Tightly Secure Inner-Product Functional Encryption Revisited: Compact, Lattice-based, and More

Shuai Han[1], **Hongxu Yi[2]**, Shengli Liu[1], Dawu Gu[1]

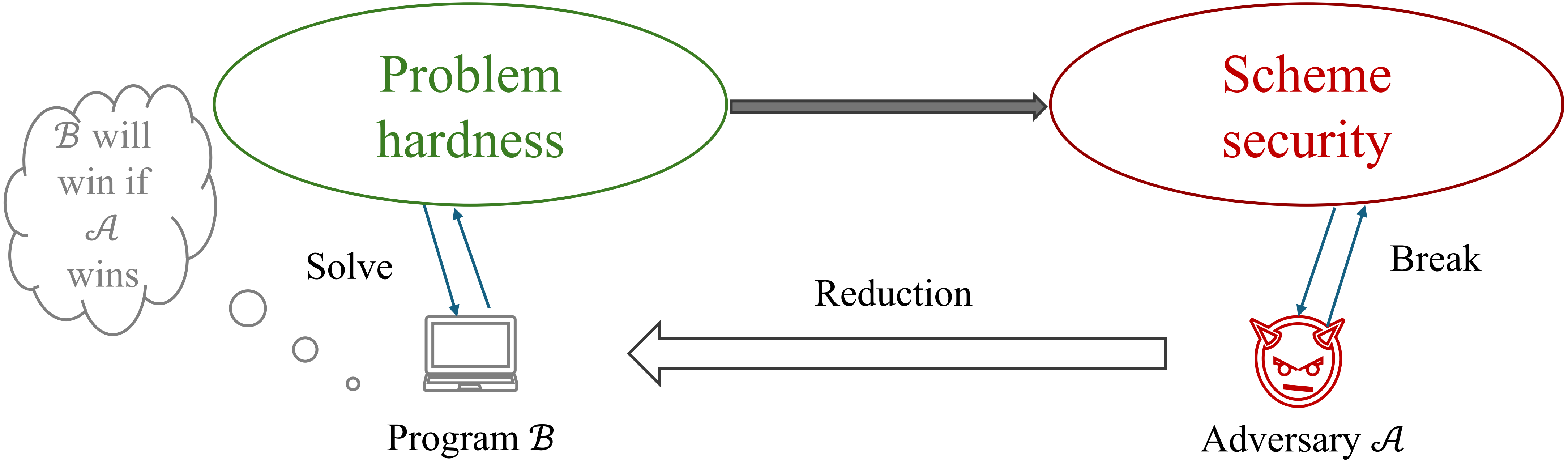
[1] Shanghai Jiao Tong University

[2] Shandong University

Crypto 2025, Santa Barbara, USA

Tight Security

Provable security of a cryptographic Scheme based on hard Problems.

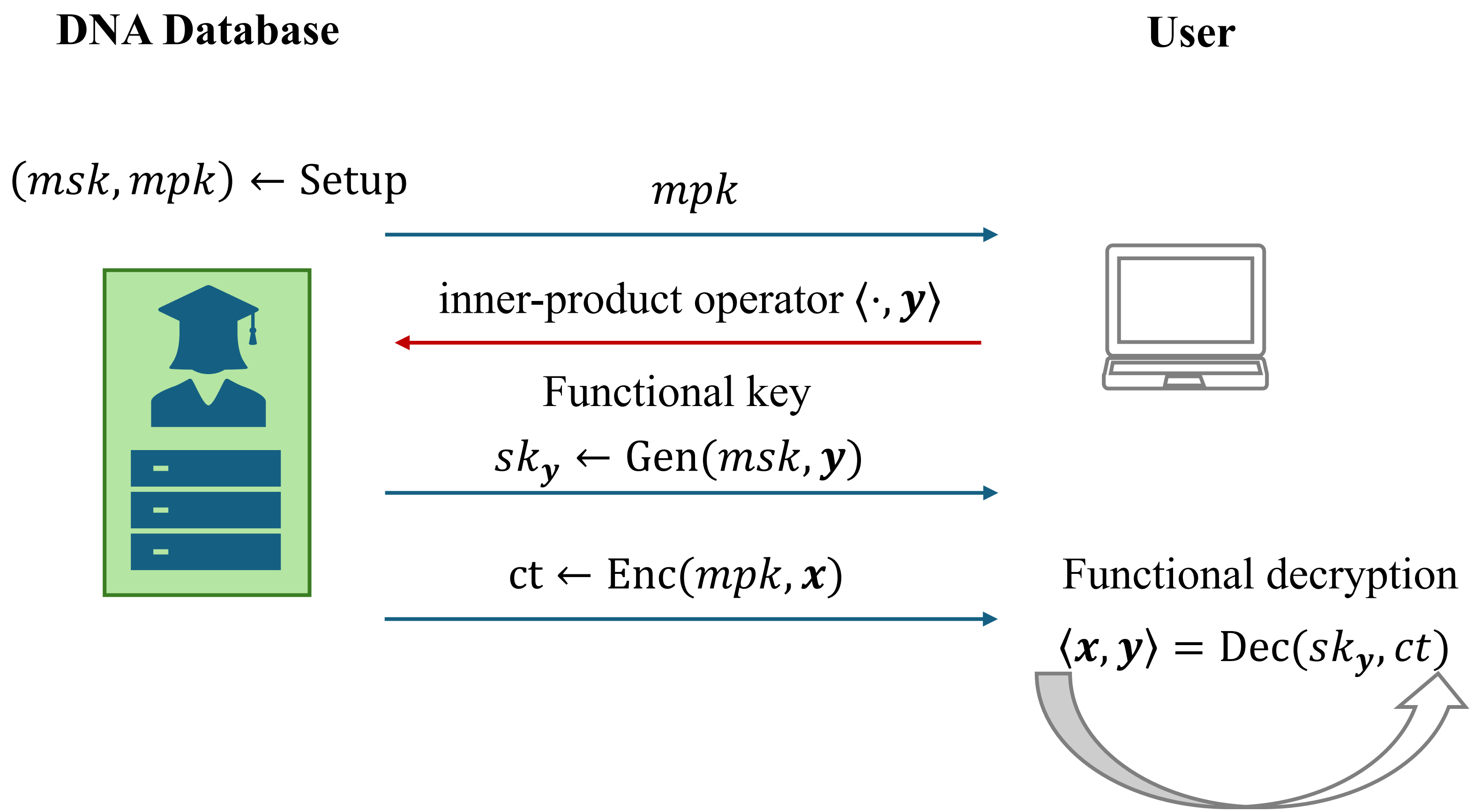


Solving Problem in time $t_{\mathcal{B}}$ with advantage $\epsilon_{\mathcal{B}}$ ⟸ Breaking Scheme in time $t_{\mathcal{A}}$ with advantage $\epsilon_{\mathcal{A}}$

