TCC 2025

中央研究院 資訊科學研究所
Institute of Information Science, Academia Sinica

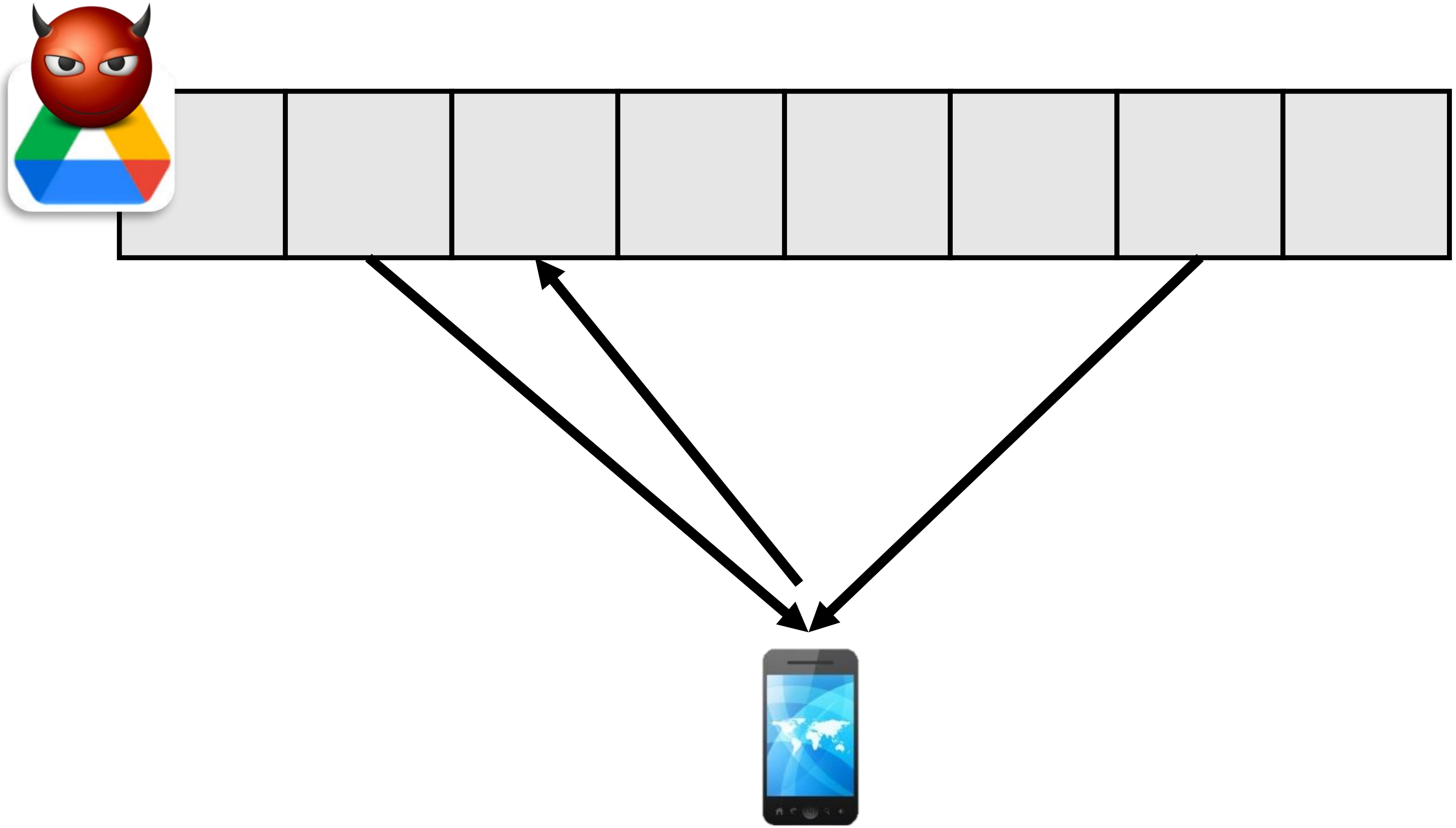
Lower Bounds on Inner-Product Functional Encryption from All-or-Nothing Encryption Primitives

Wei-Kai Lin

Jinye He   Shiyu Li

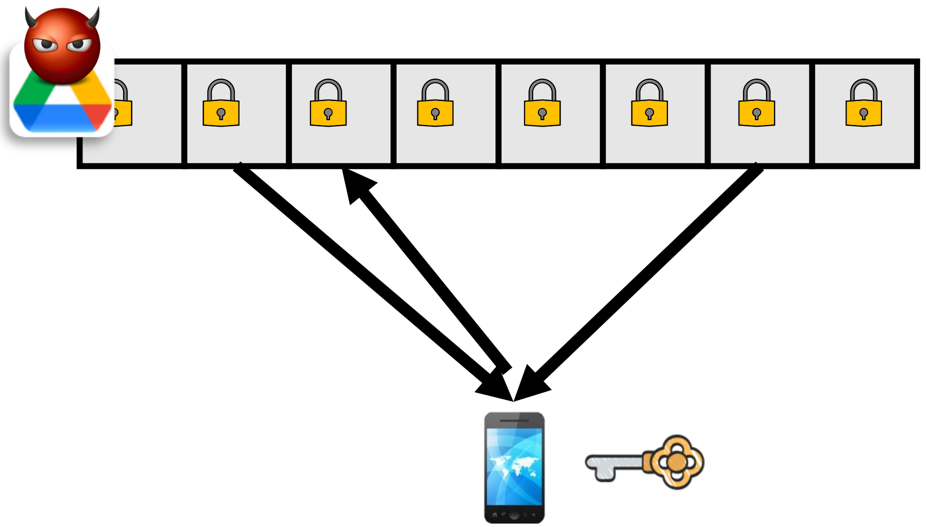
UNIVERSITY of VIRGINIA

My Research: Efficient Crypto on Large Data



My Research: Efficient Crypto on Large Data

Oblivious Random-Access Machines (RAM)

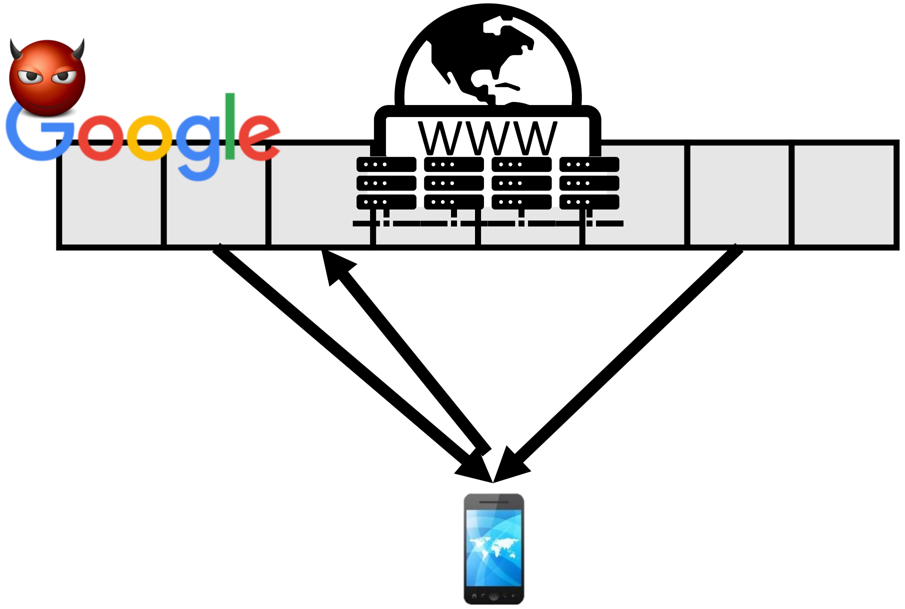


My Research: Efficient Crypto on Large Data

Oblivious Random-Access Machines (RAM)

Private Information Retrieval

RAM-FHE



My Research: Efficient Crypto on Large Data

Oblivious Random-Access Machines (RAM)

