ABE for Circuits with Constant-Size Secret Keys and Adaptive Security

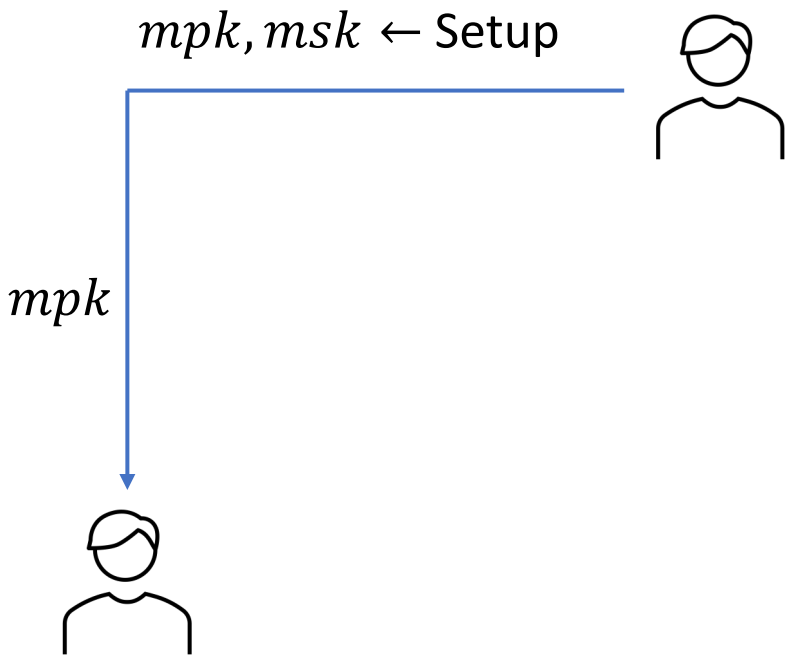
Hanjun Li, Huijia (Rachel) Lin, Ji Luo

University of Washington

Attribute Based Encryption (ABE) [SW05, GPSW06]

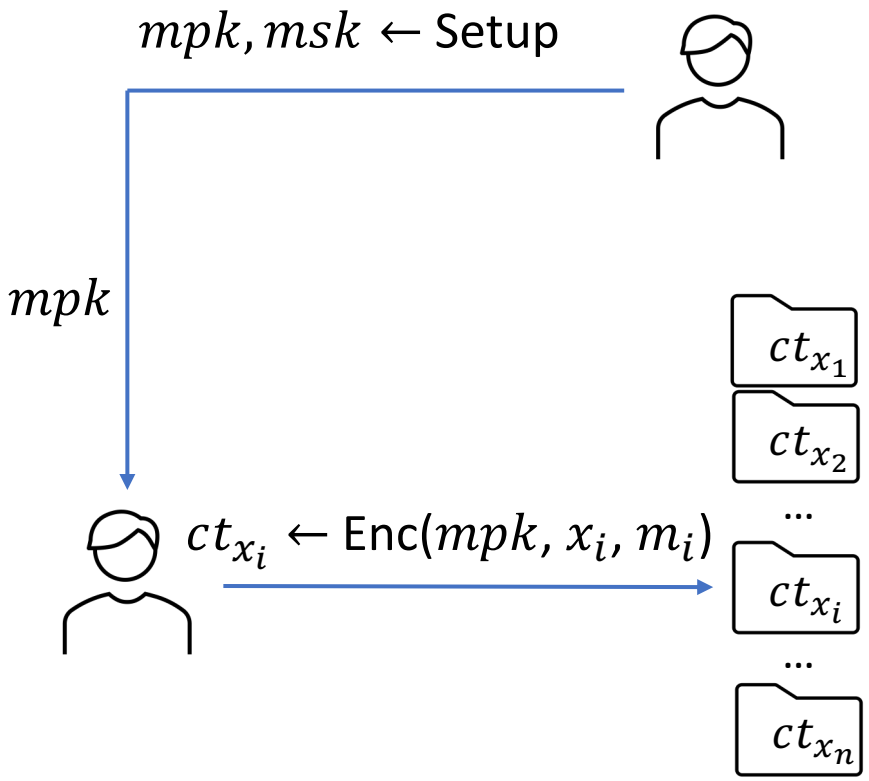
Key Policy (KP) variant

Attribute Based Encryption (ABE) [SW05, GPSW06]



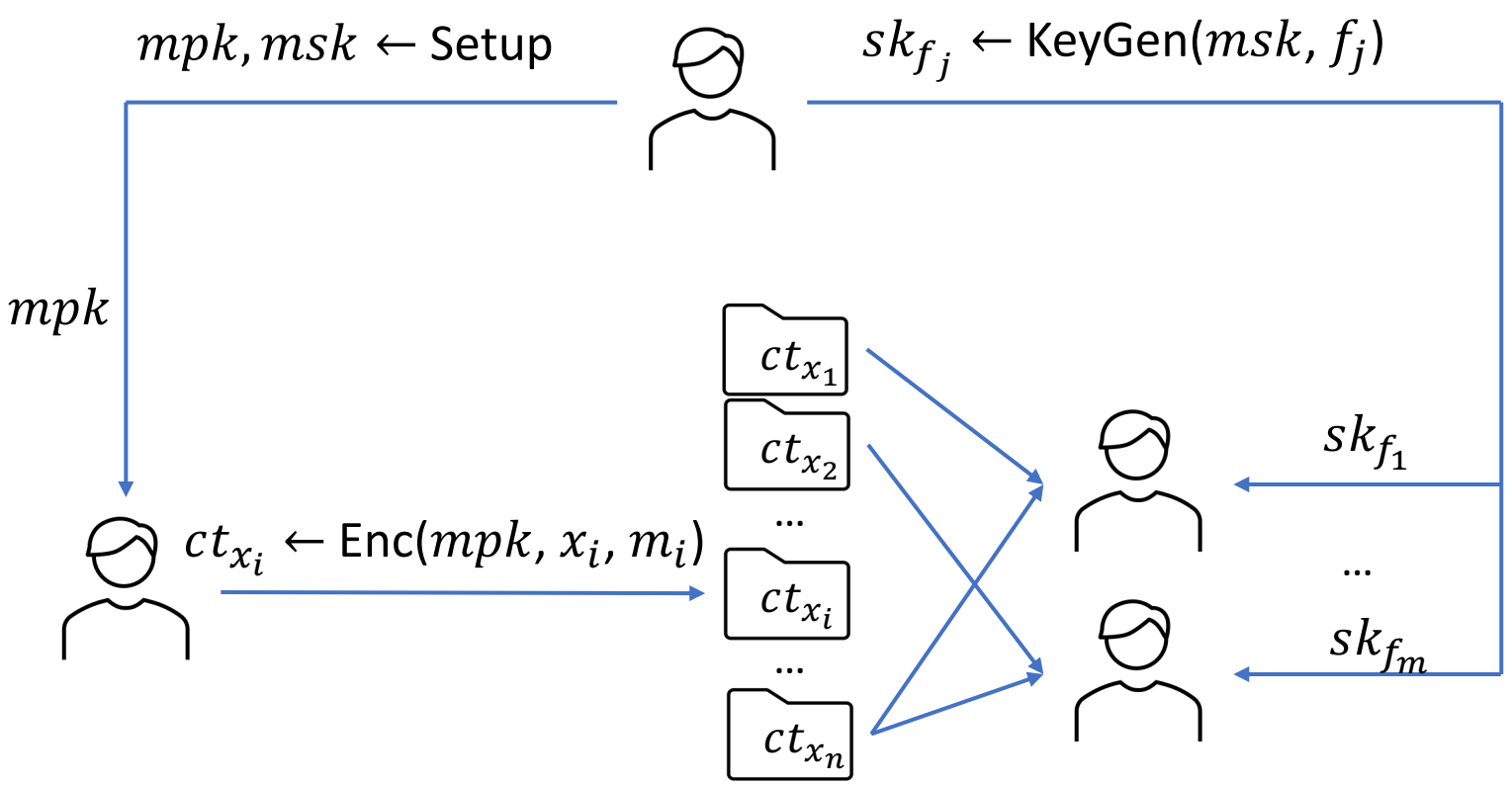
Key Policy (KP) variant

Attribute Based Encryption (ABE) [SW05, GPSW06]



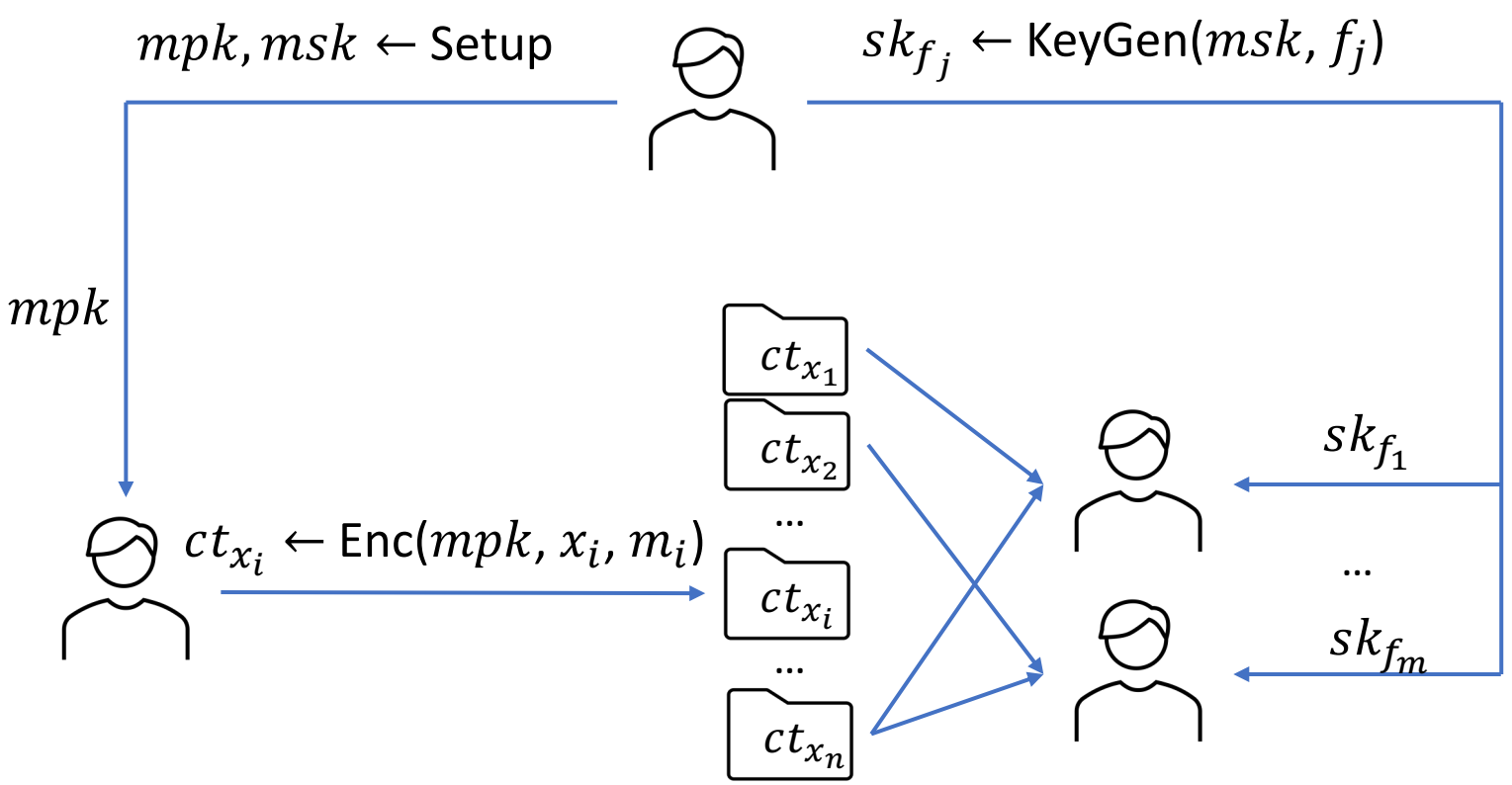
Key Policy (KP) variant

Attribute Based Encryption (ABE) [SW05, GPSW06]



Key Policy (KP) variant

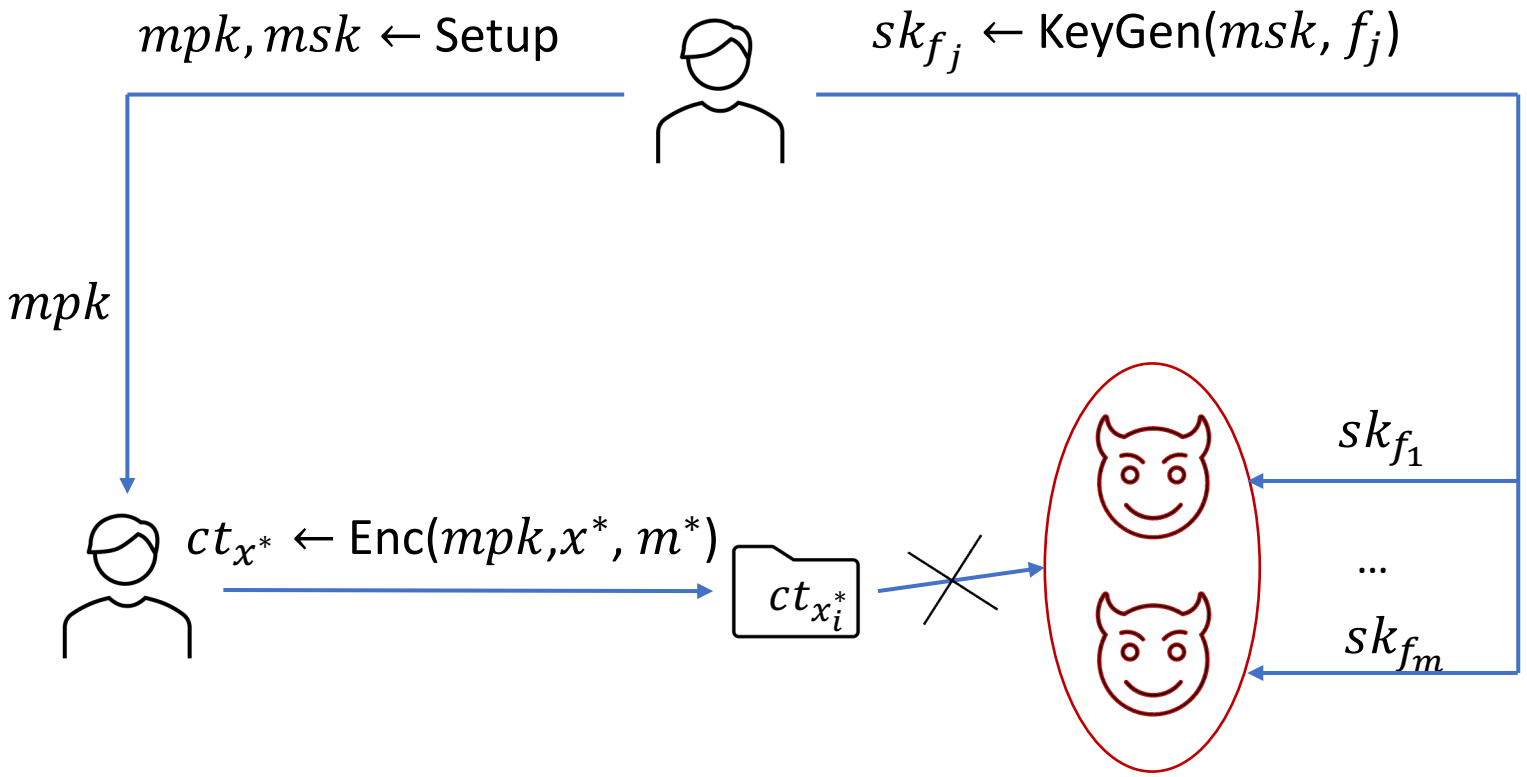
Attribute Based Encryption (ABE) [SW05, GPSW06]



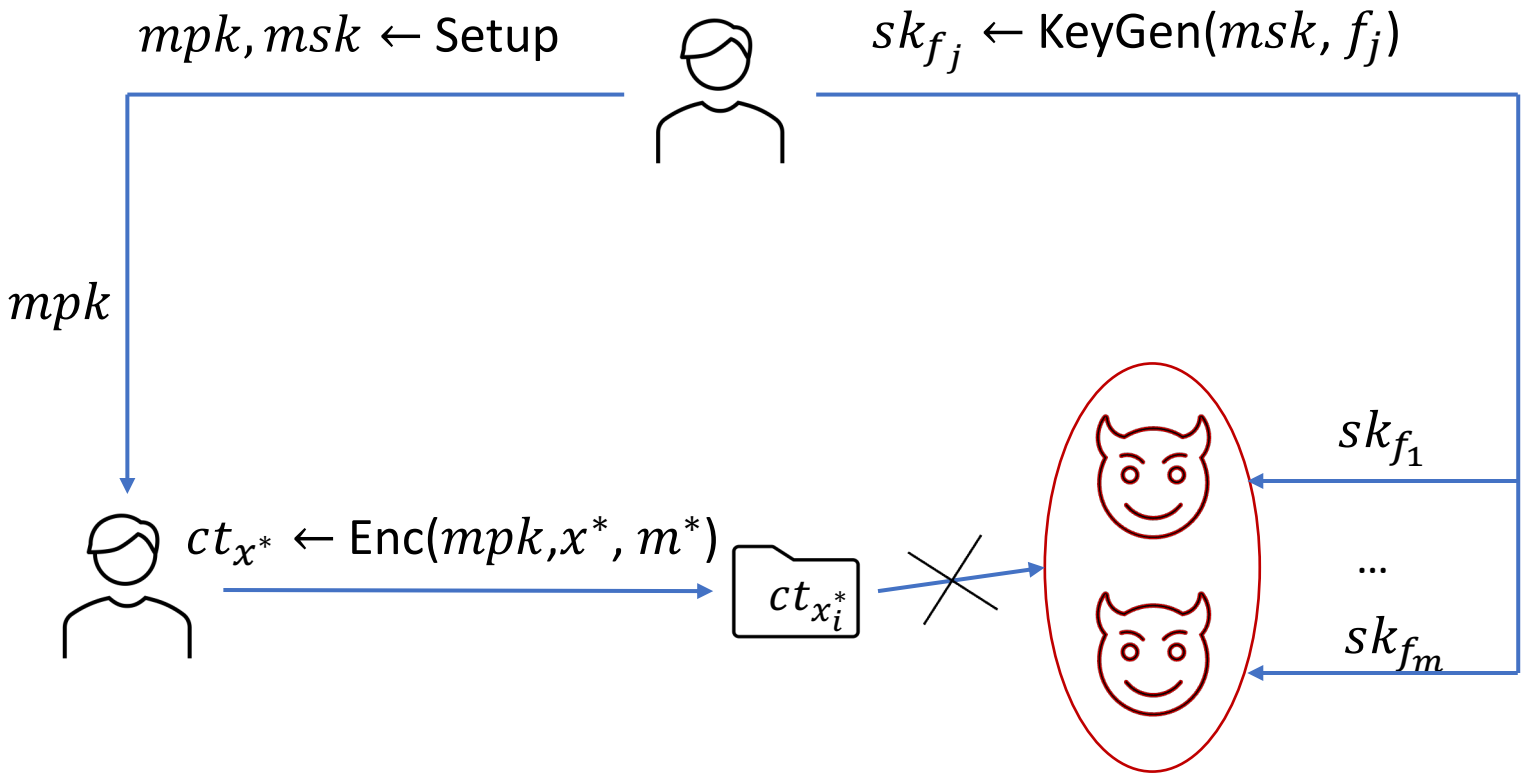
Key Policy (KP) variant

Correctness: Dec$(sk_{f_j}, ct_{x_i}) = m_i$ if $f_j(x_i) = 0$

Attribute Based Encryption (ABE) [SW05, GPSW06]

