

Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption

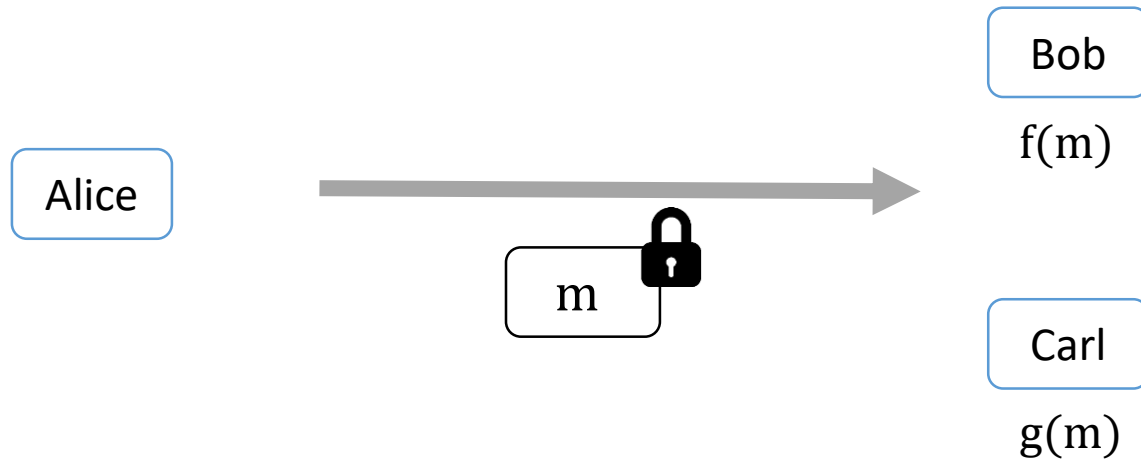
Carmen Elisabetta Zaira Baltico, Università di Catania

Dario Catalano, Università di Catania

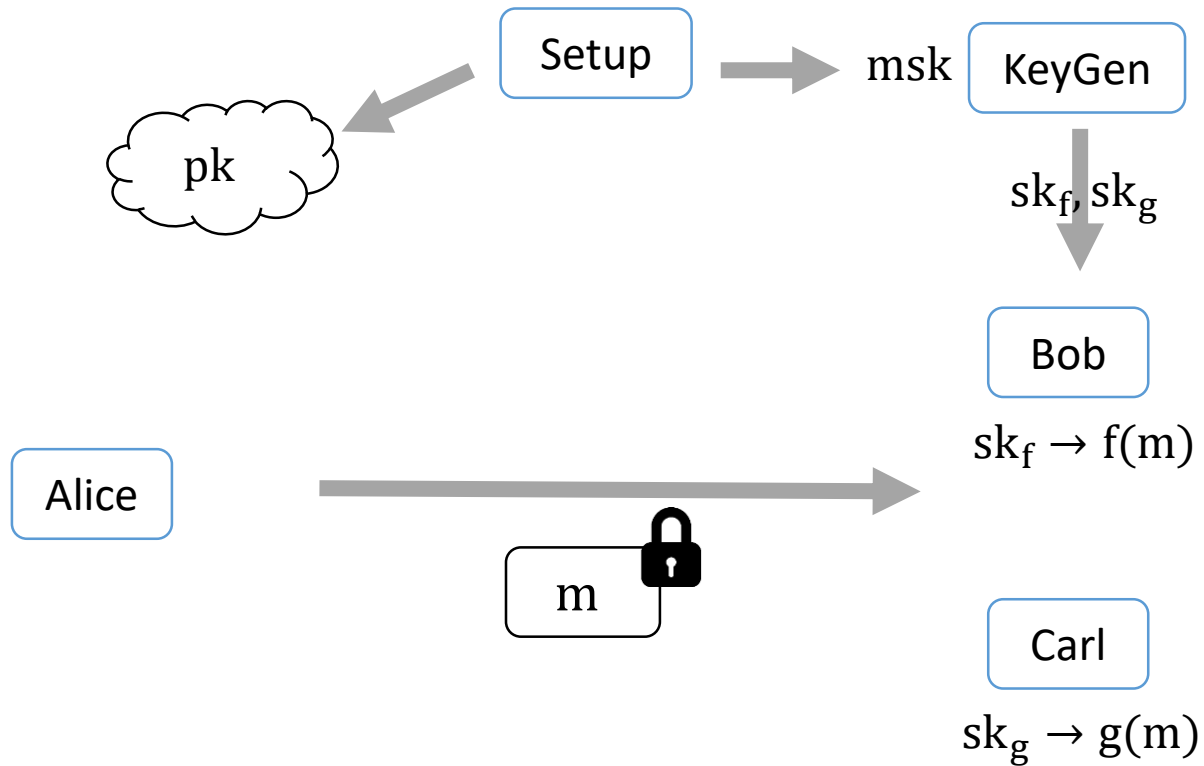
Dario Fiore, IMDEA

Romain Gay, ENS

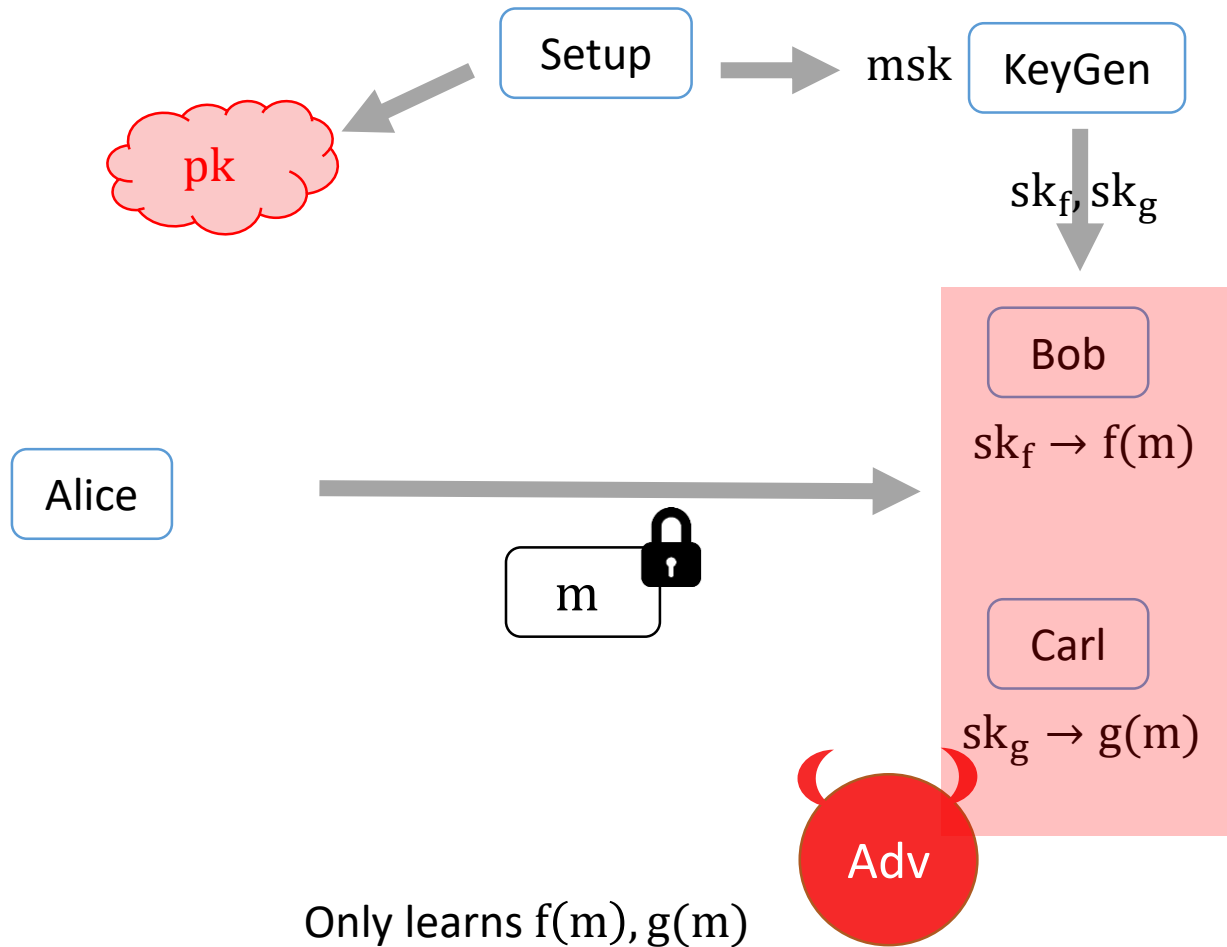
FE [Boneh, Sahai, Waters 11]



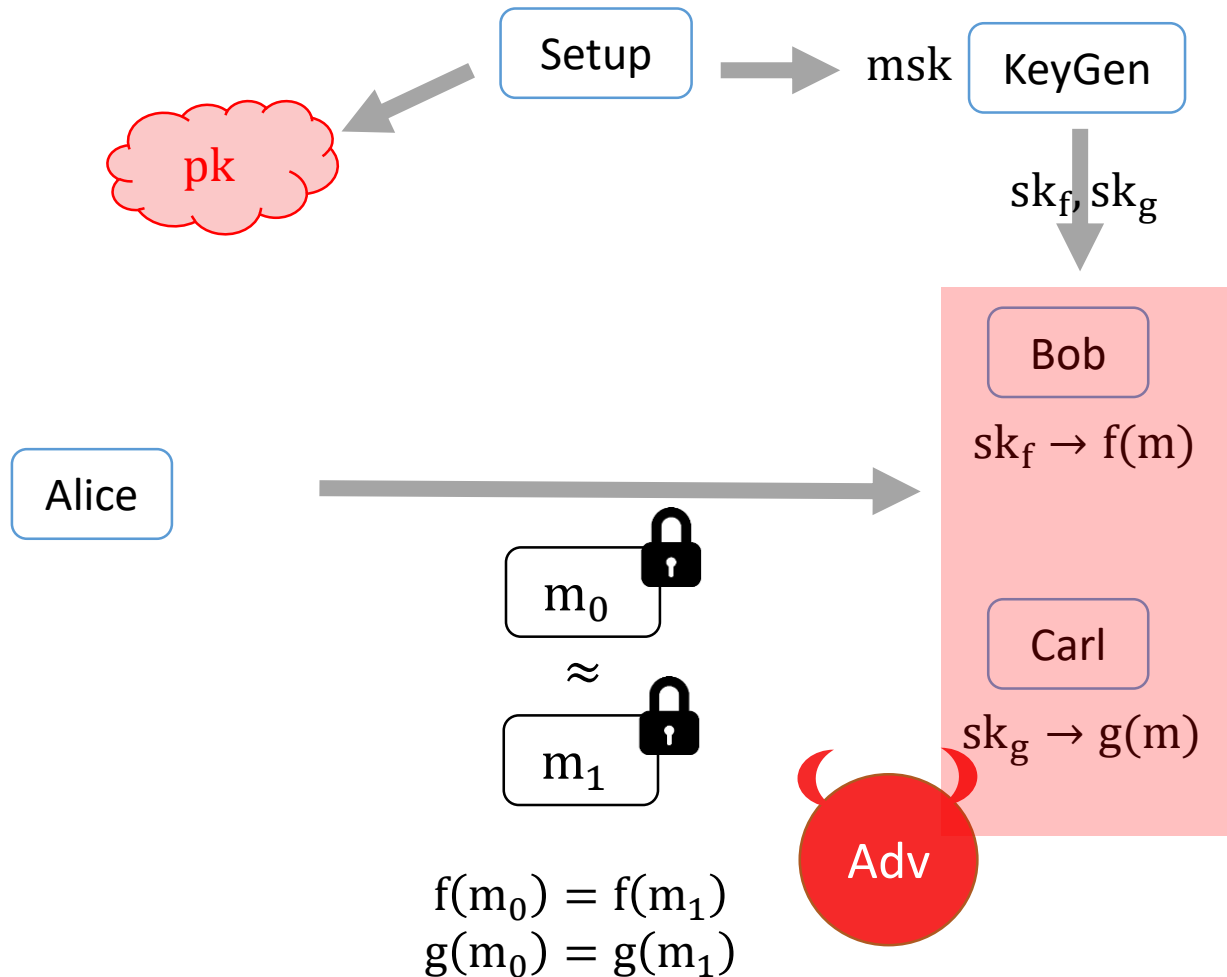
FE [Boneh, Sahai, Waters 11]





