forall a, b \in \mathbb{Z}_p, e(aP_1, bP_2) = ab\, e(P_1, P_2)$

$= ab\, P_T$

$\text{Enc}(\text{sk}_f, \vec{x}^T f \vec{y}) \in \mathbb{G}_T$

Private-Key, one-ct secure FE

FE $f\colon (\vec{x},\vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m \to \vec{x}^T f \vec{y} \in \mathbb{Z}_p$

$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ of order p, generator P_1, P_2, P_T

$\forall a, b \in \mathbb{Z}_p, aP_1 + bP_1 = (a+b)P_1$

$\mathbb{G}_1$ $\times$ $\mathbb{G}_2$

El Gamal El Gamal

$\text{Enc}(\text{msk}, (\vec{x},\vec{y}))$ = $\text{Enc}(\text{msk}, \vec{x})$, $\text{Enc}(\text{msk}, \vec{y})$

size $O(n)$ size $O(m)$

f

$e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

$\forall a, b \in \mathbb{Z}_p, e(aP_1, bP_2) = ab\, e(P_1, P_2)$

$= ab\, P_T$

$\text{Enc}(\text{sk}_f, \vec{x}^T f \vec{y})$ $\in \mathbb{G}_T$

El Gamal

$$pk = \left(\boxed{\vec{a}}_1 = \vec{a}P_1 \;,\; \boxed{\vec{u}}_1 = \vec{u}P_1 \xleftarrow{R} \mathbb{G}_1^2 \right)$$

$$Enc(pk, m \in \mathbb{Z}_p) = \boxed{\vec{a}r}_1 + \boxed{\vec{u}m}_1 = (\vec{a}r + \vec{u}m)P_1 \in \mathbb{G}_1^2 \quad \text{for } r \xleftarrow{R} \mathbb{Z}_p$$

El Gamal

$$pk = \left(\boxed{\vec{a}}_1 = \vec{a}P_1 \ , \ \boxed{\vec{u}}_1 = \vec{u}P_1 \leftarrow^R \mathbb{G}_1^2 \right)$$

$$Enc\big(pk, m \in \mathbb{Z}_p\big) = \boxed{\vec{a}r}_1 + \boxed{\vec{u}m}_1 = (\vec{a}r + \vec{u}m)P_1 \in \mathbb{G}_1^2 \quad \text{for } r \leftarrow^R \mathbb{Z}_p$$

Security: $\left(\boxed{\vec{a}}_1 \ , \ \boxed{\vec{a}r}_1 \right) \approx_c \left(\boxed{\vec{a}}_1 \ , \ \boxed{\vec{v}}_1 \right)$

for $r \leftarrow^R \mathbb{Z}_p$ DDH in $\mathbb{G}_1$ for $\vec{v} \leftarrow^R \mathbb{Z}_p^2$

El Gamal

$$pk = \left(\boxed{\vec{a}}_1 = \vec{a}P_1 \;,\; \boxed{\vec{u}}_1 = \vec{u}P_1 \leftarrow^{R} \mathbb{G}_1^2 \right)$$

$$Enc(pk, m \in \mathbb{Z}_p) = \boxed{\vec{v}}_1 \leftarrow^{R} \mathbb{G}_1^2$$

Security: $\left(\boxed{\vec{a}}_1 \;,\; \boxed{\vec{a}r}_1 \right) \approx_c \left(\boxed{\vec{a}}_1 \;,\; \boxed{\vec{v}}_1 \right)$

for $r \leftarrow^{R} \mathbb{Z}_p$ DDH in $\mathbb{G}_1$ for $\vec{v} \leftarrow^{R} \mathbb{Z}_p^2$

El Gamal

$$pk = \left(\boxed{\vec{a}}_1 = \vec{a}P_1 \; , \; \boxed{\vec{u}}_1 = \vec{u}P_1 \leftarrow^R \mathbb{G}_1^2 \right)$$

$$Enc(pk, m \in \mathbb{Z}_p) = \boxed{\vec{a}r}_1 + \boxed{\vec{u}m}_1 = (\vec{a}r + \vec{u}m)P_1 \in \mathbb{G}_1^2 \quad \text{for } r \leftarrow^R \mathbb{Z}_p$$

Correctness: $\left(\boxed{\vec{a}}_1 \; , \; \boxed{\vec{u}}_1 \right)$ is a basis of $\mathbb{G}_1^2$

El Gamal

$$pk = \left([\vec{a}]_1 = \vec{a}P_1 \;,\; [\vec{u}]_1 = \vec{u}P_1 \xleftarrow{R} \mathbb{G}_1^2 \right)$$

$$Enc(pk, m \in \mathbb{Z}_p) = [\vec{a}r]_1 + [\vec{u}m]_1 = (\vec{a}r + \vec{u}m)P_1 \in \mathbb{G}_1^2 \quad \text{for } r \xleftarrow{R} \mathbb{Z}_p$$

Correctness: $\left([\vec{a}]_1 \;,\; [\vec{u}]_1 \right)$ is a basis of $\mathbb{G}_1^2 \Rightarrow$

$\exists \vec{a}^{\perp} \in \mathbb{Z}_p^2$ such that $\vec{a}^{\perp} \cdot \vec{a} = 0, \vec{a}^{\perp} \cdot \vec{u} = 1$

El Gamal

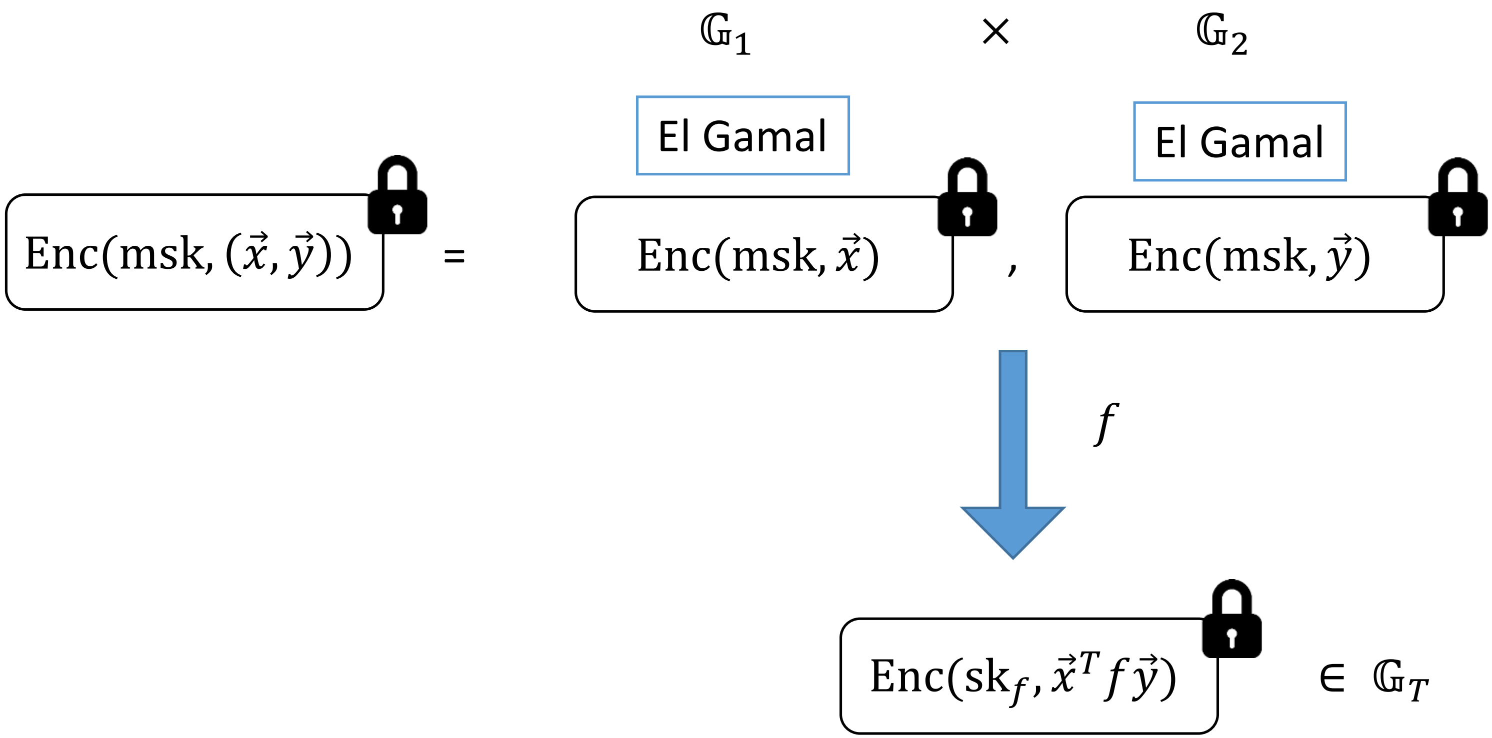
$$pk = \left(\boxed{\vec{a}}_1 = \vec{a}P_1 \ , \ \boxed{\vec{u}}_1 = \vec{u}P_1 \leftarrow^R \mathbb{G}_1^2 \right)$$

$$Enc(pk, m \in \mathbb{Z}_p) = \boxed{\vec{a}r}_1 + \boxed{\vec{u}m}_1 = (\vec{a}r + \vec{u}m)P_1 \in \mathbb{G}_1^2 \quad \text{for } r \leftarrow^R \mathbb{Z}_p$$

$$sk = \vec{a}^{\perp}$$

$$Dec\text{:} \left(\boxed{\vec{a}r \cdot \vec{a}^{\perp}}_1 + \boxed{\vec{u}m \cdot \vec{a}^{\perp}}_1 \right) = \boxed{m}_1 \in \mathbb{G}_1$$