Private Information Retrieval

RAM-FHE

(optimal / ideal) constructions

Impossibility

Others

Inner Product Functional Encryption

Garbled Lookup Tables

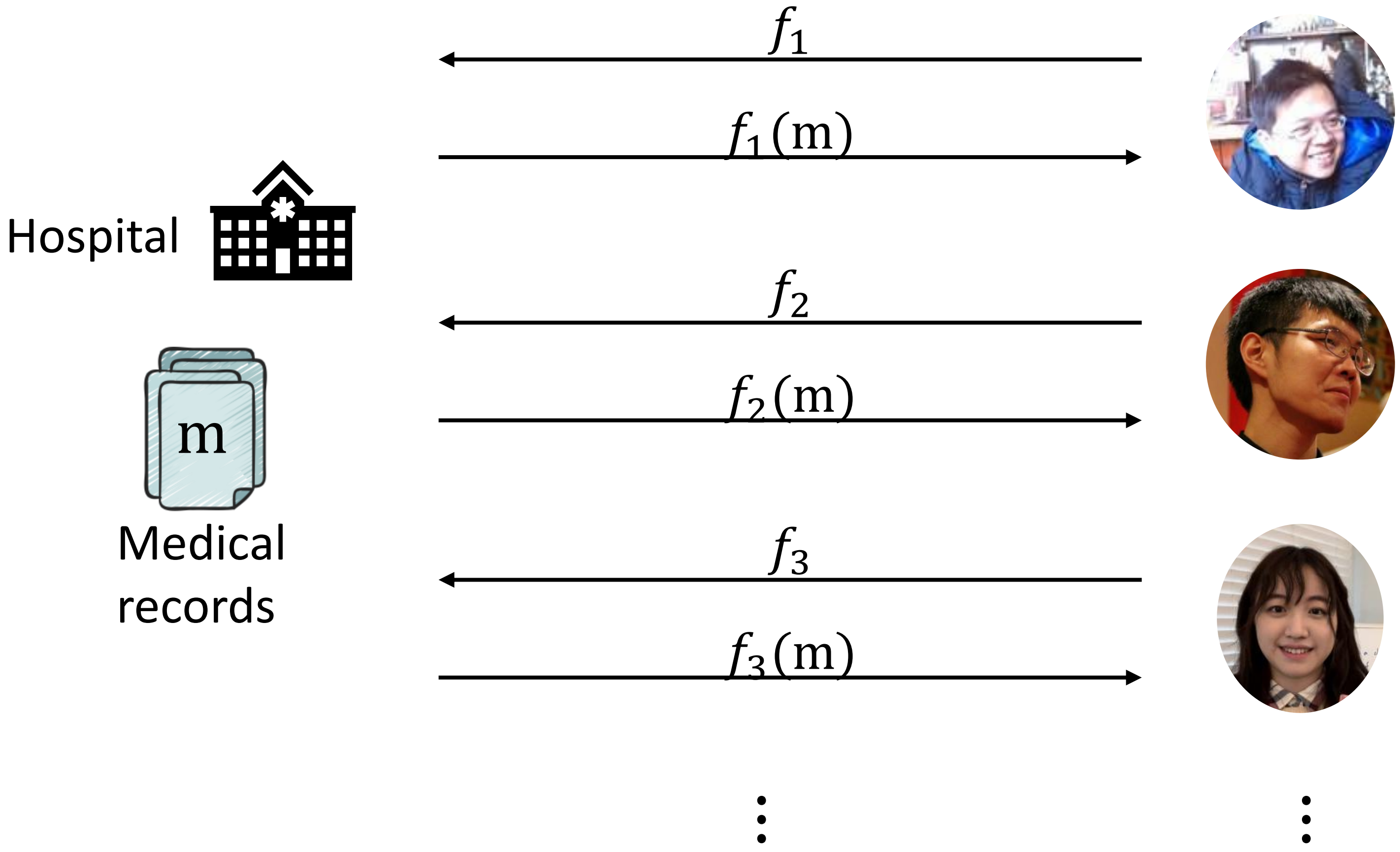
Impossibility

constructions

(In)Feasibility of (Inner Product) Functional Encryptions

Motivating Functional Encryptions

Scientists want $f(\mathrm{m})$ for some f



Potential solutions:

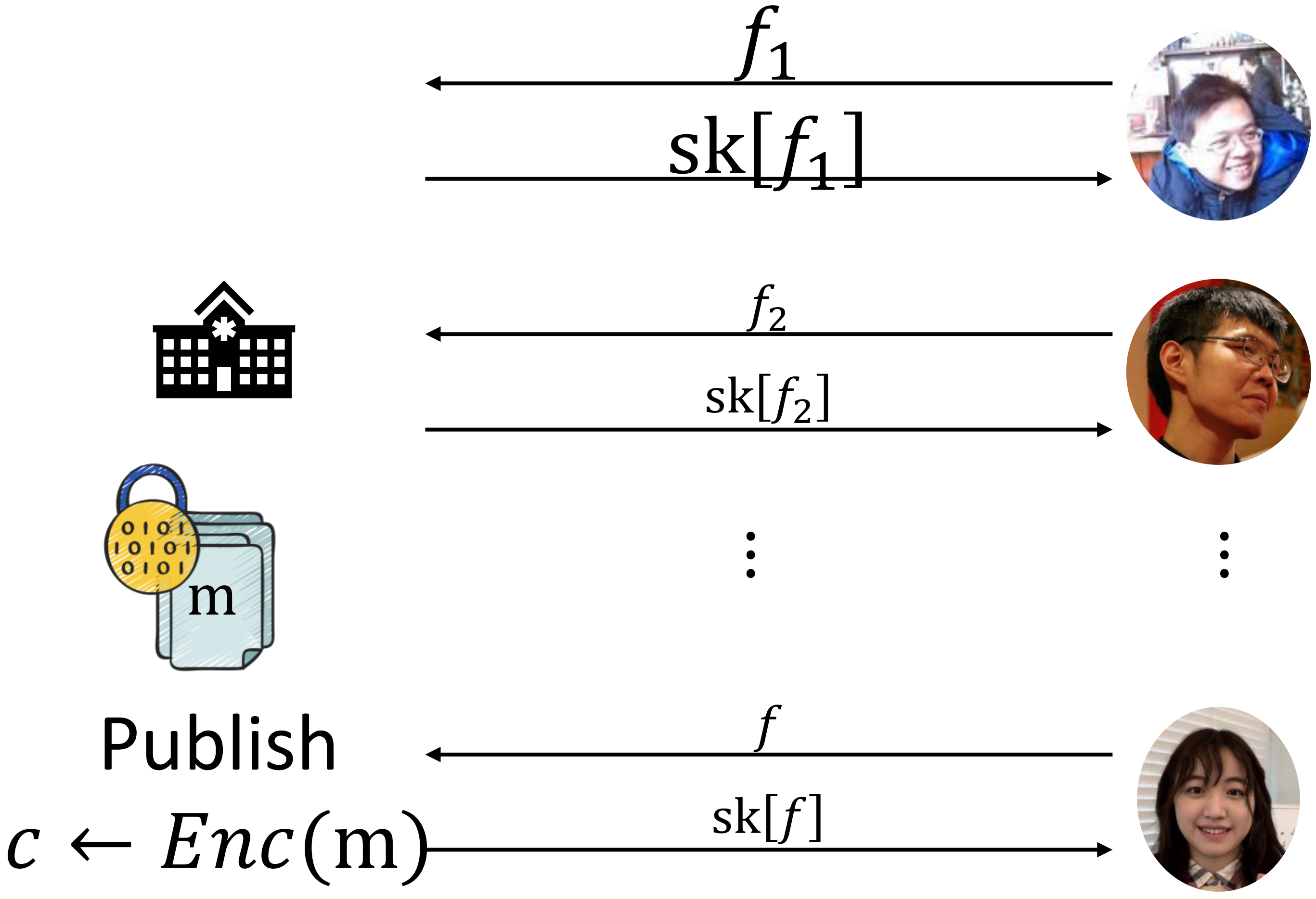
Release m in the clear?