Security Loss ℓ: $\frac{t_{\mathcal{B}}}{\epsilon_{\mathcal{B}}} \leq \frac{t_{\mathcal{A}}}{\epsilon_{\mathcal{A}}} \cdot \ell$ $\xrightarrow{t_{\mathcal{B}} \approx t_{\mathcal{A}}}$ $\ell = O(\epsilon_{\mathcal{A}}/\epsilon_{\mathcal{B}})$

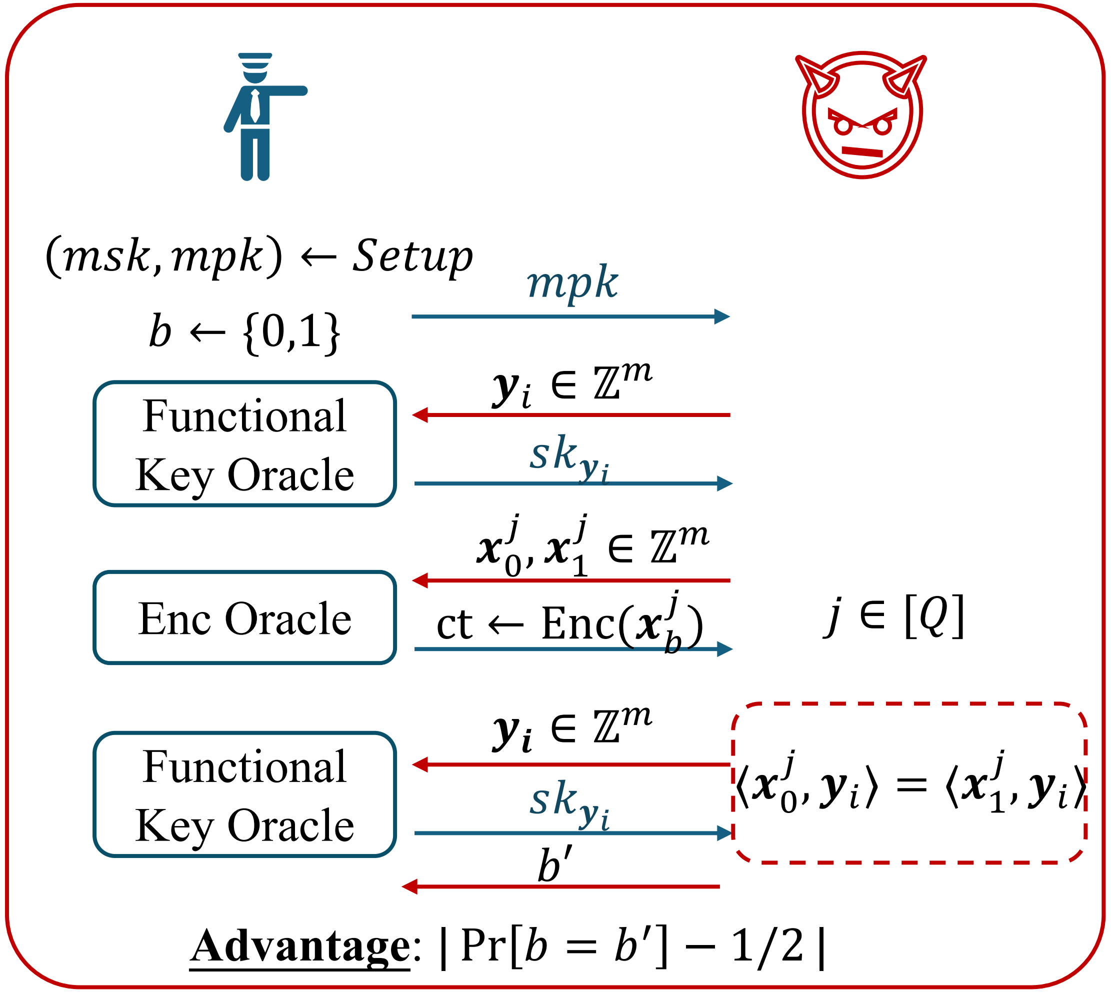
Almost Tight: $\ell = \mathrm{Poly}(\lambda)$
Tight: $\ell = O(1)$