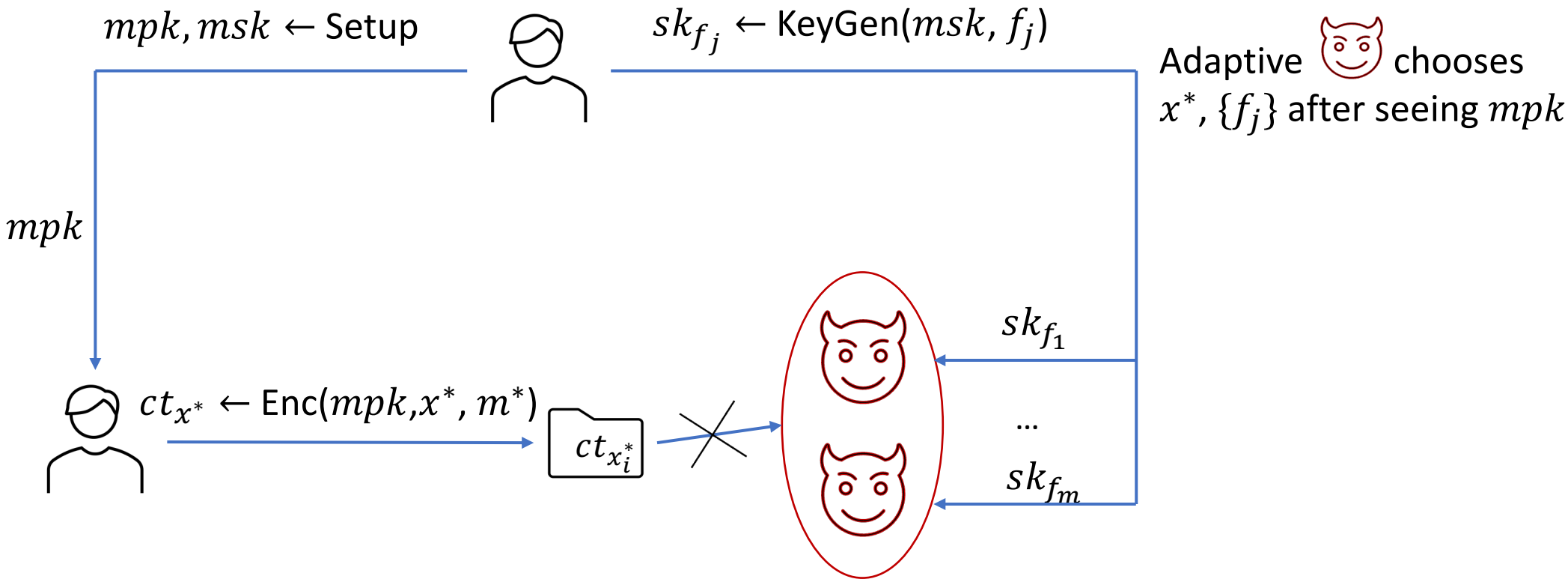


Attribute Based Encryption (ABE) [SW05, GPSW06]



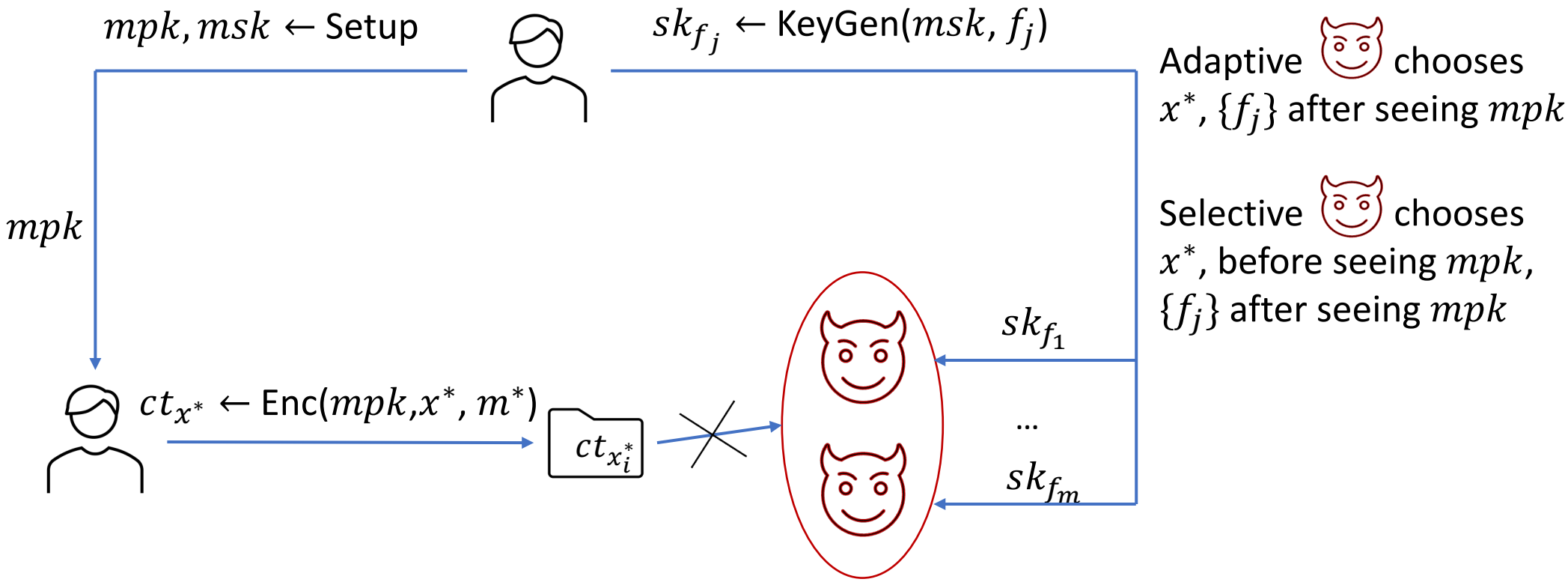
Security: m^* is hidden
if $\forall j,\ f_j(x^*) \neq 0$

Attribute Based Encryption (ABE) [SW05, GPSW06]



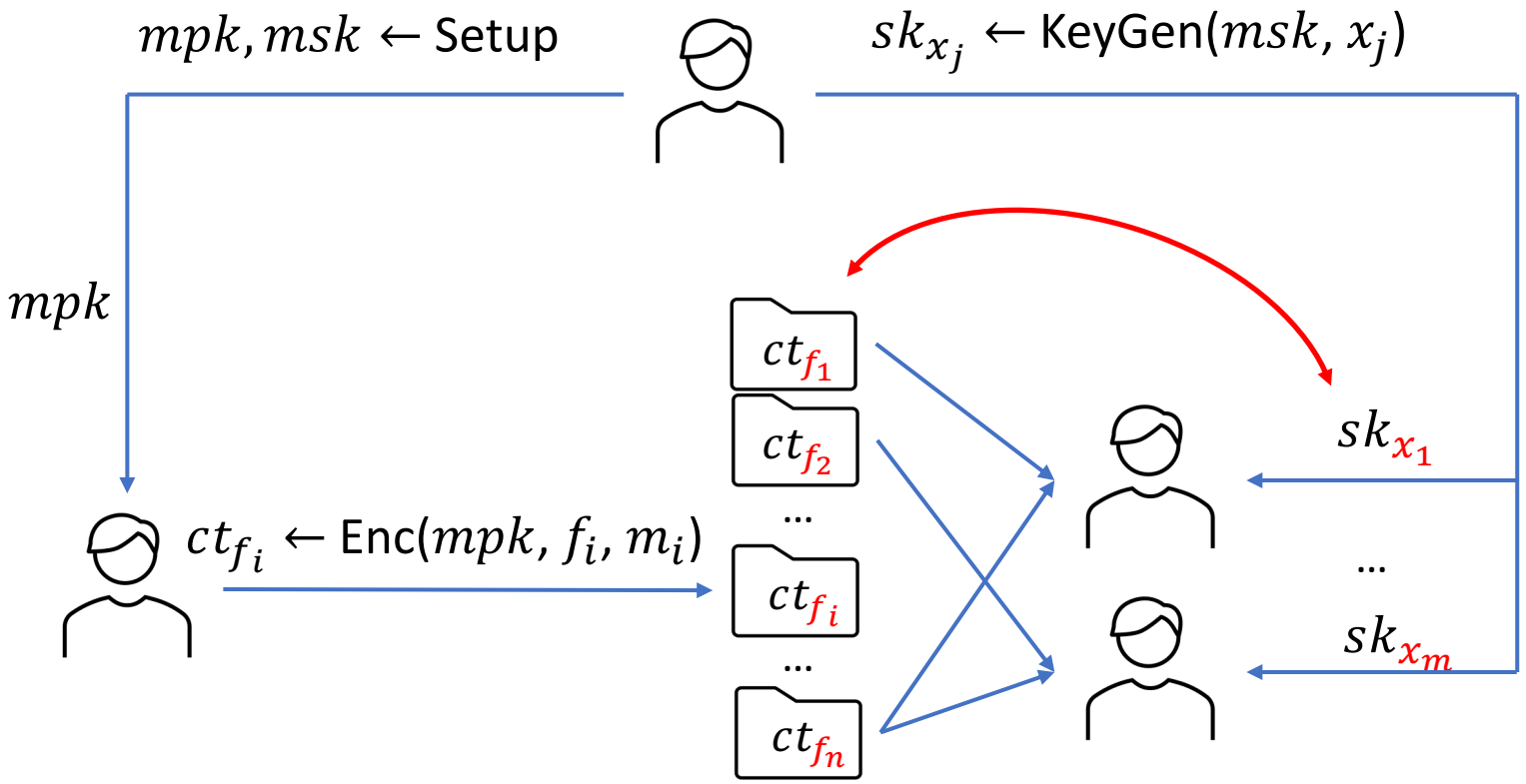
Security: m^* is hidden
if $\forall j,\ f_j(x^*) \neq 0$

Attribute Based Encryption (ABE) [SW05, GPSW06]



Security: m^* is hidden
if $\forall j,\ f_j(x^*) \neq 0$

Attribute Based Encryption (ABE) [SW05, GPSW06]



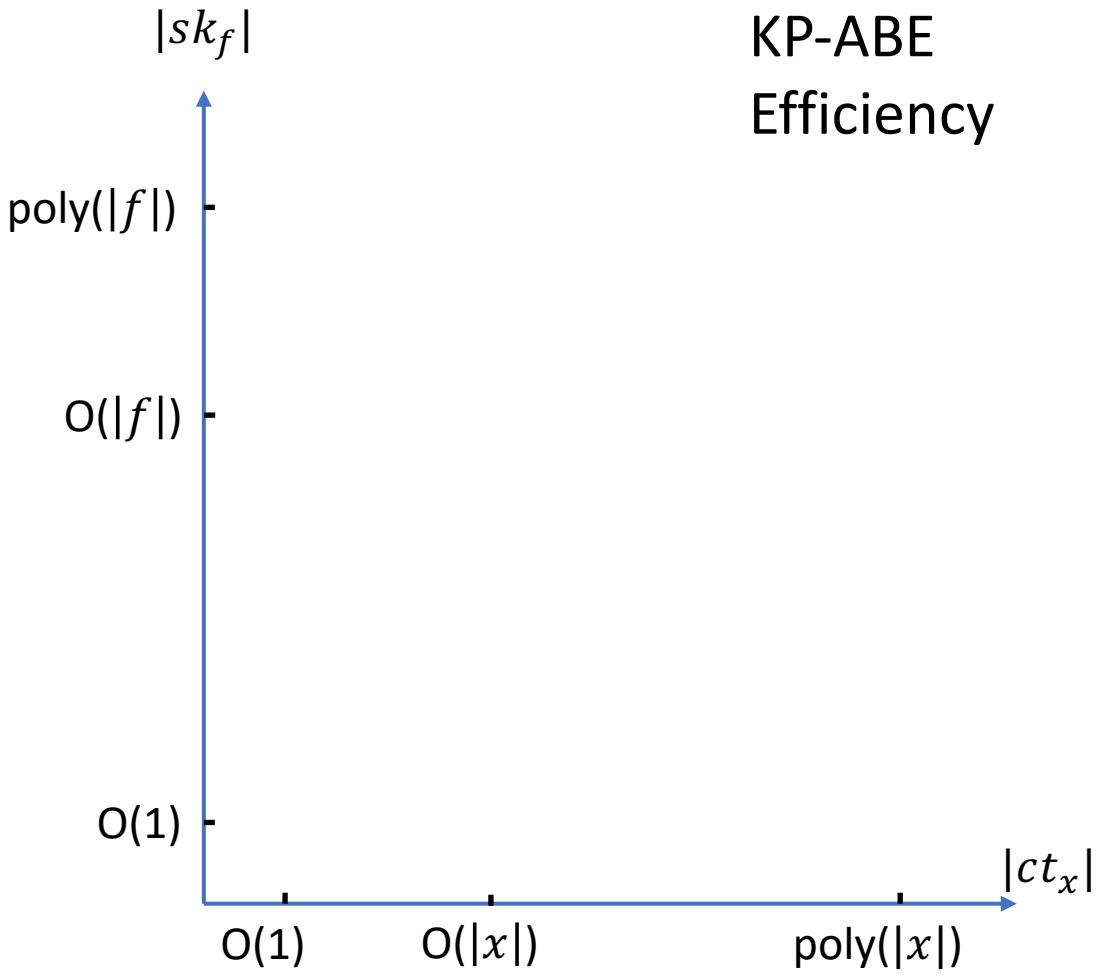
Ciphertext Policy (CP) variant

Correctness: Dec$(sk_{x_j}, ct_{f_i})= m_i$ if $f_i(x_j) = 0$

Security: analogous

Efficiency of ABE: Size of $|ct|, |sk|$

compared to $|x|, |f|$, ignoring poly(λ)

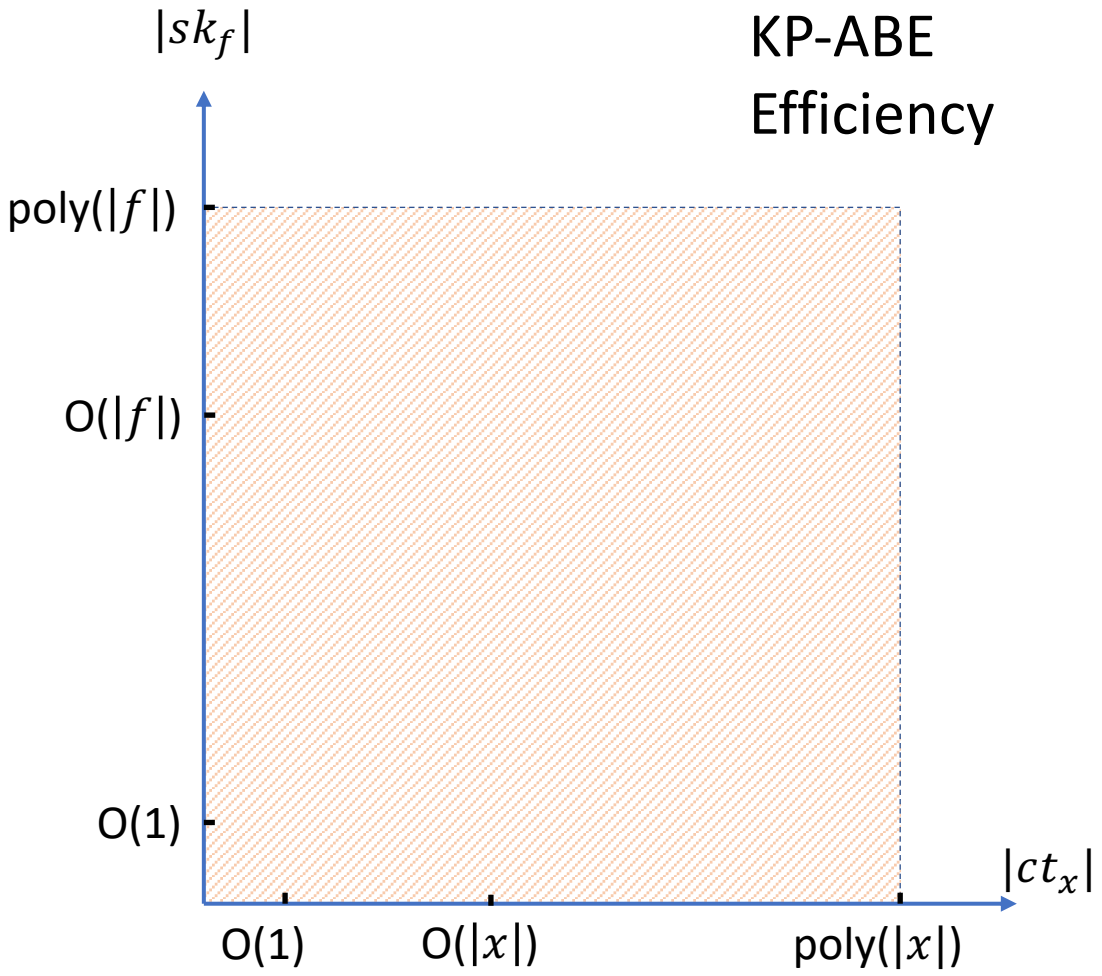


Efficiency of ABE: Size of $|ct|, |sk|$

compared to $|x|, |f|$, ignoring poly(λ)

- **Poly Efficiency**:

$|ct_x|$ = poly($|x|$), $|sk_f|$ = poly($|f|$)