Not secure

Hospital computes all f_i's?

Not efficient

Functional Encryption (FE), Correctness



Functional decryption:

$f_1(\mathrm{m}) \leftarrow Dec(\mathrm{sk}[f_1], c)$

Any f in the class,

$f(\mathrm{m}) \leftarrow Dec(\mathrm{sk}[f], c)$

Minimal FE: for Inner Products (IPFE)

$\mathbf{v}_i$ and $\mathbf{m}$ are vectors in $\mathbb{Z}_p^n$

$\mathbf{v}_1 \in \mathbb{Z}_p^n$

$\text{sk}[\mathbf{v}_1]$

Functional decryption:
$\langle \mathbf{v}_1, \mathbf{m} \rangle \leftarrow Dec(\text{sk}[\mathbf{v}_1], c)$

$\mathbf{m} \in \mathbb{Z}_p^n$

$c \leftarrow Enc(\mathbf{m})$

⋮ ⋮

$\mathbf{v}$

$\text{sk}[\mathbf{v}]$

Any $\mathbf{v} \in \mathbb{Z}_p^n$,
$\langle \mathbf{v}, \mathbf{m} \rangle \leftarrow Dec(\text{sk}[\mathbf{v}], c)$

Security of IPFE, master secret key and KGen

$c \leftarrow Enc(msk, \mathbf{m})$

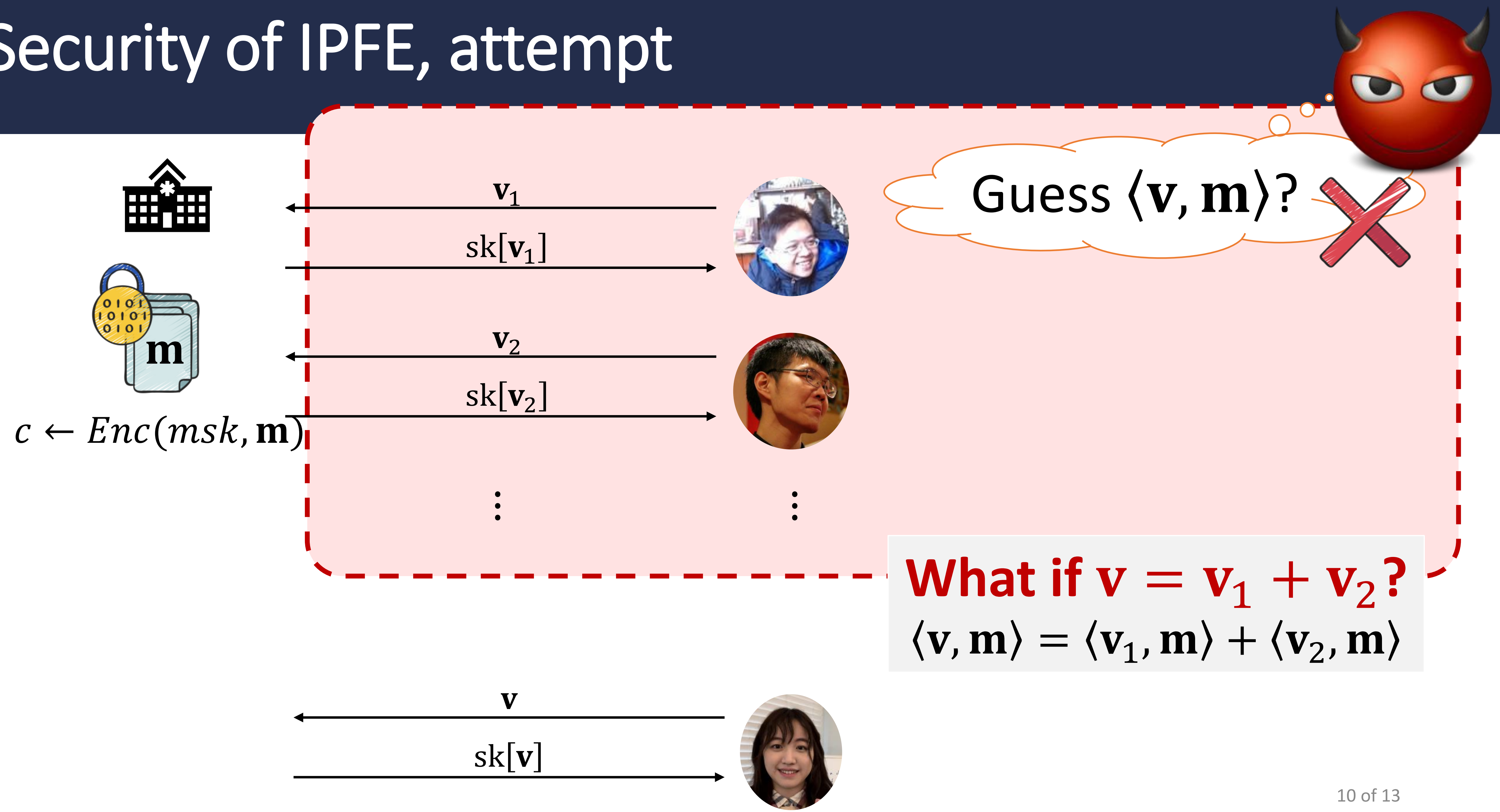
$\mathbf{v}$

$\mathrm{sk}[\mathbf{v}]$

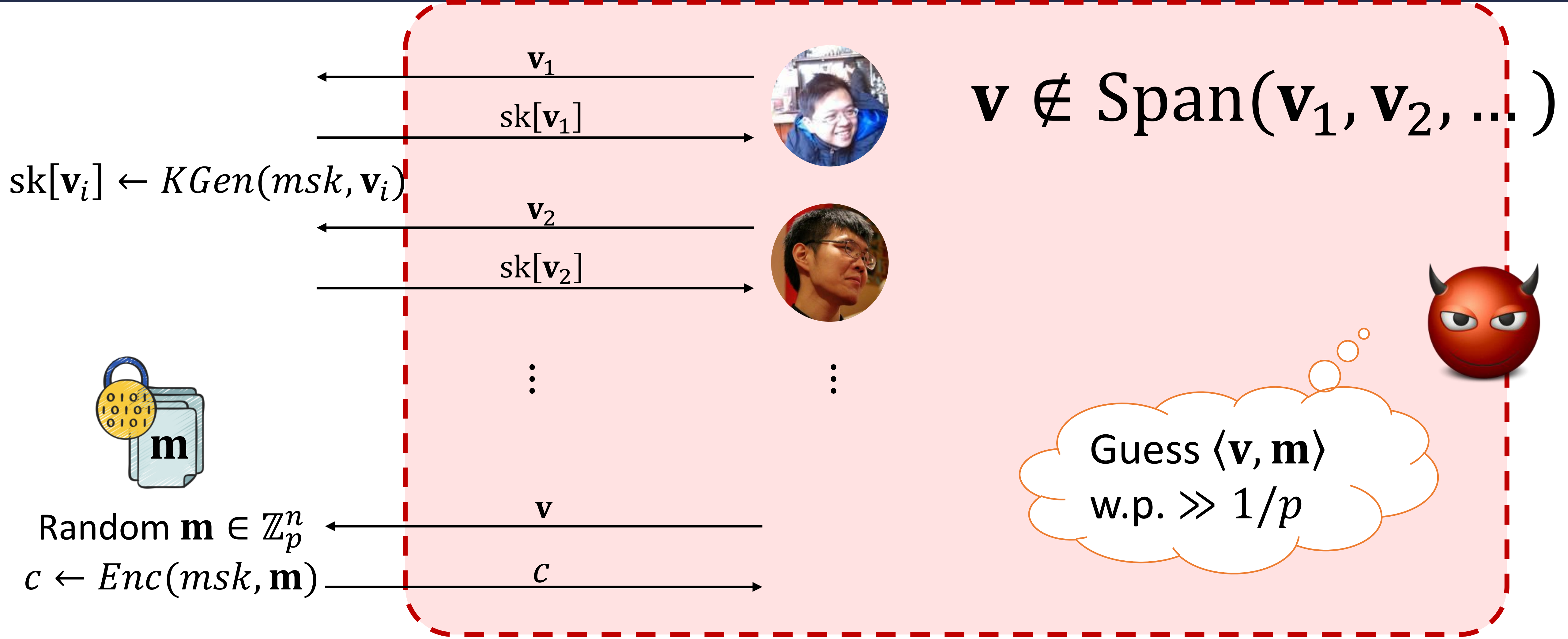
$\langle \mathbf{v}, \mathbf{m} \rangle \leftarrow Dec(\mathrm{sk}[\mathbf{v}], c)$