Private-Key, one-ct secure FE



Private-Key, one-ct secure FE

$$\mathbb{G}_1 \times \mathbb{G}_2$$

$$\text{Enc}(\text{msk}, (\vec{x}, \vec{y})) = \forall i \in [n]: \left[\vec{a} r_i\right]_1 + \left[\vec{u} x_i\right]_1 \quad , \quad \forall j \in [m]: \left[\vec{b} s_j\right]_2 + \left[\vec{v} y_j\right]_2$$

Private-Key, one-ct secure FE

$$\text{Enc}(\text{msk}, (\vec{x}, \vec{y})) = e\left([\vec{a} r_i]_1 + [\vec{u} x_i]_1 \;,\; [\vec{b} s_j]_2 + [\vec{v} y_j]_2 \right)$$

$$\Downarrow$$

$$e\left([\vec{a} r_i]_1 , [\vec{b} s_j]_2 \right) + e\left([\vec{a} r_i]_1 , [\vec{v} y_j]_2 \right) + e\left([\vec{u} x_i]_1 , [\vec{b} s_j]_2 \right) + e\left([\vec{u} x_i]_1 , [\vec{v} y_j]_2 \right)$$

Private-Key, one-ct secure FE

$$msk = \forall i, j: [\vec{a} r_i]_1, [\vec{b} s_j]_2$$

$$\text{Enc}(\text{msk}, (\vec{x}, \vec{y})) = e\left([\vec{a} r_i]_1 + [\vec{u} x_i]_1, [\vec{b} s_j]_2 + [\vec{v} y_j]_2\right)$$

$$e\left([\vec{a} r_i]_1, [\vec{b} s_j]_2\right) + e\left([\vec{a} r_i]_1, [\vec{v} y_j]_2\right) + e\left([\vec{u} x_i]_1, [\vec{b} s_j]_2\right) + e\left([\vec{u} x_i]_1, [\vec{v} y_j]_2\right)$$

$$= sk_{X_i Y_j}$$

Private-Key, one-ct secure FE

$$msk = \forall i, j: \left[\vec{a} r_i\right]_1, \left[\vec{b} s_j\right]_2$$

$$\text{Enc}(\text{msk}, (\vec{x}, \vec{y})) = e\left(\left[\vec{a} r_i\right]_1 + \left[\vec{b}^{\perp} x_i\right]_1, \left[\vec{b} s_j\right]_2 + \left[\vec{a}^{\perp} y_j\right]_2\right)$$

Dual bases: $\left[\vec{a}\right]_1, \left[\vec{b}^{\perp}\right]_1 \quad \left[\vec{b}\right]_2, \left[\vec{a}^{\perp}\right]_2$

$$e\left(\left[\vec{a} r_i\right]_1, \left[\vec{b} s_j\right]_2\right) + \cancel{e\left(\left[\vec{a} r_i\right]_1, \left[\vec{a}^{\perp} y_j\right]_2\right) + e\left(\left[\vec{b}^{\perp} x_i\right]_1, \left[\vec{b} s_j\right]_2\right)} + e\left(\left[\vec{b}^{\perp} x_i\right]_1, \left[\vec{a}^{\perp} y_j\right]_2\right)$$

$$= sk_{X_i Y_j}$$

Private-Key, one-ct secure FE

$$msk = \forall i, j: [\vec{a} r_i]_1, [\vec{b} s_j]_2$$

$$\text{Enc}(\text{msk}, (\vec{x}, \vec{y})) = e\left([\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1 \;,\; [\vec{b} s_j]_2 + [\vec{a}^{\perp} y_j]_2\right)$$

$$\Downarrow$$

$$e\left([\vec{a} r_i]_1, [\vec{b} s_j]_2\right) + e\left([\vec{b}^{\perp} x_i]_1, [\vec{a}^{\perp} y_j]_2\right)$$

$$= sk_{X_i Y_j}$$

Private-Key, one-ct secure FE

$$msk = \forall i,j: \ [\vec{a} r_i]_1 \ , \ [\vec{b} s_j]_2$$

$$\mathrm{Enc}(\mathrm{msk}, (\vec{x}, \vec{y})) = \forall i \in [n]: \ [\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1 \ , \quad \forall j \in [m]: \ [\vec{b} s_j]_2 + [\vec{a}^{\perp} y_j]_2$$

$\Downarrow f$

$$\sum_{i,j} f_{i,j}\, e\left([\vec{a} r_i]_1 \ , \ [\vec{b} s_j]_2\right) + \sum_{i,j} f_{i,j}\, e\left([\vec{b}^{\perp} x_i]_1 \ , \ [\vec{a}^{\perp} y_j]_2\right)$$

$$= sk_f$$

Private-Key, one-ct secure FE

$$msk = \forall i,j: \left[\vec{a}r_i\right]_1, \left[\vec{b}s_j\right]_2$$

$$\forall i \in [n]: \qquad\qquad \forall j \in [m]:$$

$$\text{Enc}(\text{msk}, (\vec{x}, \vec{y})) = \left[\vec{a}r_i\right]_1 + \left[\vec{b}^{\perp}x_i\right]_1, \quad \left[\vec{b}s_j\right]_2 + \left[\vec{a}^{\perp}y_j\right]_2$$

$$\Big\downarrow \; f$$

$$\sum_{i,j} f_{i,j}\, e\left(\left[\vec{a}r_i\right]_1, \left[\vec{b}s_j\right]_2\right) + \sum_{i,j} f_{i,j}x_iy_j\; e\left(\left[\vec{b}^{\perp}\right]_1, \left[\vec{a}^{\perp}\right]_2\right)$$

$$\left[\vec{a}r_i\right]_1, \left[\vec{b}s_j\right]_2 = sk_f$$

Private-Key, one-ct secure FE

$$msk = \forall i, j: [\vec{a} r_i]_1 , [\vec{b} s_j]_2$$

$$\mathrm{Enc}(\mathrm{msk}, (\vec{x}, \vec{y})) = \quad \forall i \in [n]: [\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1 \quad , \quad \forall j \in [m]: [\vec{b} s_j]_2 + [\vec{a}^{\perp} y_j]_2$$

$$pk = e\left([\vec{b}^{\perp}]_1 , [\vec{a}^{\perp}]_2 \right)$$

f

$$\sum_{i,j} \left(f_{i,j}\, e\left([\vec{a} r_i]_1 , [\vec{b} s_j]_2 \right) \right) + \sum_{i,j} f_{i,j} x_i y_j \; e\left([\vec{b}^{\perp}]_1 , [\vec{a}^{\perp}]_2 \right)$$

$$= sk_f$$

Private-Key, one-ct secure FE

$$msk = \forall i, j: \left[\vec{a} r_i\right]_1, \left[\vec{b} s_j\right]_2, \left[\vec{b}^{\perp}\right]_1, \left[\vec{a}^{\perp}\right]_2$$

$$\mathrm{Enc}(\mathrm{msk}, (\vec{x}, \vec{y})) = \forall i \in [n]: \left[\vec{a} r_i\right]_1 + \left[\vec{b}^{\perp} x_i\right]_1 , \quad \forall j \in [m]: \left[\vec{b} s_j\right]_2 + \left[\vec{a}^{\perp} y_j\right]_2$$

$$pk = e\left(\left[\vec{b}^{\perp}\right]_1, \left[\vec{a}^{\perp}\right]_2\right)$$

$$sk_f = \sum_{i,j} \left(f_{i,j}\, e\left(\left[\vec{a} r_i\right]_1, \left[\vec{b} s_j\right]_2\right)\right)$$

Private-Key, one-ct secure FE

$\forall i \in [n]$: $\quad\quad\quad\quad\quad\quad \forall j \in [m]$:

$$\boxed{\text{Enc}(\text{msk}, (\vec{x}, \vec{y}))} = [\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1 \quad , \quad [\vec{b} s_j]_2 + [\vec{a}^{\perp} y_j]_2$$

$$pk = e\left([\vec{b}^{\perp}]_1 , [\vec{a}^{\perp}]_2 \right)$$

$$sk_f = \sum_{i,j} \left(f_{i,j}\, e\left([\vec{a} r_i]_1 , [\vec{b} s_j]_2 \right) \right), sk_g \ldots$$

1. Preparatory: get rid of $\vec{a}^{\perp}$
2. DDH in $\mathbb{G}_1$
3. DDH in $\mathbb{G}_2$

Private-Key, one-ct secure FE

$$\boxed{\mathrm{Enc}(\mathrm{msk}, (\vec{x}, \vec{y}))} = \quad \forall i \in [n]: \; [\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1 \quad , \quad \forall j \in [m]: \; [\vec{b} s_j]_2 + [\vec{a}^{\perp} y_j]_2$$

$$pk = e\left([\vec{b}^{\perp}]_1, [\vec{a}^{\perp}]_2\right)$$

1. Preparatory: get rid of $\vec{a}^{\perp}$

$$sk_f = \sum_{i,j} f_{i,j} \, e\left([\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1, [\vec{b} s_j]_2 + [\vec{a}^{\perp} y_j]_2\right) - \sum_{i,j} f_{i,j} \, e\left([\vec{b}^{\perp} x_i]_1, [\vec{a}^{\perp} y_j]_2\right)$$