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 = $O(n)$

Prior works on FE

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

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

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




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



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

vs

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

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

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

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

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

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

$\forall id' \in \{0,1\}^n: sk_{id'} \rightarrow P(id) = 1$ iff $id = id'$

Prior works on Predicate Encryption

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

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

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

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

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

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

Prior works on Predicate Encryption

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

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

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

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

ct size = $O(n + m)$

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

vs

ct size = $O(n \cdot m)$

Prior works on Predicate Encryption

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

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

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

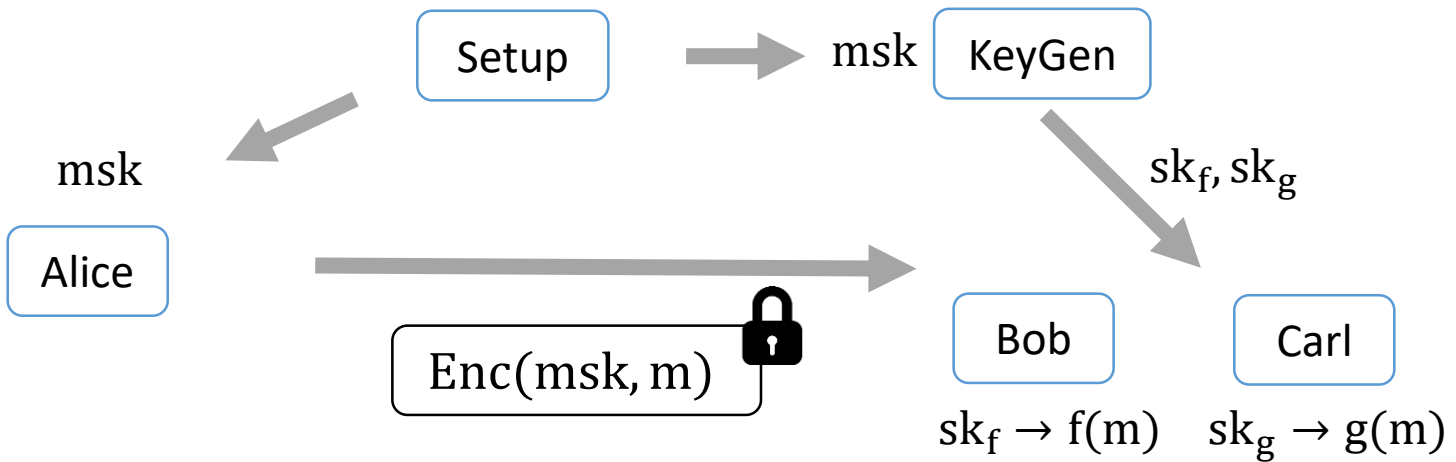
- Private-Key, one-ct secure FE
- Public-Key FE

Outline

1

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

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

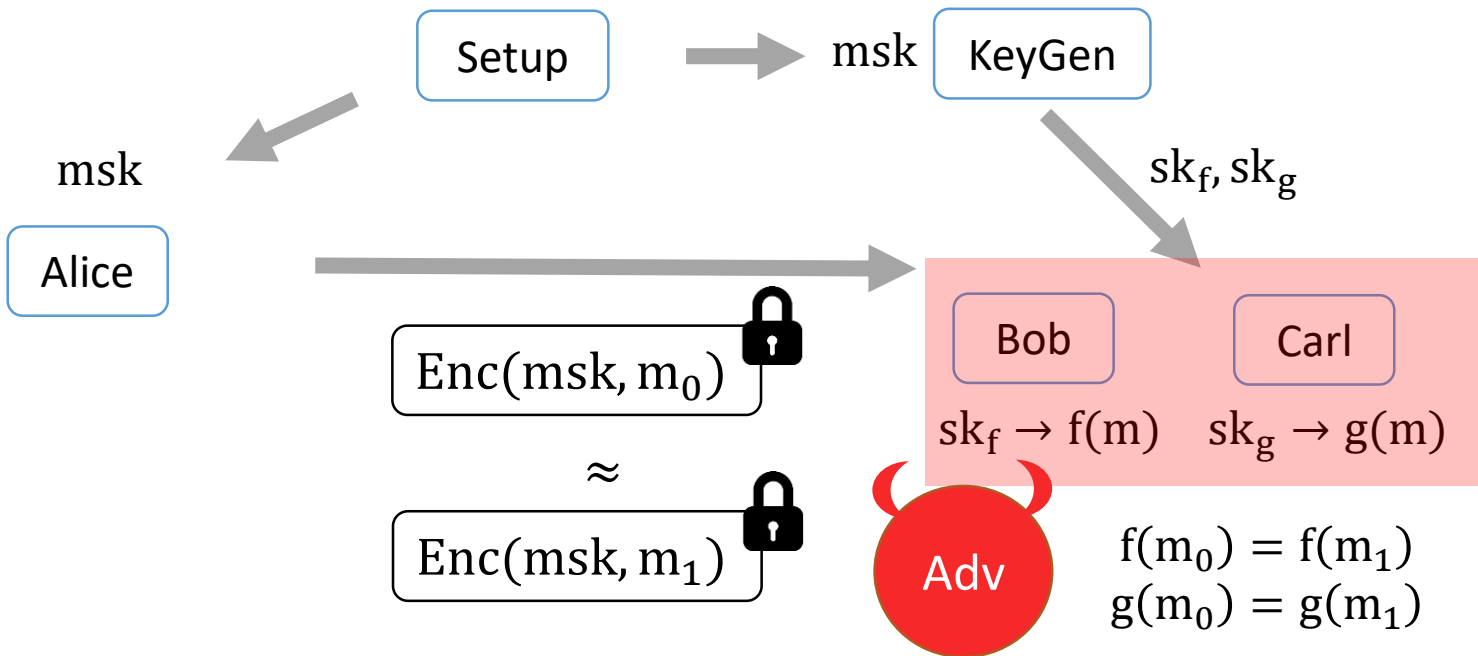


Outline

1

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

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



Outline

1

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

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

Outline

1

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

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

2

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

Private-Key, one-ct secure FE

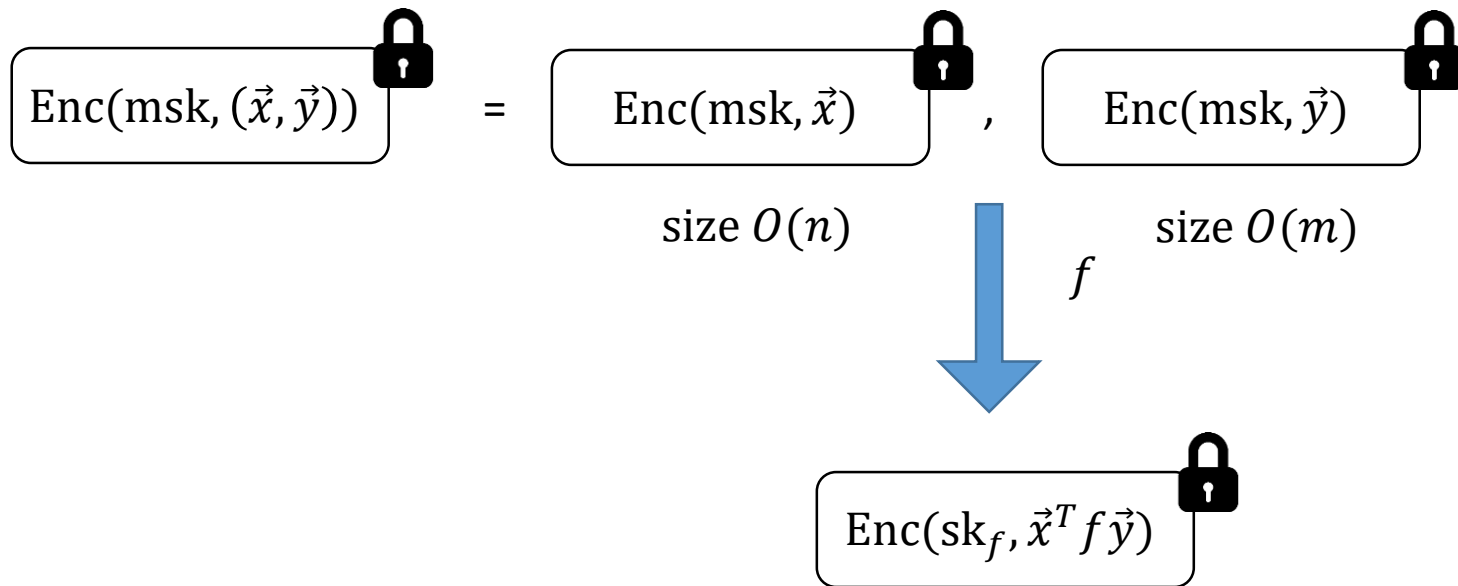
$$\text{FE } f: (\vec{x}, \vec{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m \rightarrow \vec{x}^T f \vec{y} \in \mathbb{Z}_p$$