$\mathrm{sk}[\mathbf{v}] \leftarrow KGen(msk, \mathbf{v})$

Security of IPFE, attempt



Security of IPFE, Challenge vector is restricted



Equivalent to distinguishing $(\mathbf{m}_0, \mathbf{m}_1)$ st same IP in Span

Unbounded-collusion:
Tolerate more $\mathbf{v}_i$ = stronger security

$\mathbf{v}_1$

$\mathrm{sk}[\mathbf{v}_1]$

$\mathbf{v} \notin \mathrm{Span}(\mathbf{v}_1, \mathbf{v}_2, \ldots)$

$\mathrm{sk}[\mathbf{v}_i] \leftarrow KGen(msk, \mathbf{v}_i)$

$\mathbf{v}_2$

Guess $\langle \mathbf{v}, \mathbf{m} \rangle$?

$\mathrm{sk}[\mathbf{v}_2]$

As many $\mathbf{v}_i$ as we want

⋮

Bounded collusion?

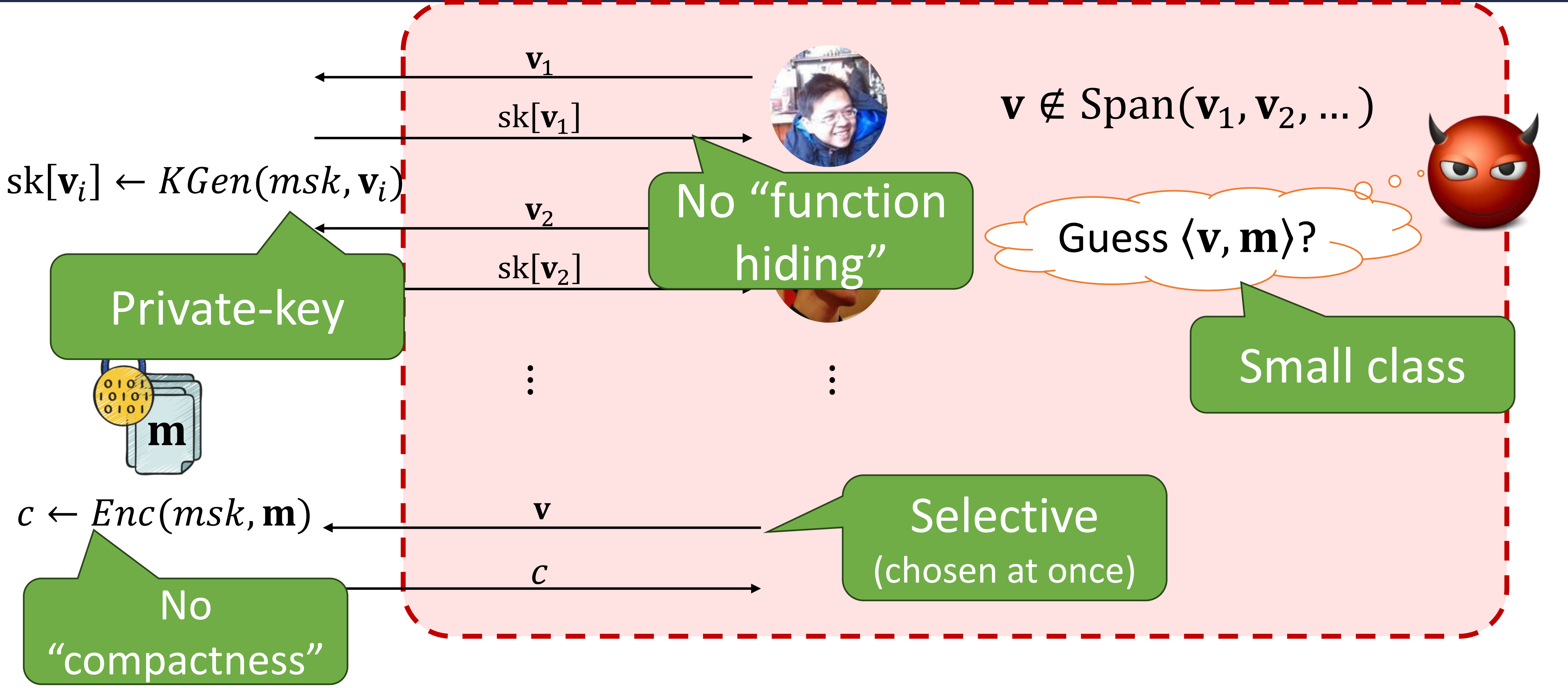
Solved from minimal assumptions [AV19]