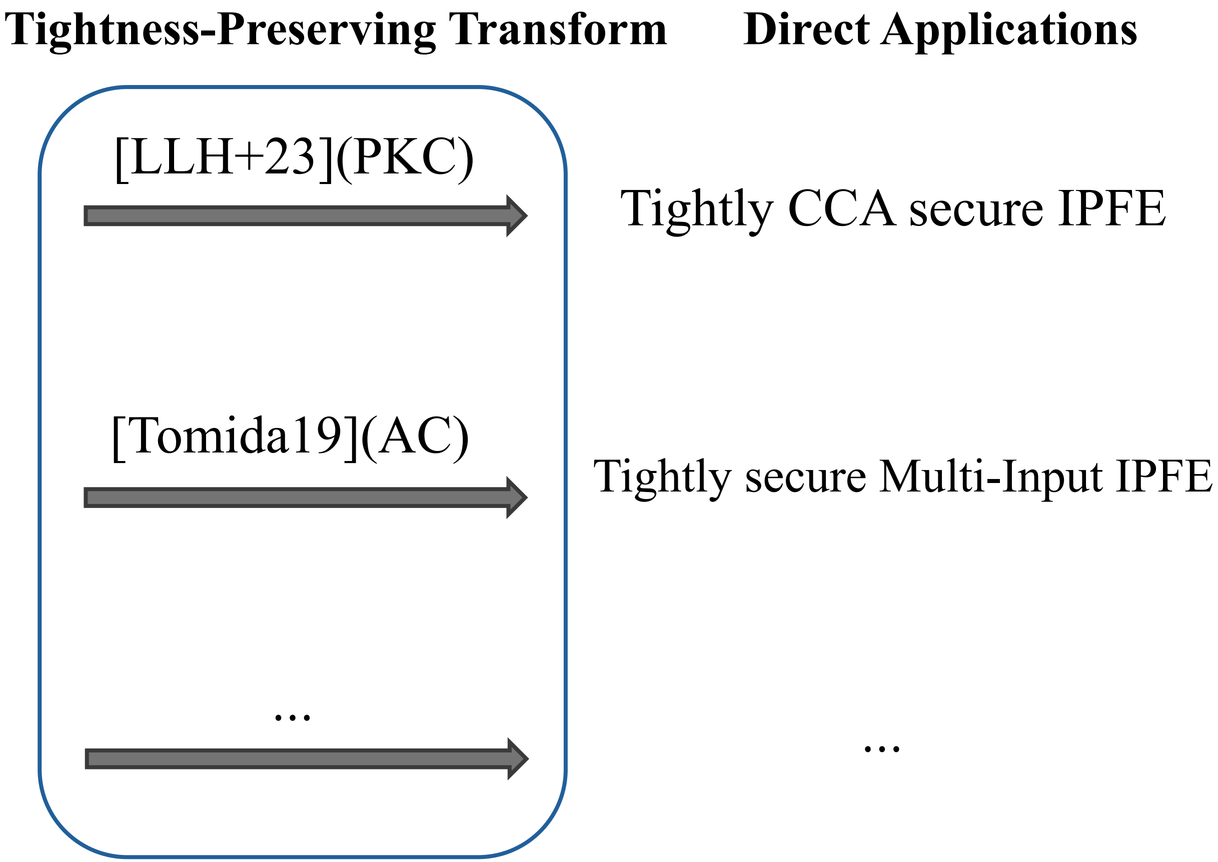
Inner-Product Functional Encryption (IPFE)



IND-CPA Security of IPFE and Its Applications

IND-CPA Security of IPFE





On Achieving Tight CPA Security of IPFE

IPFE Scheme	$\|mpk\|$	$\|msk\|$	$\|sk_y\|$	Ciphertext Expansion	Security Loss	Assumption	Tight Security
[ALS16](C)	$\approx m+1$	$\approx 2m$	≈ 2	$\approx 1+\frac{2}{m}$	$O(Q)$	DDH/DCR/ LWE	×
[Tomida19](AC)	m^2+2	$2m^2$	$2m$	3	$O(1)$	DDH	√

Large Ciphertext!

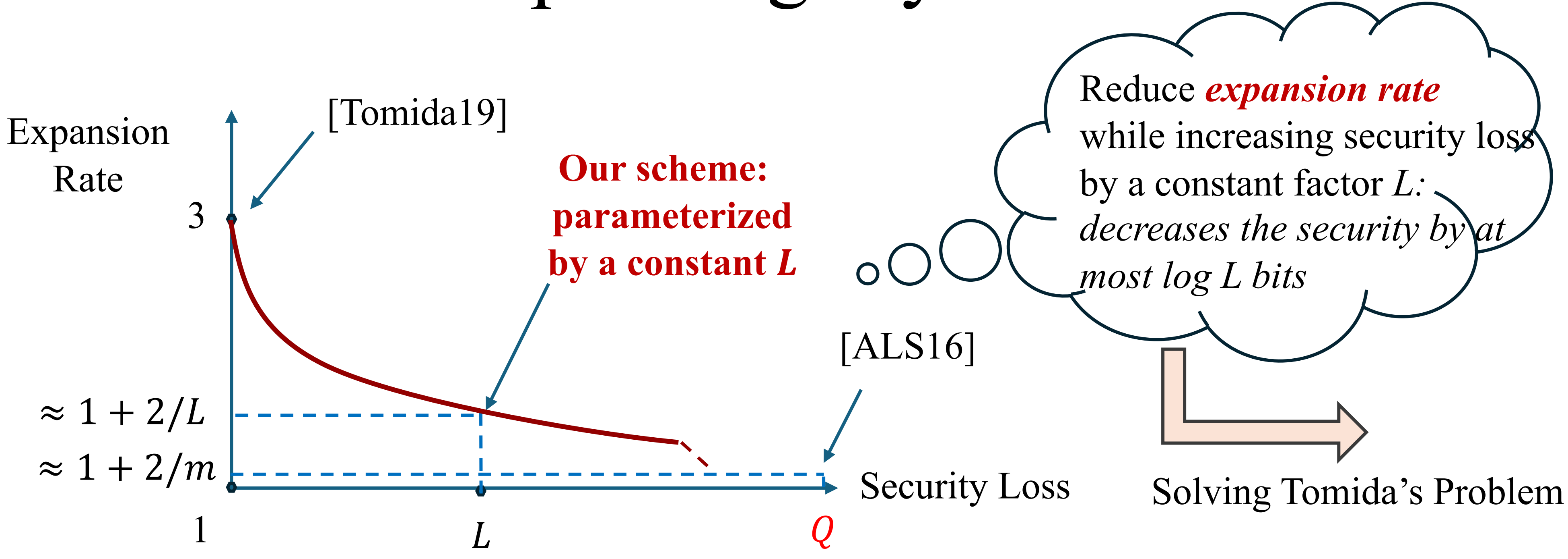
In reality, Q might be very huge, e.g., in the DNA analysis [Tomida19]:

$$m \approx 2^{13}, \qquad Q \approx 2^{27}$$

Tomida's Problem: can we construct more compact tightly secure IPFE schemes?

Another Problem: can we build tightly secure IPFE based on other assumptions, such as LWE, DCR?