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

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

Private-Key, one-ct secure FE

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



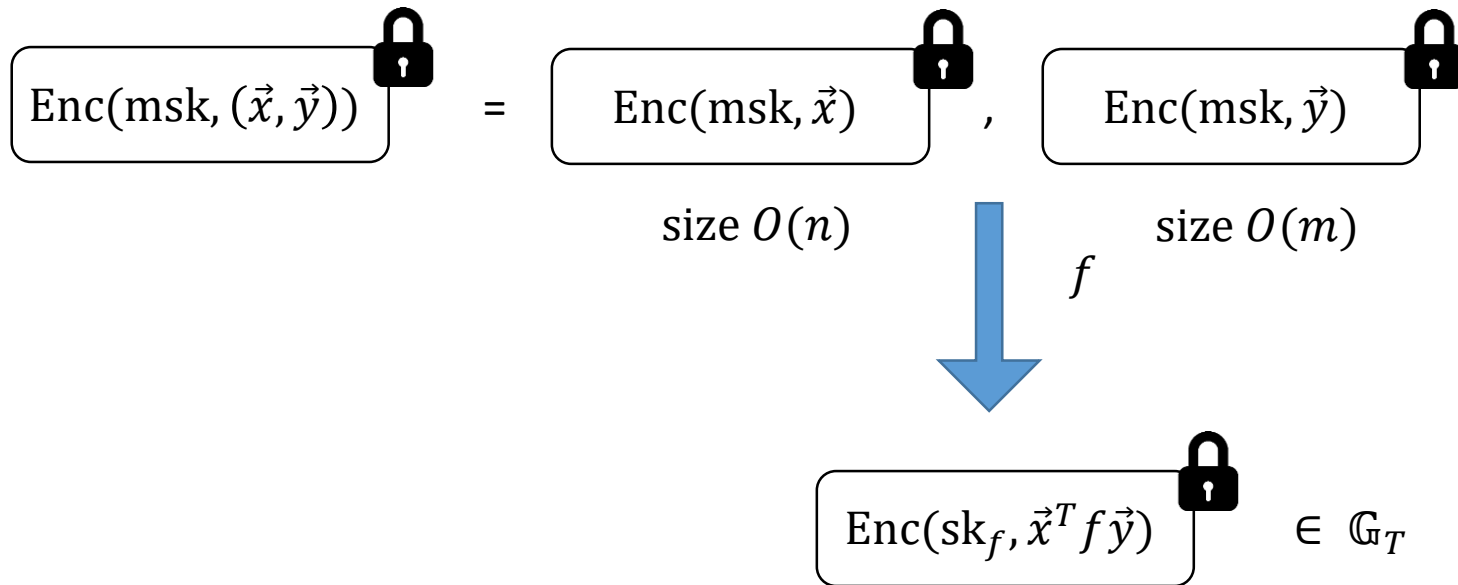
Private-Key, one-ct secure FE

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

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

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

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



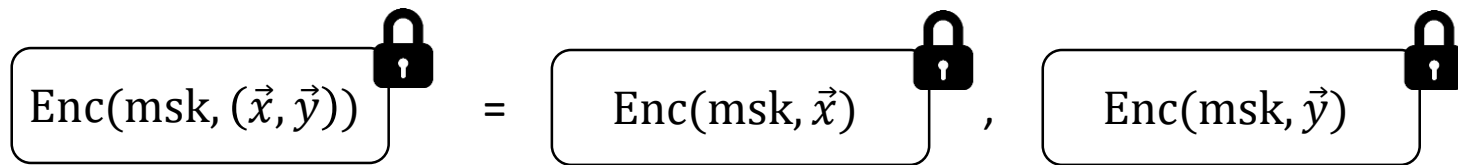
Private-Key, one-ct secure FE

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

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

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

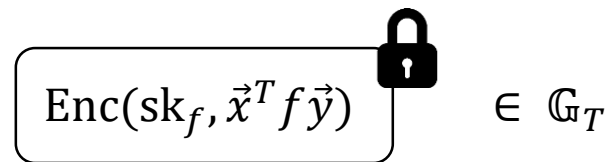
$$\mathbb{G}_1 \quad \times \quad \mathbb{G}_2$$



$$e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

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

$$= ab P_T$$

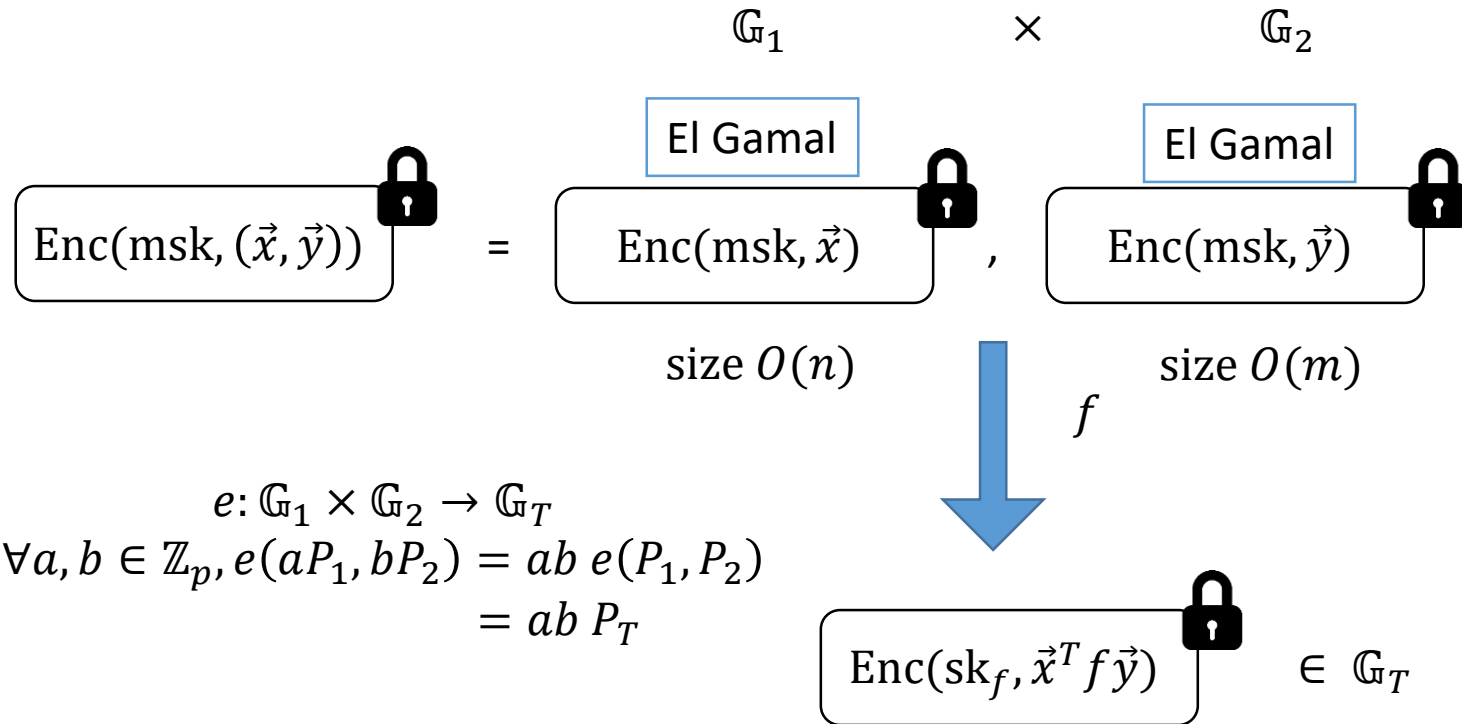


Private-Key, one-ct secure FE

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

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

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



El Gamal

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

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

El Gamal

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

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

$$\text{Security: } \left(\begin{array}{l} \boxed{\vec{a}}_1, \quad \boxed{\vec{a}r}_1 \\ \text{for } r \leftarrow^R \mathbb{Z}_p \end{array} \right) \underset{\text{DDH in } \mathbb{G}_1}{\approx_c} \left(\begin{array}{l} \boxed{\vec{a}}_1, \quad \boxed{\vec{v}}_1 \\ \text{for } \vec{v} \leftarrow^R \mathbb{Z}_p^2 \end{array} \right)$$

El Gamal

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

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

$$\text{Security: } \left(\begin{array}{l} \boxed{\vec{a}}_1, \quad \boxed{\vec{a}r}_1 \end{array} \right) \underset{\text{DDH in } \mathbb{G}_1}{\approx_c} \left(\begin{array}{l} \boxed{\vec{a}}_1, \quad \boxed{\vec{v}}_1 \end{array} \right)$$

for $r \leftarrow^R \mathbb{Z}_p$ for $\vec{v} \leftarrow^R \mathbb{Z}_p^2$

El Gamal

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

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

$$\text{Correctness: } \left(\begin{array}{c} \boxed{\vec{a}}_1, \quad \boxed{\vec{u}}_1 \end{array} \right) \text{ is a basis of } \mathbb{G}_1^2$$

El Gamal

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

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

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

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

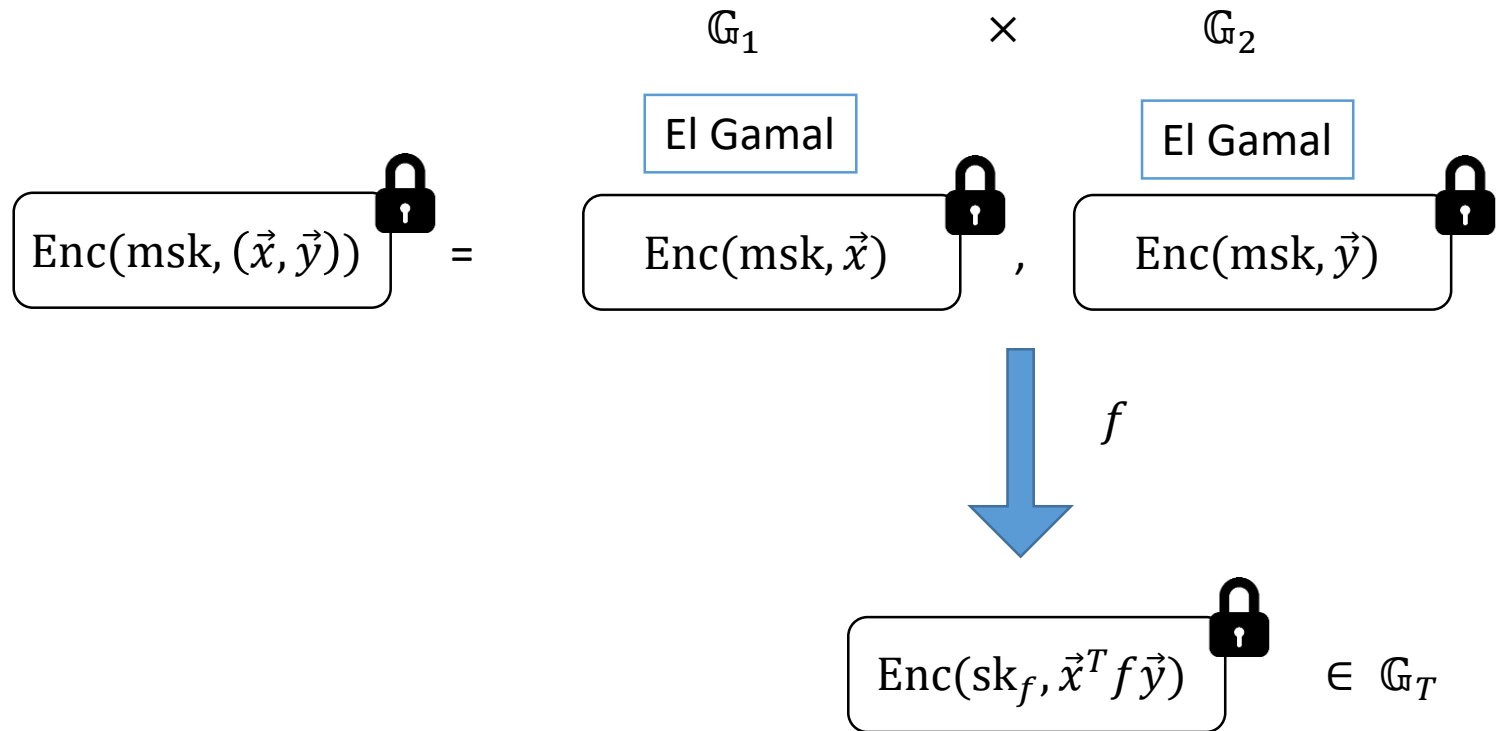
El Gamal

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

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

$$sk = \vec{a}^\perp \quad Dec: \left(\begin{array}{l} \boxed{\vec{a}r} \\ \cdot \vec{a}^\perp \end{array} \right)_1 + \left(\begin{array}{l} \boxed{\vec{u}m} \\ \cdot \vec{a}^\perp \end{array} \right)_1 = \boxed{m}_1 \in \mathbb{G}_1$$