Private-Key, one-ct secure FE

$$\mathrm{Enc}(\mathrm{msk}, (\vec{x}, \vec{y})) = \quad \forall i \in [n]: \left[\vec{a} r_i\right]_1 + \left[\vec{b}^{\perp} x_i\right]_1 , \quad \forall j \in [m]: \left[\vec{b} s_j\right]_2 + \left[\vec{a}^{\perp} y_j\right]_2$$

$$pk = e\left(\left[\vec{b}^{\perp}\right]_1, \left[\vec{a}^{\perp}\right]_2\right)$$

1. Preparatory: get rid of $\vec{a}^{\perp}$

$$sk_f = \sum_{i,j} f_{i,j}\, e\left(\left[\vec{a} r_i\right]_1 + \left[\vec{b}^{\perp} x_i\right]_1, \left[\vec{b} s_j\right]_2 + \left[\vec{a}^{\perp} y_j\right]_2\right) - \vec{x}^T f \vec{y} \cdot pk$$

Private-Key, one-ct secure FE

$$\mathrm{Enc}(\mathrm{msk}, (\vec{x}, \vec{y})) = \left(\forall i \in [n]: [\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1 \;,\; \forall j \in [m]: [\vec{b} s_j]_2 + [\vec{a}^{\perp} y_j]_2 \right)$$

$$pk = e\left([\vec{b}^{\perp}]_1 , [\vec{a}^{\perp}]_2 \right)$$

$$\vec{x}^T f \vec{y} \rightarrow sk_f$$

1. Preparatory: get rid of $\vec{a}^{\perp}$

Private-Key, one-ct secure FE

$\text{Enc}(\text{msk}, (\vec{x}, \vec{y})) = \quad \forall i \in [n]: \; [\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1 \quad , \quad \forall j \in [m]: \; [\vec{b} s_j]_2 + [\vec{b} s y_j]_2 + [\vec{a}^{\perp} y_j]_2$

$pk = e\left([\vec{b}^{\perp}]_1 , [\vec{a}^{\perp}]_2 \right)$

1. Preparatory: get rid of $\vec{a}^{\perp}$

$s_j \rightarrow s_j + s y_j$

$\vec{x}^T f \vec{y} \rightarrow sk_f$

Private-Key, one-ct secure FE

$\text{Enc}(\text{msk}, (\vec{x}, \vec{y}))$ =

$\forall i \in [n]$: $[\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1$, $\forall j \in [m]$: $[\vec{b} s_j]_2 + y_j \left([\vec{b} s]_2 + [\vec{a}^{\perp}]_2 \right)$

$$pk = e\left([\vec{b}^{\perp}]_1 , [\vec{a}^{\perp}]_2 \right)$$

$$\vec{x}^T f \vec{y} \to sk_f$$

1. Preparatory: get rid of $\vec{a}^{\perp}$

$$s_j \to s_j + s y_j$$

Private-Key, one-ct secure FE

$$\mathrm{Enc}(\mathrm{msk}, (\vec{x}, \vec{y})) = \quad \forall i \in [n]: \; [\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1 \;,\quad \forall j \in [m]: \; [\vec{b} s_j]_2 + y_j \left([\vec{b} s]_2 + [\vec{a}^{\perp}]_2 \right)$$

$$pk = e\left([\vec{b}^{\perp}]_1 \,,\, \left([\vec{b} s]_2 + [\vec{a}^{\perp}]_2 \right) \right)$$

1. Preparatory: get rid of $\vec{a}^{\perp}$

$$\vec{b}^{\perp} \cdot \vec{b} = 0$$

$$\vec{x}^T f \vec{y} \rightarrow sk_f$$

Private-Key, one-ct secure FE

$\mathrm{Enc}(\mathrm{msk}, (\vec{x}, \vec{y})) = \forall i \in [n]: [\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1 \; , \; \forall j \in [m]: [\vec{b} s_j]_2 + y_j [\vec{u}]_2$

$pk = e\left([\vec{b}^{\perp}]_1, [\vec{u}]_2\right)$

$\vec{x}^T f \vec{y} \rightarrow sk_f$

1. Preparatory: get rid of $\vec{a}^{\perp}$

$[\vec{b}]_2, [\vec{a}^{\perp}]_2$ is a basis of $\mathbb{G}_2^2$

Private-Key, one-ct secure FE

$\forall i \in [n]$: $\forall j \in [m]$:

$\boxed{\text{Enc}(\text{msk}, (\vec{x}, \vec{y}))}$ = $[\vec{v_i}]_1$, $[\vec{b} s_j]_2 + y_j [\vec{u}]_2$

$pk = e\left([\vec{b}^{\perp}]_1, [\vec{u}]_2\right)$

$\vec{x}^T f \vec{y} \to sk_f$

1. Preparatory: get rid of $\vec{a}^{\perp}$
2. DDH in $\mathbb{G}_1$

Private-Key, one-ct secure FE

$\mathrm{Enc}(\mathrm{msk}, (\vec{x}, \vec{y})) =$ $\forall i \in [n]$: $[\vec{v_i}]_1$, $\forall j \in [m]$: $[\vec{b} s_j]_2 + y_j [\vec{u}]_2$

$pk = [\$]_T$

1. Preparatory: get rid of $\vec{a}^{\perp}$
2. DDH in $\mathbb{G}_1$

$\vec{x}^T f \vec{y} \to sk_f$

Private-Key, one-ct secure FE

$\mathrm{Enc}(\mathrm{msk}, (\vec{x}, \vec{y}))$ = $\forall i \in [n]$: $[\vec{v_i}]_1$, $\forall j \in [m]$: $[\vec{w_j}]_2$

$pk = [\$]_T$

1. Preparatory: get rid of $\vec{a}^{\perp}$
2. DDH in $\mathbb{G}_1$
3. DDH in $\mathbb{G}_2$

$\vec{x}^T f \vec{y} \rightarrow sk_f$

Public-Key FE

$$pk = \forall i, j: \quad [\vec{a} r_i]_1 \,,\; [\vec{b} s_j]_2 \,,\; [\vec{b}^{\perp}]_1 \,,\; [\vec{a}^{\perp}]_2$$

$$\text{Enc}(\text{pk}, (\vec{x}, \vec{y})) = \quad \forall i \in [n]: \; [\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1 \quad , \quad \forall j \in [m]: \; [\vec{b} s_j]_2 + [\vec{a}^{\perp} y_j]_2$$

$$sk_f = \sum_{i,j} \left(f_{i,j} \, e\left([\vec{a} r_i]_1 \,,\; [\vec{b} s_j]_2 \right) \right)$$

Public-Key FE

$pk = \forall i, j$: $[\vec{a} r_i]_1$, $[\vec{b} s_j]_2$, $[\vec{b}^{\perp}]_1$, $[\vec{a}^{\perp}]_2$

violates DDH

$\mathrm{Enc}(\mathrm{pk}, (\vec{x}, \vec{y}))$ = $\forall i \in [n]$: $[\vec{a} r_i]_1 + [\vec{b}^{\perp} x_i]_1$, $\forall j \in [m]$: $[\vec{b} s_j]_2 + [\vec{a}^{\perp} y_j]_2$

$$sk_f = \sum_{i,j} f_{i,j}\, e\left([\vec{a} r_i]_1 , [\vec{b} s_j]_2 \right)$$

Public-Key FE

$$pk = \forall i,j:\ [\vec{a}r_i]_1,\ [\vec{b}s_j]_2,\ [\vec{b}^{\perp}]_1,\ [\vec{a}^{\perp}]_2$$

$$\mathrm{Enc}(\mathrm{pk}, (\vec{x}, \vec{y})) = \forall i \in [n]:\ [\vec{a}r_i]_1 + [\vec{b}^{\perp}x_i]_1,\quad \forall j \in [m]:\ [\vec{b}s_j]_2 + [\vec{a}^{\perp}y_j]_2$$

$$sk_f = \sum_{i,j} f_{i,j}\, e\left([\vec{a}r_i]_1, [\vec{b}s_j]_2\right)$$

Dual bases:

$$[\vec{a}]_1,\ [\vec{b}^{\perp}]_1,\ [\vec{a}^{*}]_1$$

$$[\vec{b}]_2,\ [\vec{a}^{\perp}]_2,\ [\vec{b}^{*}]_2$$

Public-Key FE

DDH in $\mathbb{G}_1$

$$\left([\vec{a}]_1, [\vec{a}^{\perp}]_2, [\vec{a}r]_1 \right) \approx_c \left([\vec{a}]_1, [\vec{a}^{\perp}]_2, [\vec{a}r]_1 + [\vec{a}^* s]_1 \right)$$

for $r \leftarrow^R \mathbb{Z}_p$ for $r, s \leftarrow^R \mathbb{Z}_p$

Dual bases:

$[\vec{a}]_1, [\vec{b}^{\perp}]_1, [\vec{a}^*]_1$

$[\vec{b}]_2, [\vec{a}^{\perp}]_2, [\vec{b}^*]_2$

Public-Key FE

DDH in $\mathbb{G}_2$

$$\left([\vec{b}]_2 ,\ [\vec{b}^\perp]_1 ,\ [\vec{b}r]_2 \right) \approx_c \left([\vec{b}]_2 ,\ [\vec{b}^\perp]_1 ,\ [\vec{b}r]_2 + [\vec{b}^* s]_2 \right)$$

for $r \leftarrow^R \mathbb{Z}_p$ for $r, s \leftarrow^R \mathbb{Z}_p$

Dual bases:

$$[\vec{a}]_1 ,\ [\vec{b}^\perp]_1 ,\ [\vec{a}^*]_1$$

$$[\vec{b}]_2 ,\ [\vec{a}^\perp]_2 ,\ [\vec{b}^*]_2$$

Public-Key FE

$$pk = \forall i,j: \; [\vec{a}r_i]_1, \; [\vec{b}s_j]_2, \; [\vec{b}^{\perp}]_1, \; [\vec{a}^{\perp}]_2$$

$$\text{Enc}(\text{pk}, (\vec{x}, \vec{y})) = \quad \forall i \in [n]: \; [\vec{a}r_i]_1 + [\vec{b}^{\perp}x_i]_1 \quad , \quad \forall j \in [m]: \; [\vec{b}s_j]_2 + [\vec{a}^{\perp}y_j]_2$$

$$sk_f = \sum_{i,j} \left(f_{i,j} \, e\left([\vec{a}r_i]_1 , [\vec{b}s_j]_2 \right) \right)$$

Mix & match attacks

Public-Key FE

$$pk = \forall i,j: \; [\vec{a}r_i]_1, \; [\vec{b}s_j]_2, \; [\vec{b}^\perp]_1, \; [\vec{a}^\perp]_2$$

$$\mathrm{Enc}(\mathrm{pk}, (\vec{x}, \vec{y})) = \forall i \in [n]: \left([\vec{a}r_i]_1 + [\vec{b}^\perp x_i]_1\right) W^{-1}, \; \forall j \in [m]: W\left([\vec{b}s_j]_2 + [\vec{a}^\perp y_j]_2\right)$$

$$W \leftarrow^R GL_3$$

$$sk_f = \sum_{i,j} \left(f_{i,j} \, e\left([\vec{a}r_i]_1, [\vec{b}s_j]_2 \right) \right)$$

Mix & match attacks

Public-Key FE

$$pk = \forall i,j:\ [\vec{a}r_i]_1,\ [\vec{b}s_j]_2,\ [\vec{b}^{\perp}]_1,\ [\vec{a}^{\perp}]_2$$

$$\mathrm{Enc}(\mathrm{pk}, (\vec{x}, \vec{y})) = \forall i \in [n]: \left([\vec{a}r_i]_1 + [\vec{b}^{\perp}x_i]_1\right)W^{-1},\ \forall j \in [m]: W\left([\vec{b}s_j]_2 + [\vec{a}^{\perp}y_j]_2\right)$$

$$W \leftarrow^{R} GL_3$$

$$sk_f = \sum_{i,j} f_{i,j}\, e\left([\vec{a}r_i]_1, [\vec{b}s_j]_2\right)$$

!

sk_f can be computed from pk

Public-Key FE

$$pk = \forall i,j: \; [\vec{a} r_i]_1, \; [\vec{b} s_j]_2, \; [\vec{b}^{\perp}]_1, \; [\vec{a}^{\perp}]_2$$

$$\mathrm{Enc}(\mathrm{pk}, (\vec{x}, \vec{y})) = \forall i \in [n]: \left([\vec{a} r_i \gamma]_1 + [\vec{b} s_j]_1\right) W^{-1}, \; \forall j \in [m]: W\left([\vec{b} s_j \sigma]_2 + [\vec{a}^{\perp} y_j]_2\right), \; [\gamma\sigma]_2$$

$W \leftarrow^R GL_3$

$\gamma, \sigma \leftarrow^R \mathbb{Z}_p$

$$sk_f = \sum_{i,j} \left(f_{i,j} \, e\left([\vec{a} r_i]_1, [\vec{b} s_j]_2\right)\right)$$

sk_f can be computed from pk

Public-Key FE

$$pk = \forall i,j:\ [\vec{a} r_i]_1,\ [\vec{b} s_j]_2,\ [\vec{b}^{\perp}]_1,\ [\vec{a}^{\perp}]_2$$

$\forall i \in [n]$: $\qquad$ $\forall j \in [m]$:

$$\mathrm{Enc}(\mathrm{pk}, (\vec{x}, \vec{y})) = \left([\vec{a} r_i \gamma]_1 + [\vec{b} s_j]_1 \right) W^{-1},\ W \left([\vec{b} s_j \sigma]_2 + [\vec{a}^{\perp} y_j]_2 \right),\ [\gamma\sigma]_2$$

$W \leftarrow^R GL_3$

$\gamma, \sigma \leftarrow^R \mathbb{Z}_p$

f

$$sk_f = \sum_{i,j} \left(f_{i,j}\, e\left([\vec{a} r_i]_1, [\vec{b} s_j]_2 \right) \right)$$

$$\gamma\sigma \cdot sk_f + \vec{x}^T f \vec{y}\ \ e\left([\vec{b}^{\perp}]_1, [\vec{a}^{\perp}]_2 \right)$$

Public-Key FE

$$pk = \forall i,j: \quad \boxed{\vec{a} r_i}_1 , \quad \boxed{\vec{b} s_j}_2 , \quad \boxed{\vec{b}^{\perp}}_1 , \quad \boxed{\vec{a}^{\perp}}_2$$

$$\mathrm{Enc}(\mathrm{pk}, (\vec{x}, \vec{y})) = \quad \forall i \in [n]: \left(\boxed{\vec{a} r_i \gamma}_1 + \boxed{\vec{b} s_j}_1 \right) W^{-1}, \quad \forall j \in [m]: W \left(\boxed{\vec{b} s_j \sigma}_2 + \boxed{\vec{a}^{\perp} y_j}_2 \right), \quad \boxed{\gamma\sigma}_2$$

$$W \xleftarrow{R} GL_3$$

$$\gamma, \sigma \xleftarrow{R} \mathbb{Z}_p$$

$\Downarrow f$

$$sk_f = \sum_{i,j} \left(f_{i,j} \boxed{\vec{a} r_i \cdot \vec{b} s_j}_1 \right) \in \mathbb{G}_1$$

$$e\left(sk_f, \boxed{\gamma\sigma}_2\right) + \vec{x}^T f \vec{y} \; e\left(\boxed{\vec{b}^{\perp}}_1 , \boxed{\vec{a}^{\perp}}_2 \right)$$

Public-Key FE

$$pk = \forall i,j: \ [\vec{a}r_i]_1, \ [\vec{b}s_j]_2, \ [\vec{b}^\perp]_1, \ [\vec{a}^\perp]_2$$

$$\mathrm{Enc}(\mathrm{pk}, (\vec{x}, \vec{y})) = \forall i \in [n]: \left([\vec{a}r_i\gamma]_1 + [\vec{b}s_j]_1\right) W^{-1}, \ \forall j \in [m]: W\left([\vec{b}s_j\sigma]_2 + [\vec{a}^\perp y_j]_2\right), \ [\gamma\sigma]_2$$