Efficiency of ABE: Size of $|ct|, |sk|$

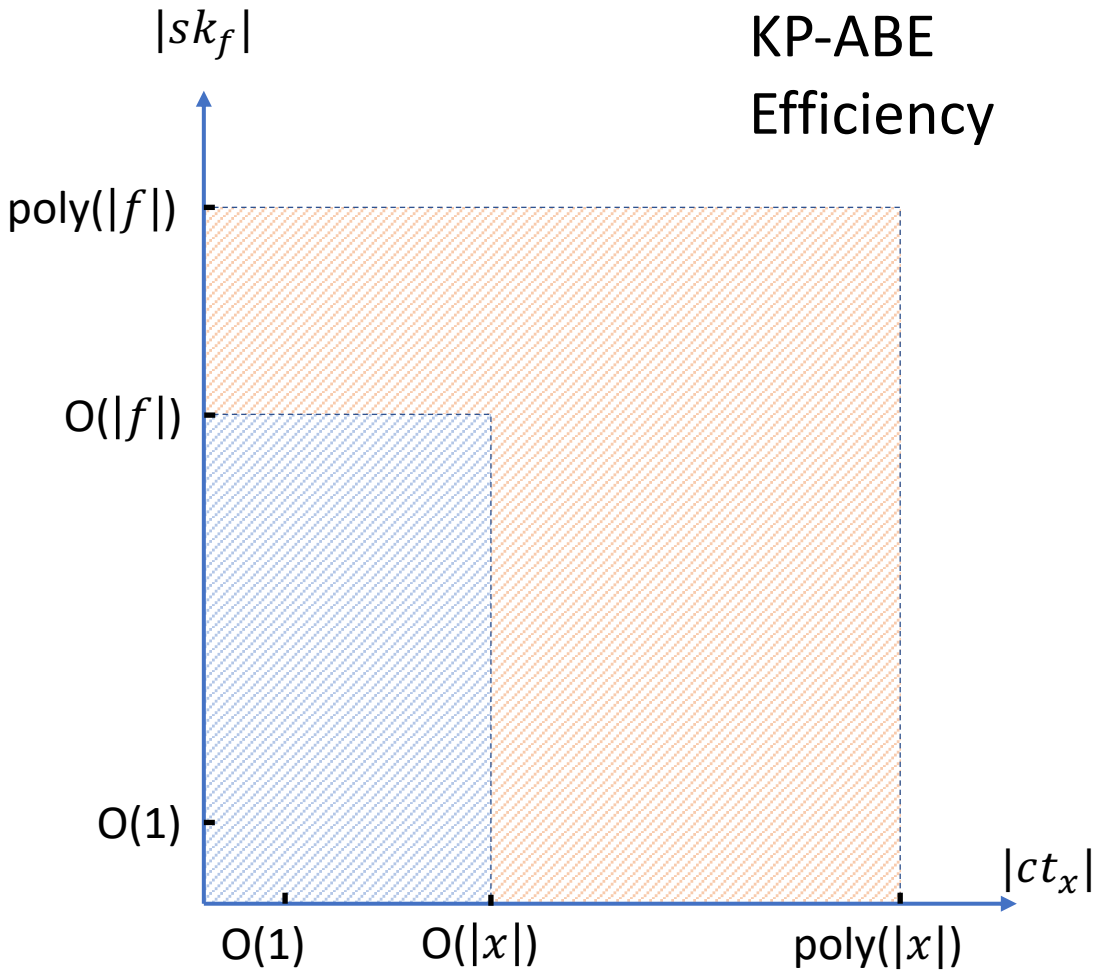
compared to $|x|, |f|$, ignoring poly(λ)

- **Poly Efficiency**:

  $|ct_x|$ = poly($|x|$), $|sk_f|$ = poly($|f|$)

- **Compact**:

  $|ct_x|$ = O($|x|$), $|sk_f|$ = O($|f|$)



Efficiency of ABE: Size of $|ct|, |sk|$

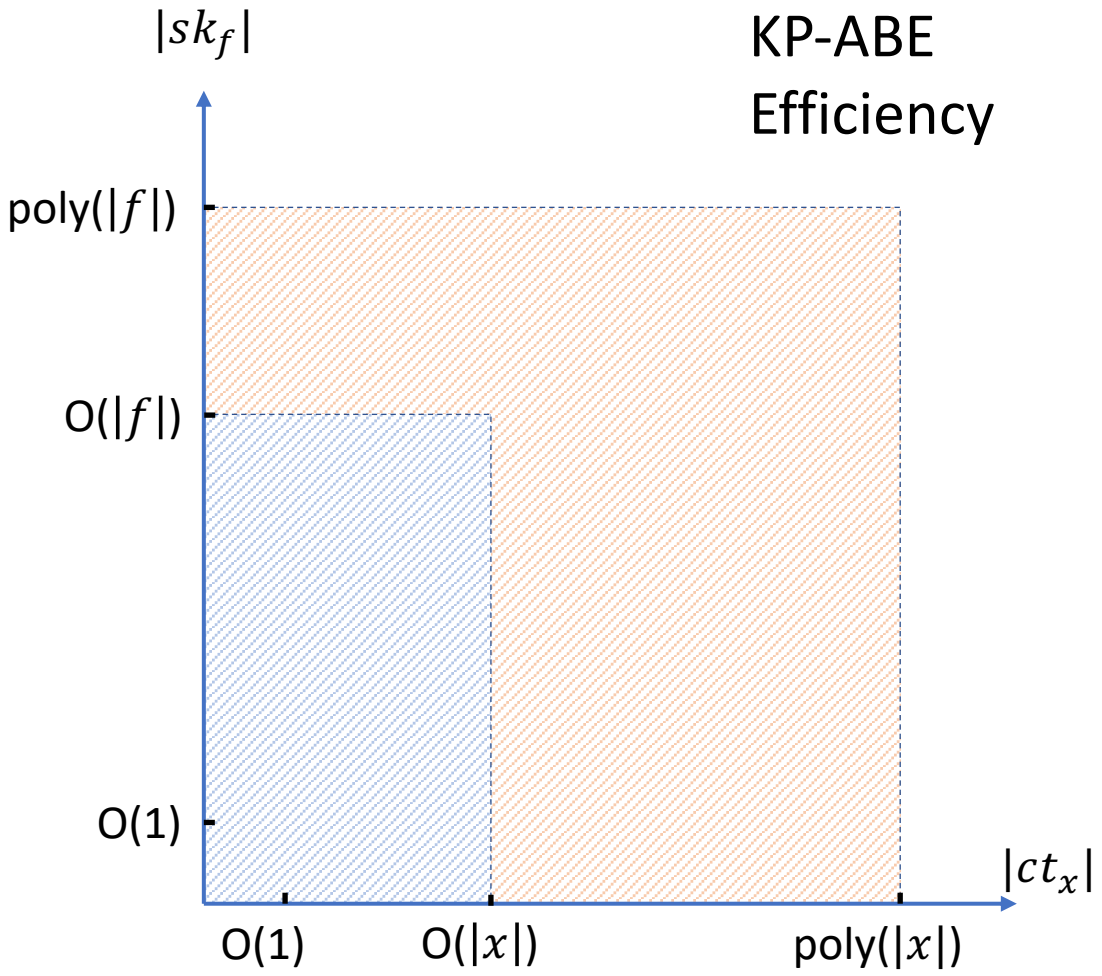
compared to $|x|, |f|$, ignoring poly(λ)

- **Poly Efficiency**:

  $|ct_x|$ = poly($|x|$), $|sk_f|$ = poly($|f|$)

- **Compact**: Best?

  $|ct_x|$ = O($|x|$), $|sk_f|$ = O($|f|$)



Efficiency of ABE: Size of $|ct|, |sk|$

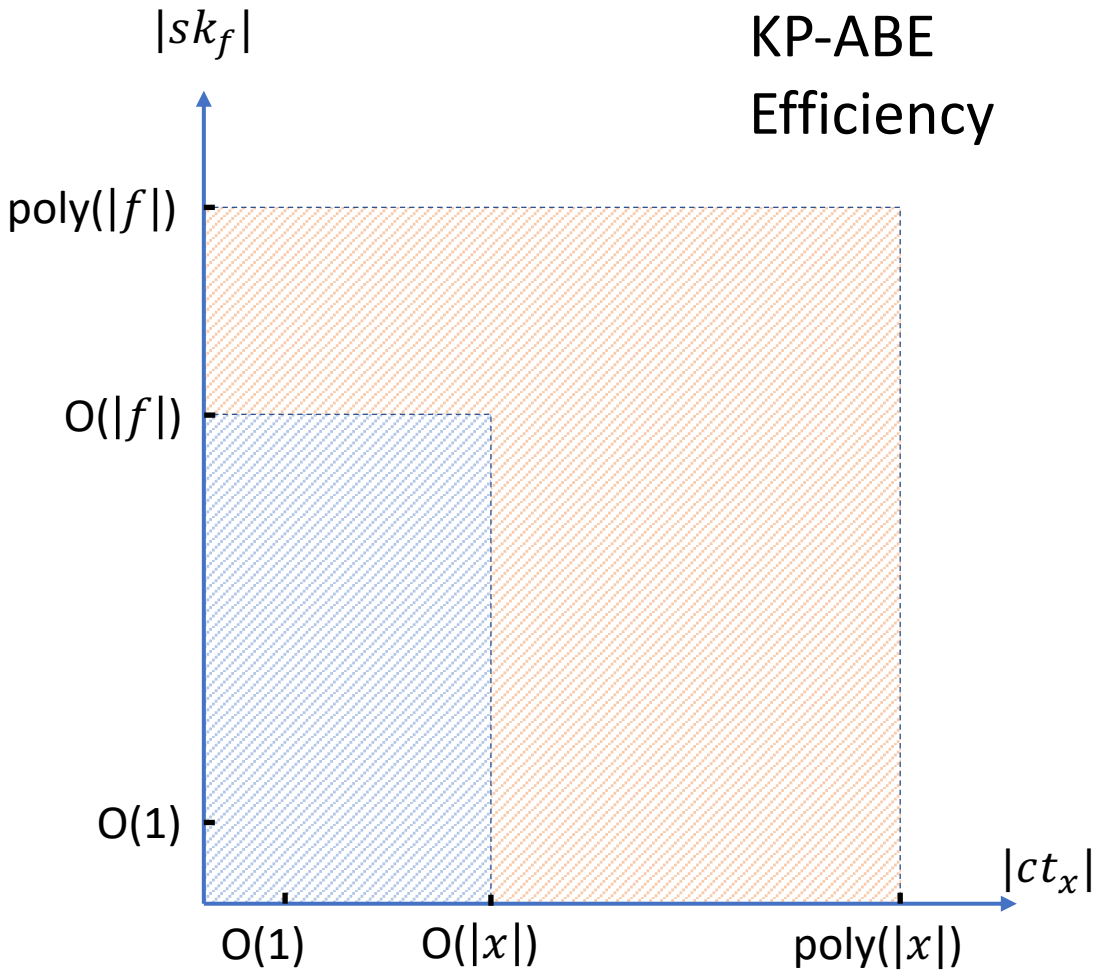
compared to $|x|, |f|$, ignoring poly(λ)

- **Poly Efficiency**:

  $|ct_x|$ = poly($|x|$), $|sk_f|$ = poly($|f|$)

- **Compact**: Best?

  $|ct_x|$ = O($|x|$), $|sk_f|$ = O($|f|$)



No hiding x, f!

Transmit x, f in the clear, i.e. Dec$(x, f, sk_f, ct_x) = m$.

Possible to have $|ct_x| < |x|, |sk_f| < |f|$.

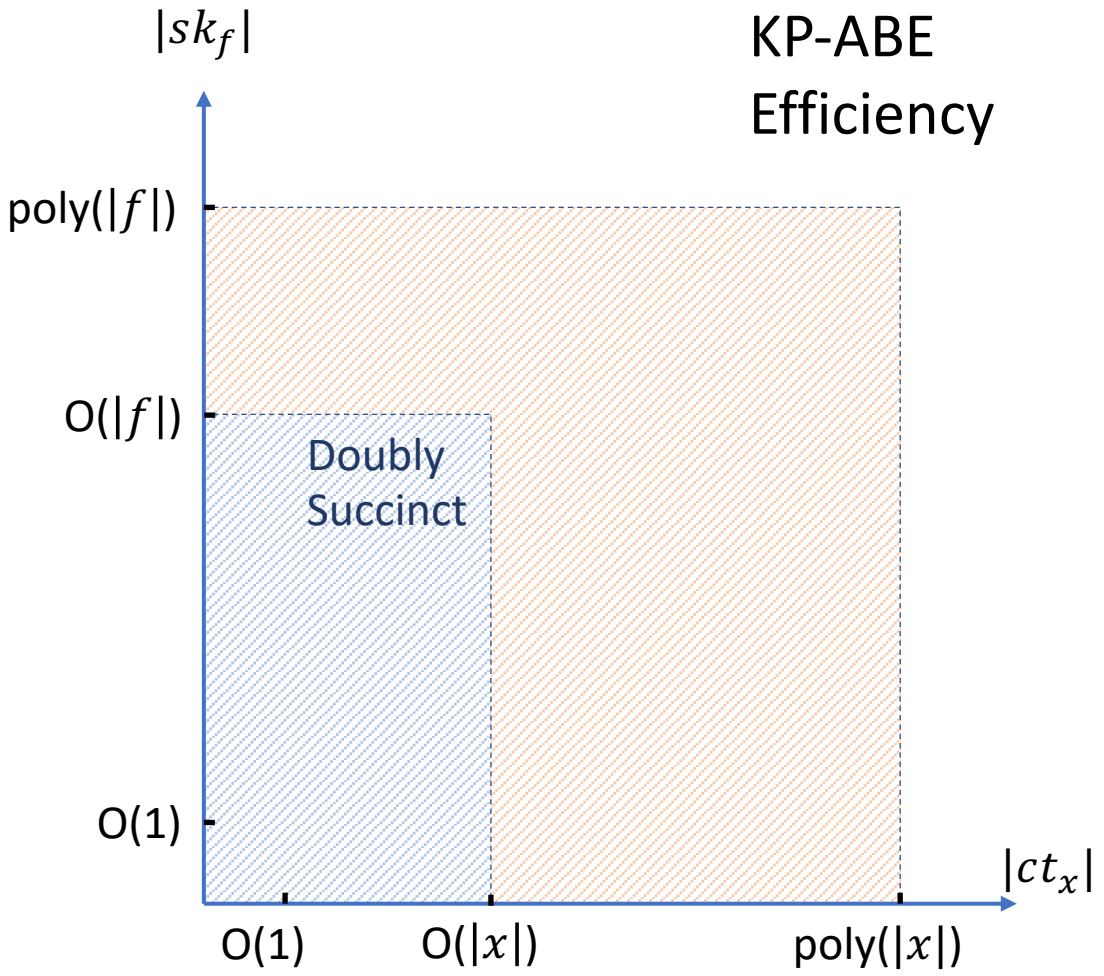
Efficiency of ABE: Size of $|ct|, |sk|$

compared to $|x|, |f|$, ignoring poly(λ)

- **Succinct**:

  $|ct_x|$ = o($|x|$), $|sk_f|$ = o($|f|$)

  (Doubly succinct if satisfying both.)



No hiding x, f!

Transmit x, f in the clear, i.e. Dec$(x, f, sk_f, ct_x) = m$.

Possible to have $|ct_x| < |x|, |sk_f| < |f|$.

Efficiency of ABE: Size of $|ct|, |sk|$

compared to $|x|, |f|$, ignoring poly(λ)

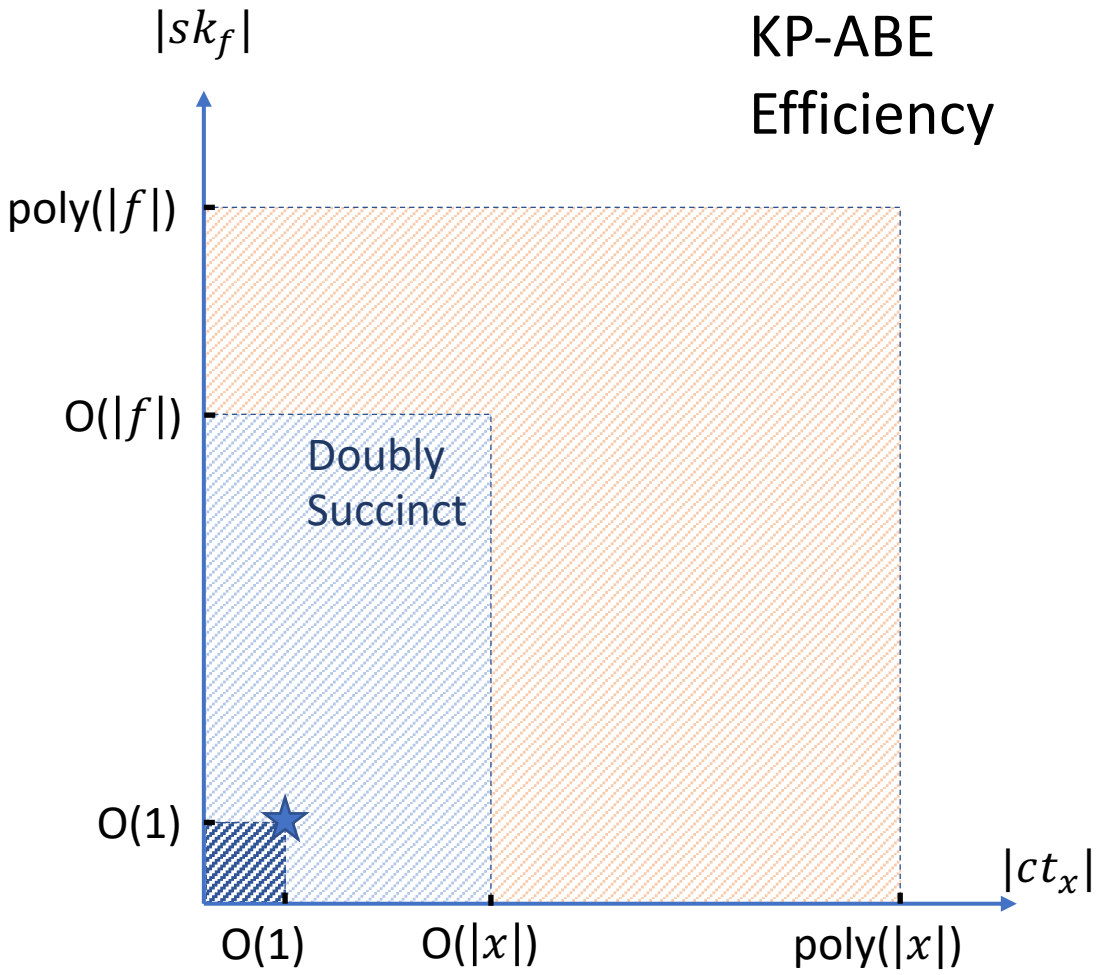
- **Succinct**:

  $|ct_x|$ = o($|x|$), $|sk_f|$ = o($|f|$)

  (Doubly succinct if satisfying both.)