Private-Key, one-ct secure FE



Private-Key, one-ct secure FE

$$\text{Enc}(\text{msk}, (\vec{x}, \vec{y})) \quad \text{🔒} = e \left(\begin{array}{c} \boxed{\vec{a}r_i}_1 + \boxed{\vec{u}x_i}_1 \\ \boxed{\vec{b}s_j}_2 + \boxed{\vec{v}y_j}_2 \end{array} \right)$$



$$e \left(\begin{array}{c} \boxed{\vec{a}r_i}_1 \\ \boxed{\vec{b}s_j}_2 \end{array} \right) + e \left(\begin{array}{c} \boxed{\vec{a}r_i}_1 \\ \boxed{\vec{v}y_j}_2 \end{array} \right) + e \left(\begin{array}{c} \boxed{\vec{u}x_i}_1 \\ \boxed{\vec{b}s_j}_2 \end{array} \right) + e \left(\begin{array}{c} \boxed{\vec{u}x_i}_1 \\ \boxed{\vec{v}y_j}_2 \end{array} \right)$$

Private-Key, one-ct secure FE

$$msk = \forall i, j: \begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix}$$

$$\text{Enc}(msk, (\vec{x}, \vec{y})) \quad \text{🔒} = e \left(\begin{matrix} \boxed{\vec{a}r_i} + \boxed{\vec{u}x_i} \\ 1 \quad 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} + \boxed{\vec{v}y_j} \\ 2 \quad 2 \end{matrix} \right)$$



$$e \left(\begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix} \right) + e \left(\begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{v}y_j} \\ 2 \end{matrix} \right) + e \left(\begin{matrix} \boxed{\vec{u}x_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix} \right) + e \left(\begin{matrix} \boxed{\vec{u}x_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{v}y_j} \\ 2 \end{matrix} \right)$$

$$= sk_{x_i y_j}$$

Private-Key, one-ct secure FE

$$msk = \forall i, j: \begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix}$$

$$\text{Enc}(msk, (\vec{x}, \vec{y})) = e \left(\begin{matrix} \boxed{\vec{a}r_i} + \boxed{\vec{b}^\perp x_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} + \boxed{\vec{a}^\perp y_j} \\ 2 \end{matrix} \right)$$

Dual bases: $\begin{matrix} \boxed{\vec{a}} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}^\perp} \\ 1 \end{matrix} \quad \begin{matrix} \boxed{\vec{b}} \\ 2 \end{matrix}, \begin{matrix} \boxed{\vec{a}^\perp} \\ 2 \end{matrix}$

$$e \left(\begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix} \right) + e \left(\begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{a}^\perp y_j} \\ 2 \end{matrix} \right) + e \left(\begin{matrix} \boxed{\vec{b}^\perp x_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix} \right) + e \left(\begin{matrix} \boxed{\vec{b}^\perp x_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{a}^\perp y_j} \\ 2 \end{matrix} \right)$$

$= sk_{x_i y_j}$

Private-Key, one-ct secure FE

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

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

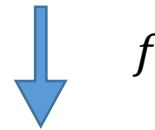


$$e \left(\boxed{\vec{a}r_i}_1, \boxed{\vec{b}s_j}_2 \right) + e \left(\boxed{\vec{b}^\perp x_i}_1, \boxed{\vec{a}^\perp y_j}_2 \right) \\ = sk_{x_i y_j}$$

Private-Key, one-ct secure FE

$$msk = \forall i, j: \begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix}$$

$$\text{Enc}(msk, (\vec{x}, \vec{y})) \quad \text{🔒} = \begin{matrix} \forall i \in [n]: \\ \boxed{\vec{a}r_i} \\ 1 \end{matrix} + \begin{matrix} \boxed{\vec{b}^\perp x_i} \\ 1 \end{matrix}, \begin{matrix} \forall j \in [m]: \\ \boxed{\vec{b}s_j} \\ 2 \end{matrix} + \begin{matrix} \boxed{\vec{a}^\perp y_j} \\ 2 \end{matrix}$$



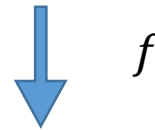
$$\sum_{i,j} f_{i,j} e \left(\begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix} \right) + \sum_{i,j} f_{i,j} e \left(\begin{matrix} \boxed{\vec{b}^\perp x_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{a}^\perp y_j} \\ 2 \end{matrix} \right)$$

$= sk_f$

Private-Key, one-ct secure FE

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

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



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

$= sk_f$

Private-Key, one-ct secure FE

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

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

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



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

$= sk_f$

Private-Key, one-ct secure FE

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

$\forall i \in [n]:$

$\forall j \in [m]:$

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

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

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

Private-Key, one-ct secure FE

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

$$\forall i \in [n]: \quad \vec{a}r_i \quad + \quad \vec{b}^\perp x_i \quad , \quad \forall j \in [m]: \quad \vec{b}s_j \quad + \quad \vec{a}^\perp y_j$$

$\begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}$
 $\begin{matrix} \boxed{\vec{b}^\perp x_i} \\ 1 \end{matrix}$
 $\begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix}$
 $\begin{matrix} \boxed{\vec{a}^\perp y_j} \\ 2 \end{matrix}$

$$pk = e \left(\begin{matrix} \boxed{\vec{b}^\perp} \\ 1 \end{matrix} , \begin{matrix} \boxed{\vec{a}^\perp} \\ 2 \end{matrix} \right)$$

$$sk_f = \sum_{i,j} f_{i,j} e \left(\begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix} , \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix} \right) , sk_g \dots$$

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

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

$$\forall i \in [n]: \quad \vec{a}r_i + \vec{b}^\perp x_i, \quad \forall j \in [m]: \quad \vec{b}s_j + \vec{a}^\perp y_j$$

$$pk = e \left(\vec{b}^\perp_1, \vec{a}^\perp_2 \right)$$

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

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



Private-Key, one-ct secure FE

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



=

$\forall i \in [n]:$

$$\vec{a}r_i + \vec{b}^\perp x_i$$

$\forall j \in [m]:$

$$\vec{b}s_j + \vec{a}^\perp y_j$$

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

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

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



Private-Key, one-ct secure FE

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



$$\forall i \in [n]: \quad \vec{a}r_i + \vec{b}^\perp x_i, \quad \forall j \in [m]: \quad \vec{b}s_j + \vec{a}^\perp y_j$$

$$pk = e \left(\vec{b}^\perp_1, \vec{a}^\perp_2 \right)$$

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

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



Private-Key, one-ct secure FE

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



$$\forall i \in [n]: \quad \vec{a}r_i + \vec{b}^\perp x_i \quad , \quad \forall j \in [m]: \quad \vec{b}s_j + \vec{b}s y_j + \vec{a}^\perp y_j$$

$$pk = e \left(\vec{b}^\perp_1, \vec{a}^\perp_2 \right)$$

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

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



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

$$pk = e \left(\vec{b}^\perp_1, \vec{a}^\perp_2 \right)$$

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

$$s_j \rightarrow s_j + sy_j$$

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



Private-Key, one-ct secure FE

$$\text{Enc}(\text{msk}, (\vec{x}, \vec{y})) = \left(\begin{array}{c} \vec{a}r_i \\ \vec{b}^\perp x_i \end{array} \right)_1 + \left(\begin{array}{c} \vec{b}s_j \\ \vec{b}s + \vec{a}^\perp \end{array} \right)_2, \quad \forall i \in [n], \forall j \in [m]$$

$$pk = e \left(\begin{array}{c} \vec{b}^\perp \\ \vec{b}s + \vec{a}^\perp \end{array} \right)$$

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

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



$$\forall i \in [n]: \quad \vec{a}r_i + \vec{b}^\perp x_i \quad , \quad \forall j \in [m]: \quad \vec{b}s_j + y_j \vec{u}$$

$$pk = e \left(\begin{array}{c} \vec{b}^\perp \\ 1 \end{array} , \begin{array}{c} \vec{u} \\ 2 \end{array} \right)$$

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

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

$$\begin{array}{c} \vec{b} \\ 2 \end{array} , \begin{array}{c} \vec{a}^\perp \\ 2 \end{array} \text{ is a basis of } \mathbb{G}_2^2$$



Private-Key, one-ct secure FE

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



$$pk = e \left(\begin{array}{c} \vec{b}^\perp \\ 1 \end{array}, \begin{array}{c} \vec{u} \\ 2 \end{array} \right)$$

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

$\forall i \in [n]:$

$$\begin{array}{c} \vec{v}_i \\ 1 \end{array}$$

$\forall j \in [m]:$

$$, \begin{array}{c} \vec{b}s_j \\ 2 \end{array} + y_j \begin{array}{c} \vec{u} \\ 2 \end{array}$$

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



Private-Key, one-ct secure FE

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

$\forall i \in [n]:$

$$\vec{v}_i \quad 1$$

$\forall j \in [m]:$

$$, \vec{b}s_j + y_j \vec{u} \quad 2$$

$$pk = \$ \quad T$$

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

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



Private-Key, one-ct secure FE

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

$\forall i \in [n]:$

$$\vec{v}_i \quad 1$$

$\forall j \in [m]:$

$$\vec{w}_j \quad 2$$

$$pk = \$ \quad T$$

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

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



Public-Key FE

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

$$\text{Enc}(pk, (\vec{x}, \vec{y})) \text{ } \img alt="lock icon" data-bbox="288 428 318 482" = \forall i \in [n]: \boxed{\vec{a}r_i}_1 + \boxed{\vec{b}^\perp x_i}_1, \forall j \in [m]: \boxed{\vec{b}s_j}_2 + \boxed{\vec{a}^\perp y_j}_2$$

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

Public-Key FE

$$pk = \forall i, j: \begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix}, \begin{matrix} \boxed{\vec{b}^\perp} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{a}^\perp} \\ 2 \end{matrix}$$


violates DDH

$$\text{Enc}(pk, (\vec{x}, \vec{y})) = \begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix} + \begin{matrix} \boxed{\vec{b}^\perp x_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix} + \begin{matrix} \boxed{\vec{a}^\perp y_j} \\ 2 \end{matrix}$$