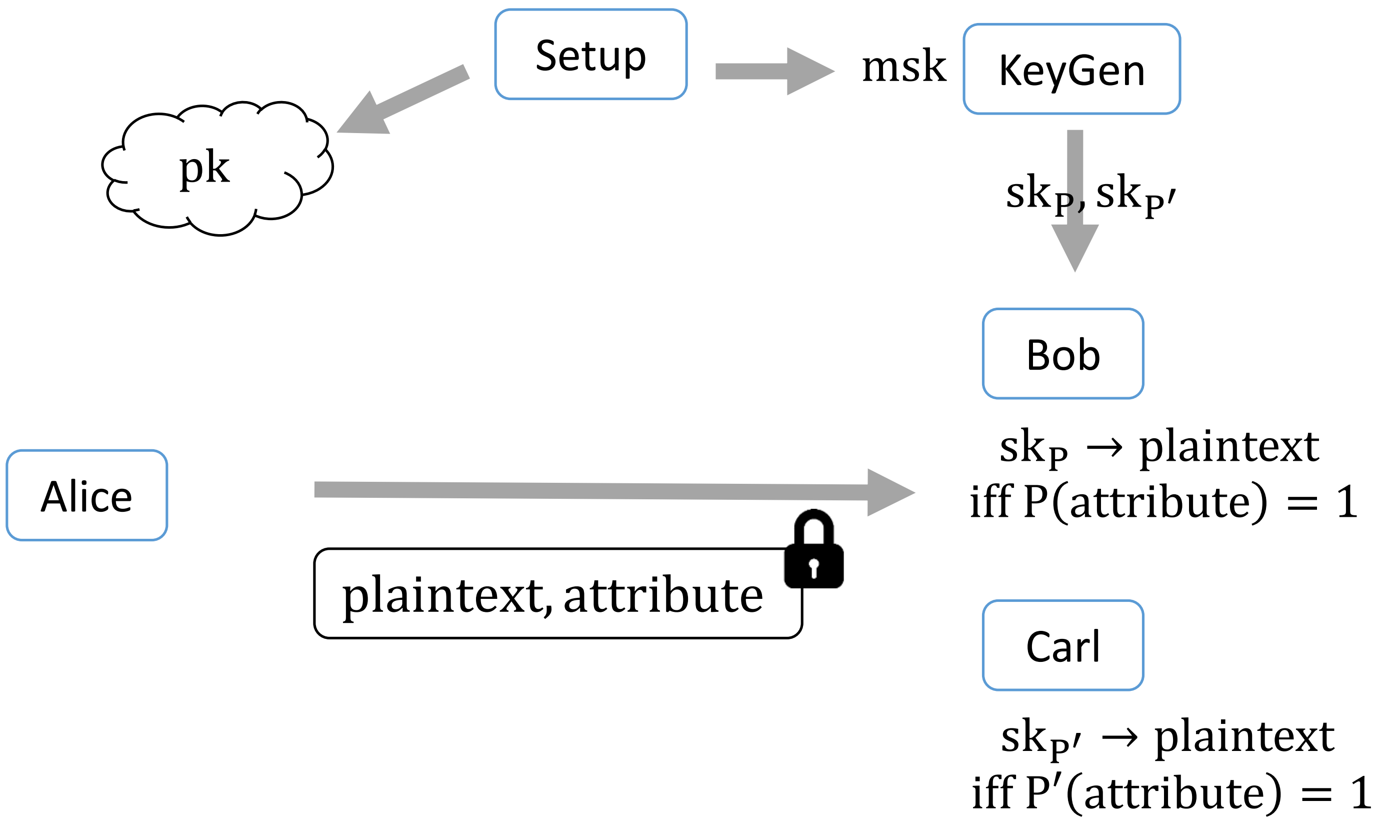
$$W \leftarrow^R GL_3$$

$$\gamma, \sigma \leftarrow^R \mathbb{Z}_p$$

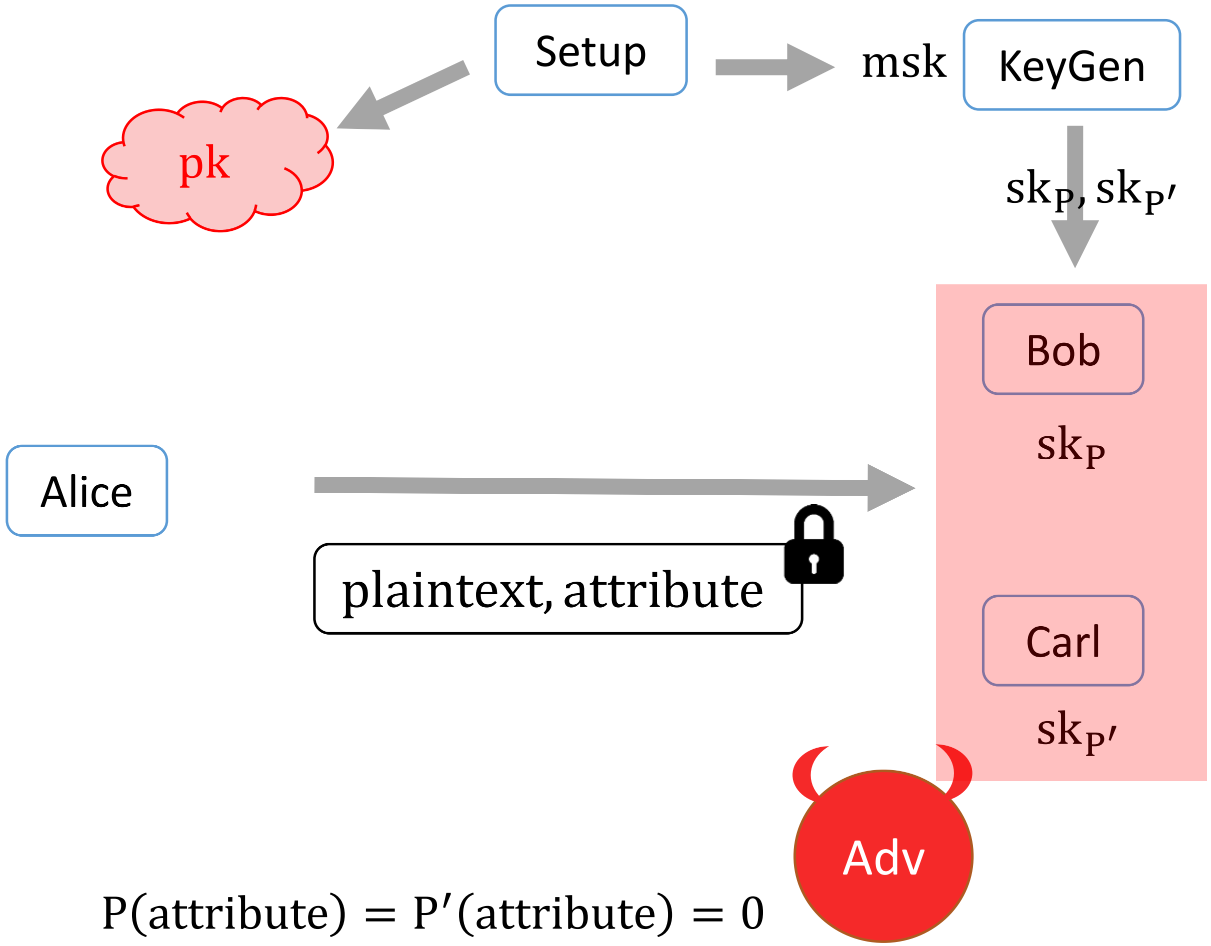
$$sk_f = \sum_{i,j} \left(f_{i,j} [\vec{a}r_i \cdot \vec{b}s_j]_1 \right) \in \mathbb{G}_1$$

$$msk = \forall i,j: [\vec{a}r_i \cdot \vec{b}s_j]_1 \in \mathbb{G}_1$$

PE [Boneh Waters 06;Katz, Sahai, Waters 08]

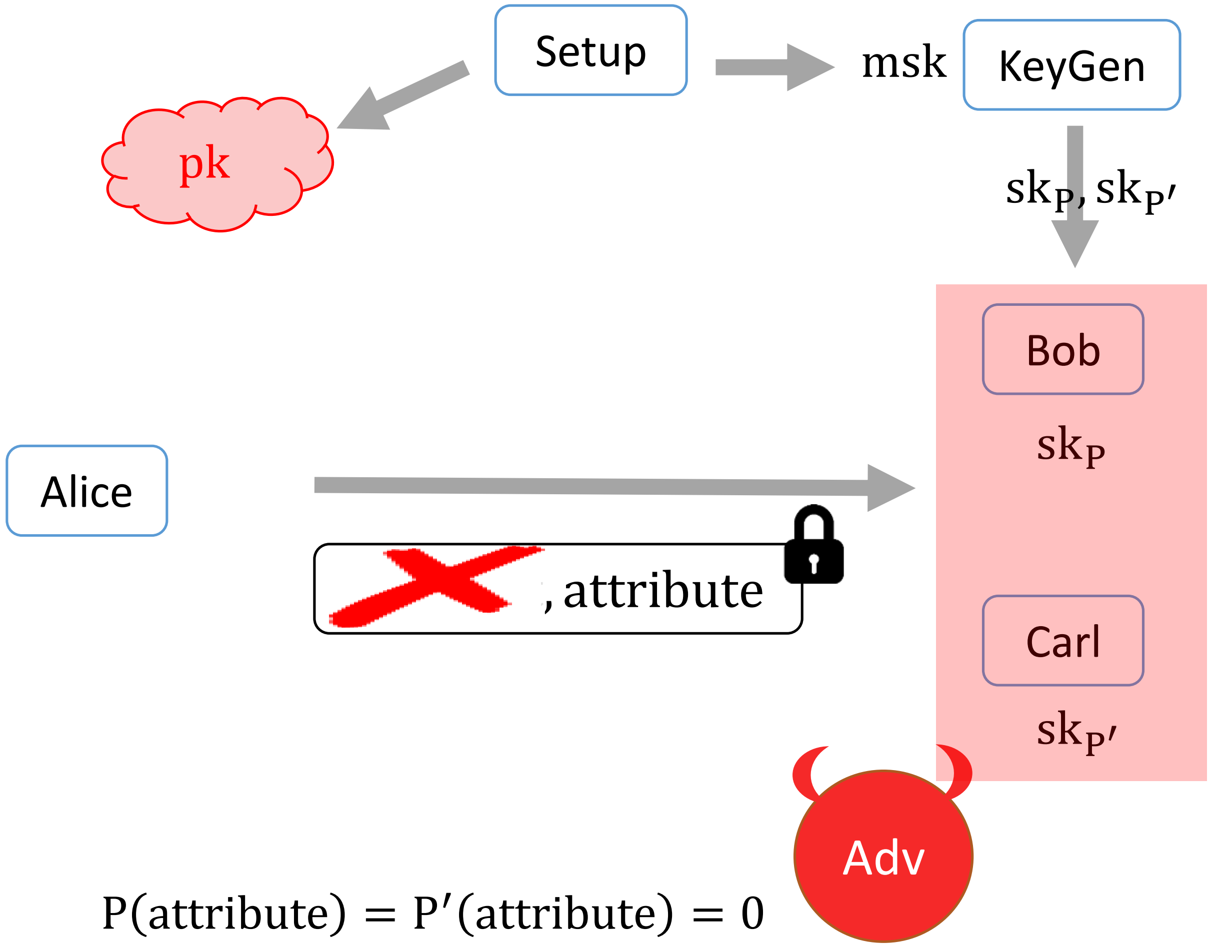


PE [Boneh Waters 06;Katz, Sahai, Waters 08]