- **Constant**: (Dream)

  $|ct_x|$ = O(1), $|sk_f|$ = O(1)

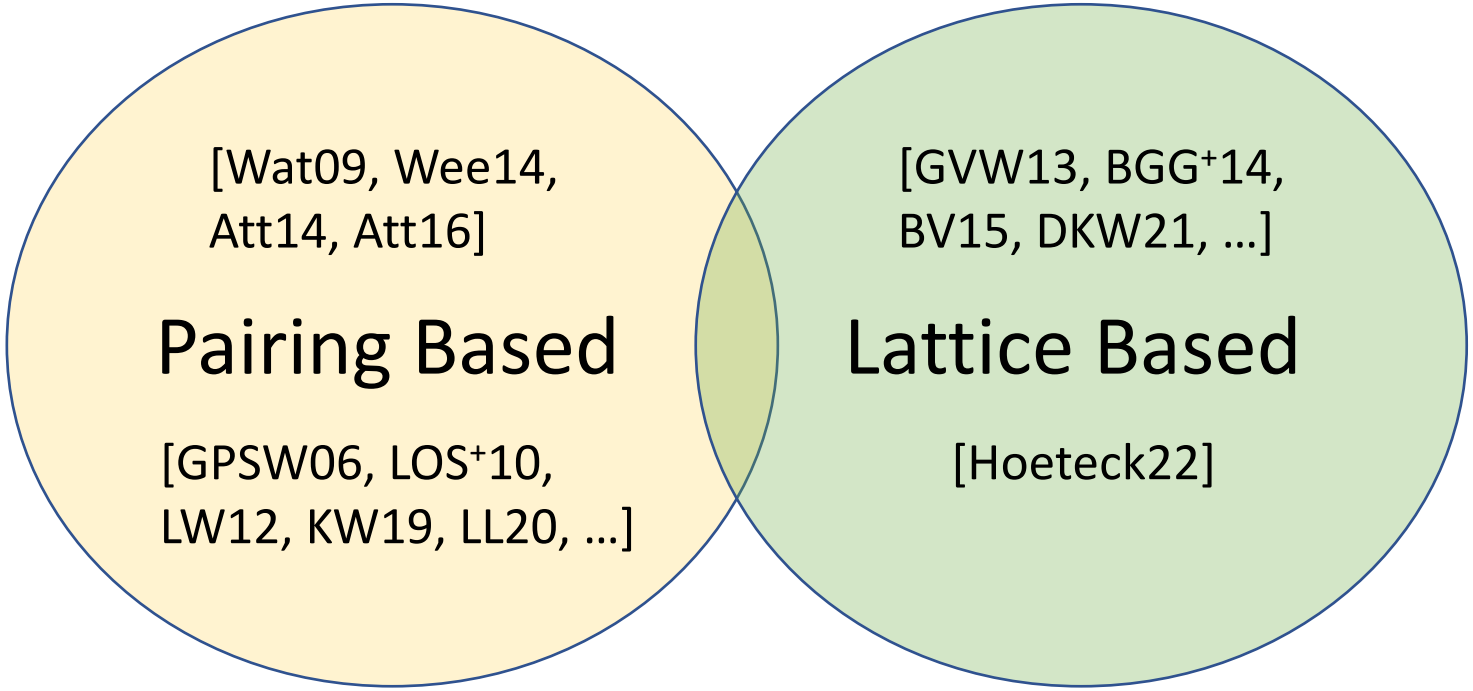


No hiding x, f!

Transmit x, f in the clear, i.e. Dec$(x, f, sk_f, ct_x) = m$.

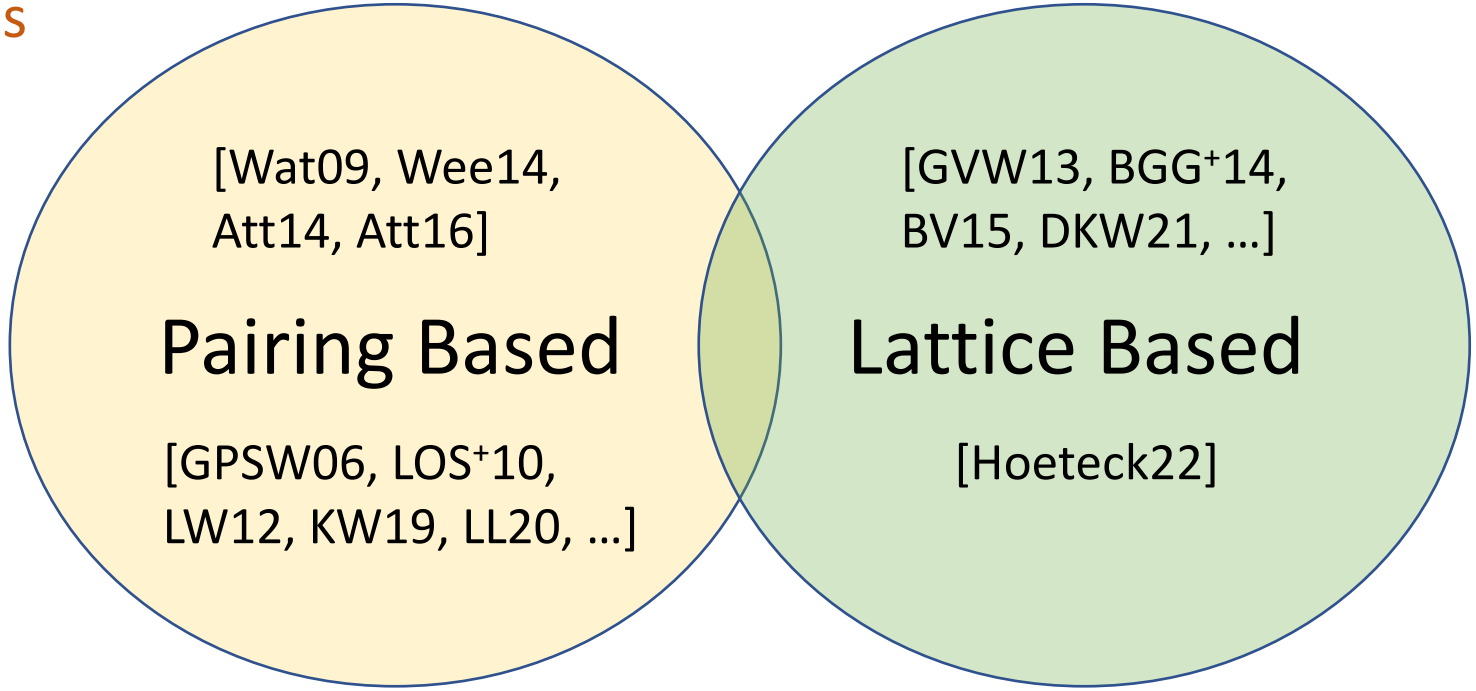
Possible to have $|ct_x| < |x|, |sk_f| < |f|$.

ABE Constructions



ABE Constructions

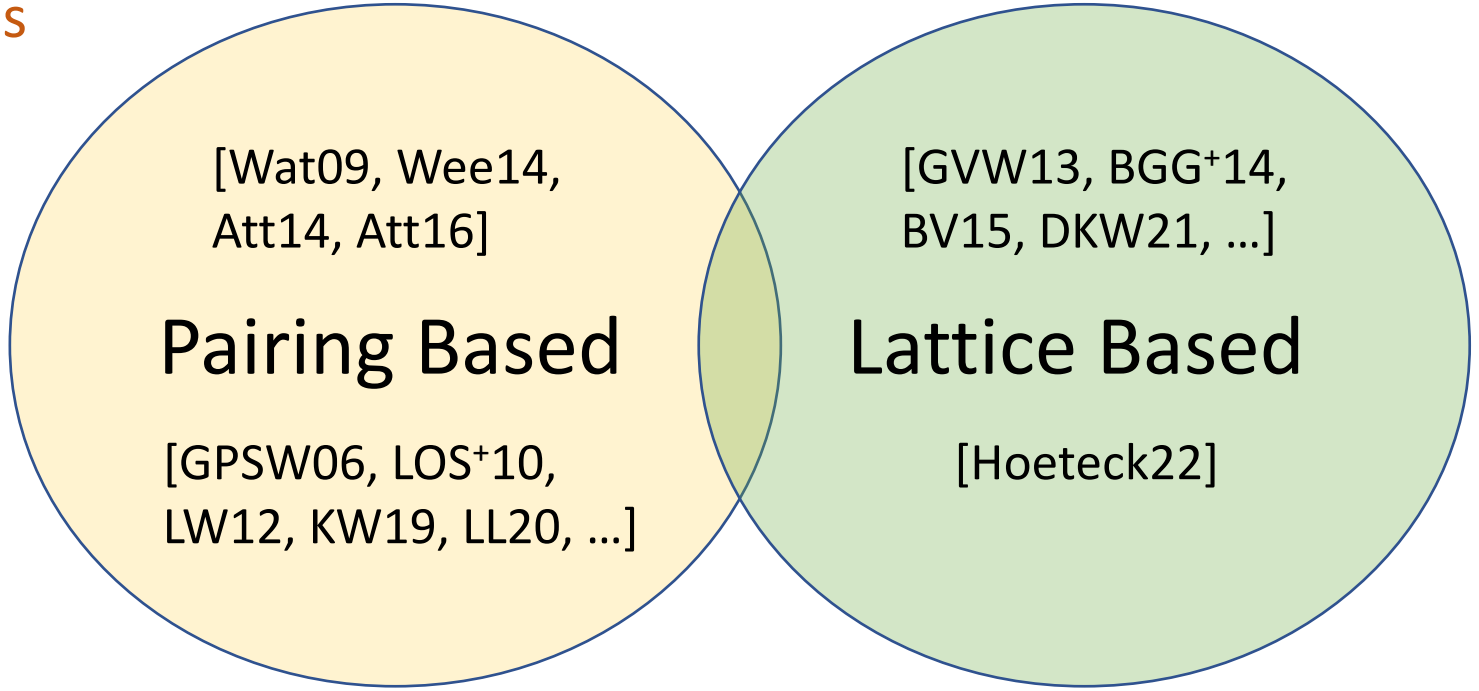
Low-depth policies



ABE Constructions

Low-depth policies

$$|sk| \cdot |ct| \geq |f| \cdot |x|$$

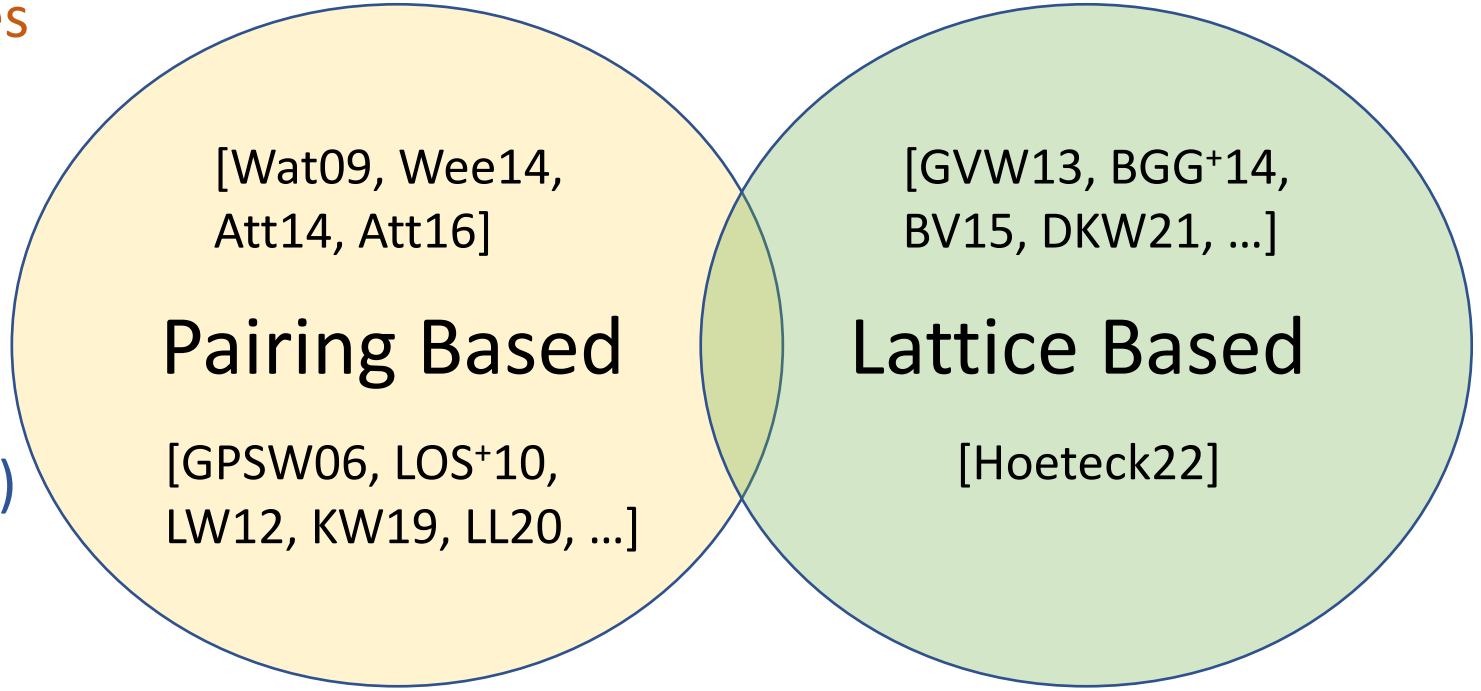


ABE Constructions

Low-depth policies

$|sk| \cdot |ct|$
$\geq |f| \cdot |x|$

$|sk|$ or $|ct|$ = O(1)



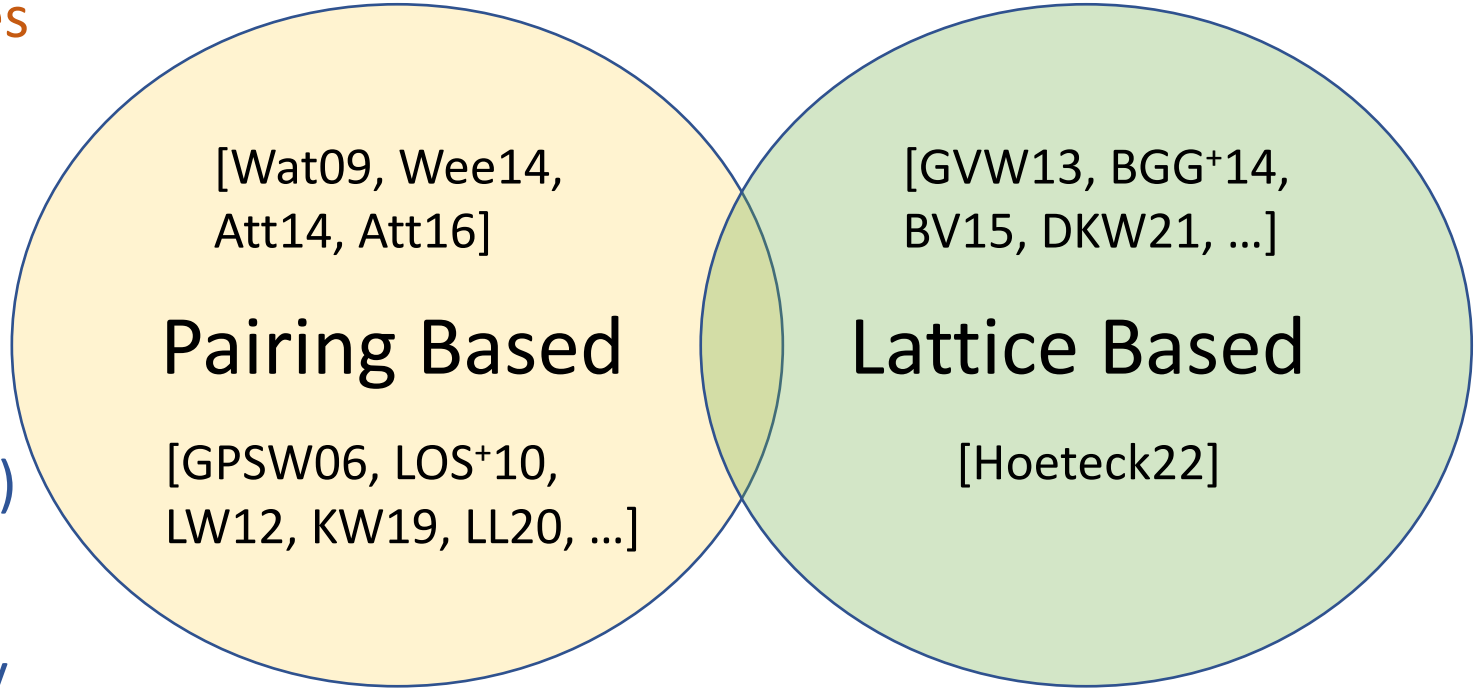
ABE Constructions

Low-depth policies

$|sk| \cdot |ct|$
$\geq |f| \cdot |x|$

$|sk|$ or $|ct|$ = O(1)