Contribution I: More Compact Tightly Secure IPFE



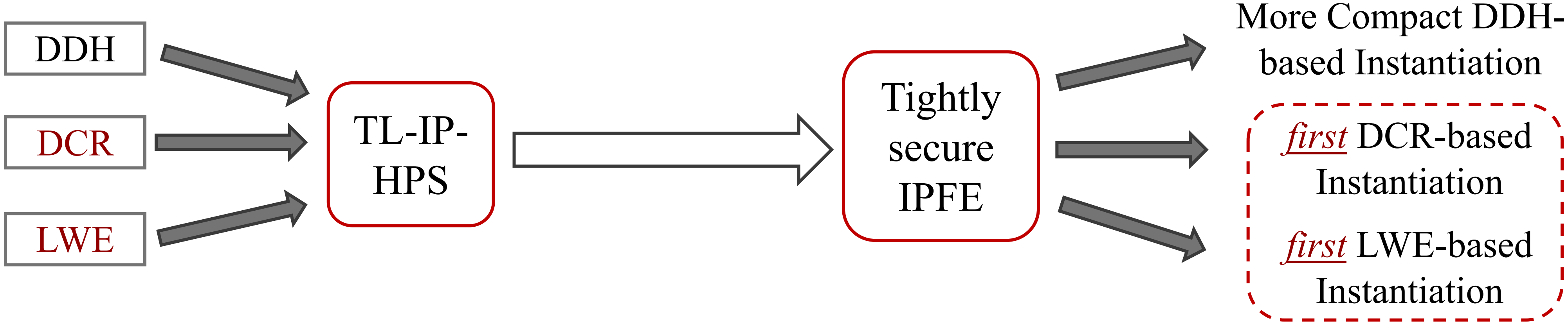
IPFE Scheme	|mpk|	|msk|	$\|sk_y\|$	Ciphertext Expansion	Security Loss	Assumption	Tight Security
[Tomida19]	$m^2 + 2$	$2m^2$	$2m$	3	$O(1) = 3$	DDH	√
Ours ($L = 100$)	$\frac{m^2}{100} + 2$	$\frac{m^2}{50}$	$\frac{m}{50}$	1.02	$O(1) = 300$	DDH	√

Our technique: Compact design & Economic proof strategy

Contribution II: Tightly Secure IPFE from DCR/LWE

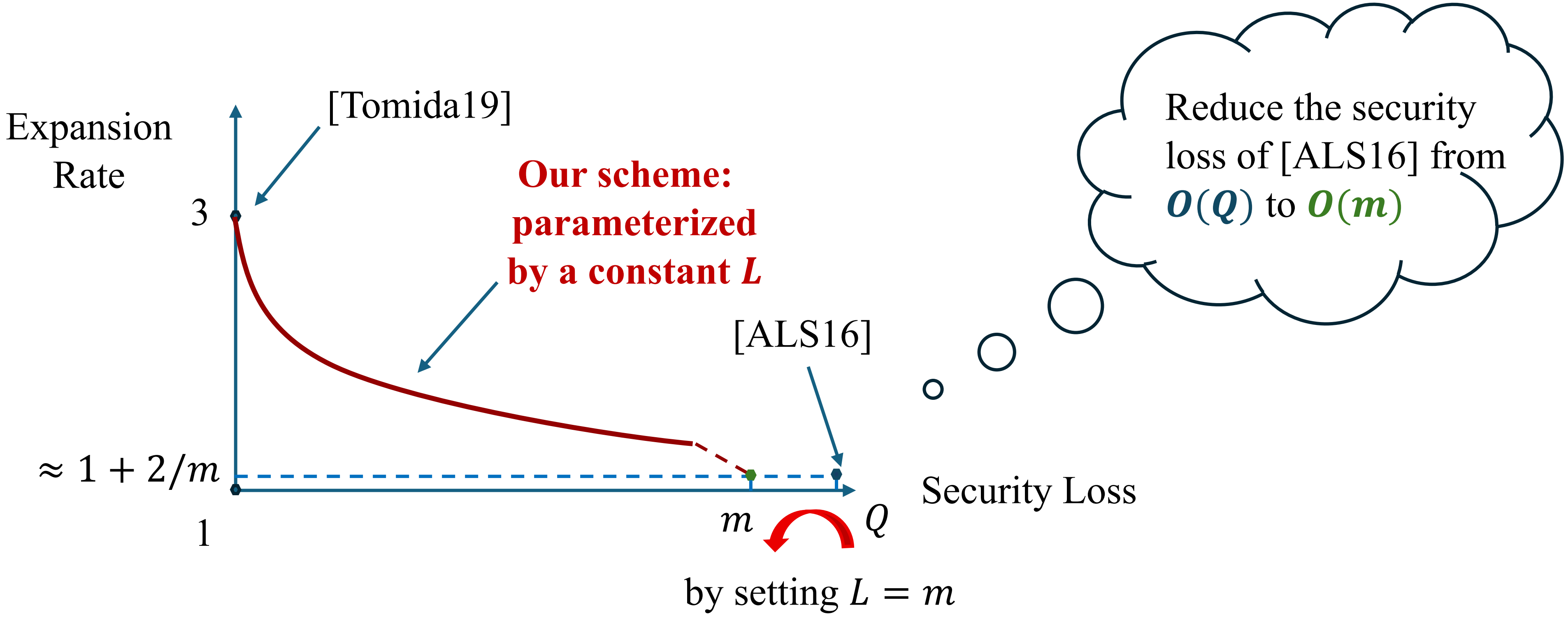
A **unified framework** from a new technical tool called

Two-Leveled Inner-Product Hash Proof System (TL-IP-HPS)



IPFE Scheme	|mpk|	|msk|	$\|sk_y\|$	Ciphertext Expansion	Security Loss	Assumption	Tight Security
[Tomida19]	m^2+2	$2m^2$	$2m$	3	$O(1)$	DDH	√
Ours ($L=100$)	$\frac{m^2}{100}+1$	$\frac{m^2}{100}$	$\frac{m}{100}$	1.01	$O(1)=300$	DCR	√
Ours ($L=100$)	$\frac{m}{100}+1$	$\frac{m}{100}$	$\frac{m}{100}$	$1+\frac{l}{100}$	$O(\lambda^2)=100\lambda^2$	LWE	√

Byproduct: Tighter security for ALS Scheme



IPFE Scheme	|mpk|	|msk|	$\|sk_y\|$	Ciphertext Expansion	Security Loss	Assumption
[ALS16]	$\approx m + 1$	$\approx 2m$	≈ 2	$1 + \frac{2}{m}$	$O(m)$	DDH/DCR

Our parameterized scheme builds a bridge between [ALS16] and [Tomida19]