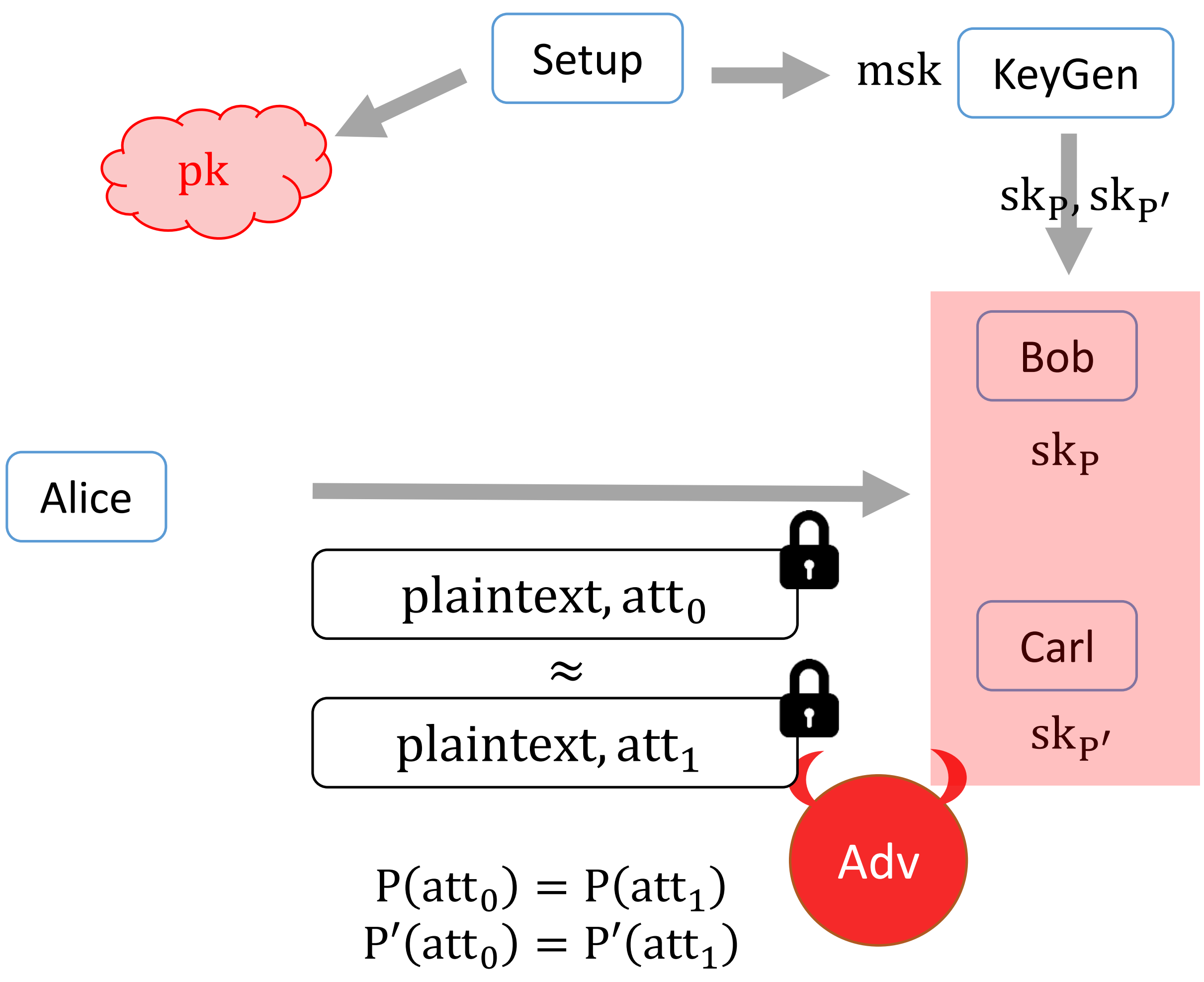
$P(\text{attribute}) = P'(\text{attribute}) = 0$

PE [Boneh Waters 06;Katz, Sahai, Waters 08]



$$\mathrm{P(attribute)} = \mathrm{P'(attribute)} = 0$$

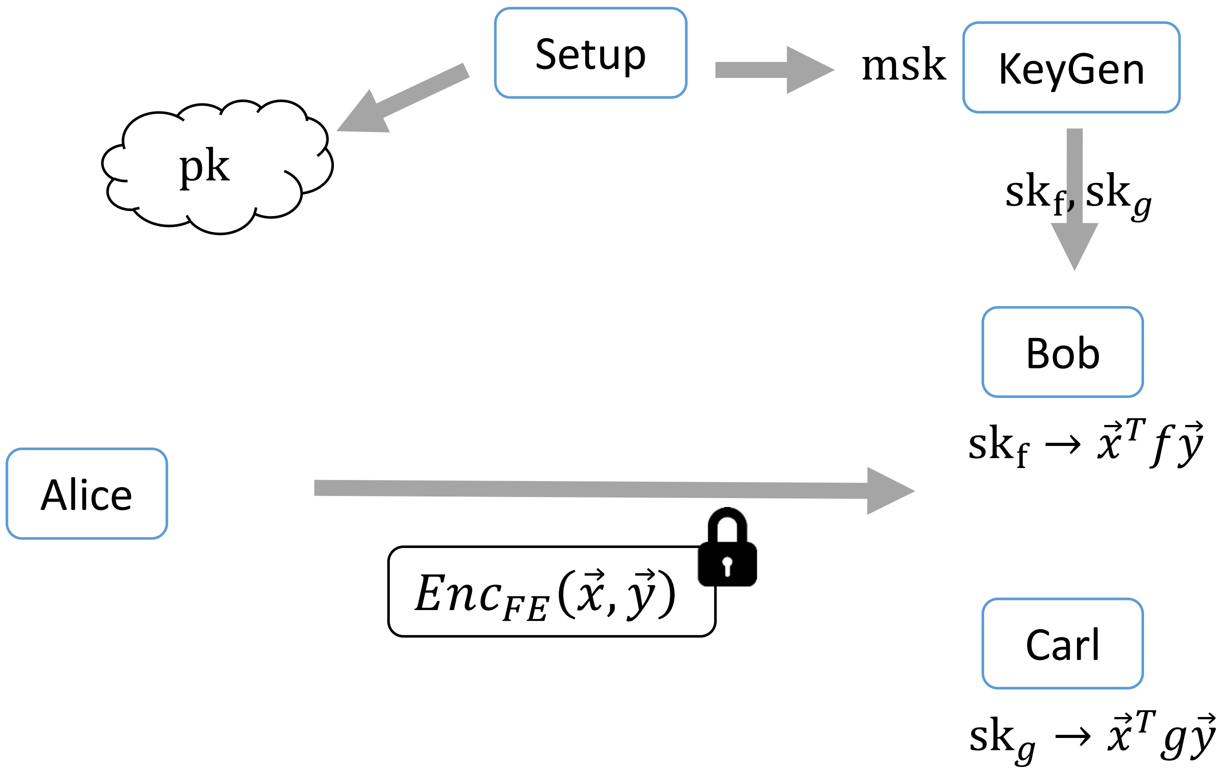
PE [Boneh Waters 06;Katz, Sahai, Waters 08]



PE for bilinear maps from FE

FE: $f \in \mathbb{Z}_p^{n\times m}, (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m$