Adaptive Security



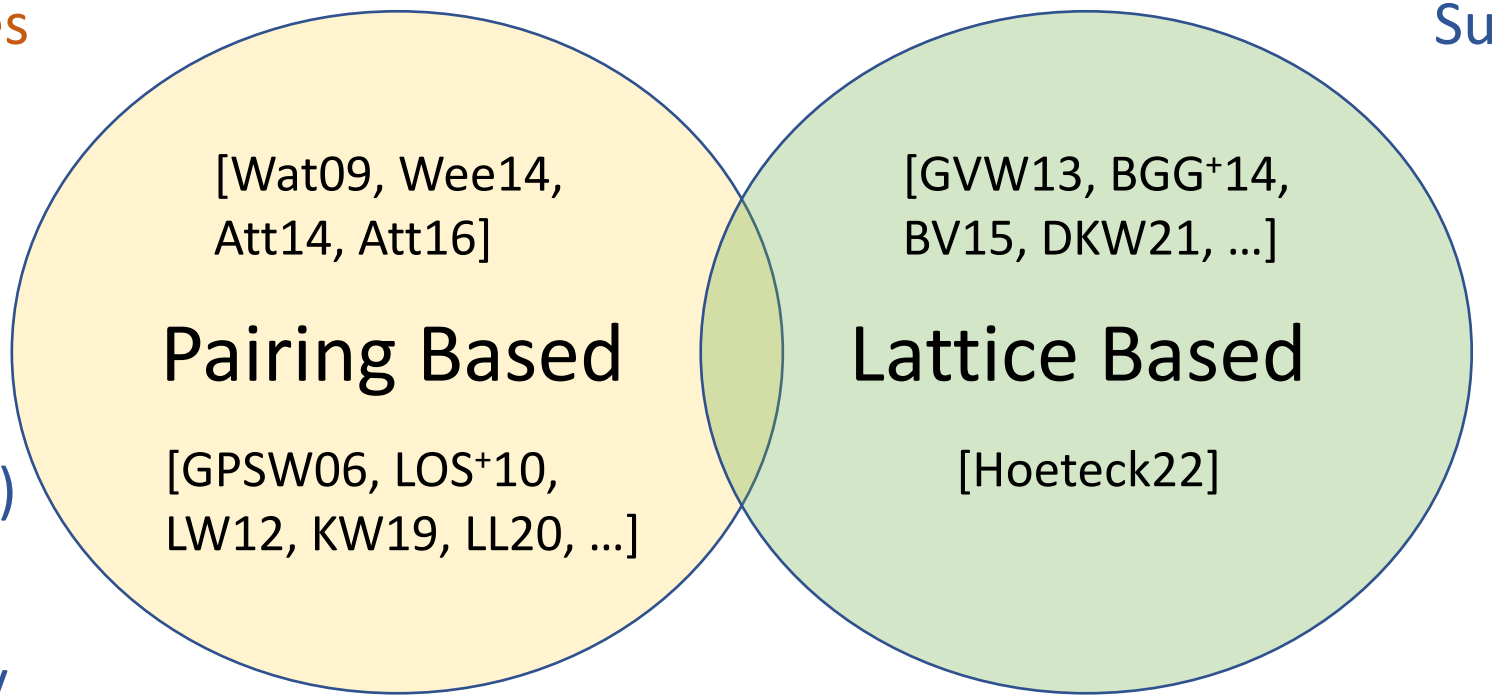
ABE Constructions

Low-depth policies

$|sk| \cdot |ct|$
$\geq |f| \cdot |x|$

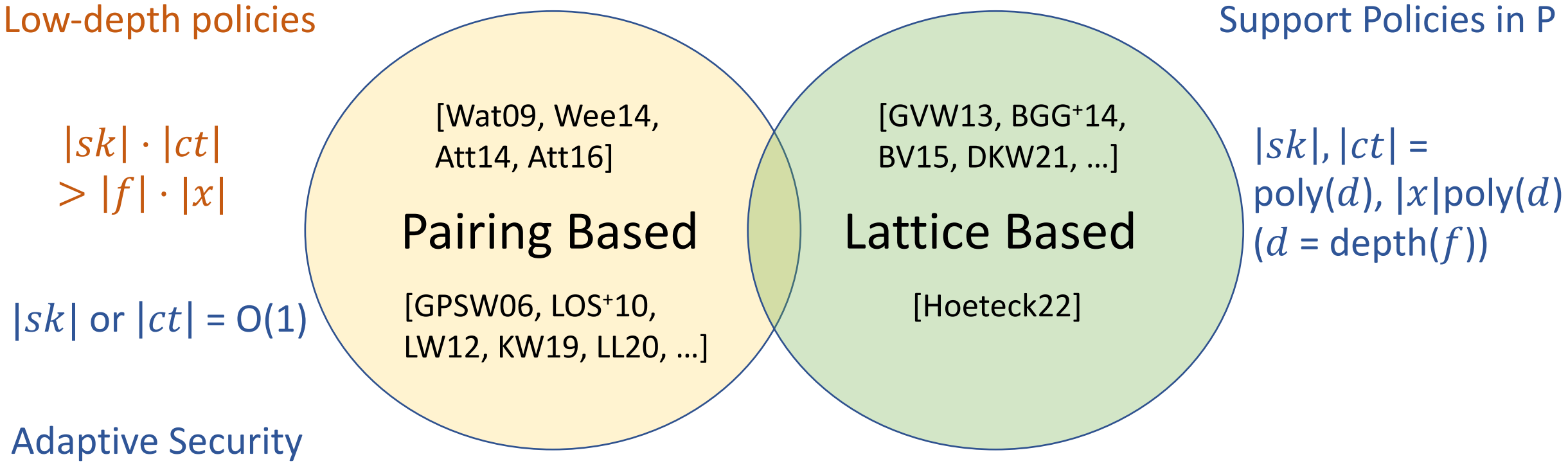
$|sk|$ or $|ct|$ = O(1)