Recap: Classic IPFE Construction Paradigm

Recap: ALS Scheme, Single-Challenge Ciphertext

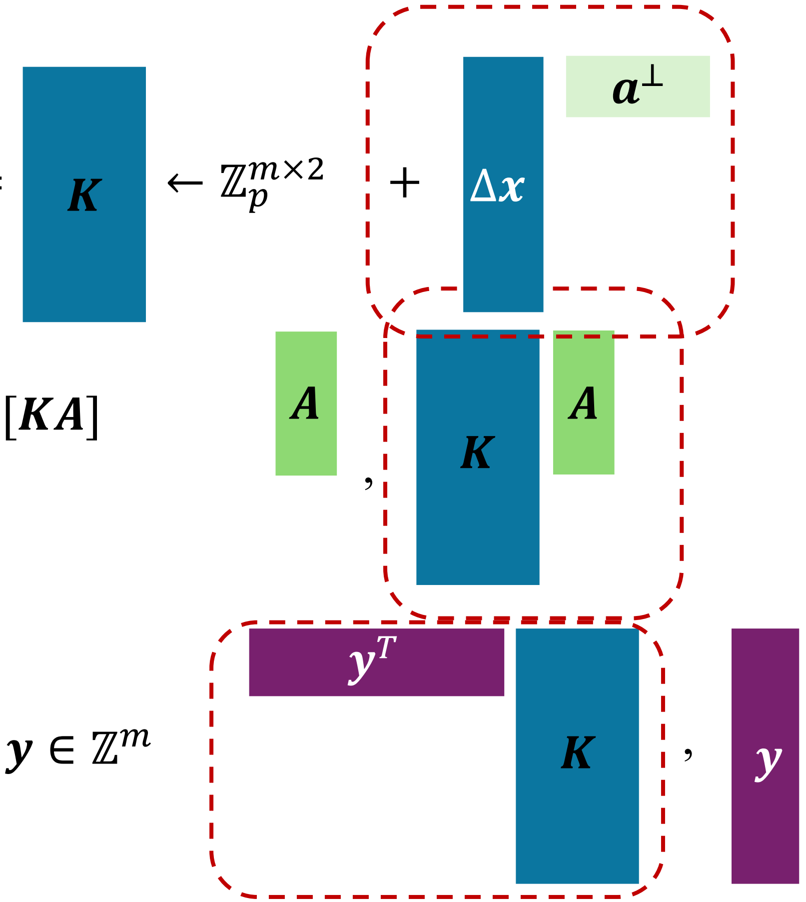
$\boldsymbol{A} = \boldsymbol{A} \leftarrow \mathbb{Z}_p^{2\times1}$ $[\boldsymbol{A}] \in \mathbb{G}_p^{2\times1}$

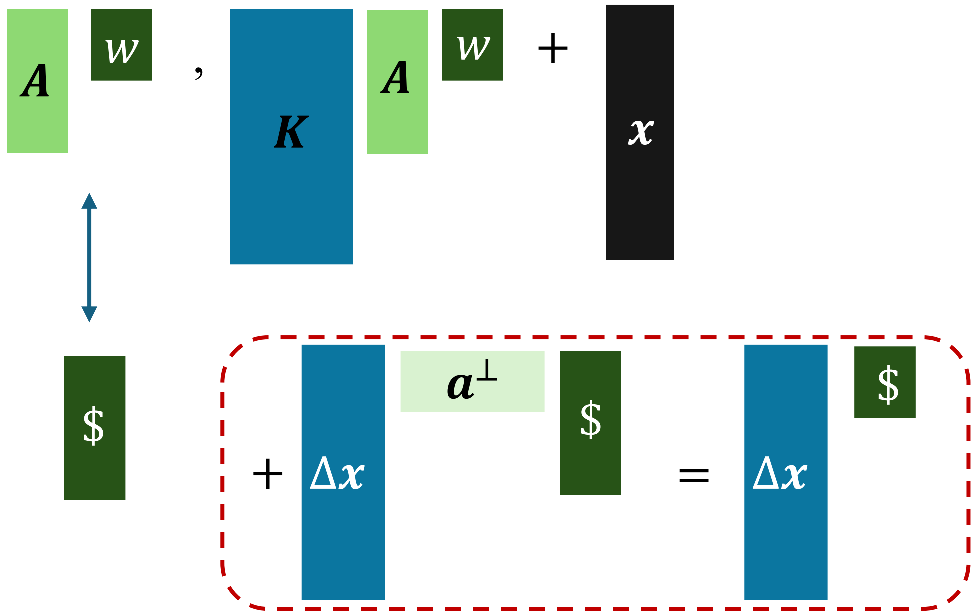
$ct_{\boldsymbol{x}} = [\boldsymbol{A}w], [\boldsymbol{KA}w + \boldsymbol{x}]$

$msk = \boldsymbol{K} = \boldsymbol{K} \leftarrow \mathbb{Z}_p^{m\times2} + \Delta\boldsymbol{x}\,\boldsymbol{a}^{\perp}$

$mpk = [\boldsymbol{A}], [\boldsymbol{KA}]$

$sk_{\boldsymbol{y}} = \boldsymbol{y}^T\boldsymbol{K}, \boldsymbol{y} \in \mathbb{Z}^m$





Proof Sketch

- ☐ DDH Assumption
- ☐ Guess $\boldsymbol{\Delta x}$ (Complexity Leverage)
- ☐ Statistical Argument = 0

This strategy works only in the single-ciphertext setting.