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

$$sk_f = \sum_{i,j} f_{i,j} e \left(\begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix} \right)$$

Public-Key FE

$$pk = \forall i, j: \begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}^\perp \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{a}^\perp \\ \hline 2 \\ \hline \end{array}$$

$$\text{Enc}(pk, (\vec{x}, \vec{y})) = \begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array} + \begin{array}{|c|} \hline \vec{b}^\perp x_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array} + \begin{array}{|c|} \hline \vec{a}^\perp y_j \\ \hline 2 \\ \hline \end{array}$$

$$sk_f = \sum_{i,j} f_{i,j} e \left(\begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array} \right)$$

Dual bases:

$$\begin{array}{|c|} \hline \vec{a} \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}^\perp \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{a}^* \\ \hline 1 \\ \hline \end{array}$$

$$\begin{array}{|c|} \hline \vec{b} \\ \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{a}^\perp \\ \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}^* \\ \hline 2 \\ \hline \end{array}$$

Public-Key FE

DDH in \mathbb{G}_1

$$\left(\begin{array}{c} \vec{a} \\ 1 \end{array}, \begin{array}{c} \vec{a}^\perp \\ 2 \end{array}, \begin{array}{c} \vec{a}r \\ 1 \end{array} \right) \approx_c \left(\begin{array}{c} \vec{a} \\ 1 \end{array}, \begin{array}{c} \vec{a}^\perp \\ 2 \end{array}, \begin{array}{c} \vec{a}r \\ 1 \end{array} + \begin{array}{c} \vec{a}^*s \\ 1 \end{array} \right)$$

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

Dual bases:

$$\begin{array}{c} \vec{a} \\ 1 \end{array}, \begin{array}{c} \vec{b}^\perp \\ 1 \end{array}, \begin{array}{c} \vec{a}^* \\ 1 \end{array}$$

$$\begin{array}{c} \vec{b} \\ 2 \end{array}, \begin{array}{c} \vec{a}^\perp \\ 2 \end{array}, \begin{array}{c} \vec{b}^* \\ 2 \end{array}$$

Public-Key FE

DDH in \mathbb{G}_2

$$\left(\begin{array}{c} \vec{b} \\ 2 \end{array}, \begin{array}{c} \vec{b}^\perp \\ 1 \end{array}, \begin{array}{c} \vec{br} \\ 2 \end{array} \right) \approx_c \left(\begin{array}{c} \vec{b} \\ 2 \end{array}, \begin{array}{c} \vec{b}^\perp \\ 1 \end{array}, \begin{array}{c} \vec{br} \\ 2 \end{array} + \begin{array}{c} \vec{b}^*s \\ 2 \end{array} \right)$$

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

Dual bases:

$$\begin{array}{c} \begin{array}{c} \vec{a} \\ 1 \end{array}, \begin{array}{c} \vec{b}^\perp \\ 1 \end{array}, \begin{array}{c} \vec{a}^* \\ 1 \end{array} \\ \begin{array}{c} \vec{b} \\ 2 \end{array}, \begin{array}{c} \vec{a}^\perp \\ 2 \end{array}, \begin{array}{c} \vec{b}^* \\ 2 \end{array} \end{array}$$

Public-Key FE

$$pk = \forall i, j: \begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}^\perp \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{a}^\perp \\ \hline 2 \\ \hline \end{array}$$

$$\text{Enc}(pk, (\vec{x}, \vec{y})) \quad \text{🔒} = \begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array} + \begin{array}{|c|} \hline \vec{b}^\perp x_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array} + \begin{array}{|c|} \hline \vec{a}^\perp y_j \\ \hline 2 \\ \hline \end{array}$$

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

$$sk_f = \sum_{i,j} f_{i,j} e \left(\begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array} \right)$$



Mix & match attacks


Public-Key FE

$$pk = \forall i, j: \begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix}, \begin{matrix} \boxed{\vec{b}^\perp} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{a}^\perp} \\ 2 \end{matrix}$$

$$\text{Enc}(pk, (\vec{x}, \vec{y})) \stackrel{W \leftarrow^R GL_3}{=} \left(\begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix} + \begin{matrix} \boxed{\vec{b}^\perp x_i} \\ 1 \end{matrix} \right) W^{-1}, W \left(\begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix} + \begin{matrix} \boxed{\vec{a}^\perp y_j} \\ 2 \end{matrix} \right)$$

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

$$sk_f = \sum_{i,j} f_{i,j} e \left(\begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix} \right)$$


Mix & match attacks

Public-Key FE

$$pk = \forall i, j: \begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}^\perp \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{a}^\perp \\ \hline 2 \\ \hline \end{array}$$

$$\text{Enc}(pk, (\vec{x}, \vec{y})) \stackrel{W \leftarrow^R GL_3}{=} \left(\begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array} + \begin{array}{|c|} \hline \vec{b}^\perp x_i \\ \hline 1 \\ \hline \end{array} \right) W^{-1}, W \left(\begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array} + \begin{array}{|c|} \hline \vec{a}^\perp y_j \\ \hline 2 \\ \hline \end{array} \right)$$

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

$$sk_f = \sum_{i,j} f_{i,j} e \left(\begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array} \right)$$



sk_f can be computed from pk

Public-Key FE

$$pk = \forall i, j: \begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}^\perp \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{a}^\perp \\ \hline 2 \\ \hline \end{array}$$

$$\text{Enc}(pk, (\vec{x}, \vec{y})) = \left(\begin{array}{|c|} \hline \vec{a}r_i\gamma + \vec{b}s_j \\ \hline 1 \\ \hline \end{array} + \begin{array}{|c|} \hline \vec{b}^\perp \\ \hline 1 \\ \hline \end{array} \right) W^{-1}, W \left(\begin{array}{|c|} \hline \vec{b}s_j\sigma + \vec{a}^\perp y_j \\ \hline 2 \\ \hline \end{array} + \begin{array}{|c|} \hline \vec{a}^\perp \\ \hline 2 \\ \hline \end{array} \right), \begin{array}{|c|} \hline \gamma\sigma \\ \hline 2 \\ \hline \end{array}$$

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

$W \leftarrow^R GL_3$
 $\gamma, \sigma \leftarrow^R \mathbb{Z}_p$

$$sk_f = \sum_{i,j} f_{i,j} e \left(\begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array} \right)$$



sk_f can be computed from pk

Public-Key FE

$$pk = \forall i, j: \begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}^\perp \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{a}^\perp \\ \hline 2 \\ \hline \end{array}$$

$$\text{Enc}(pk, (\vec{x}, \vec{y})) \begin{array}{|c|} \hline \text{lock} \\ \hline \end{array} = \begin{array}{|c|} \hline \forall i \in [n]: \\ \hline \end{array} \left(\begin{array}{|c|} \hline \vec{a}r_i\gamma \\ \hline 1 \\ \hline \end{array} + \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 1 \\ \hline \end{array} \right) W^{-1}, W \begin{array}{|c|} \hline \forall j \in [m]: \\ \hline \end{array} \left(\begin{array}{|c|} \hline \vec{b}s_j\sigma \\ \hline 2 \\ \hline \end{array} + \begin{array}{|c|} \hline \vec{a}^\perp y_j \\ \hline 2 \\ \hline \end{array} \right), \begin{array}{|c|} \hline \gamma\sigma \\ \hline 2 \\ \hline \end{array}$$

$W \leftarrow^R GL_3$
 $\gamma, \sigma \leftarrow^R \mathbb{Z}_p$

$$sk_f = \sum_{i,j} f_{i,j} e \left(\begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array} \right)$$

$\downarrow f$

$$\gamma\sigma \cdot sk_f + \vec{x}^T f \vec{y} e \left(\begin{array}{|c|} \hline \vec{b}^\perp \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{a}^\perp \\ \hline 2 \\ \hline \end{array} \right)$$

Public-Key FE

$$pk = \forall i, j: \begin{matrix} \boxed{\vec{a}r_i} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{b}s_j} \\ 2 \end{matrix}, \begin{matrix} \boxed{\vec{b}^\perp} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{a}^\perp} \\ 2 \end{matrix}$$

$$\text{Enc}(pk, (\vec{x}, \vec{y})) \begin{matrix} \text{lock} \\ \downarrow \end{matrix} = \begin{matrix} \forall i \in [n]: \\ \left(\begin{matrix} \boxed{\vec{a}r_i\gamma} \\ 1 \end{matrix} + \begin{matrix} \boxed{\vec{b}s_j} \\ 1 \end{matrix} \right) W^{-1}, W \left(\begin{matrix} \boxed{\vec{b}s_j\sigma} \\ 2 \end{matrix} + \begin{matrix} \boxed{\vec{a}^\perp y_j} \\ 2 \end{matrix} \right), \begin{matrix} \boxed{\gamma\sigma} \\ 2 \end{matrix} \end{matrix}$$

$W \leftarrow^R GL_3$
 $\gamma, \sigma \leftarrow^R \mathbb{Z}_p$

$$sk_f = \sum_{i,j} f_{i,j} \begin{matrix} \boxed{\vec{a}r_i \cdot \vec{b}s_j} \\ 1 \end{matrix} \in \mathbb{G}_1$$

$$e(sk_f, \begin{matrix} \boxed{\gamma\sigma} \\ 2 \end{matrix}) + \vec{x}^T f \vec{y} e \left(\begin{matrix} \boxed{\vec{b}^\perp} \\ 1 \end{matrix}, \begin{matrix} \boxed{\vec{a}^\perp} \\ 2 \end{matrix} \right)$$

Public-Key FE

$$pk = \forall i, j: \begin{array}{|c|} \hline \vec{a}r_i \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}s_j \\ \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{b}^\perp \\ \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline \vec{a}^\perp \\ \hline 2 \\ \hline \end{array}$$

$$\text{Enc}(pk, (\vec{x}, \vec{y})) = \begin{array}{|c|} \hline \vec{a}r_i\gamma + \vec{b}s_j \\ \hline 1 \\ \hline \end{array} W^{-1}, W \begin{array}{|c|} \hline \vec{b}s_j\sigma + \vec{a}^\perp y_j \\ \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline \gamma\sigma \\ \hline 2 \\ \hline \end{array}$$