Adaptive Security

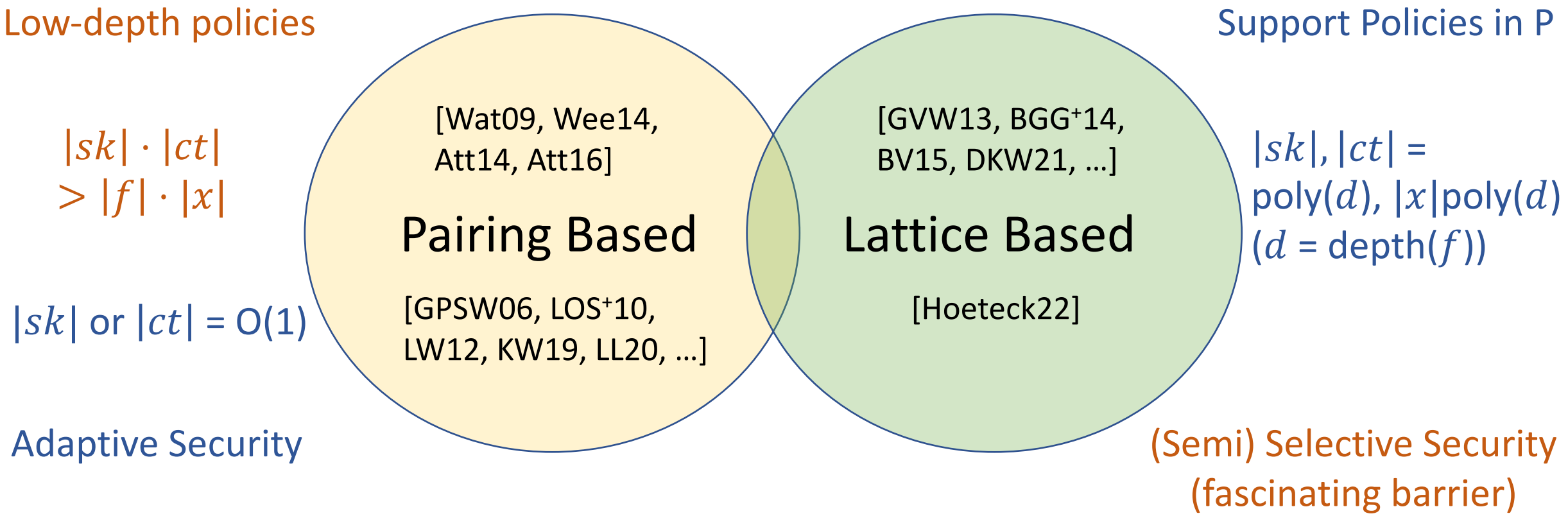


Support Policies in P

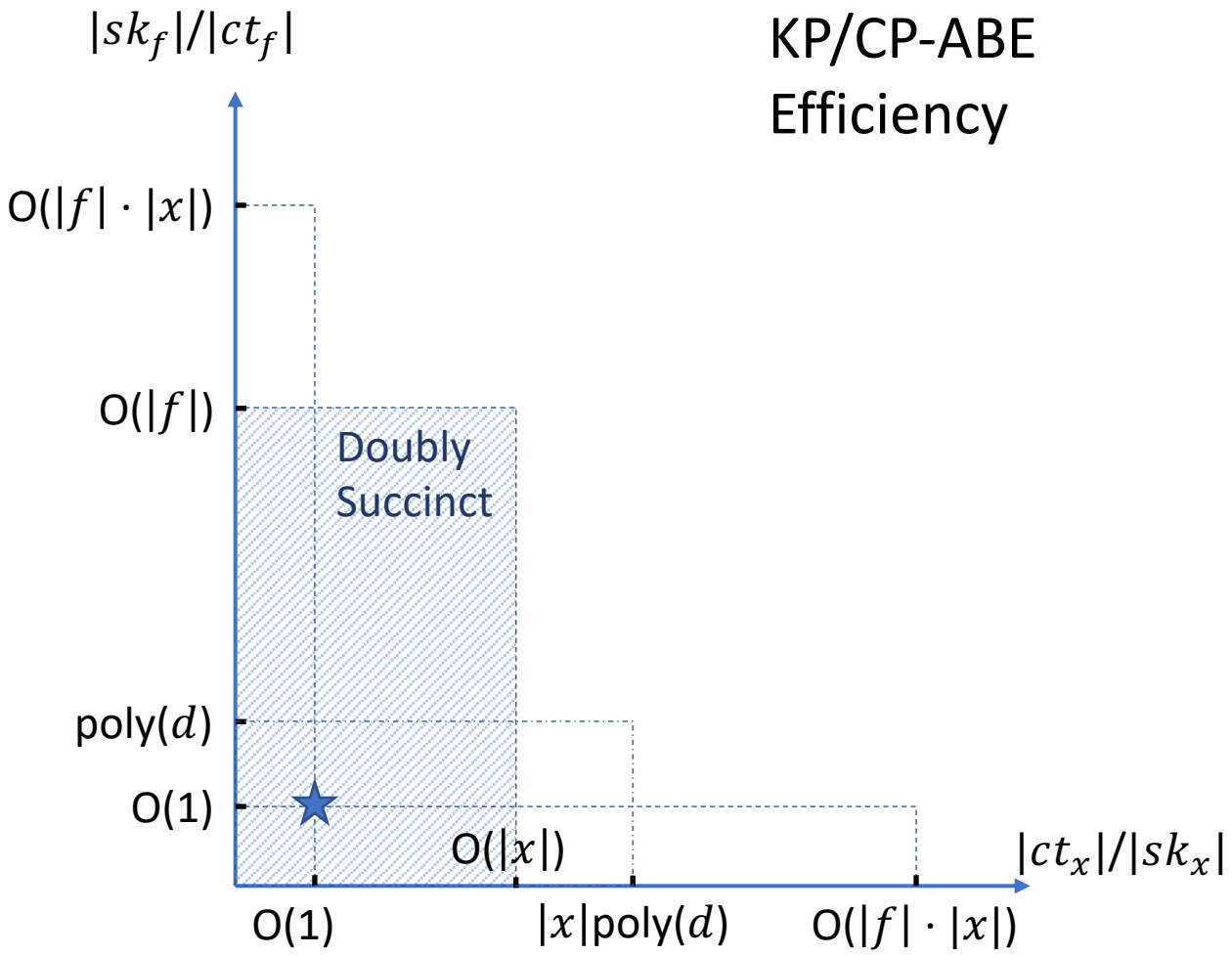
ABE Constructions



ABE Constructions

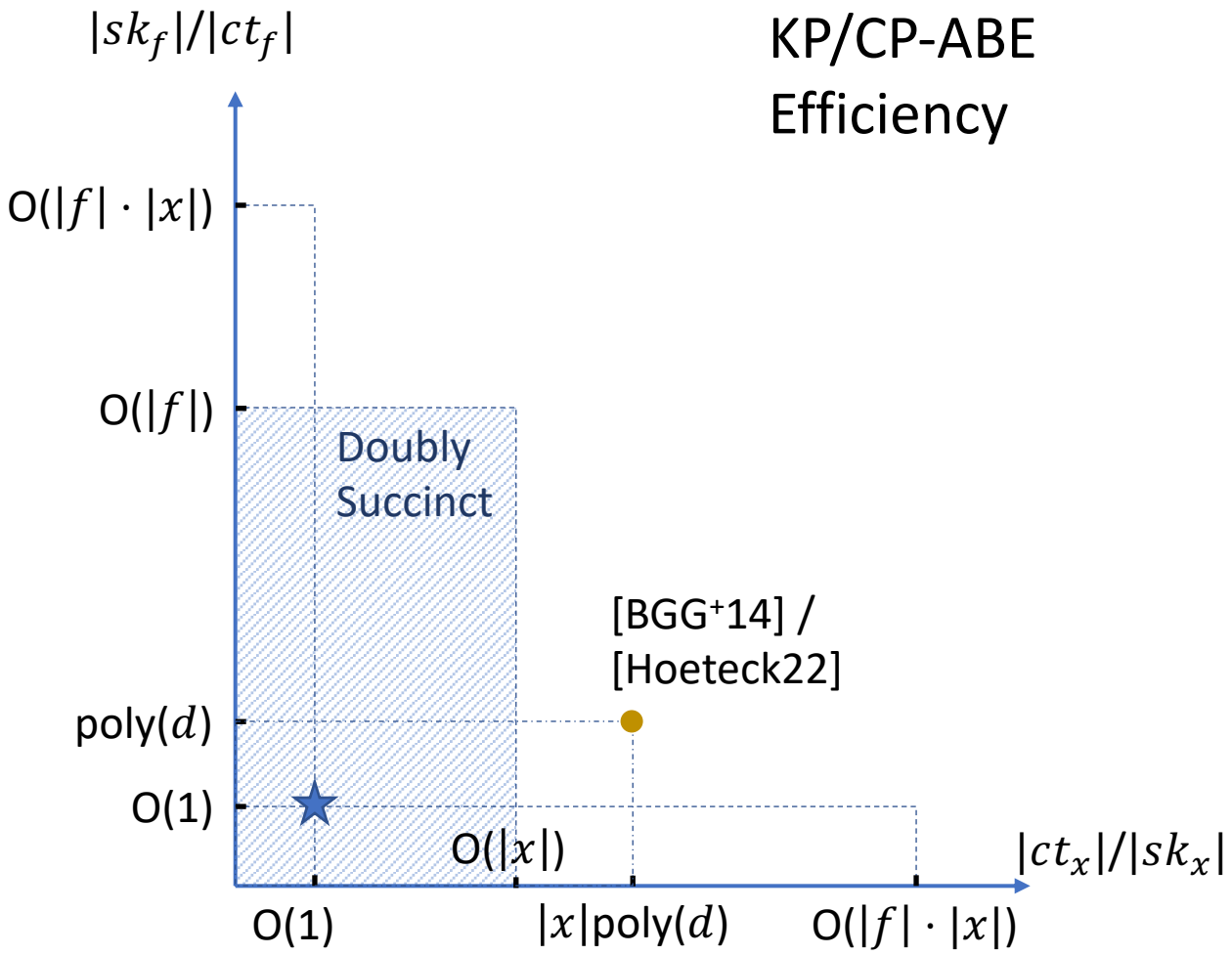


ABE Constructions

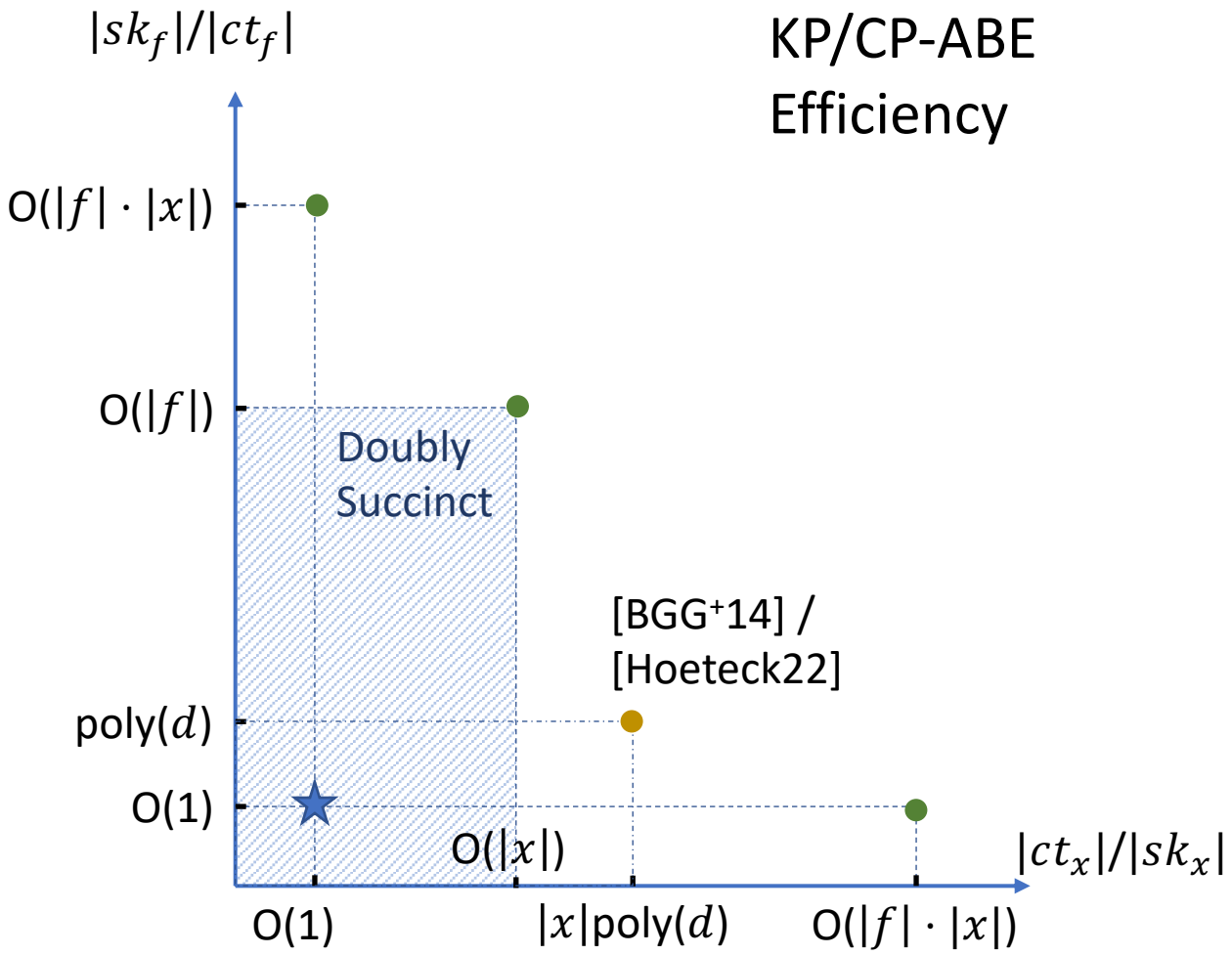


KP/CP-ABE
Efficiency

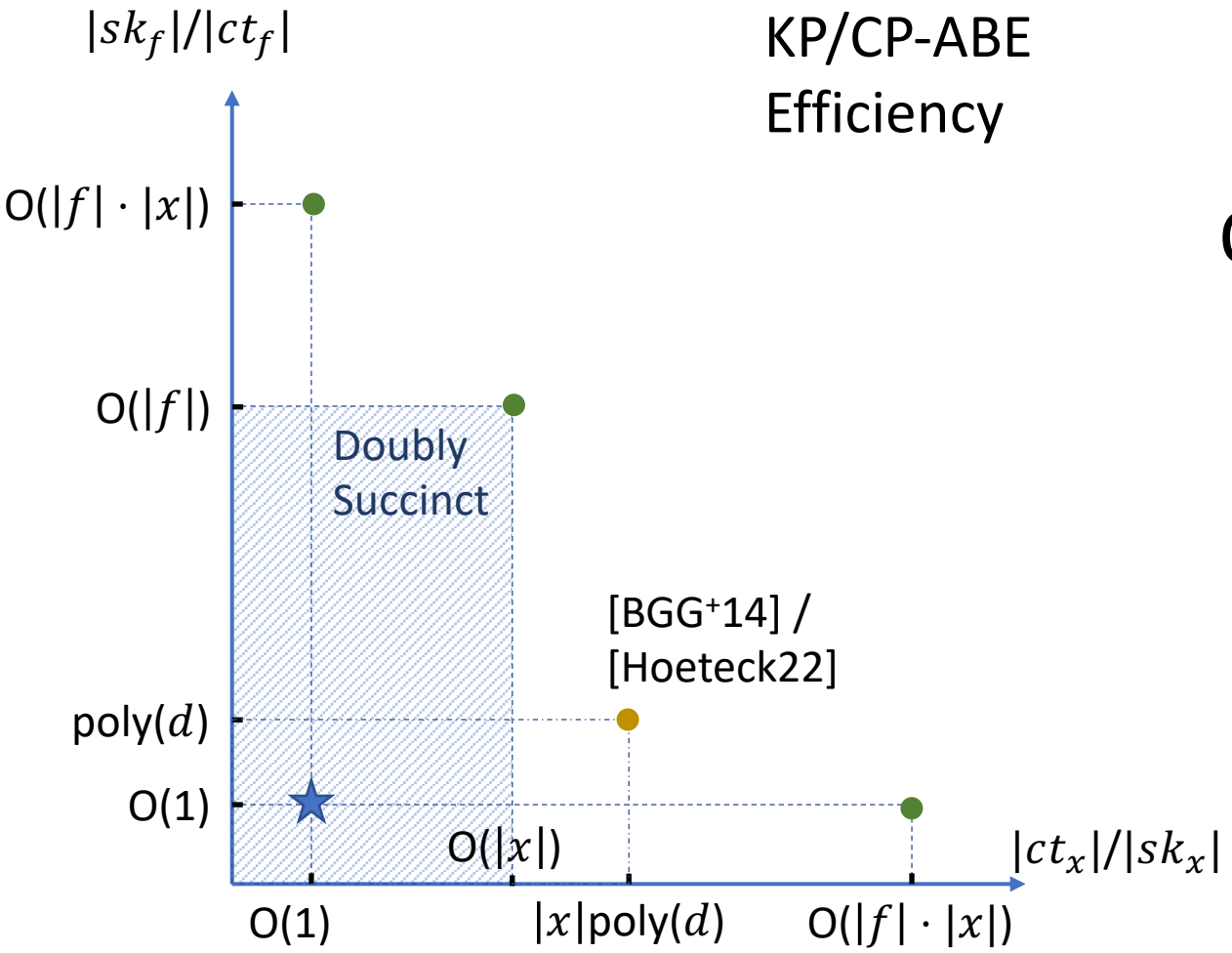
ABE Constructions



ABE Constructions



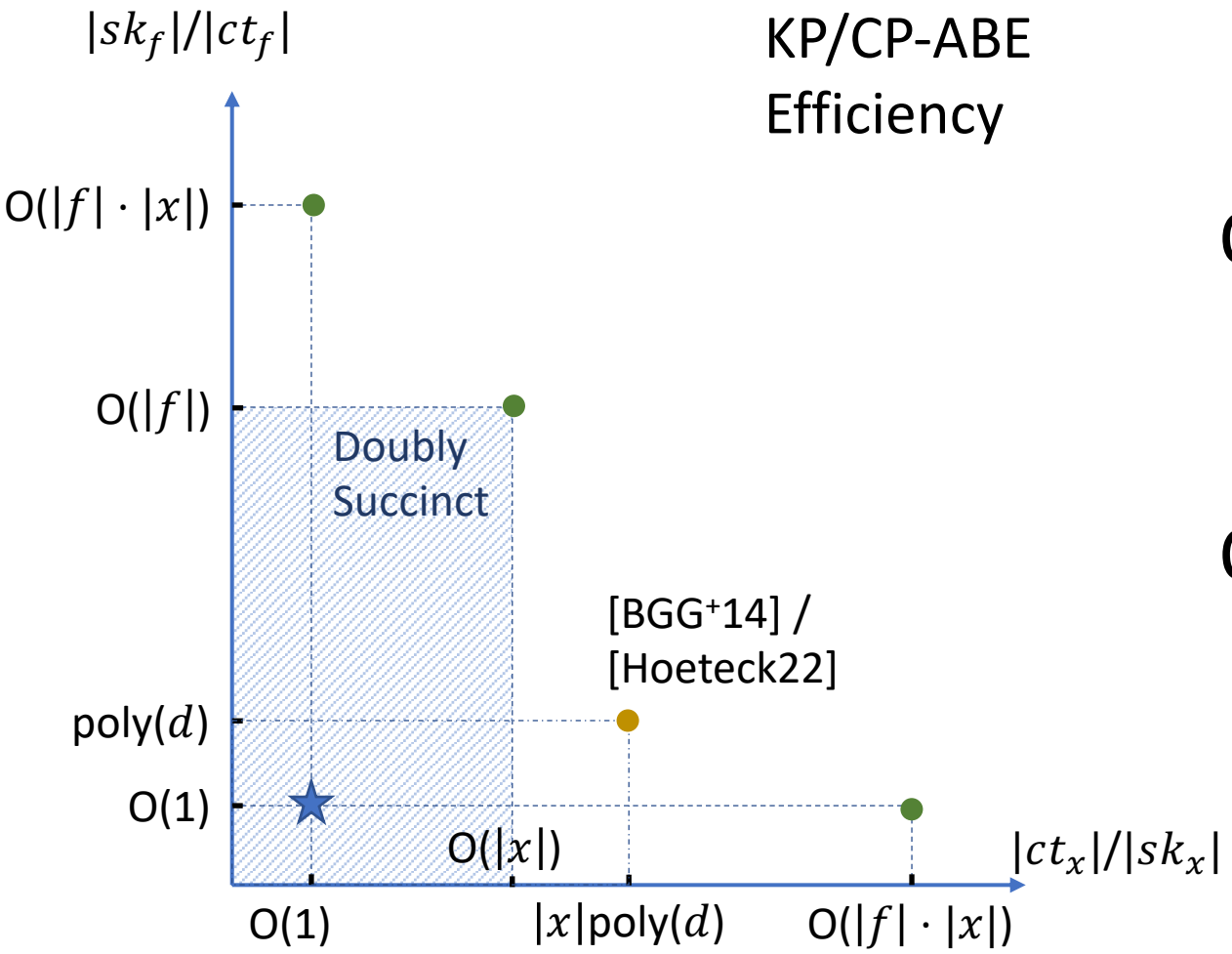
ABE Constructions



KP/CP-ABE
Efficiency

Q1: Closer to dream efficiency?

ABE Constructions



KP/CP-ABE
Efficiency

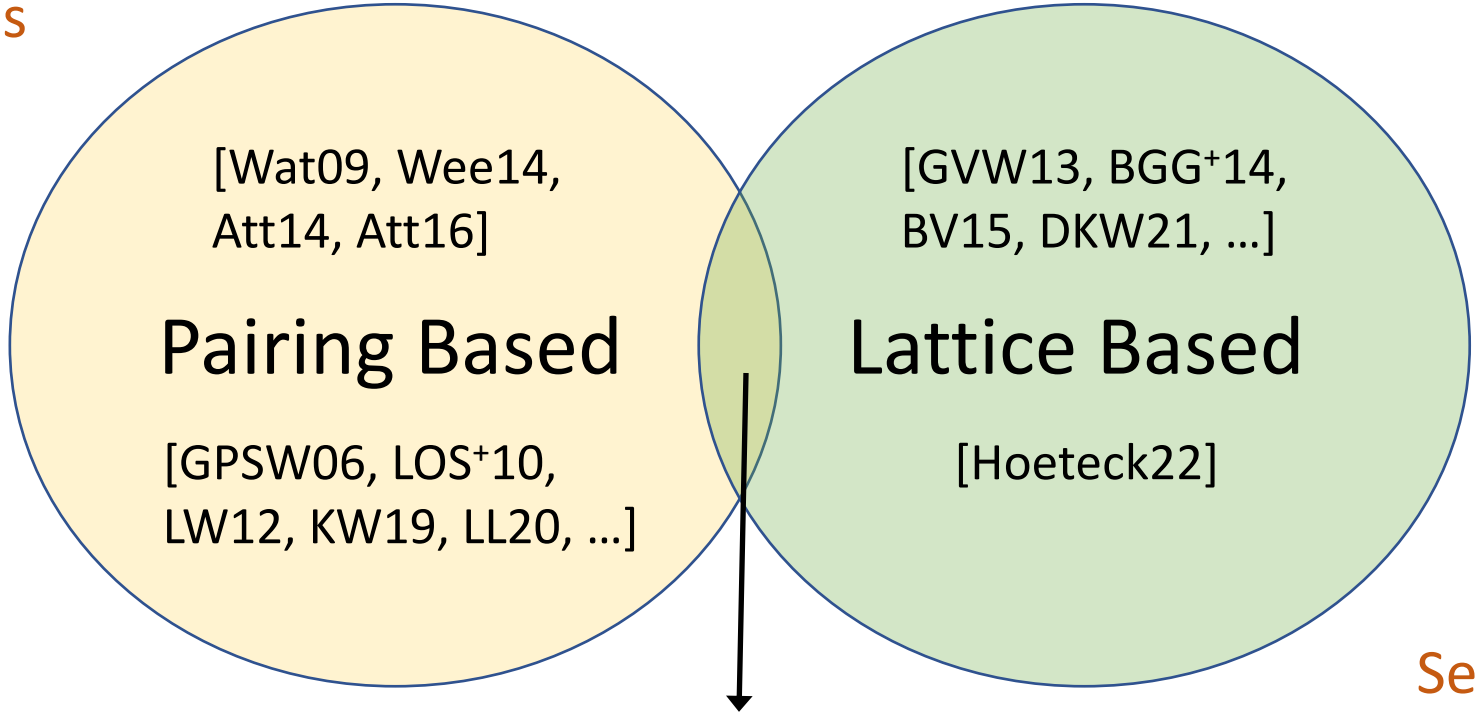
Q1: Closer to dream efficiency?

Q2: Can pairing + lattice help?

Recent Development

Low-depth policies

$|sk| \cdot |ct|$
$\not\geq$ $|f| \cdot |x|$
$<$



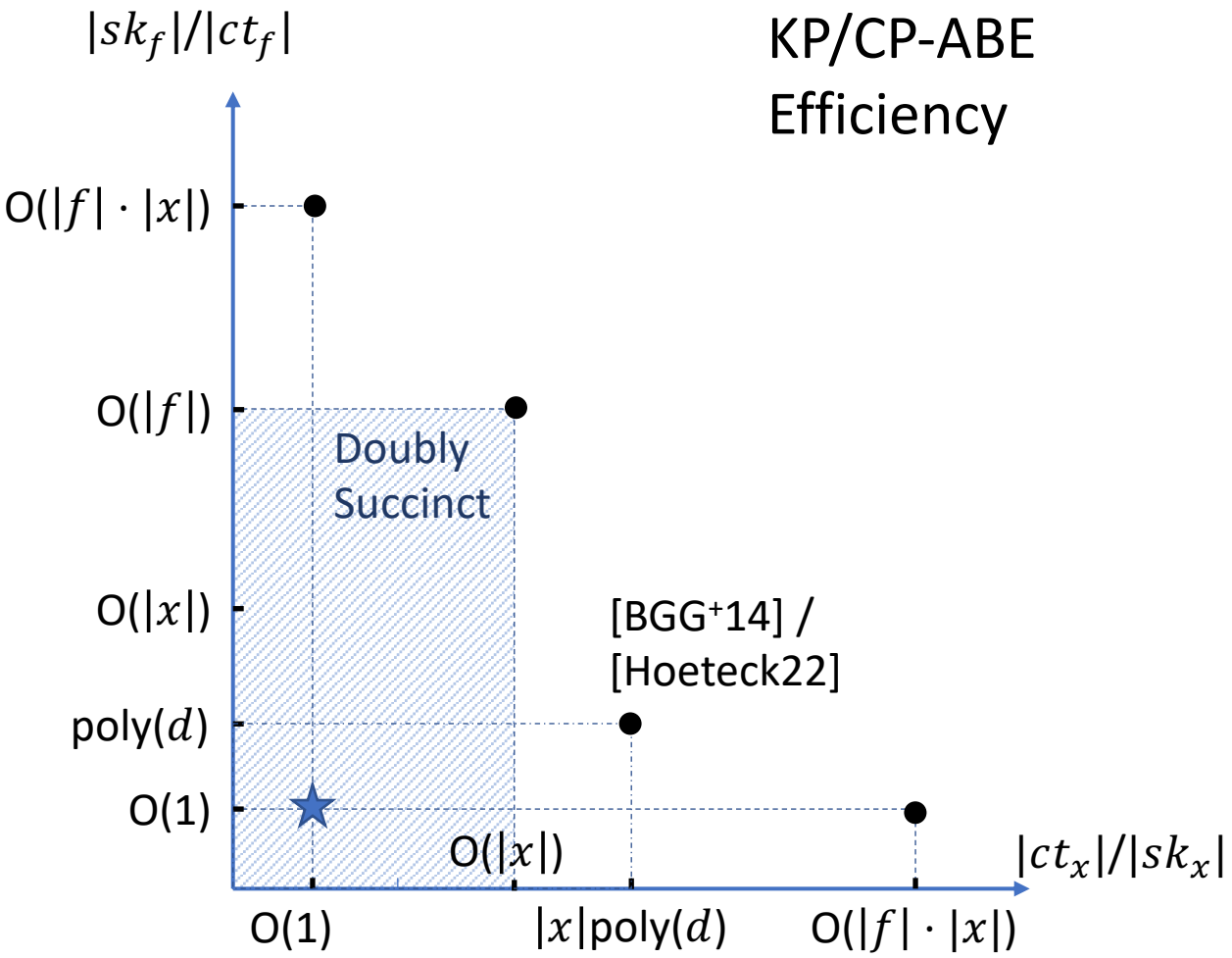
Selective Security (fascinating barrier)

[AY, AWY20]: CP-ABE for NC1

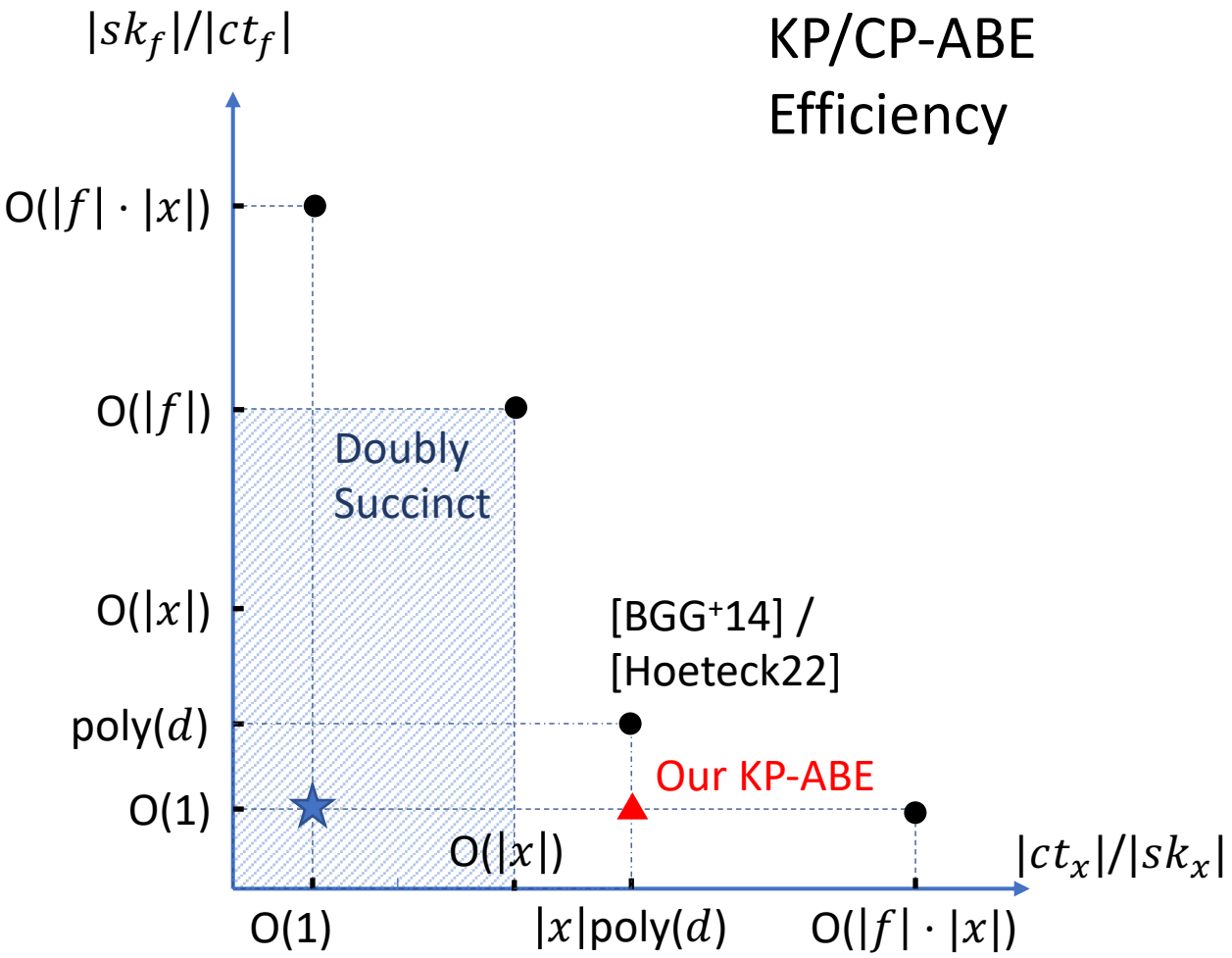
- Lattice + pairing
- $|sk_f|$= O($|x|$), $|ct_x|$= O($|x|$)
- Selective security