Recap: Tomida Scheme*, Multi-Challenge Ciphertexts

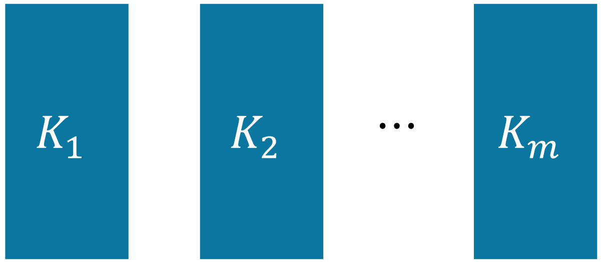
$\boldsymbol{A} \leftarrow \mathbb{Z}_p^{2\times 1}$

Multiple Copies

$msk = \boldsymbol{K}_1, \boldsymbol{K}_2, \cdots, \boldsymbol{K}_m$

$mpk = [\boldsymbol{A}], [\boldsymbol{K}_1\boldsymbol{A}], [\boldsymbol{K}_2\boldsymbol{A}], \cdots, [\boldsymbol{K}_m\boldsymbol{A}]$

$sk_{\boldsymbol{y}} = \boldsymbol{y}^T\boldsymbol{K}_1, \boldsymbol{y}^T\boldsymbol{K}_2, \cdots, \boldsymbol{y}^T\boldsymbol{K}_m, \boldsymbol{y} \in \mathbb{Z}^m$



$$ct_{\boldsymbol{x}} = \begin{bmatrix} [\boldsymbol{A}w_1], [\boldsymbol{A}w_2], \cdots [\boldsymbol{A}w_m], \\ [K_1Aw_1] + [K_2Aw_2] + \cdots + [K_mAw_m] + [x^*] \end{bmatrix}$$

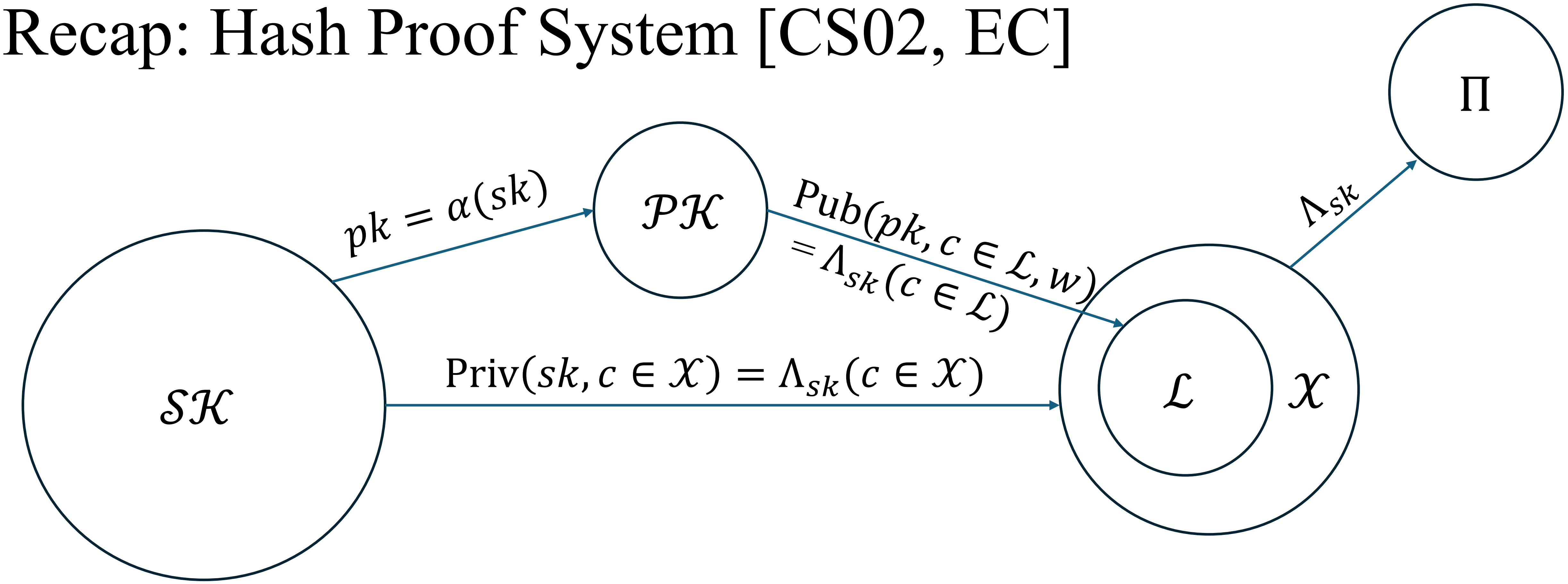
- ☐ High ciphertext expansion
- ☐ Large msk and mpk
- ☐ DDH-based

Can we reduce the ciphertext size & generalize it to other assumptions?

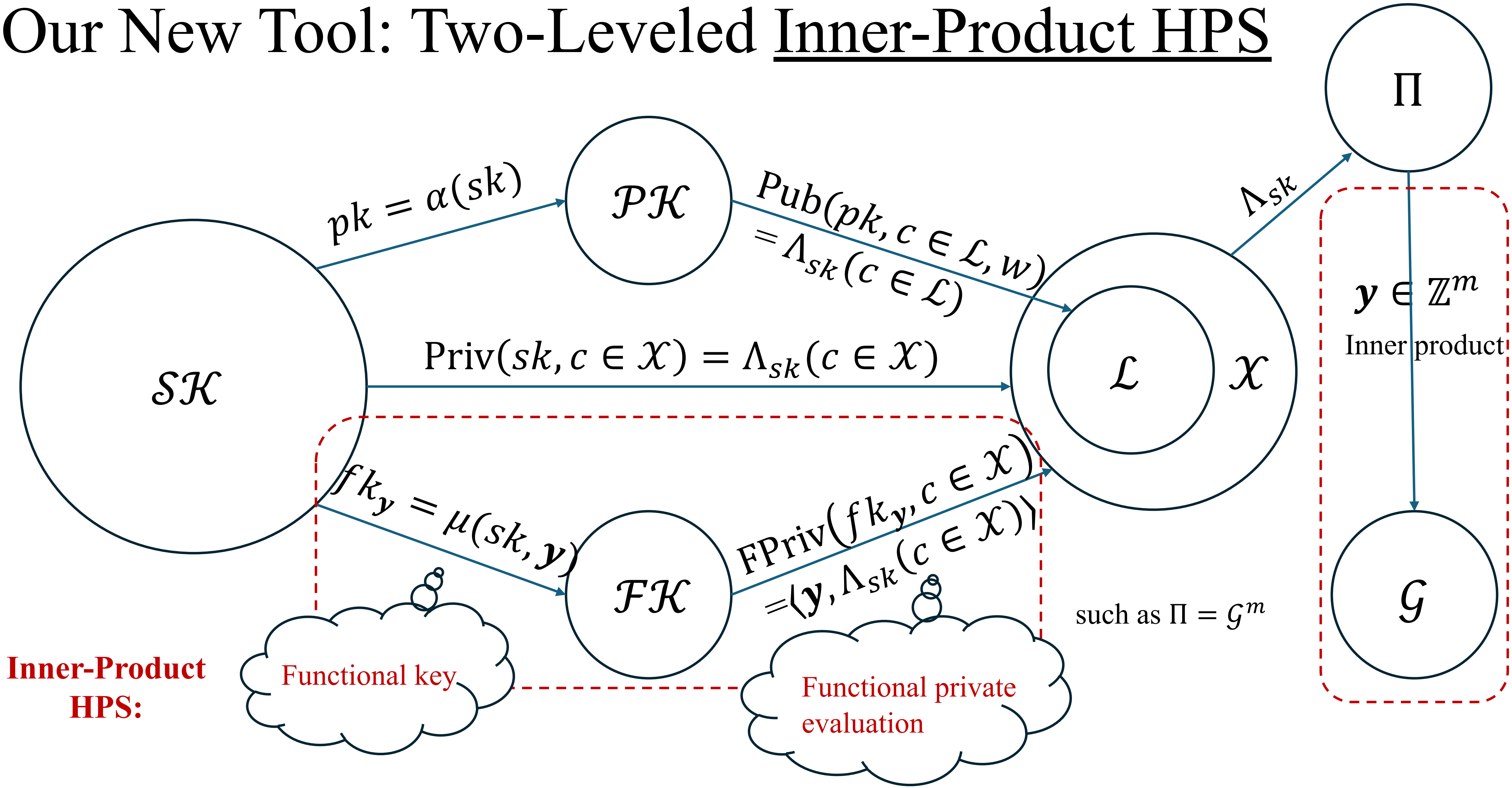
*an equivalent form with [Tomida19]