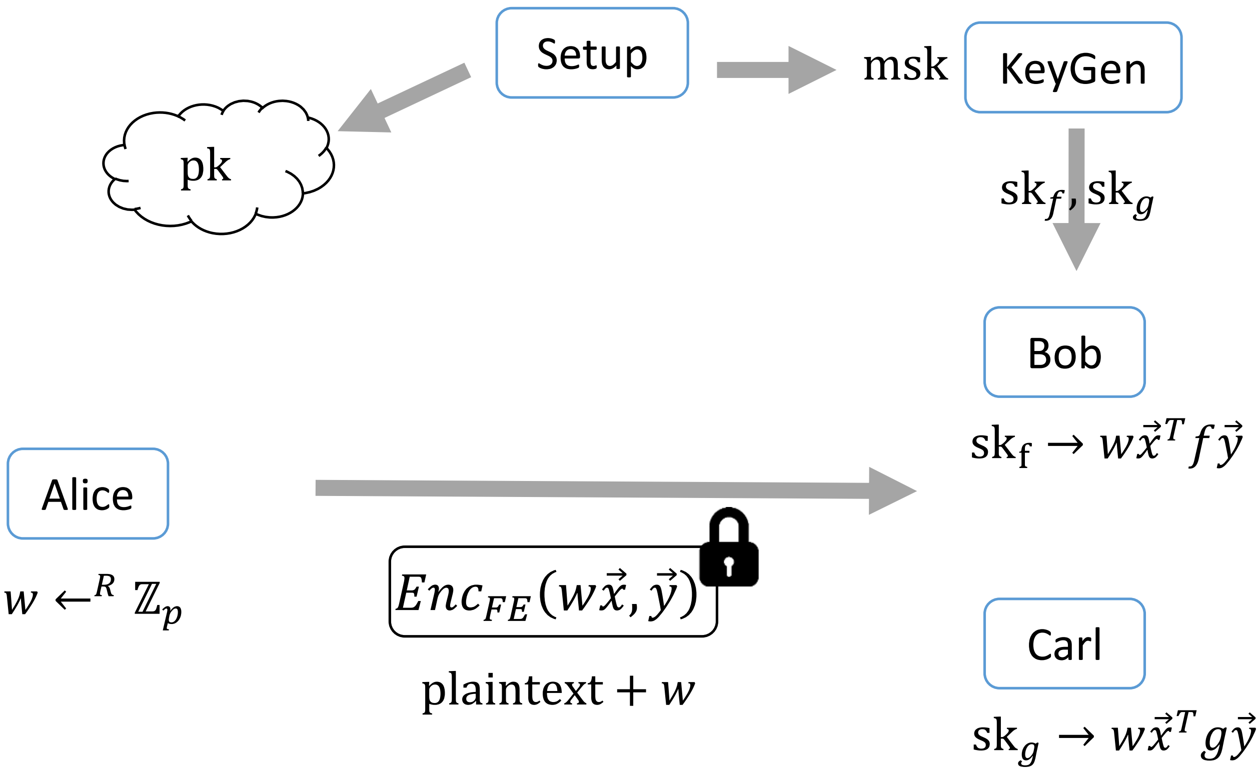
$$f(m) = \vec{x}^T f \vec{y} \in \mathbb{Z}_p$$



PE for bilinear maps from FE

PE: $P: \mathbb{Z}_p^n \times \mathbb{Z}_p^m \to \{0,1\},\ P(\vec{x},\vec{y}) = 1 \text{ iff } \vec{x}^T f \vec{y} = 1$

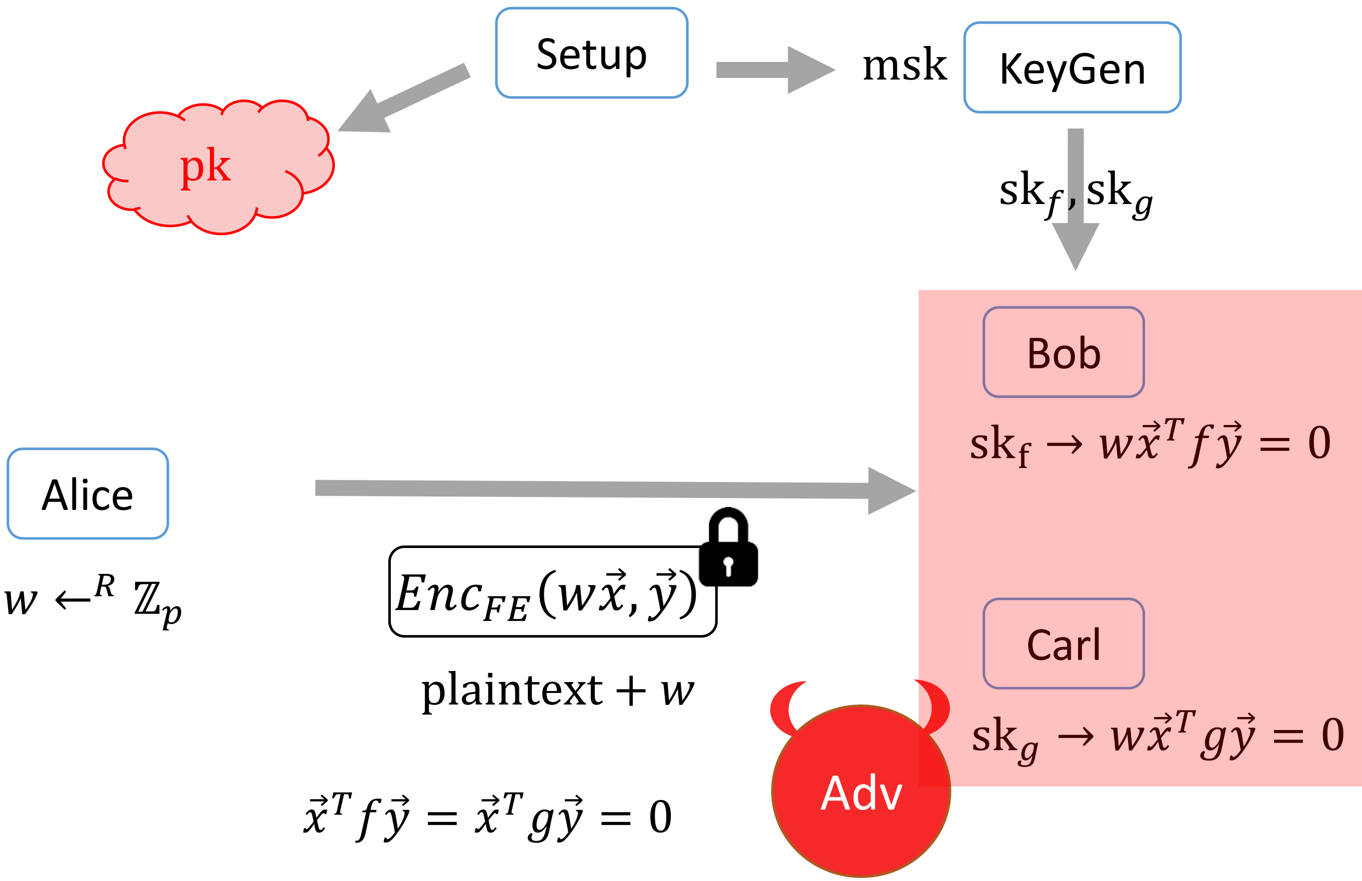
For $f \in \mathbb{Z}_p^{n\times m}, (\vec{x},\vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m$ such that $\vec{x}^T f \vec{y} \in \{0,1\}$



PE for bilinear maps from FE

PE: $P: \mathbb{Z}_p^n \times \mathbb{Z}_p^m \rightarrow \{0,1\},\ P(\vec{x}, \vec{y}) = 1 \text{ iff } \vec{x}^T f \vec{y} = 1$

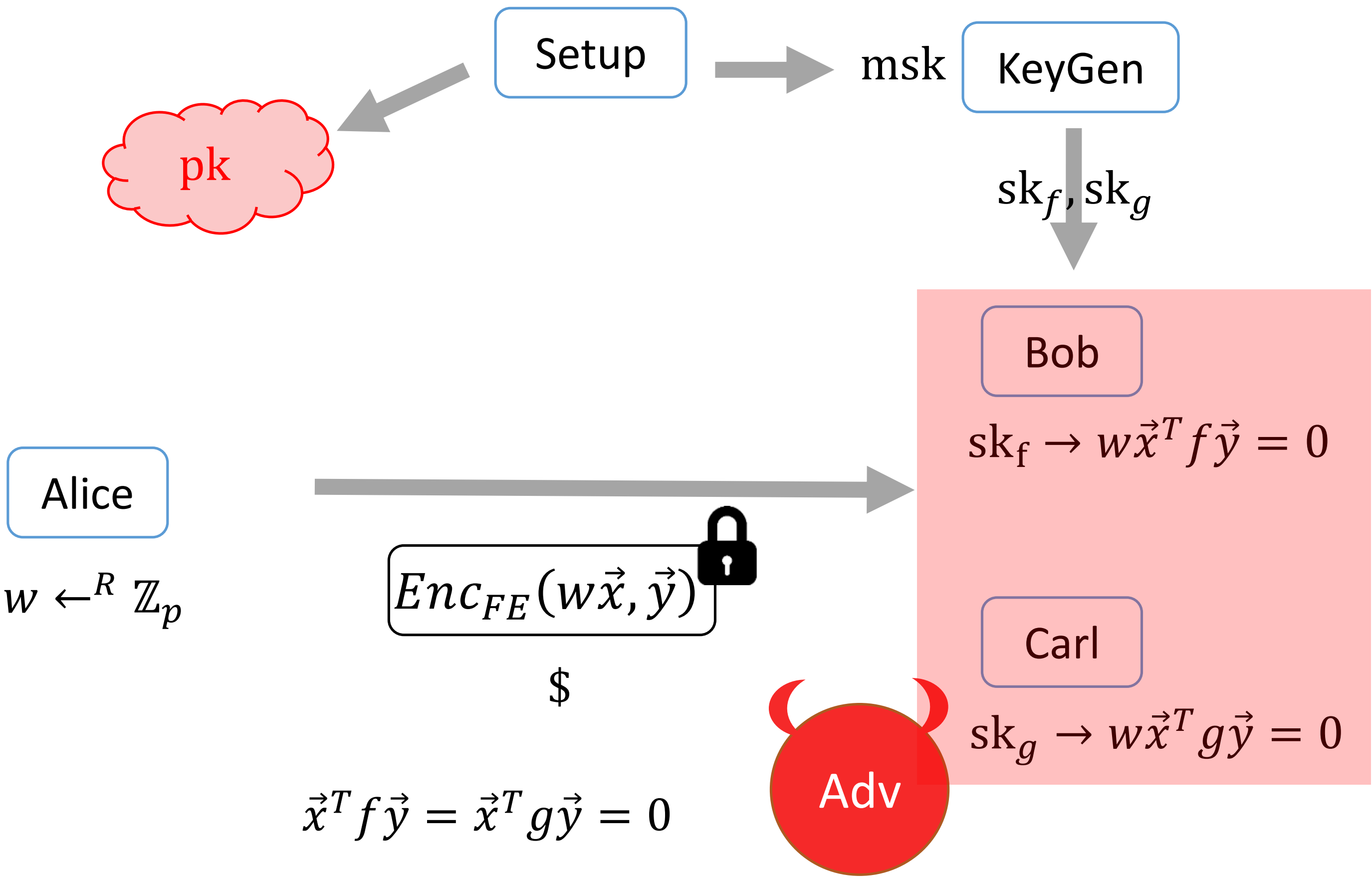
For $f \in \mathbb{Z}_p^{n \times m}, (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m$ such that $\vec{x}^T f \vec{y} \in \{0,1\}$