$c \leftarrow Enc(msk, \mathbf{m})$

$\mathbf{v}$

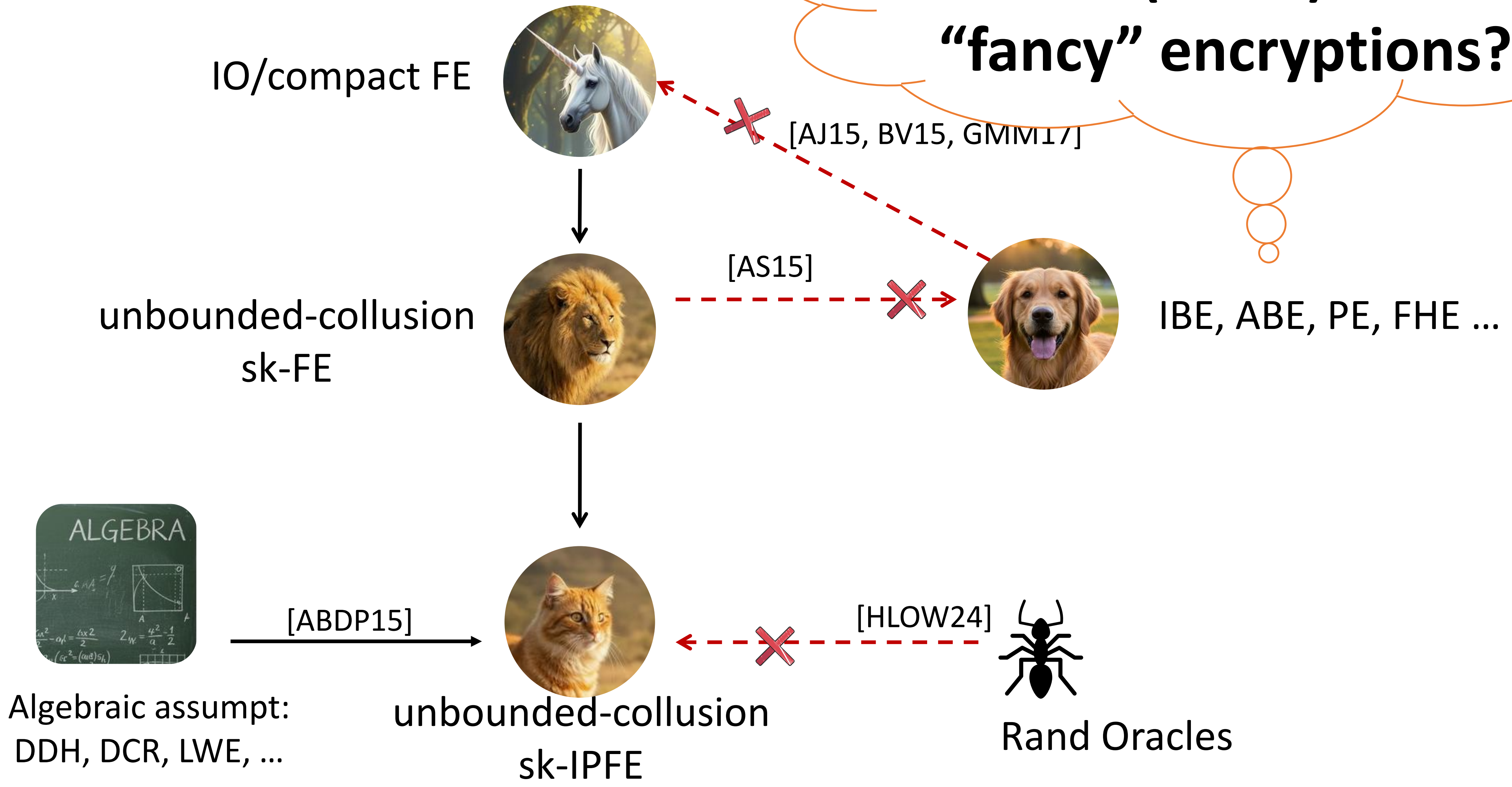
c

Weak settings (arguably weakest) make strong LB

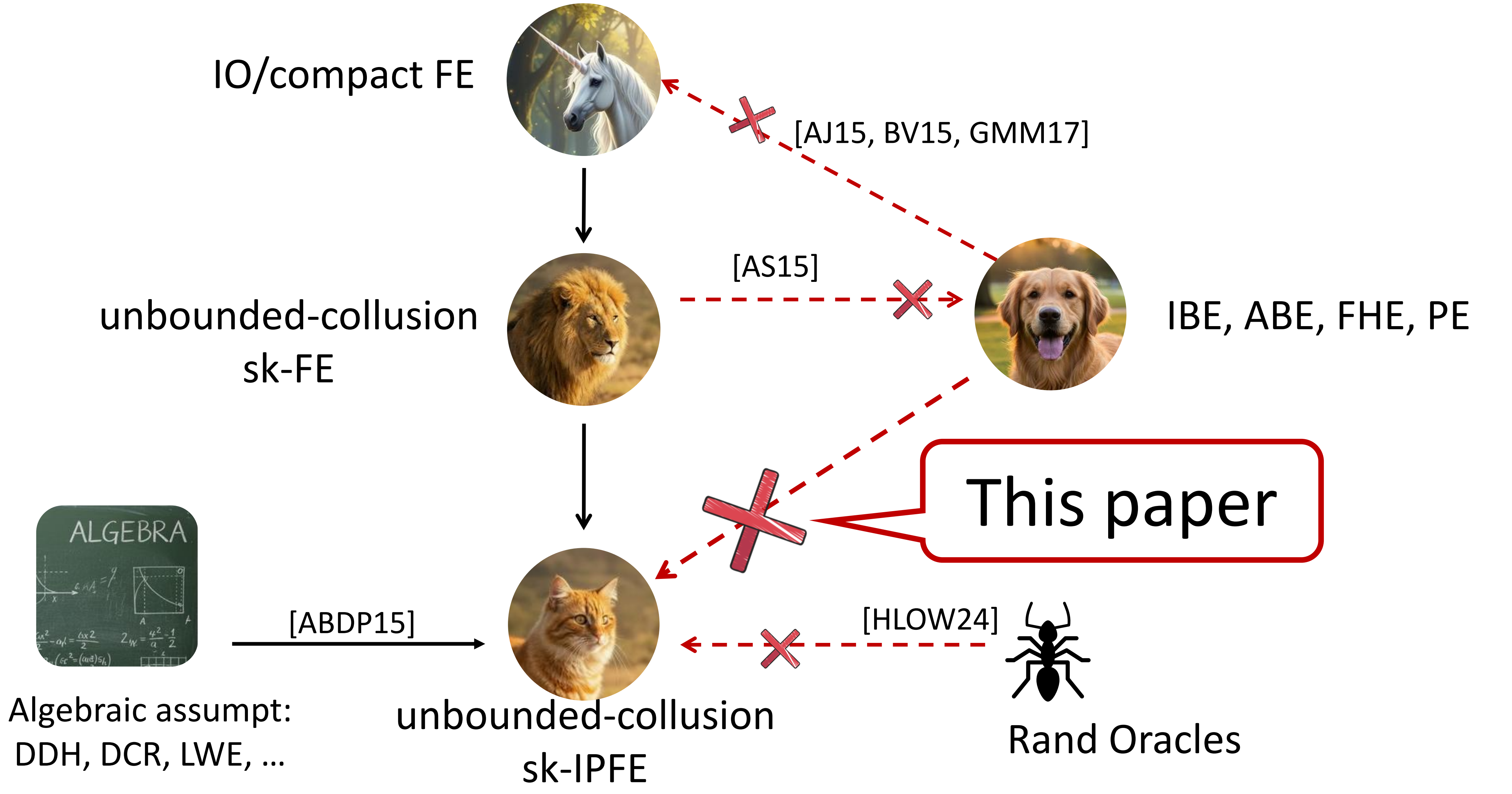


Previous Works

Question:
Obtain (weak) FE from "fancy" encryptions?