Technique Tool: Two-Leveled Inner-Product Hash Proof System

Recap: Hash Proof System [CS02, EC]

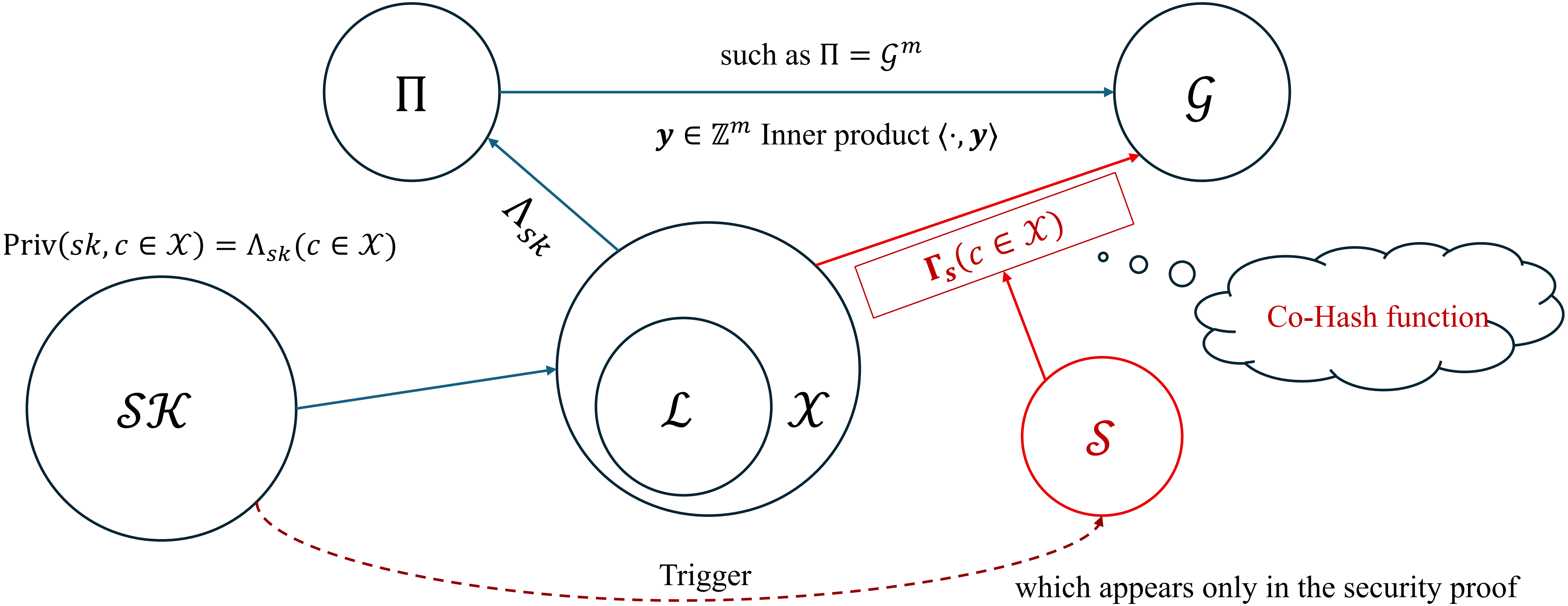


Our New Tool: Two-Leveled Inner-Product HPS



Our New Tool: Two-Leveled Inner-Product HPS

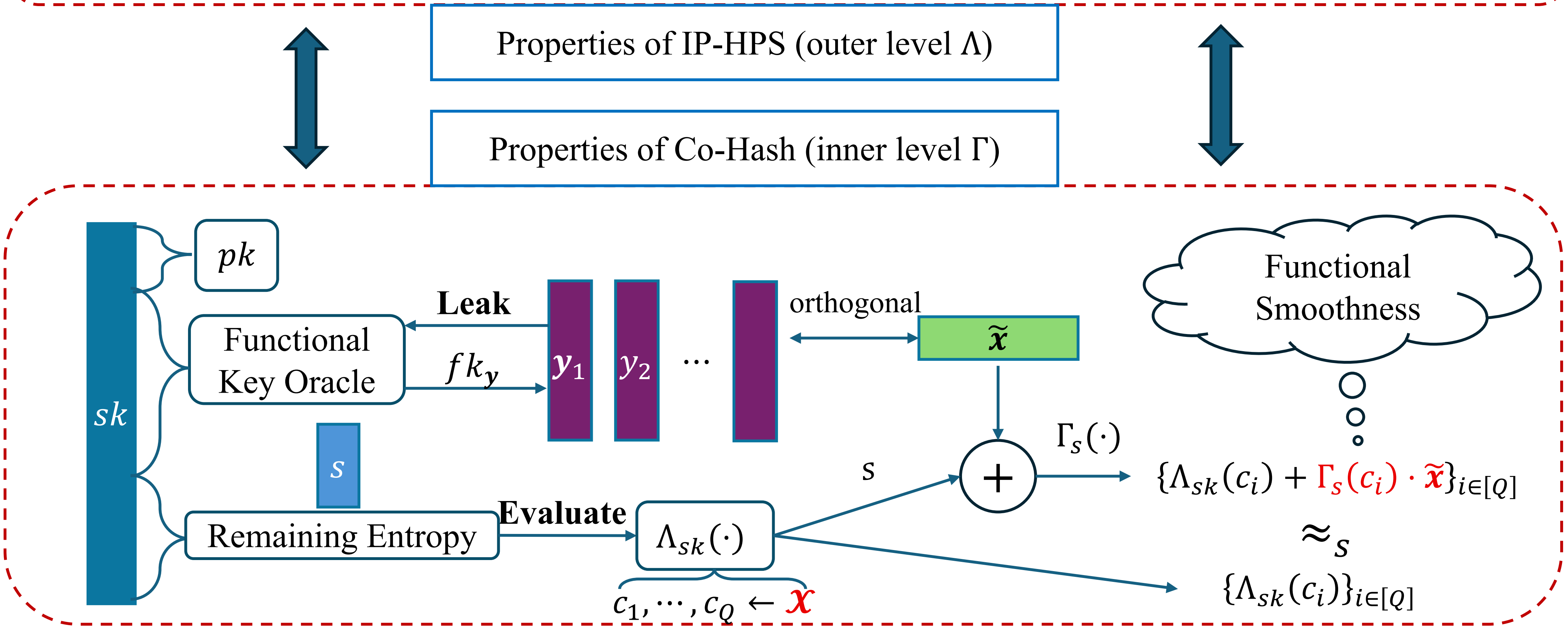