PE for bilinear maps from FE

PE: $P\colon \mathbb{Z}_p^n \times \mathbb{Z}_p^m \to \{0,1\},\ P(\vec{x},\vec{y}) = 1 \text{ iff } \vec{x}^T f \vec{y} = 1$

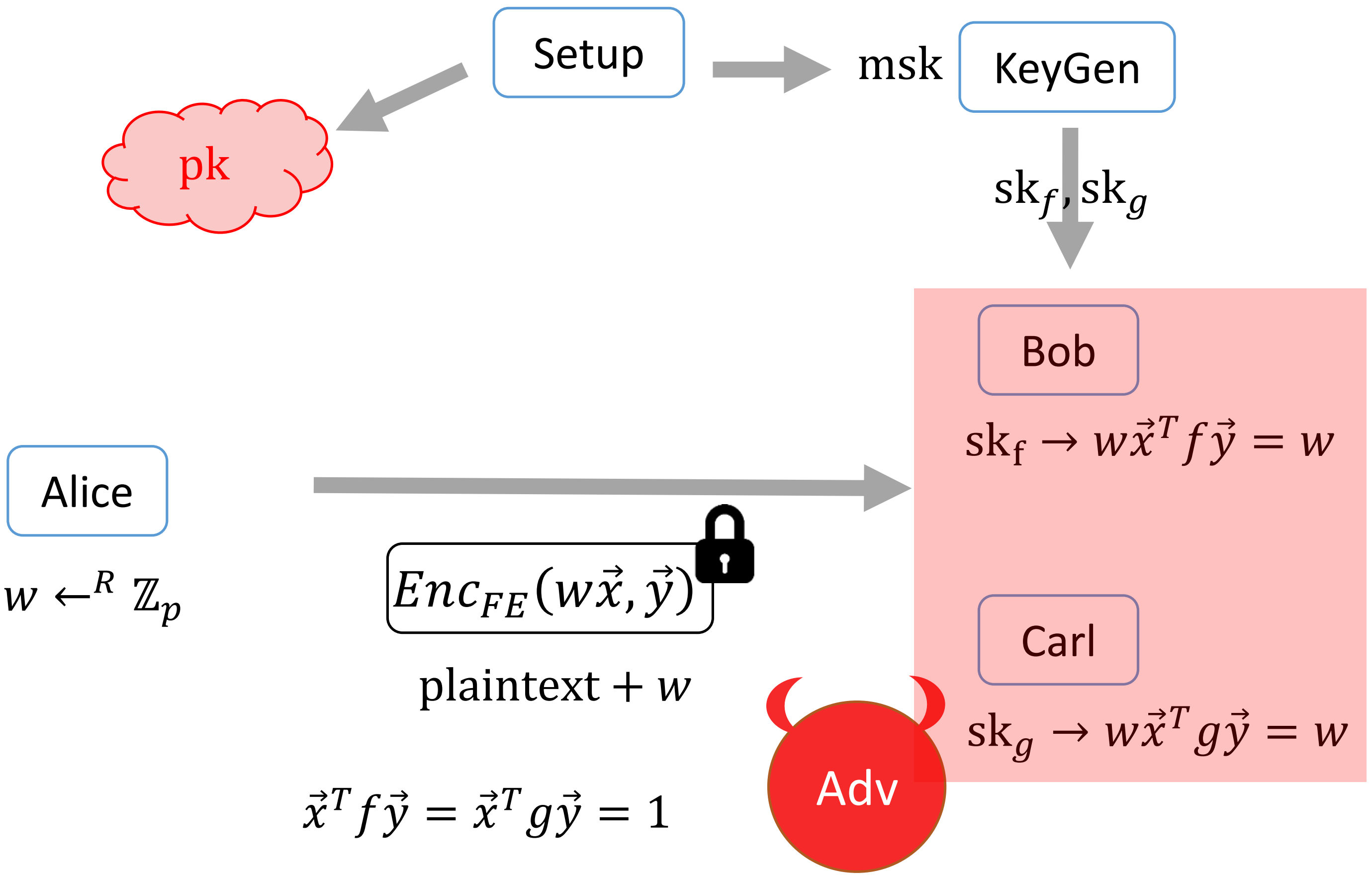
For $f \in \mathbb{Z}_p^{n\times m}, (\vec{x},\vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m$ such that $\vec{x}^T f \vec{y} \in \{0,1\}$



PE for bilinear maps from FE

PE: $P\colon \mathbb{Z}_p^n \times \mathbb{Z}_p^m \to \{0,1\},\ P(\vec{x},\vec{y}) = 1 \text{ iff } \vec{x}^T f \vec{y} = 1$

For $f \in \mathbb{Z}_p^{n\times m}, (\vec{x},\vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m$ such that $\vec{x}^T f \vec{y} \in \{0,1\}$



PE for constant depth boolean formulas

PE: $P: \{0,1\}^n \to \{0,1\}$, of constant degree $d \ll n$

- [KSW 08]:

$$\vec{x} \in \{0,1\}^n \to \vec{x}' = \begin{pmatrix} x_1 \\ x_1 x_2 \\ \dots \\ x_1 \dots x_d \\ \dots \end{pmatrix} \in \mathbb{Z}_p^{d'}, d' = \sum_{i=0}^{d} \binom{n}{i} \sim n^d$$

$$P = \sum_{j=1}^{d'} \mathrm{p_j} \cdot \mathrm{Monomial_j} \to \vec{y} = \begin{pmatrix} p_1 \\ \dots \\ p_{d'} \end{pmatrix} \in \mathbb{Z}_p^{d'}$$

$$P(\vec{x}) = 1 \text{ iff } \langle \vec{x}', \vec{y} \rangle = 1$$

PE for constant depth boolean formulas

PE: $P: \{0,1\}^n \rightarrow \{0,1\}$, of constant degree $d \ll n$

- [This work]:

$$\vec{x} \in \{0,1\}^n \rightarrow \vec{x}' = \begin{pmatrix} x_1 \\ x_1 x_2 \\ \dots \\ x_1 \dots x_{\frac{d}{2}} \\ \dots \end{pmatrix}, \vec{y}' = \begin{pmatrix} x_1 \\ x_1 x_2 \\ \dots \\ x_1 \dots x_{\frac{d}{2}} \\ \dots \end{pmatrix} \in \mathbb{Z}_p^{d'}, d' = \sum_{i=0}^{d/2} \binom{n}{i} \sim n^{d/2}$$

$$P = \sum_{i,j=1}^{d'} \mathrm{p_{i,j}} \cdot \mathrm{Monomial_{i,j}} \rightarrow \begin{pmatrix} p_{1,1} & \cdots & p_{1,d'} \\ \vdots & \ddots & \vdots \\ p_{d',1} & \cdots & p_{d',d'} \end{pmatrix} \in \mathbb{Z}_p^{d' \times d'}$$

$$P(\vec{x}) = 1 \text{ iff } \vec{x}'^T f \vec{y}' = 1$$

PE for constant depth boolean formulas

PE: $P\colon \{0,1\}^n \to \{0,1\}$, of constant degree $d \ll n$

- [This work]:

$$\vec{x} \in \{0,1\}^n \to \vec{x}' = \begin{pmatrix} x_1 \\ x_1 x_2 \\ \dots \\ x_1 \dots x_{\frac{d}{2}} \\ \dots \end{pmatrix}, \vec{y}' = \begin{pmatrix} x_1 \\ x_1 x_2 \\ \dots \\ x_1 \dots x_{\frac{d}{2}} \\ \dots \end{pmatrix} \in \mathbb{Z}_p^{d'}, d' = \sum_{i=0}^{d/2} \binom{n}{i} \sim n^{d/2}$$

$$P = \sum_{i,j=1}^{d'} \mathrm{p_{i,j}} \cdot \mathrm{Monomial_{i,j}} \to \begin{pmatrix} p_{1,1} & \cdots & p_{1,d'} \\ \vdots & \ddots & \vdots \\ p_{d',1} & \cdots & p_{d',d'} \end{pmatrix} \in \mathbb{Z}_p^{d' \times d'}$$

$$P(\vec{x}) = 1 \text{ iff } \vec{x}'^T f \vec{y}' = 1$$

Ct size: [KSW 08]$\sim n^d$ vs [this work]:$\sim n^{d/2}$