Succinct sk_f

Our Results


$|sk_f|/|ct_f|$
KP/CP-ABE
Efficiency
O($|f| \cdot |x|$)
O($|f|$)
O($|x|$)
poly(d)
O(1)
Doubly
Succinct
[BGG+14] /
[Hoeteck22]
O($|x|$)
$|ct_x|/|sk_x|$
O(1)
$|x|$poly(d)
O($|f| \cdot |x|$)

Our Results



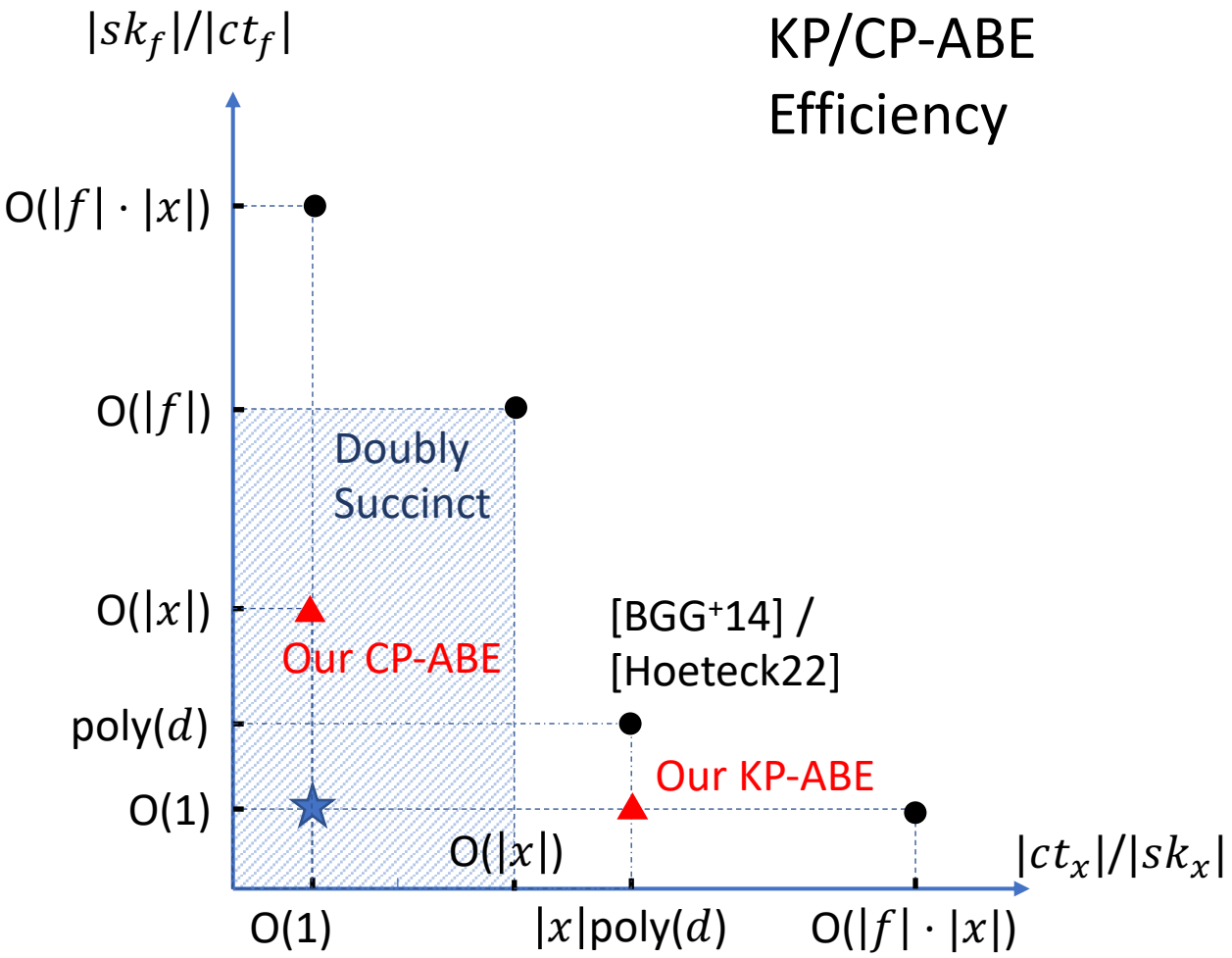
KP/CP-ABE Efficiency

Thm1: Assuming LWE + GGM

∃KP-ABE for P:

- $|sk_f|$ = O(1), $|ct_x|$ = $|x|$poly(d),
- Selective secure.

Our Results



Thm1: Assuming LWE + GGM

∃KP-ABE for P:

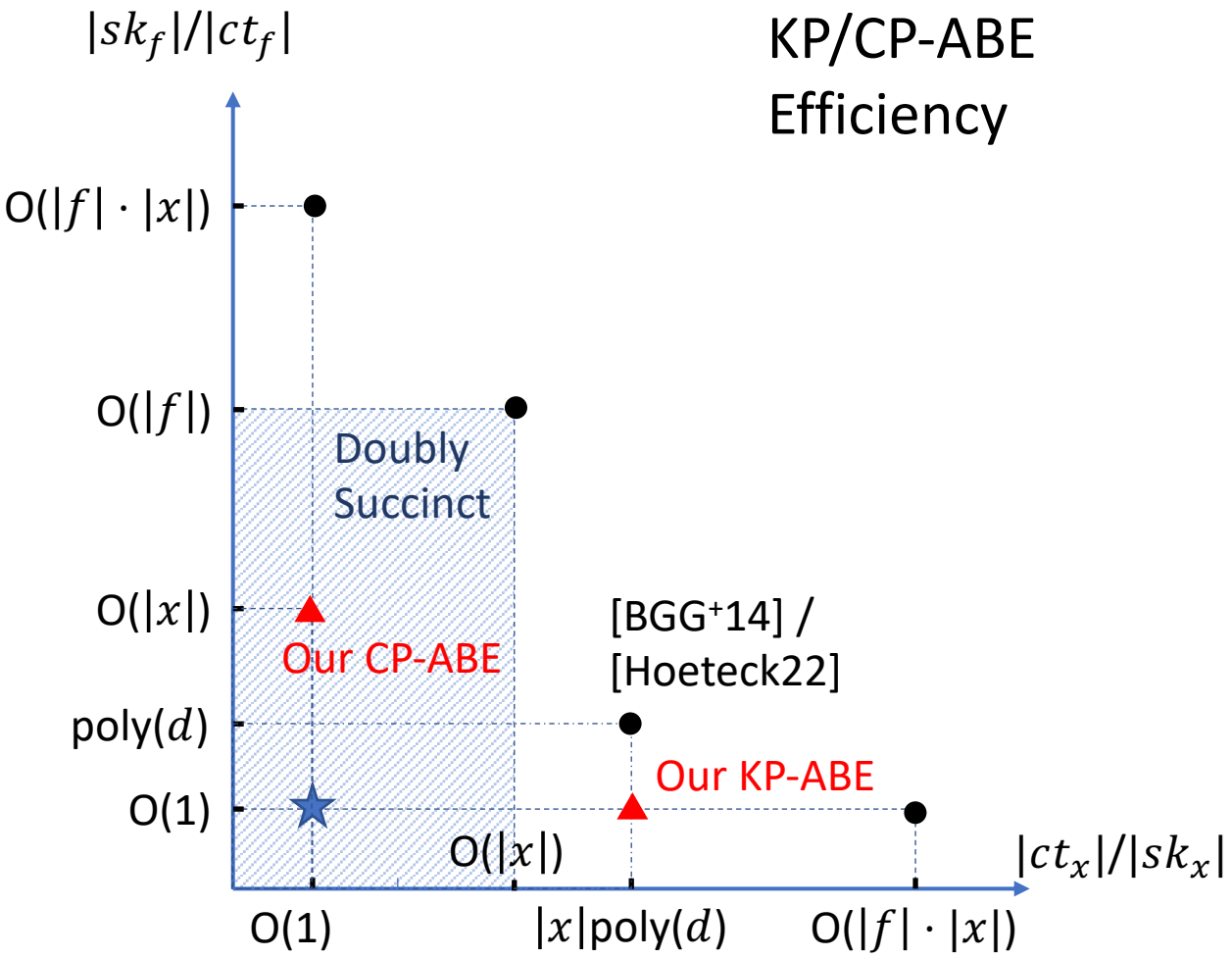
- $|sk_f|$ = O(1), $|ct_x|$ = $|x|$poly(d),
- Selective secure.

Thm2: Assuming LWE + GGM

∃CP-ABE for NC1:

- $|sk_x|$ = O(1), $|ct_f| = |x|^2$,
- Selective secure.

Our Results



Adaptive LWE[QWW18]

Thm1: Assuming ~~LWE~~ + GGM
∃KP-ABE for P:
- $|sk_f|$ = O(1), $|ct_x|$ = $|x|$poly(d),
- Adaptive secure.

Thm2: Assuming ~~LWE~~ + GGM
∃CP-ABE for NC1:
- $|sk_x|$ = O(1), $|ct_f| = |x|^2$,
- Adaptive secure.

Technique In A Nutshell

Technique In A Nutshell

KP-ABE for P [GVW13, BGG+14,..] uses lattice trapdoors

→ Bottleneck: large keys, sel-security

Lattice based Secure Function Evaluation (SFE) [QWW18]
(< 1-key ABE)

Multi-key ABE

Technique In A Nutshell

KP-ABE for P [GVW13, BGG+14,..] uses lattice trapdoors

→ Bottleneck: large keys, sel-security

Lattice based Secure Function Evaluation (SFE) [QWW18]

(< 1-key ABE)

+ Pairing →

Multi-key ABE

- Avoids trapdoors
- Adp-security from Adp-LWE

Technique In A Nutshell

Lattice based Secure Function Evaluation (SFE) [QWW18]
(< 1-key ABE)

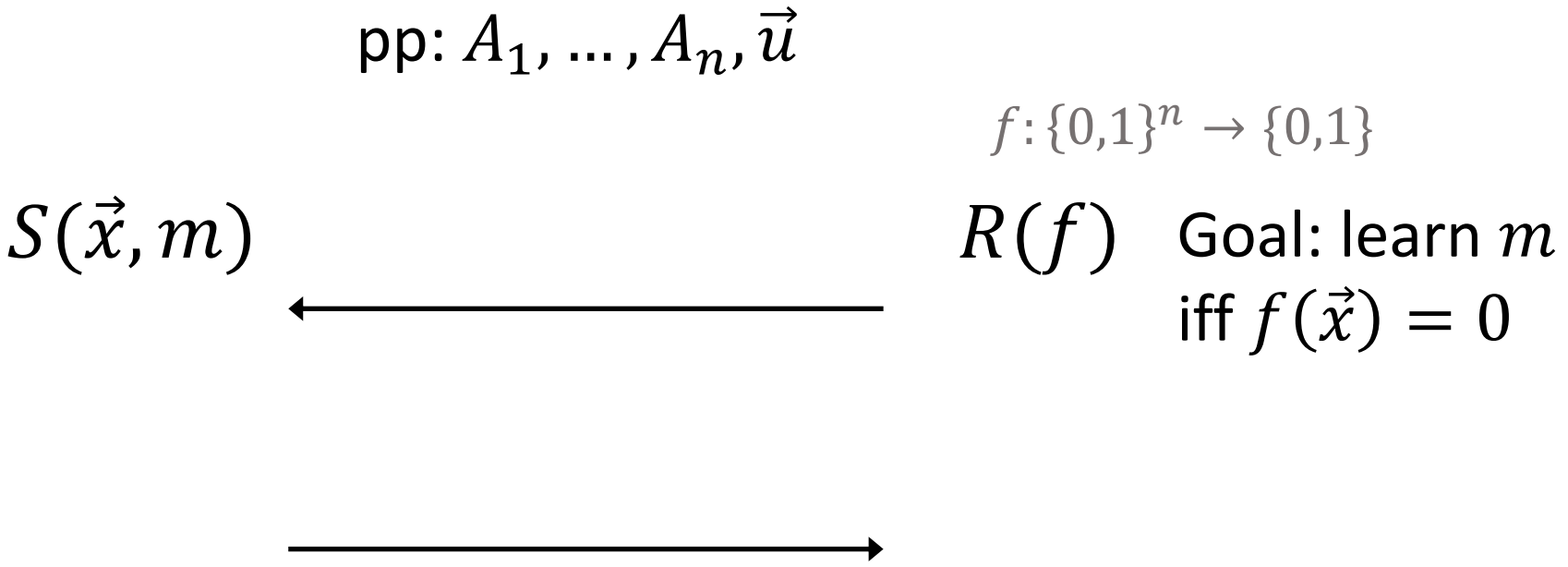
Multi-key ABE

Difficulty:

Lattice world:
Generates large noises
(e.g. HEval, noise flooding)

Pairing world:
Only allows small noises
(in the exponent)

The SFE Protocol [QWW18]



The SFE Protocol [QWW18]

pp: $A_1, \ldots, A_n, \vec{u}$

$S(\vec{x}, m)$ $\longleftarrow A_f$ $R(f)$ Goal: learn m iff $f(\vec{x}) = 0$

$\longrightarrow$

[BGG+14]: EvalPP$(f, \{A_i\}_i) \rightarrow A_f$

The SFE Protocol [QWW18]

pp: $A_1, \ldots, A_n, \vec{u}$

$S(\vec{x}, m)$ $\xleftarrow{A_f}$ $R(f)$ Goal: learn m iff $f(\vec{x}) = 0$

$ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i$

$\xrightarrow{\qquad\qquad}$

$\vec{s}$: LWE secret,
G: gadget matrix,
G^{-1}: public trapdoor

[BGG+14]: EvalPP$(f, \{A_i\}_i) \to A_f$

The SFE Protocol [QWW18]

pp: $A_1, \ldots, A_n, \vec{u}$

$S(\vec{x}, m)$ $\xleftarrow{\quad A_f \quad}$ $R(f)$ Goal: learn m iff $f(\vec{x}) = 0$

$ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i$

$\longrightarrow$

[BGG+14]: EvalPP$(f, \{A_i\}_i) \to A_f$

EvalCT$(f, \vec{x}, \{\vec{s}^\top (A_i + x_i G)\}_i) \to \vec{s}^\top \left(A_f + f(\vec{x}) G\right)$

The SFE Protocol [QWW18]

pp: $A_1, \ldots, A_n, \vec{u}$

$S(\vec{x}, m)$ $\xleftarrow{A_f}$ $R(f)$ Goal: learn m iff $f(\vec{x}) = 0$

$ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i$

$\longrightarrow$

[BGG+14]: EvalPP$(f, \{A_i\}_i) \to A_f$

EvalCT$(f, \vec{x}, \{\vec{s}^\top (A_i + x_i G)\}_i) \to \vec{s}^\top \left(A_f + \cancel{f(\vec{x})} G\right)$

$f(\vec{x}) = 0$

The SFE Protocol [QWW18]

pp: $A_1, \ldots, A_n, \vec{u}$

$S(\vec{x}, m)$ $\xleftarrow{A_f}$ $R(f)$ Goal: learn m iff $f(\vec{x}) = 0$

$ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i$ $\xrightarrow{\quad}$

$\vec{s}^\top A_f G^{-1}(\vec{u})$

[BGG+14]: EvalPP$(f, \{A_i\}_i) \to A_f$

EvalCT$(f, \vec{x}, \{\vec{s}^\top (A_i + x_i G)\}_i) \to \vec{s}^\top A_f$

$\times G^{-1}(\vec{u})$

The SFE Protocol [QWW18]

pp: $A_1, \ldots, A_n, \vec{u}$

$S(\vec{x}, m)$ $\xleftarrow{A_f}$ $R(f)$ Goal: learn m iff $f(\vec{x}) = 0$

$ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i$

$ct_m \approx \boxed{\vec{s}^\top A_f G^{-1}(\vec{u})} + m\lfloor q/2 \rfloor$ $\xrightarrow{\quad}$

$\boxed{\vec{s}^\top A_f G^{-1}(\vec{u})}$

[BGG+14]: $\mathsf{EvalPP}(f, \{A_i\}_i) \to A_f$

$\mathsf{EvalCT}(f, \vec{x}, \{\vec{s}^\top (A_i + x_i G)\}_i) \to \vec{s}^\top A_f$

The SFE Protocol [QWW18]

pp: $A_1, \ldots, A_n, \vec{u}$

$S(\vec{x}, m)$ $\xleftarrow{A_f}$ $R(f)$ Goal: learn m iff $f(\vec{x}) = 0$

$ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i$

$ct_m \approx \boxed{\vec{s}^\top A_f G^{-1}(\vec{u})} + m\lceil q/2 \rfloor$ $\xrightarrow{\quad}$

$ct_m - \boxed{\vec{s}^\top A_f G^{-1}(\vec{u})} \approx m\lceil q/2 \rfloor$

[BGG+14]: $\mathsf{EvalPP}(f, \{A_i\}_i) \to A_f$

$\mathsf{EvalCT}(f, \vec{x}, \{\vec{s}^\top (A_i + x_i G)\}_i) \to \vec{s}^\top A_f$

SFE to KP-ABE

ABE.mpk = pp: $A_1, \ldots, A_n, \vec{u}$

$S(\vec{x}, m)$ $\xleftarrow{A_f}$ $R(f)$ Goal: learn m iff $f(\vec{x}) = 0$

ABE.$ct_x(m) = \{$

$ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i$

$ct_m \approx \vec{s}^\top A_f G^{-1}(\vec{u}) + m\lceil q/2 \rfloor$ $\xrightarrow{\quad}$

$ct_m - \boxed{\vec{s}^\top A_f G^{-1}(\vec{u})} \approx m\lceil q/2 \rfloor$

[BGG+14]: EvalPP$(f, \{A_i\}_i) \to A_f$,

EvalCT$(f, \vec{x}, \{\vec{s}^\top (A_i + x_i G)\}_i) \to \vec{s}^\top A_f$

SFE to KP-ABE

ABE.mpk = pp: $A_1, \ldots, A_n, \vec{u}$

$S(\vec{x}, m)$ $\xleftarrow{\quad A_f \quad}$ $R(f)$ Goal: learn m iff $f(\vec{x}) = 0$

ABE.$ct_x(m) = \{$

$ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i$

$ct_m \approx \vec{s}^\top \cancel{A_f} G^{-1}(\vec{u}) + m\lceil q/2 \rfloor$ $\xrightarrow{\quad\quad}$

$ct_m - \boxed{\vec{s}^\top A_f G^{-1}(\vec{u})}$
$\approx m\lceil q/2 \rfloor$

- Dep. on f
- What's sk_f?