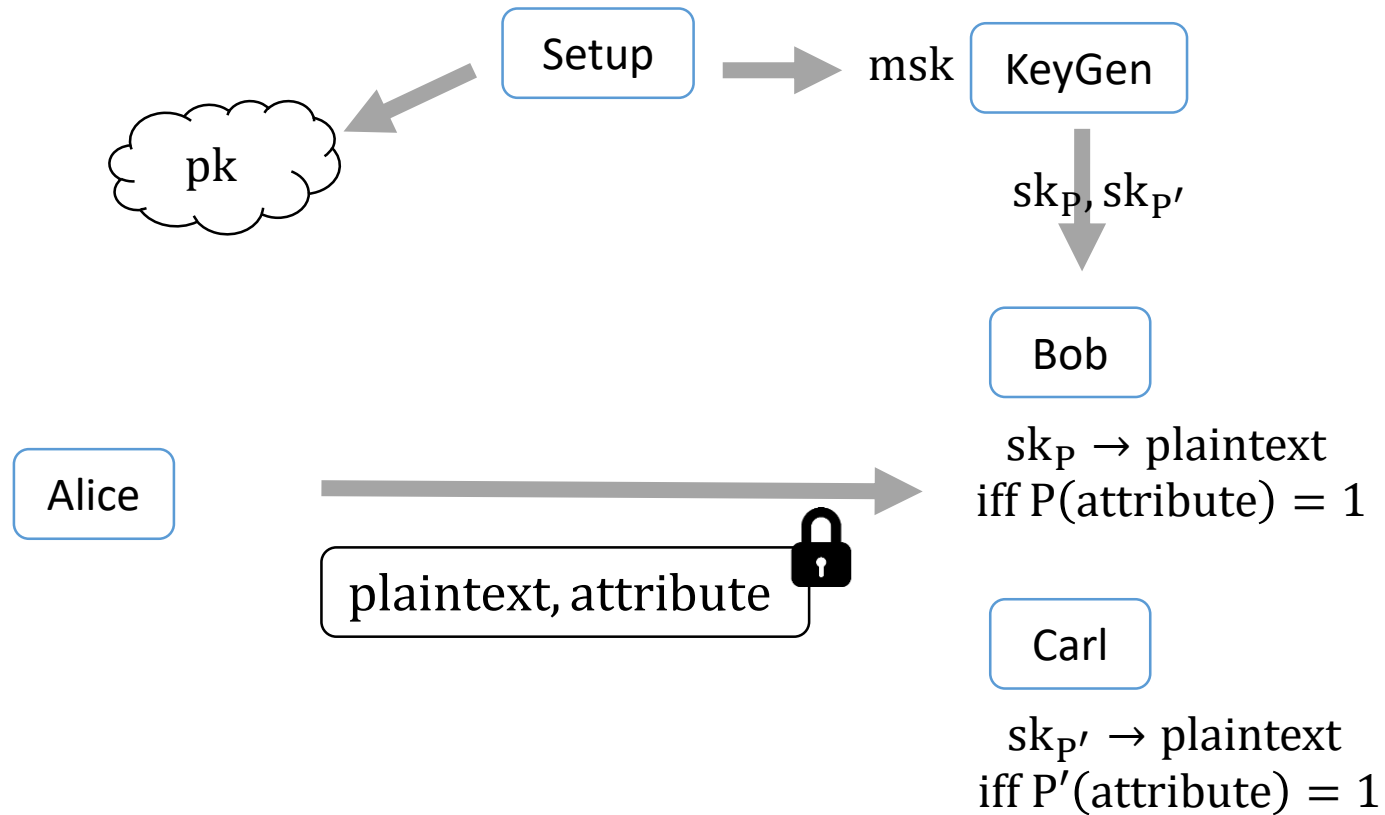
$\forall i \in [n]:$ $\forall j \in [m]:$

$W \leftarrow^R GL_3$
 $\gamma, \sigma \leftarrow^R \mathbb{Z}_p$

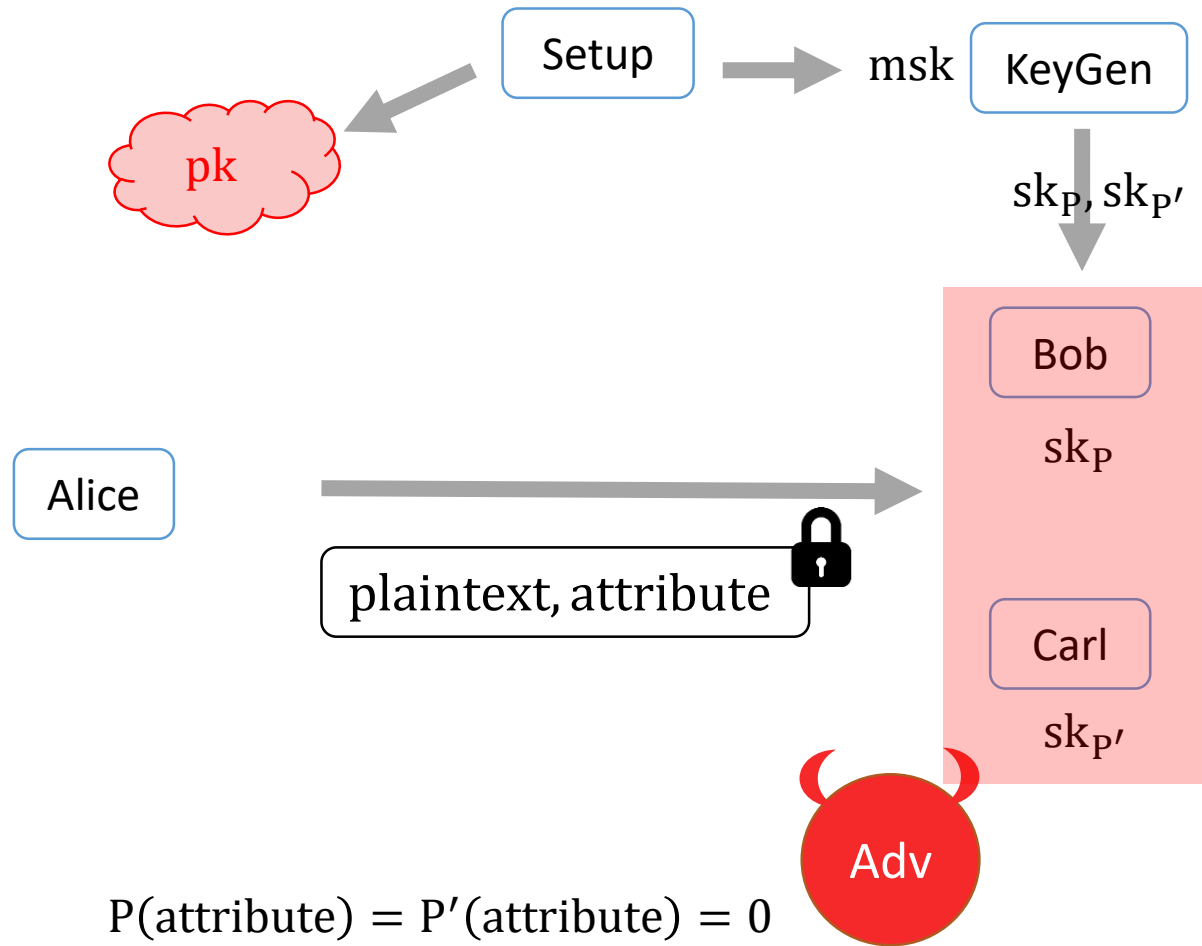
$$sk_f = \sum_{i,j} f_{i,j} \begin{array}{|c|} \hline \vec{a}r_i \cdot \vec{b}s_j \\ \hline 1 \\ \hline \end{array} \in \mathbb{G}_1$$

$$msk = \forall i, j: \begin{array}{|c|} \hline \vec{a}r_i \cdot \vec{b}s_j \\ \hline 1 \\ \hline \end{array} \in \mathbb{G}_1$$

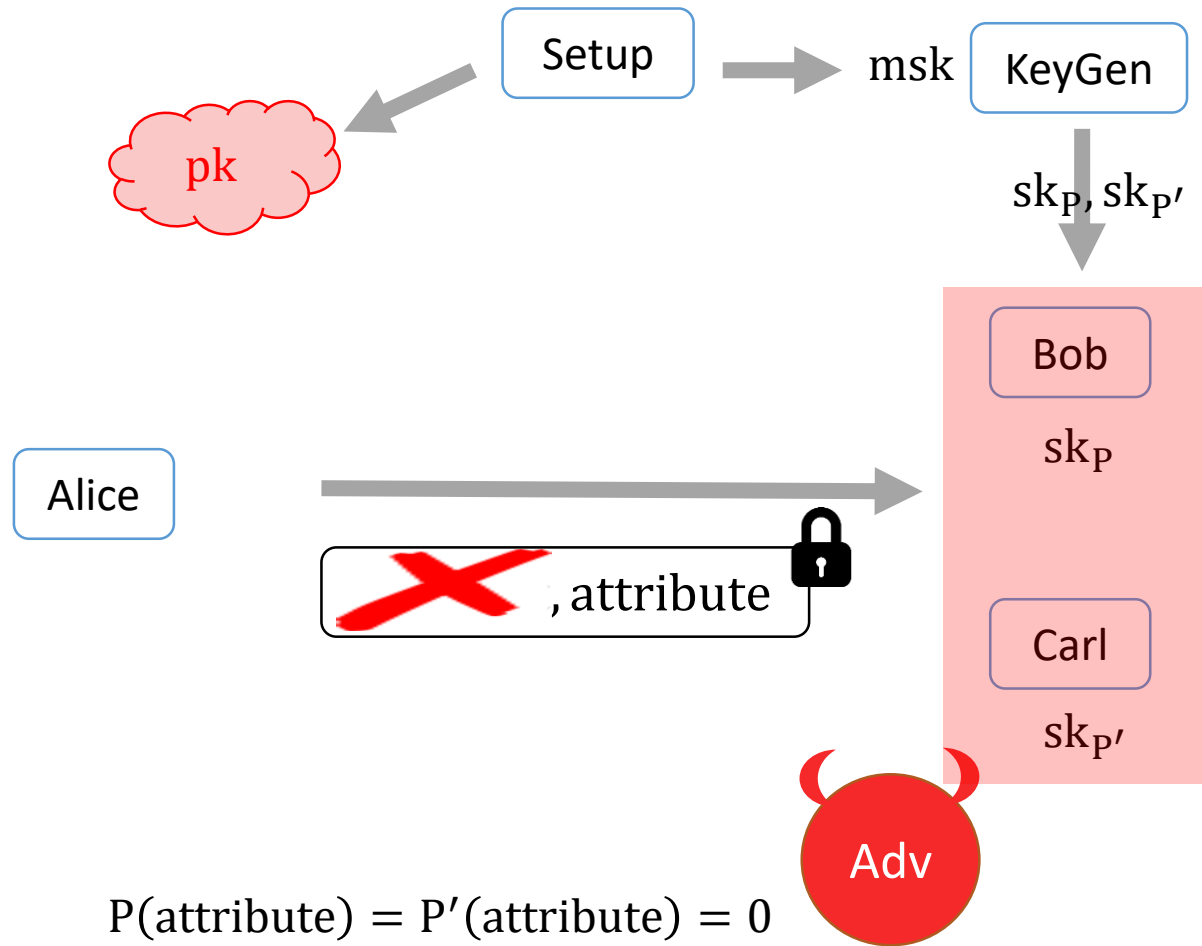
PE [Boneh Waters 06; Katz, Sahai, Waters 08]