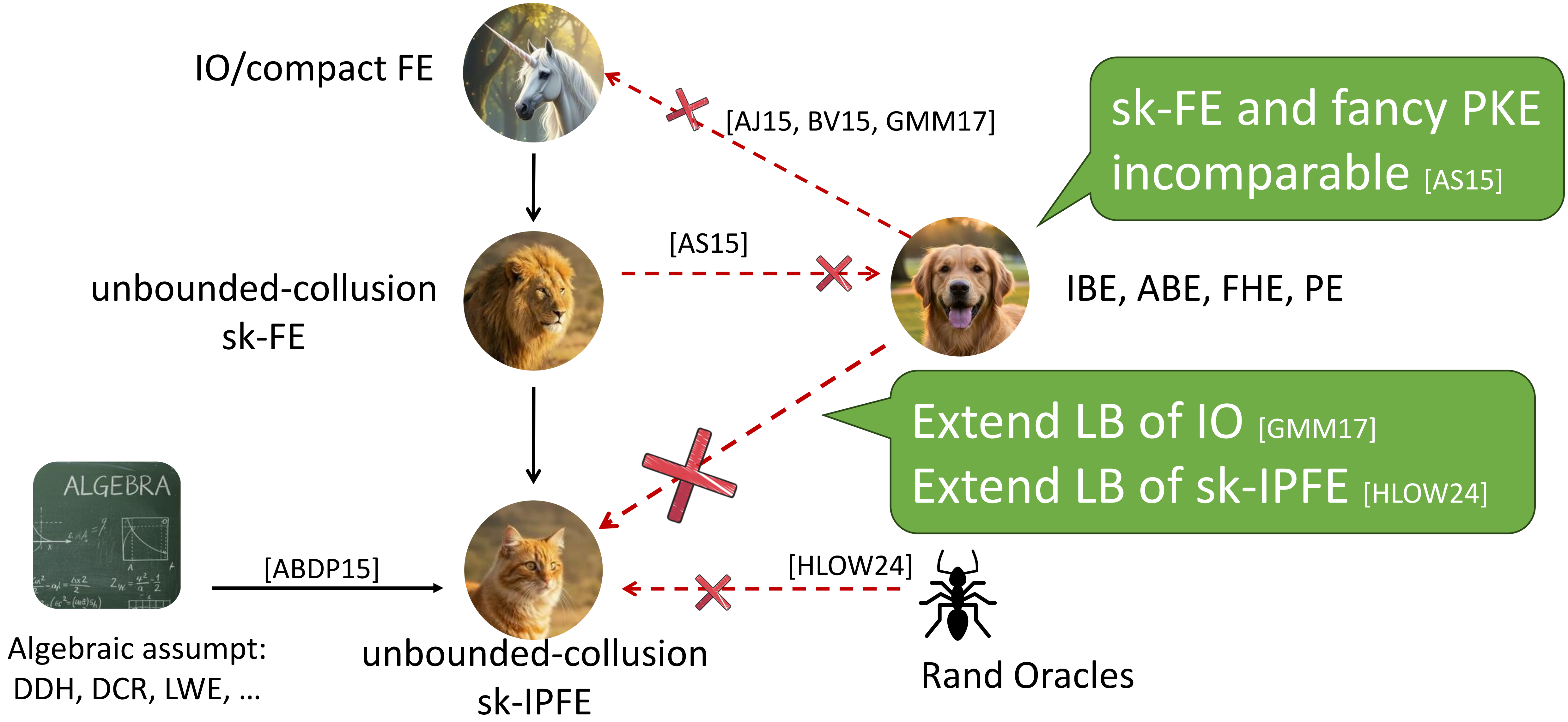


Result: No FE construction from ABE, FHE, PE

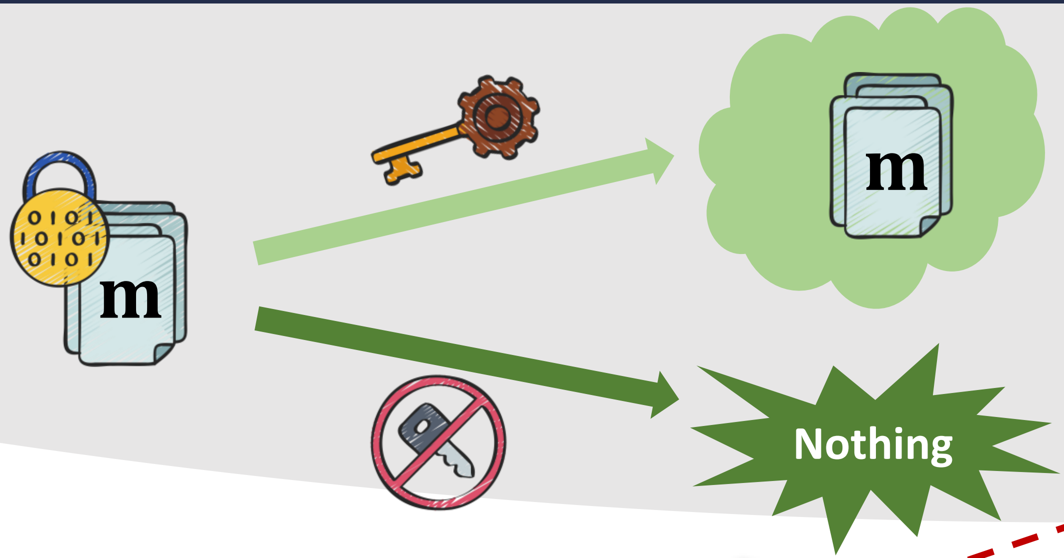


Comparisons

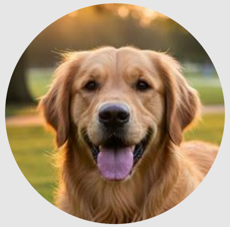
Match bounded-collusion FEs [AV19]



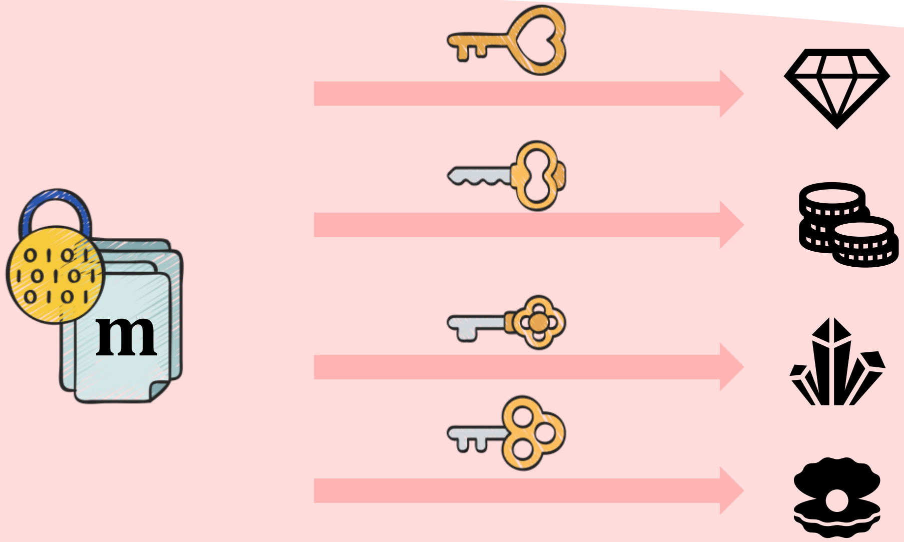
(Informal) FE vs "All-or-Nothing" Encryptions



All-or-Nothing Encryptions [GMM17]

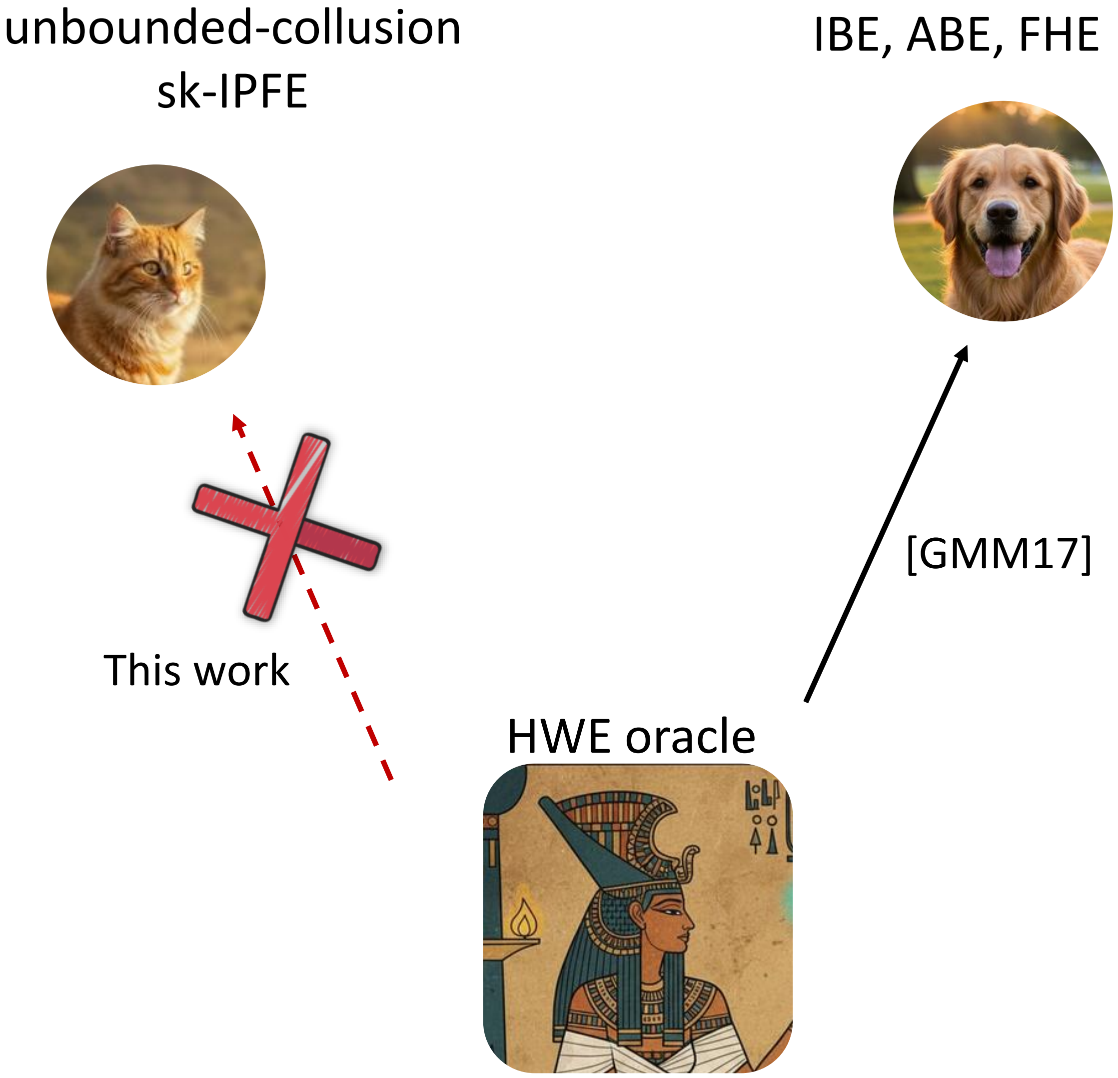


IBE, ABE, PE, FHE



(unbounded-collusion
Sk-IP) FE

Separate from Homomorphic Witness Encryption



HWE Oracle $\mathcal{O}$:

- $\mathrm{lb} \leftarrow e(a, x)$:
  permute instance a, plaintext x
- $x \leftarrow d\big(w, \mathrm{lb} = (a, y)\big)$:
  invert lb iff witness w is valid, $a(w) = 1$; $\perp$ o.w.
- $\mathrm{lb}' \leftarrow eval(f, \mathrm{lb}_1, \mathrm{lb}_2 \dots)$:
  homomorphic evaluate labels

Capture Attribute-Based FHE

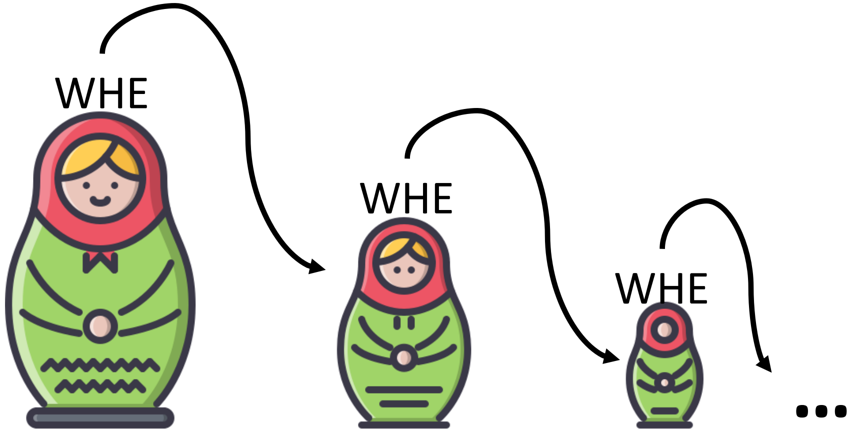
For PE, we use another WE oracle

Monolithic Model: Capture Oracle-Aided Circuits

[GMM17]

$eval(\boldsymbol{f}^{\mathcal{O}}, \ldots$
$a^{\mathcal{O}}(w) = 1\ldots$

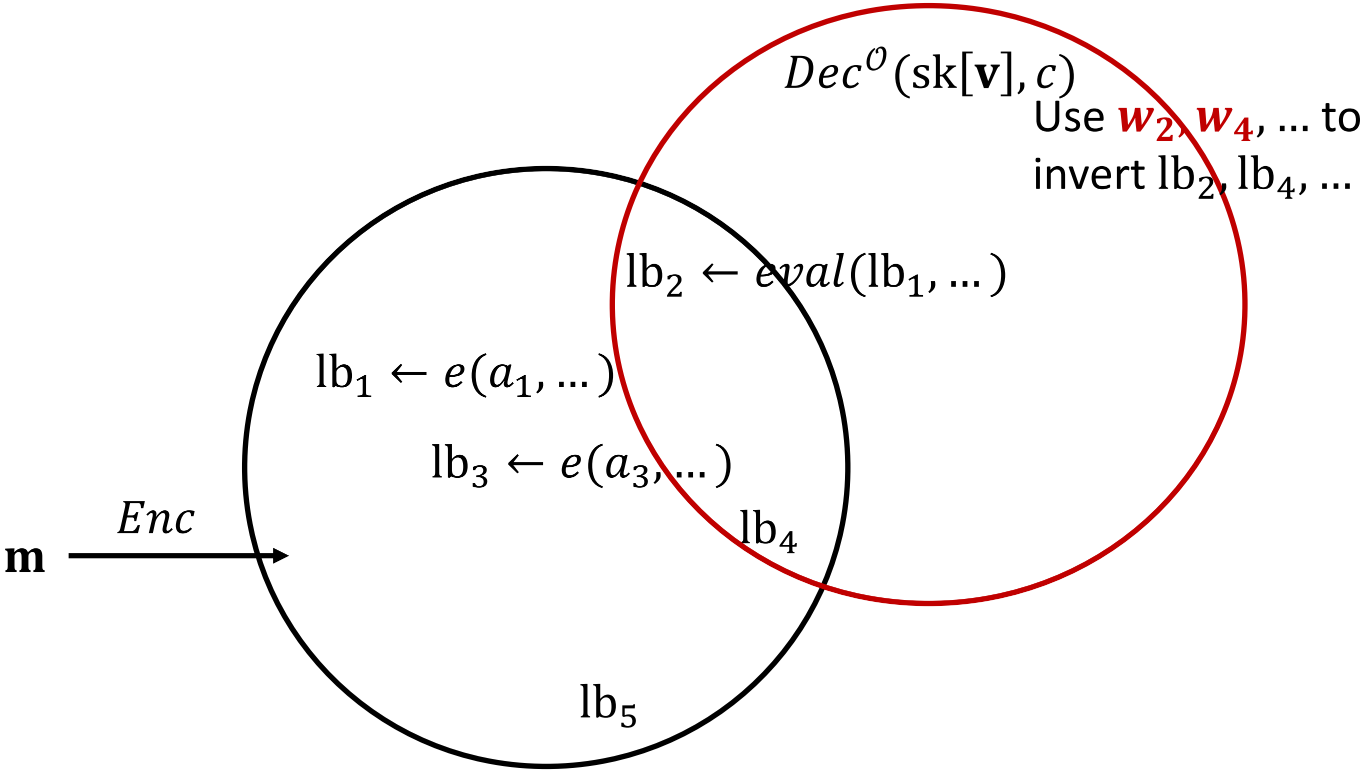
$f^{\mathcal{O}}$ and $a^{\mathcal{O}}$ are circuits that query oracle $\mathcal{O}$
Example: bootstrapping FHE



HWE Oracle $\mathcal{O}$:

- $\mathrm{lb} \leftarrow e(a, x)$:
  permute instance a, plaintext x
- $x \leftarrow d\big(w, \mathrm{lb} = (a, y)\big)$:
  invert lb iff witness w is valid,
  $a(w) = 1$; $\perp$ o.w.
- $\mathrm{lb}' \leftarrow eval(f, \mathrm{lb}_1, \mathrm{lb}_2 \ldots)$:
  homomorphic evaluate labels