[BGG+14]: EvalPP$(f, \{A_i\}_i) \to A_f$,
EvalCT$(f, \vec{x}, \{\vec{s}^\top (A_i + x_i G)\}_i) \to \vec{s}^\top A_f$

SFE to KP-ABE w/ IPFE

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$$\text{ABE.ct}_x(m): \begin{cases} ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i \\ \end{cases}$$

$$\text{ABE.sk}_f:$$

Pairing based IPFE

$$\left.\begin{array}{l} \text{IPFE}.ct([\![\vec{u}]\!]_1) \\ \text{IPFE}.sk([\![\vec{v}]\!]_2) \end{array}\right\} \text{ decrypt to } [\![\langle \vec{u}, \vec{v} \rangle]\!]_T$$

SFE to KP-ABE w/ IPFE

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$$\text{ABE.ct}_x(m): \begin{cases} ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i \\ \end{cases}$$

$$\text{ABE.sk}_f:$$

Pairing based IPFE

$$\left.\begin{array}{l} \text{IPFE}.ct([\![\vec{u}]\!]_1) \\ \text{IPFE}.sk([\![\vec{v}]\!]_2) \end{array}\right\} \text{ decrypt to } [\![\langle \vec{u}, \vec{v} \rangle]\!]_T$$

$\vec{u}$ is hidden. Only $[\![\vec{v}]\!]_2$ and $[\![\langle \vec{u}, \vec{v} \rangle]\!]_T$ are revealed.

SFE to KP-ABE w/ IPFE

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$$\text{ABE.ct}_x(m): \begin{cases} ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i \\ \\ \text{ABE.sk}_f: \end{cases} \Bigg\} \underbrace{[\![\vec{s}^\top A_f G^{-1}(\vec{u}) + m\lceil q/2 \rfloor]\!]_T}_{[\![ct_m]\!]_T}$$

Pairing based IPFE

$$\left.\begin{matrix} \text{IPFE}.ct([\![\vec{u}]\!]_1) \\ \text{IPFE}.sk([\![\vec{v}]\!]_2) \end{matrix}\right\} \text{ decrypt to } [\![\langle \vec{u}, \vec{v} \rangle]\!]_T$$

$\vec{u}$ is hidden. Only $[\![\vec{v}]\!]_2$ and $[\![\langle \vec{u}, \vec{v} \rangle]\!]_T$ are revealed.

SFE to KP-ABE w/ IPFE

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$$\text{ABE.ct}_x(m): \begin{cases} ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i \\ \text{IPFE.}ct([\![\vec{s}, m]\!]_1) \end{cases}$$

$$\text{ABE.sk}_f: \text{IPFE.}sk\left([\![A_f G^{-1}(\vec{u}), \lceil q/2 \rfloor]\!]_2\right)$$

$$\Big\} \quad \underbrace{[\![\vec{s}^\top A_f G^{-1}(\vec{u}) + m\lceil q/2 \rfloor]\!]_T}_{[\![ct_m]\!]_T}$$

Pairing based IPFE

$$\left.\begin{array}{l} \text{IPFE.}ct([\![\vec{u}]\!]_1) \\ \text{IPFE.}sk([\![\vec{v}]\!]_2) \end{array}\right\} \text{ decrypt to } [\![\langle \vec{u}, \vec{v} \rangle]\!]_T$$

$\vec{u}$ is hidden. Only $[\![\vec{v}]\!]_2$ and $[\![\langle \vec{u}, \vec{v} \rangle]\!]_T$ are revealed.

KP-ABE w/ IPFE: Correctness

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$$\text{ABE.ct}_x(m): \begin{cases} ct_x \approx \{\vec{s}^{\mathsf{T}}(A_i + x_i G)\}_i \\ \text{IPFE.}ct([\![\vec{s}, m]\!]_1) \end{cases}$$

$$\text{ABE.sk}_f: \text{IPFE.}sk\left([\![A_f G^{-1}(\vec{u}), \lceil q/2 \rfloor]\!]_2\right)$$

$$\Big\} \quad [\![ct_m]\!]_{\mathrm{T}}$$

ABE.Dec:

KP-ABE w/ IPFE: Correctness

ABE.mpk = $A_1, \ldots, A_n, \vec{u}$

ABE.$\mathrm{ct}_x(m)$: $\begin{cases} ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i \\ \text{IPFE}.ct([\![\vec{s}, m]\!]_1) \end{cases}$

ABE.sk_f: IPFE.$sk\left([\![A_f G^{-1}(\vec{u}), \lceil q/2 \rfloor]\!]_2\right)$

$\Big\}$ $[\![ct_m]\!]_T$

ABE.Dec:

$\vec{s}^\top A_f G^{-1}(\vec{u})$

KP-ABE w/ IPFE: Correctness

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$$\text{ABE.ct}_x(m): \begin{cases} ct_x \approx \{\vec{s}^\top (A_i + x_i G)\}_i \\ \text{IPFE.}ct([\![\vec{s}, m]\!]_1) \end{cases}$$

$$\text{ABE.sk}_f: \text{IPFE.}sk\left([\![A_f G^{-1}(\vec{u}), \lceil q/2 \rfloor]\!]_2\right)$$

$$\Big\} \; [\![ct_m]\!]_T$$

ABE.Dec:

$$[\![ct_m]\!]_T - \boxed{\vec{s}^\top A_f G^{-1}(\vec{u})} \approx [\![m\lceil q/2 \rfloor]\!]_T$$

KP-ABE w/ IPFE: Correctness Problems

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$$\text{ABE.ct}_x(m): \begin{cases} ct_x = \{\vec{s}^{\mathsf{T}}(A_i + x_i G)\}_i + e_i \\ \text{IPFE.}ct([\![\vec{s}, m]\!]_1) \end{cases}$$

$$\text{ABE.sk}_f: \text{IPFE.}sk\left([\![A_f G^{-1}(\vec{u}), \lceil q/2 \rfloor]\!]_2\right)$$

$$\Big\} \quad [\![ct_m]\!]_{\mathrm{T}}$$

ABE.Dec:

KP-ABE w/ IPFE: Correctness Problems

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$\text{ABE.ct}_x(m)$: $\begin{cases} ct_x = \{\vec{s}^\top (A_i + x_i G)\}_i + e_i \\ \text{IPFE.}ct([\![\vec{s}, m]\!]_1) \end{cases}$

ABE.sk_f: $\text{IPFE.}sk\left([\![A_f G^{-1}(\vec{u}), \lceil q/2 \rfloor]\!]_2\right)$

$\Big\}$ $[\![ct_m]\!]_T$

ABE.Dec:

$$\vec{s}^\top A_f G^{-1}(\vec{u}) + e_f$$

KP-ABE w/ IPFE: Correctness Problems

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$$\text{ABE.ct}_x(m): \begin{cases} ct_x = \{\vec{s}^\top (A_i + x_i G)\}_i + e_i \\ \text{IPFE.}ct([\![\vec{s}, m]\!]_1) \end{cases}$$

$$\text{ABE.sk}_f: \text{IPFE.}sk\left([\![A_f G^{-1}(\vec{u}), \lceil q/2 \rfloor]\!]_2\right)$$

$$\Big\} \; [\![ct_m]\!]_T$$

ABE.Dec:

$$[\![ct_m]\!]_T - \boxed{\vec{s}^\top A_f G^{-1}(\vec{u}) + e_f} = [\![m\lceil q/2 \rfloor + e_f]\!]_T$$

KP-ABE w/ IPFE: Correctness Problems

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$$\text{ABE.ct}_x(m): \begin{cases} ct_x = \{\vec{s}^\top (A_i + x_i G)\}_i + e_i \\ \text{IPFE.}ct([\![\vec{s}, m]\!]_1) \end{cases}$$

$$\text{ABE.sk}_f: \text{IPFE.}sk\left([\![A_f G^{-1}(\vec{u}), \lceil q/2 \rfloor]\!]_2\right)$$

$$\Big\} \; [\![ct_m]\!]_T$$

ABE.Dec:

$$[\![ct_m]\!]_T - \boxed{\vec{s}^\top A_f G^{-1}(\vec{u}) + e_f} = [\![m\lceil q/2 \rfloor + e_f]\!]_T$$

Probalem1:
Huge noise! $2^{\text{poly}(d)}$

KP-ABE w/ IPFE: Correctness Problems

ABE.mpk = $A_1, \ldots, A_n, \vec{u}$

ABE.$\mathrm{ct}_x(m)$: $\begin{cases} ct_x = \{\vec{s}^\top (A_i + x_i G)\}_i + e_i \\ \text{IPFE}.ct([\![\vec{s}, m]\!]_1) \end{cases}$

ABE.sk_f: IPFE.$sk\left([\![A_f G^{-1}(\vec{u}), \lceil q/2 \rfloor]\!]_2\right)$

$[\![ct_m]\!]_T$

Problem2:
$\mathrm{poly}(q) = \mathrm{poly}(d)$ size!

ABE.Dec:

$$[\![ct_m]\!]_T - \boxed{\vec{s}^\top A_f G^{-1}(\vec{u}) + e_f} = [\![m\lceil q/2 \rfloor + e_f]\!]_T$$

Probalem1:
Huge noise! $2^{\mathrm{poly}(d)}$

KP-ABE w/ IPFE: Correctness by rounding

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$\text{ABE.ct}_x(m)$: $\begin{cases} ct_x = \{\vec{s}^\top (A_i + x_i G)\}_i + e_i \\ \text{IPFE.}ct([\![\vec{s}, m]\!]_1) \end{cases}$ $\Big\}$ $[\![ct_m]\!]_T$

ABE.sk_f:

ABE.Dec:

KP-ABE w/ IPFE: Correctness by rounding

ABE.mpk = $A_1, \ldots, A_n, \vec{u}$

ABE.$\mathrm{ct}_x(m)$: $\begin{cases} ct_x = \{\vec{s}^\top (A_i + x_i G)\}_i + e_i \\ \mathsf{IPFE}.ct([\![\vec{s}, m]\!]_1) \end{cases}$ $\Big\}$ $[\![ct_m]\!]_T$

ABE.sk_f:

ABE.Dec:

$$\left\lceil \vec{s}^\top A_f G^{-1}(\vec{u}) + e_f \right\rfloor_p$$

KP-ABE w/ IPFE: Correctness by rounding

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$\text{ABE.ct}_x(m)$: $\begin{cases} ct_x = \{\vec{s}^\top (A_i + x_i G)\}_i + e_i \\ \text{IPFE.}ct([\![\vec{s}, m]\!]_1) \end{cases}$ $\Big\}$ $[\![ct_m]\!]_T$

ABE.sk_f:

ABE.Dec:

$$\boxed{\left\lceil \vec{s}^\top A_f G^{-1}(\vec{u}) + e_f \right\rfloor_p}$$

$$= \vec{s}^\top \left\lceil A_f G^{-1}(\vec{u}) \right\rfloor_p + \text{error}$$

KP-ABE w/ IPFE: Correctness by rounding

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$$\text{ABE.ct}_x(m): \begin{cases} ct_x = \{\vec{s}^\top (A_i + x_i G)\}_i + e_i \\ \text{IPFE.}ct([\![\vec{s}, m]\!]_1) \end{cases}$$

$$\text{ABE.sk}_f: \text{IPFE.}sk\left([\![\lceil A_f G^{-1}(\vec{u}) \rfloor_p, \lceil p/2 \rfloor]\!]_2\right)$$

$$\Big\} \quad [\![ct_m]\!]_T$$

ABE.Dec:

$$[\![ct'_m]\!]_T - \boxed{\lceil \vec{s}^\top A_f G^{-1}(\vec{u}) + e_f \rfloor_p} = [\![m\lceil q/2 \rfloor - \text{error}]\!]_T$$

$$= \vec{s}^\top \lceil A_f G^{-1}(\vec{u}) \rfloor_p + \text{error}$$

KP-ABE w/ IPFE: Correctness by rounding

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$$\text{ABE.ct}_x(m): \begin{cases} ct_x = \{\vec{s}^\top (A_i + x_i G)\}_i + e_i \\ \text{IPFE.}ct([\![\vec{s}, m]\!]_1) \end{cases}$$

$$\text{ABE.sk}_f: \text{IPFE.}sk\left([\![\lceil A_f G^{-1}(\vec{u}) \rfloor_p, \lceil p/2 \rfloor]\!]_2\right)$$

$$\Big\} \; [\![ct_m]\!]_T$$

ABE.Dec:

$$[\![ct'_m]\!]_T - \boxed{\lceil \vec{s}^\top A_f G^{-1}(\vec{u}) + e_f \rfloor_p} = [\![m\lceil q/2 \rfloor - \text{error}]\!]_T$$

$$= \vec{s}^\top \lceil A_f G^{-1}(\vec{u}) \rfloor_p + \text{error}$$

Small

KP-ABE w/ IPFE: Correctness by rounding

$$\text{ABE.mpk} = A_1, \ldots, A_n, \vec{u}$$

$$\text{ABE.ct}_x(m): \begin{cases} ct_x = \{\vec{s}^\top (A_i + x_i G)\}_i + e_i \\ \text{IPFE.}ct([\![\vec{s}, m]\!]_1) \end{cases}$$

$\text{poly}(p) = \text{poly}(\lambda)$ size!

$$\text{ABE.sk}_f: \text{IPFE.}sk\left([\![\lfloor A_f G^{-1}(\vec{u}) \rceil_p, \lceil p/2 \rfloor]\!]_2\right)$$

$[\![ct_m]\!]_T$

ABE.Dec:

$$[\![ct'_m]\!]_T - \boxed{\lfloor \vec{s}^\top A_f G^{-1}(\vec{u}) + e_f \rceil_p} = [\![m\lceil q/2 \rfloor - \text{error}]\!]_T$$

$$= \vec{s}^\top \lfloor A_f G^{-1}(\vec{u}) \rceil_p + \text{error}$$

Small

Other Challenges

- 1-key Security
  - SFE relies on noise flooding

Other Challenges

- 1-key Security
  - SFE relies on noise flooding
  - Sol: Remove flooding noise

Other Challenges

- 1-key Security
  - SFE relies on noise flooding
  - Sol: Remove flooding noise

Show ct_m entropic,
$\equiv$ random in GGM

Other Challenges

- 1-key Security
  - SFE relies on noise flooding
  - Sol: Remove flooding noise

Show ct_m entropic,
$\equiv$ random in GGM

- Multi-key Security
  - Borrow ideas from [AY,AWY20]

Other Challenges

- 1-key Security
  - SFE relies on noise flooding
  - Sol: Remove flooding noise

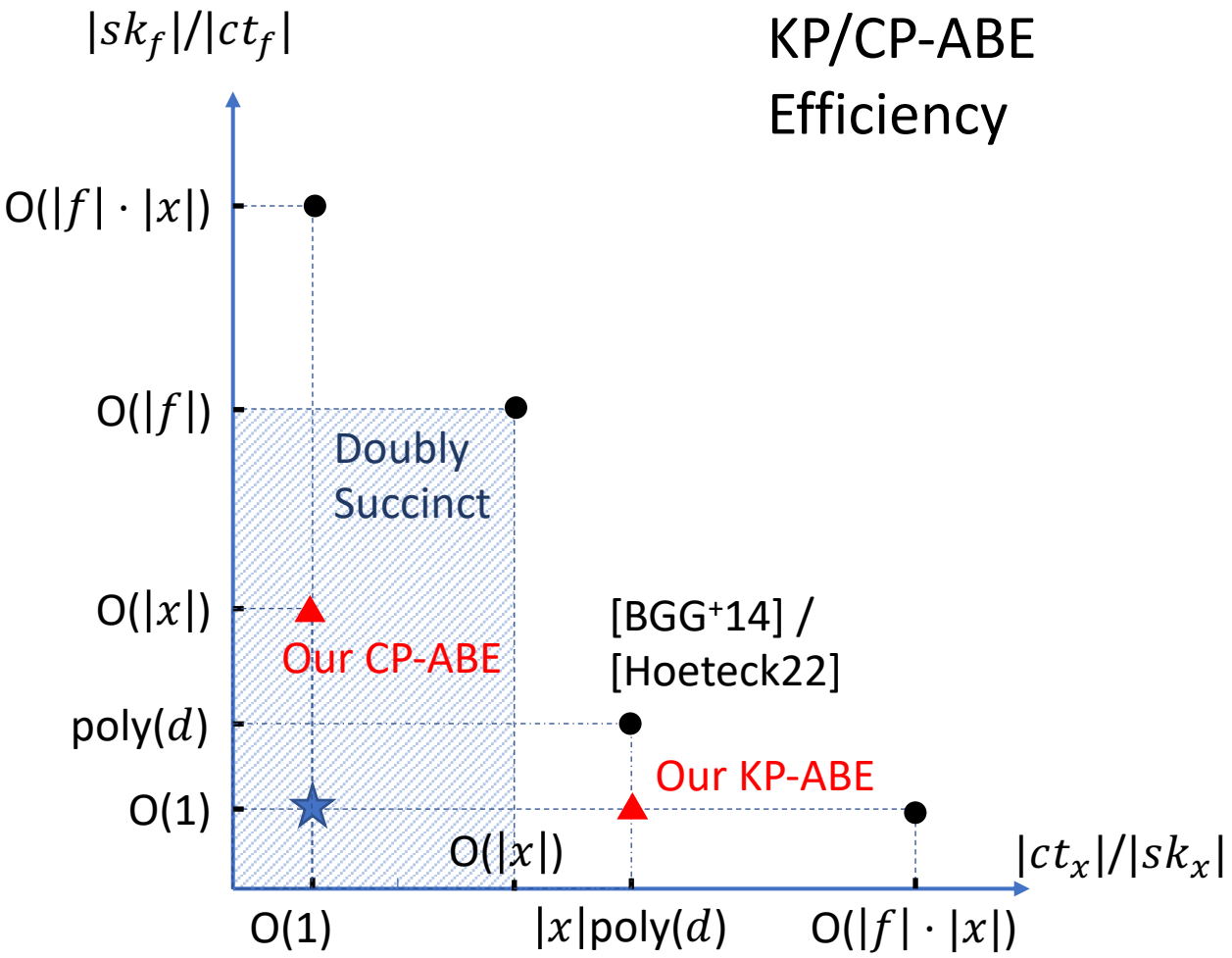
Show ct_m entropic,
$\equiv$ random in GGM

- Multi-key Security
  - Borrow ideas from [AY,AWY20]

Also relies on GGM

Thank You!

Eprint:2022/659



Adaptive LWE

Thm1: Assuming ~~LWE~~ + GGM

∃KP-ABE for P:

- $|sk_f|$ = O(1), $|ct_x|$ = $|x|$poly(d),
- Adaptive secure.

Thm2: Assuming ~~LWE~~ + GGM

∃CP-ABE for NC1:

- $|sk_x|$ = O(1), $|ct_f| = |x|^2$,
- Adaptive secure.