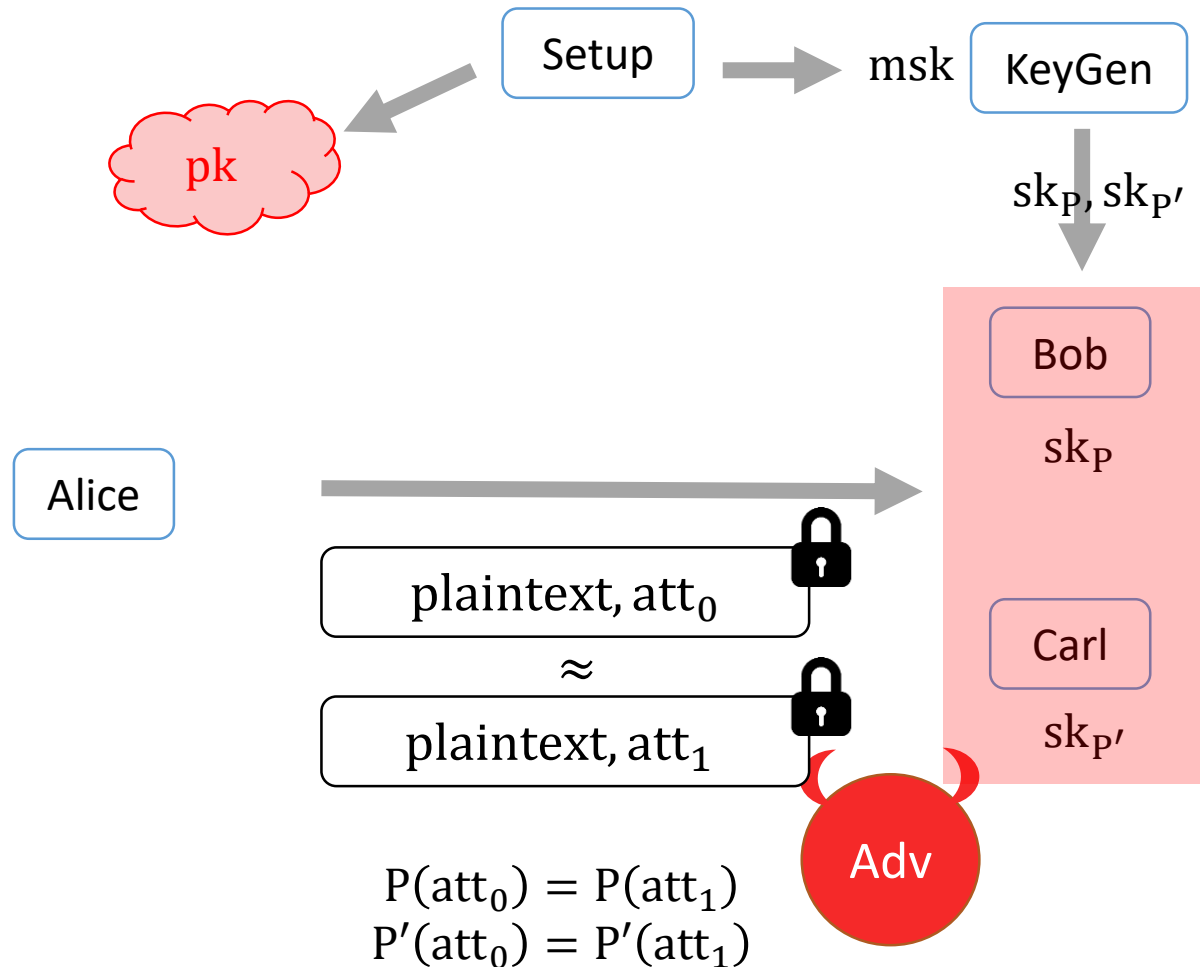
PE [Boneh Waters 06; Katz, Sahai, Waters 08]



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

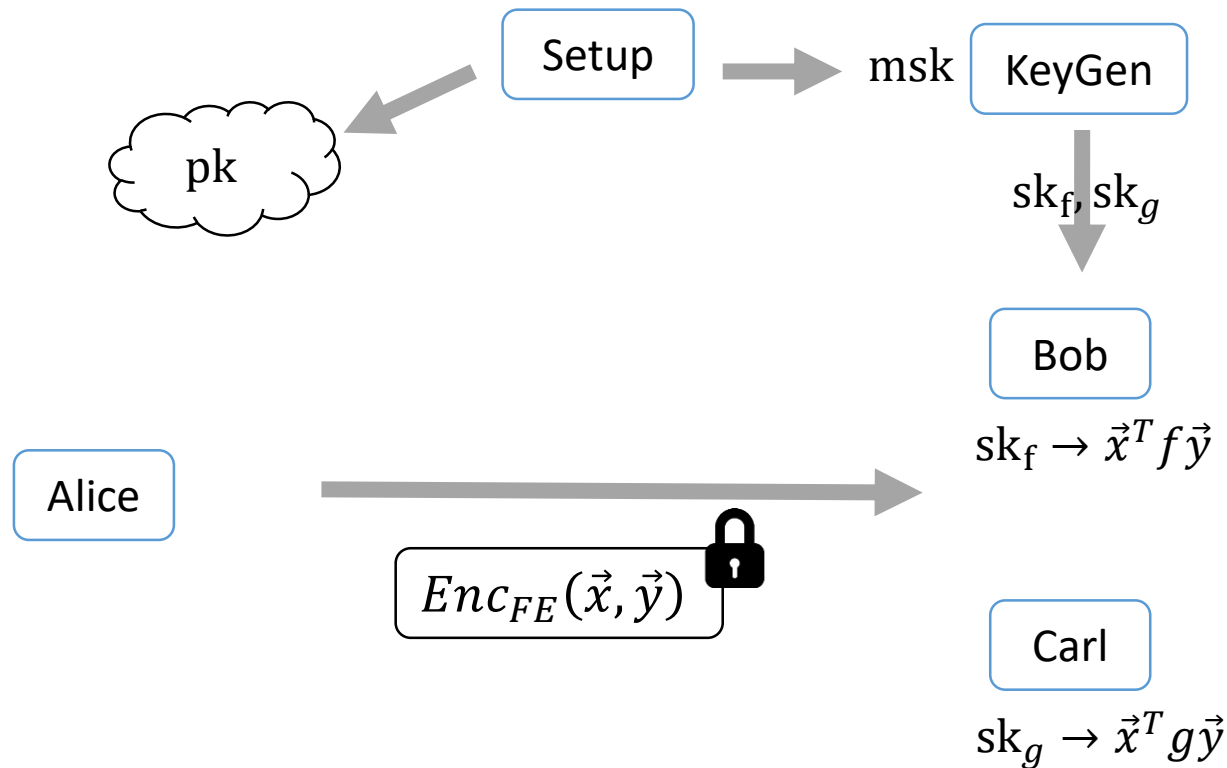


PE [Boneh Waters 06; Katz, Sahai, Waters 08]