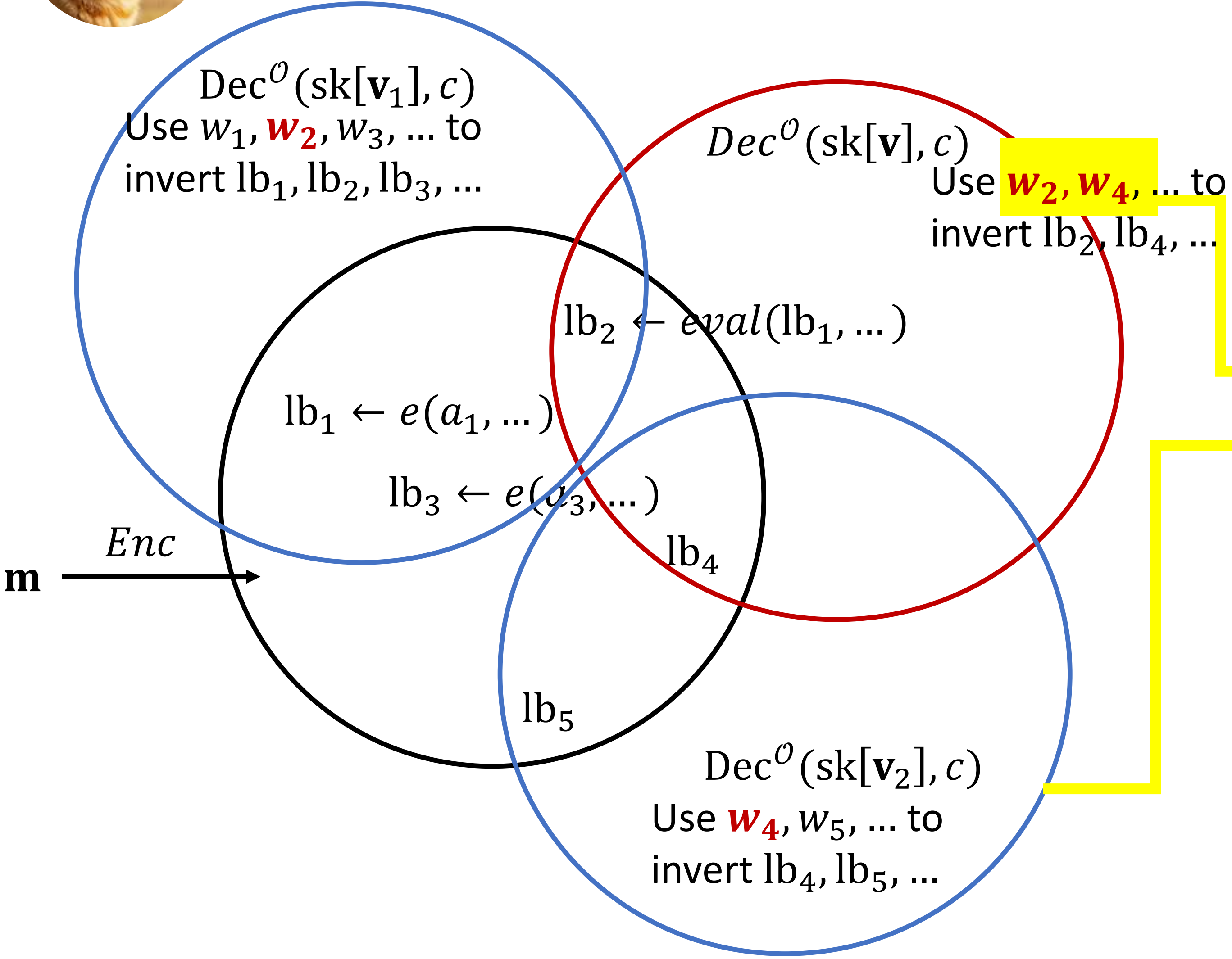
Intuition behind the Separation



HWE Oracle $\mathcal{O}$:

- $\mathrm{lb} \leftarrow e(a, x)$:
  permute instance a, plaintext x
- $x \leftarrow d\big(w, \mathrm{lb} = (a, y)\big)$:
  invert lb iff witness w is valid, $a(w) = 1$; $\perp$ o.w.
- $\mathrm{lb}' \leftarrow eval(f, \mathrm{lb}_1, \mathrm{lb}_2 \dots)$:
  homomorphic evaluate labels

Break IPFE: Collect the "Right" Witnesses



Given:

- $c \leftarrow \mathrm{Enc}^{\mathcal{O}}(\mathrm{msk}, \mathrm{m})$
- $\mathrm{sk}[\mathbf{v}_i] \leftarrow \mathrm{KGen}^{\mathcal{O}}(\mathrm{msk}, \mathbf{v}_i)$

Goal:

- Obtain $\langle \mathbf{v}, \mathbf{m} \rangle$ by simulating $\mathrm{Dec}^{\mathcal{O}}(\mathrm{sk}[\mathbf{v}], c)$

Want to cover witnesses using colluded keys

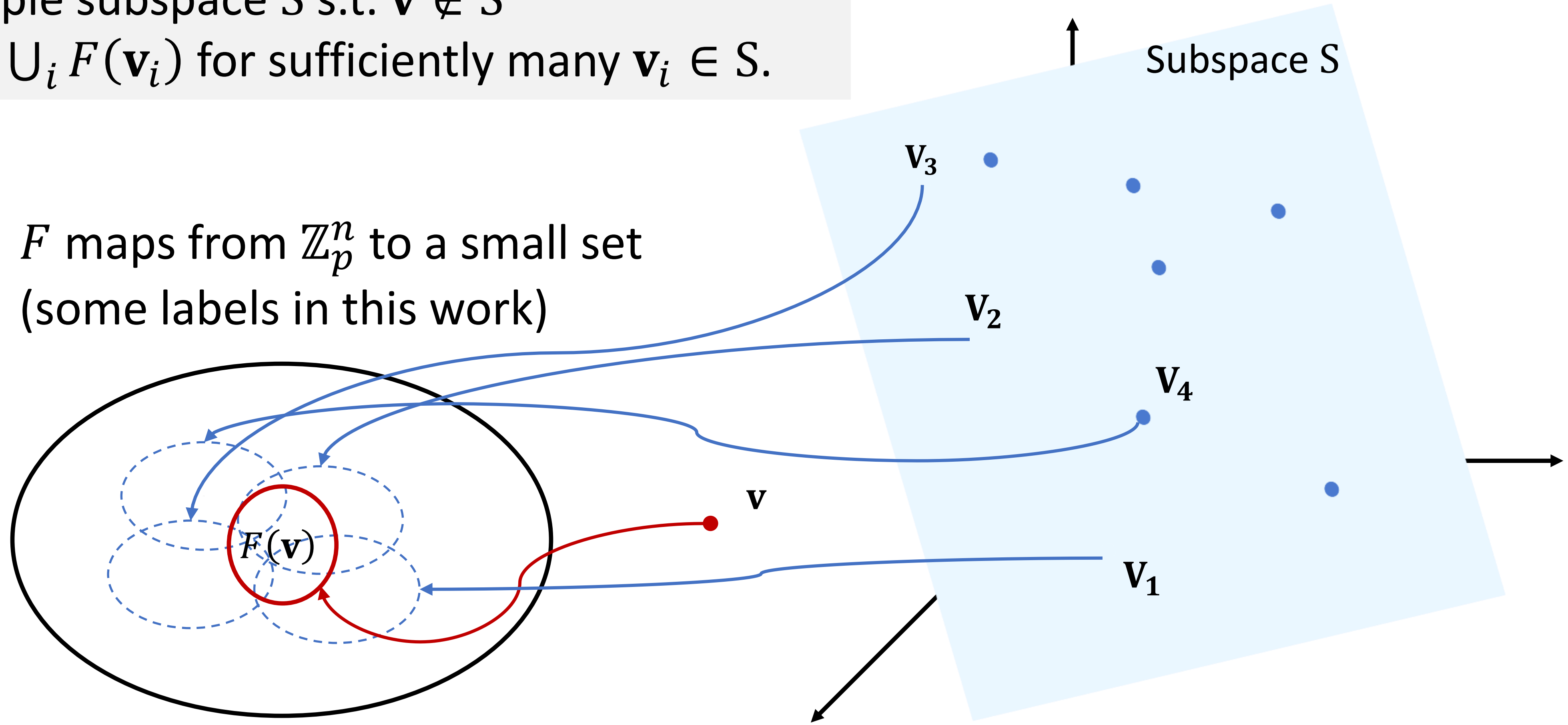
Observe: witnesses (and labels) is a **function of $\mathbf{v}$ and $\mathbf{v}_i$**
$\Rightarrow$ Coverage holds by **[HLOW24] Lemma**

HLOW Combinatorial Lemma

[Hajiabadi-Langrehr-O'Neil-Wang'24]

For any small-range function F,
- randomly sample vector $\mathbf{v}$
- randomly sample subspace S s.t. $\mathbf{v} \notin S$

W.h.p., $F(\mathbf{v}) \subseteq \bigcup_i F(\mathbf{v}_i)$ for sufficiently many $\mathbf{v}_i \in S$.



Questions?