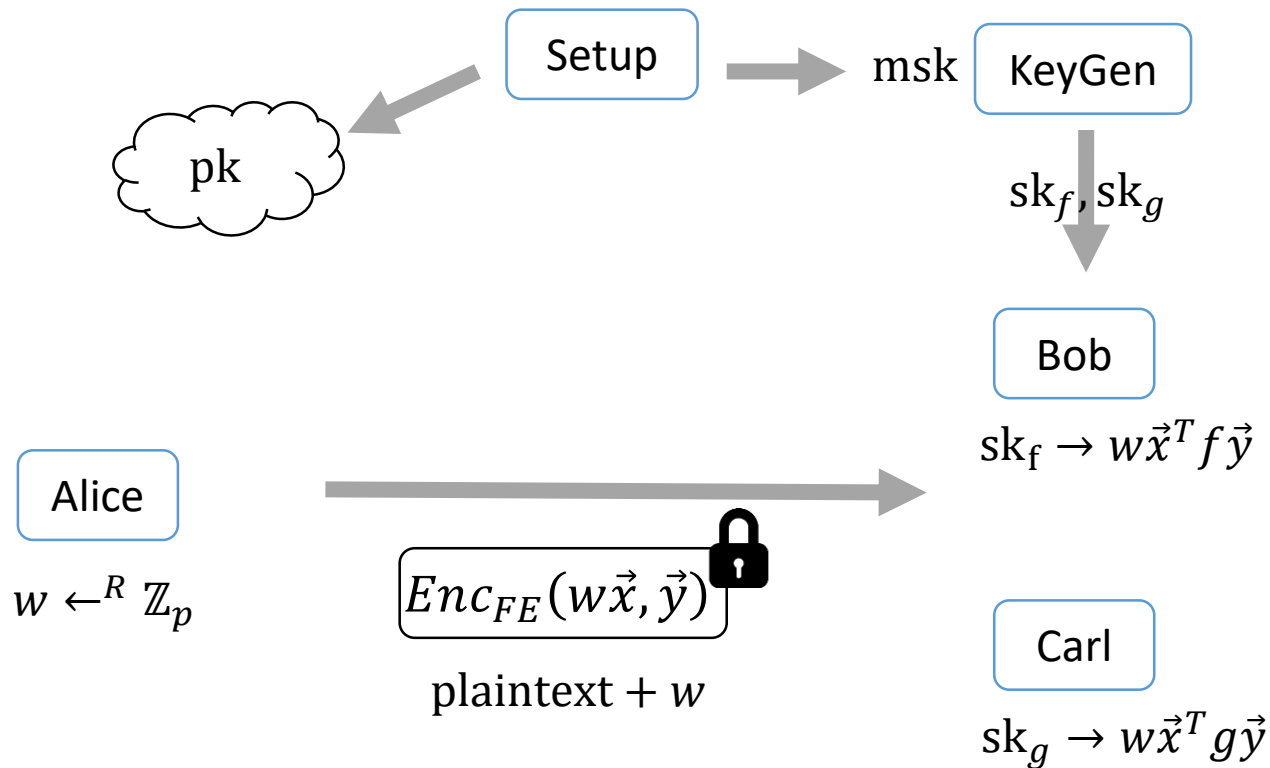
PE for bilinear maps from FE

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



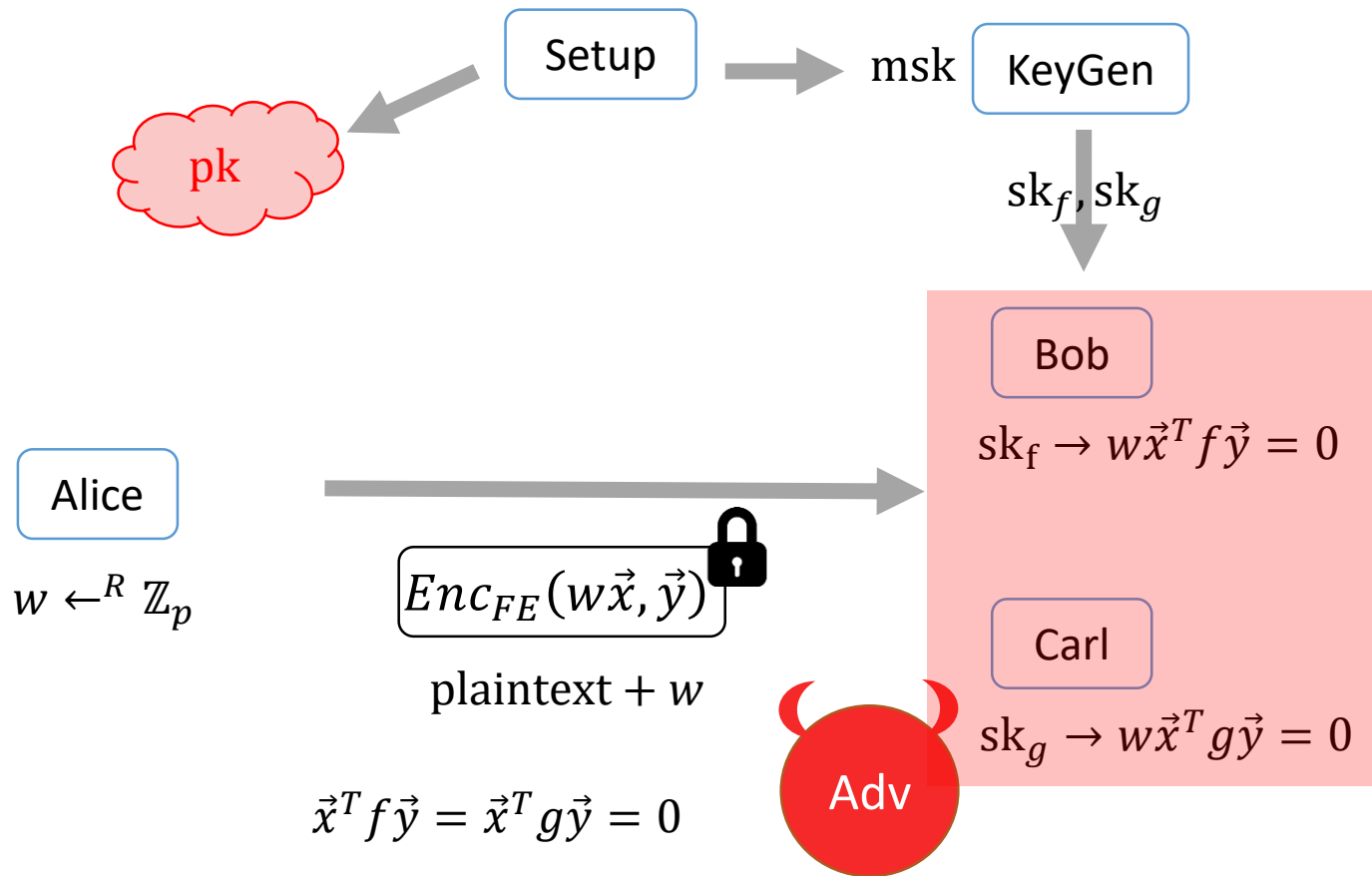
PE for bilinear maps from FE

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



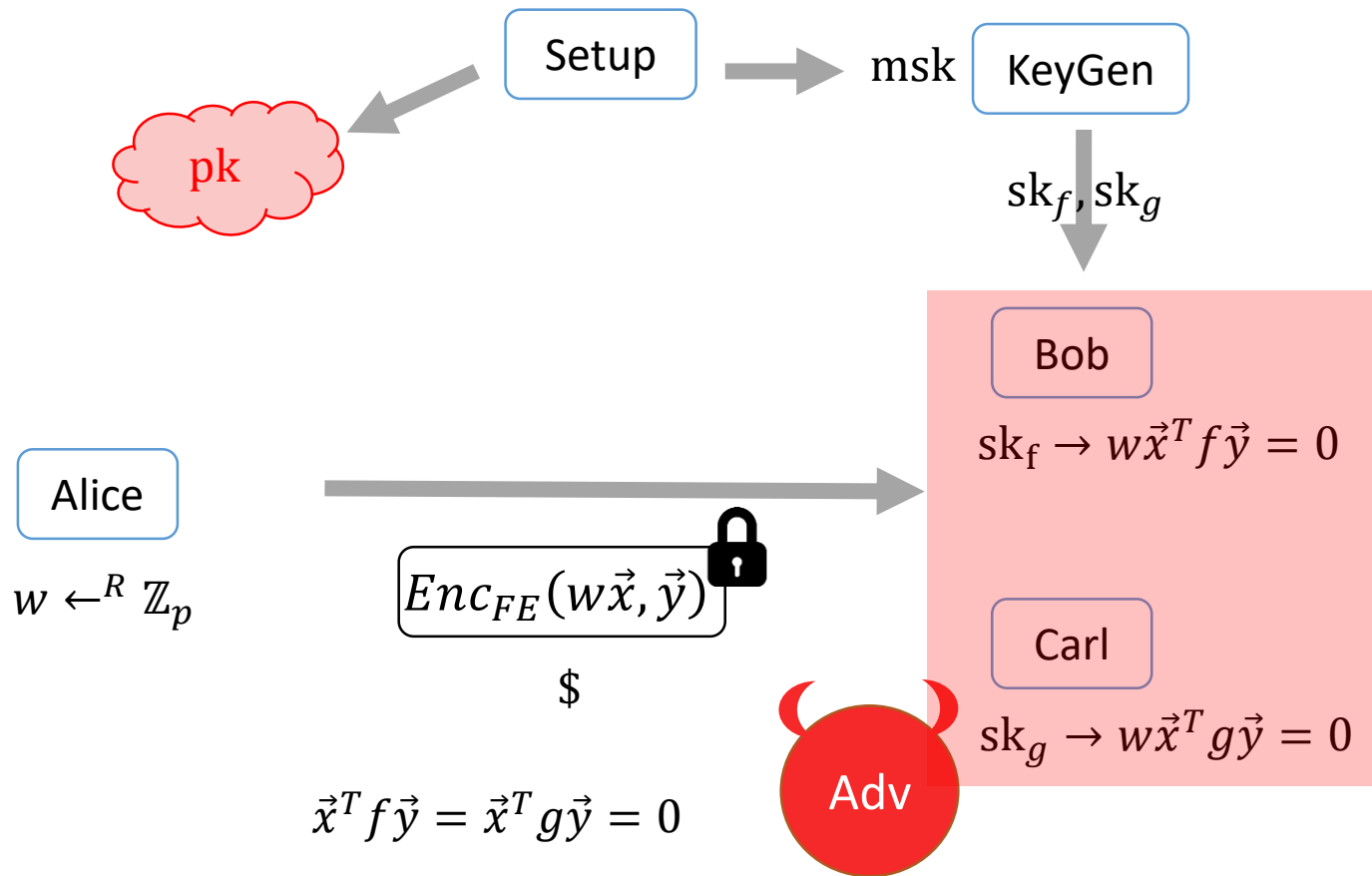
PE for bilinear maps from FE

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



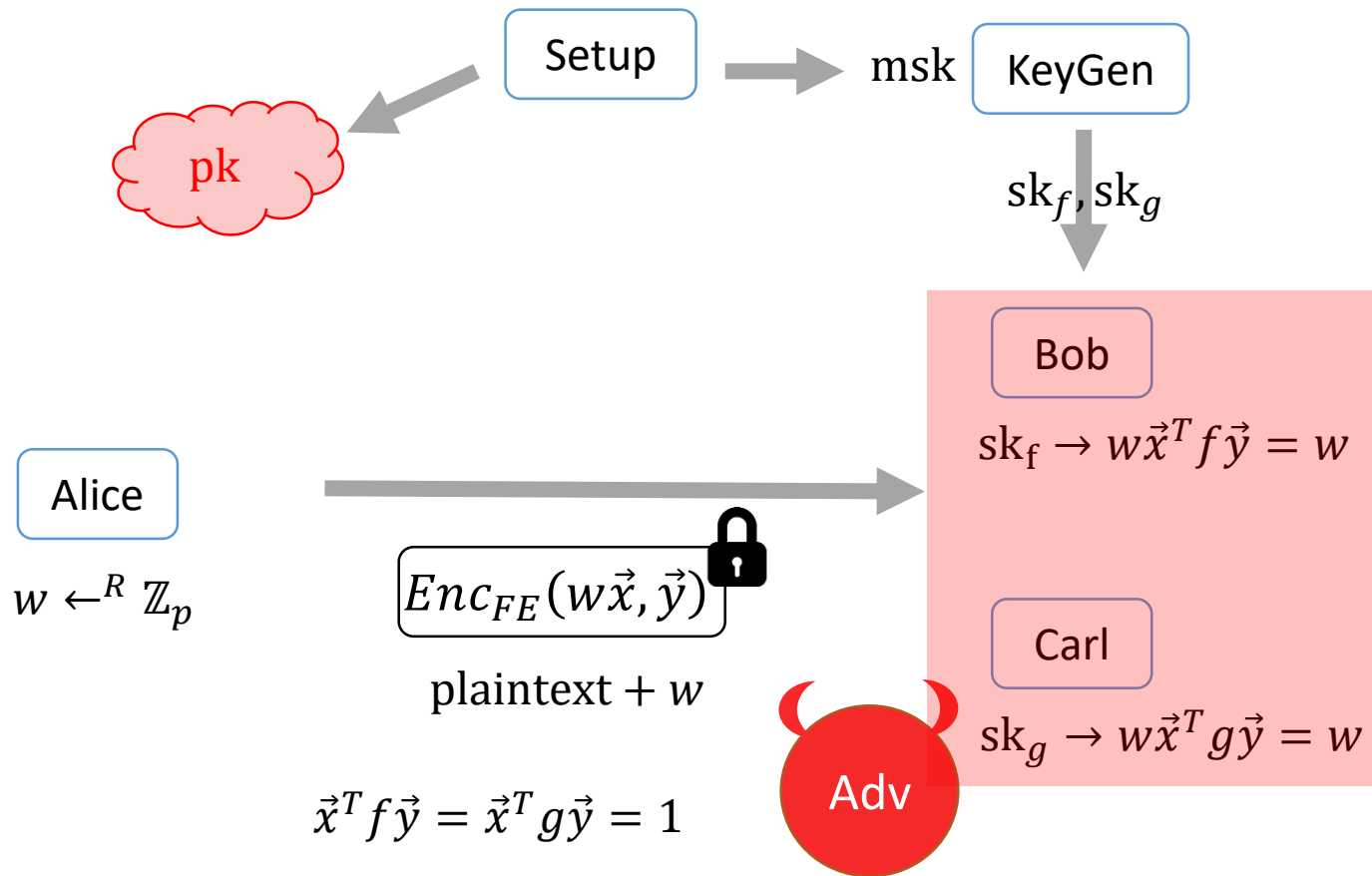
PE for bilinear maps from FE

PE: $P: \mathbb{Z}_p^n \times \mathbb{Z}_p^m \rightarrow \{0,1\}$, $P(\vec{x}, \vec{y}) = 1$ 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: $P: \mathbb{Z}_p^n \times \mathbb{Z}_p^m \rightarrow \{0,1\}$, $P(\vec{x}, \vec{y}) = 1$ 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: $P: \{0,1\}^n \rightarrow \{0,1\}$, of constant degree $d \ll n$

- [KSW 08]:

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

$$P = \sum_{j=1}^{d'} p_j \cdot \text{Monomial}_j \rightarrow \vec{y} = \begin{pmatrix} p_1 \\ \dots \\ p_{d'} \end{pmatrix} \in \mathbb{Z}_p^{d'}$$

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

PE for constant depth boolean formulas

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

- [This work]:

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

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

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

PE for constant depth boolean formulas

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

- [This work]:

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

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

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

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