The outer IP-HPS Λ is associated with an **inner co-Hash function** Γ



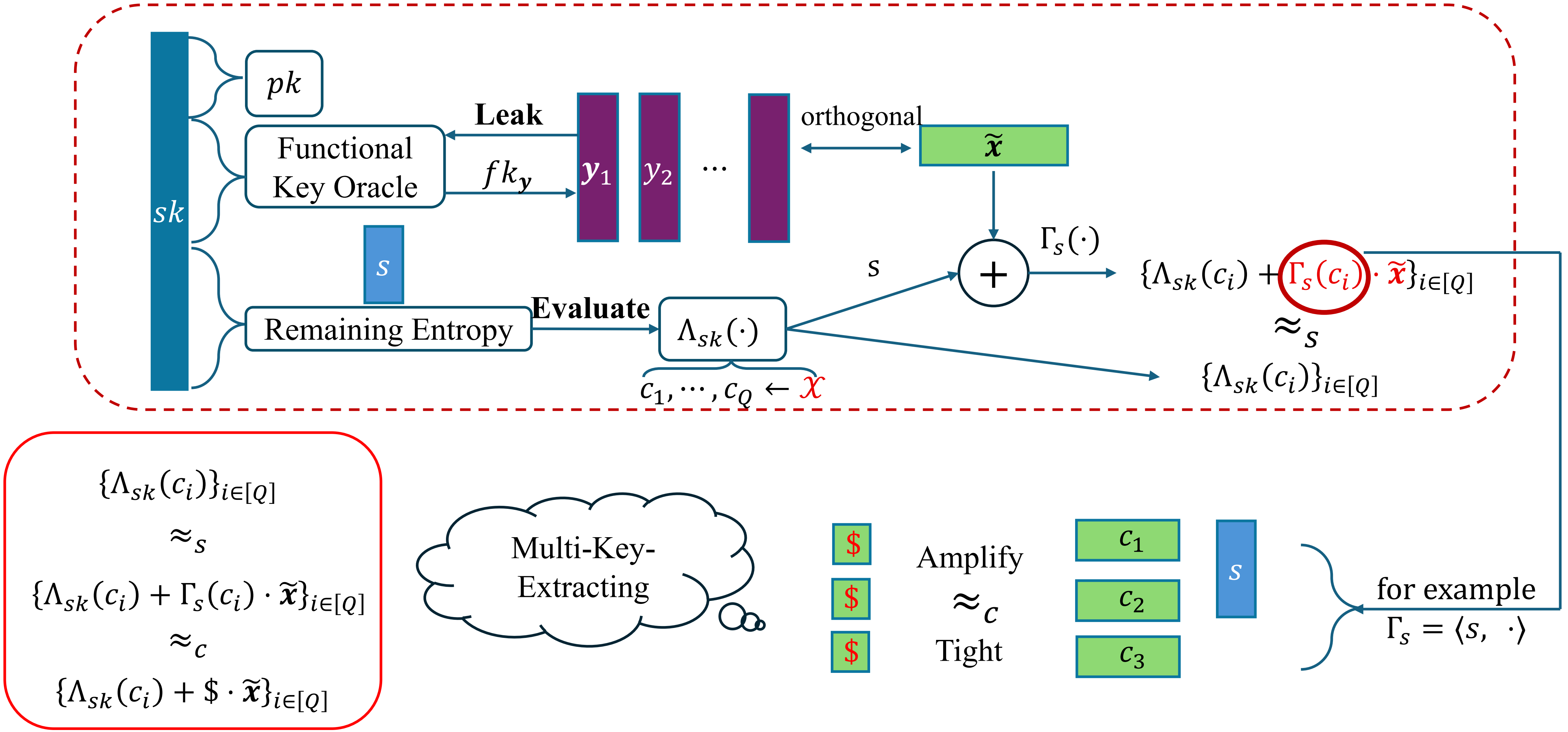
Properties of TL-IP-HPS: Functional Smoothness

Completeness:

- Correctness: $\mathrm{Priv}(sk, c) = \Lambda_{sk}(c) = \mathrm{Pub}(pk, c, w)$ for $c \in \mathcal{L}$, where $pk = \alpha(sk)$
- Functional correctness: $\mathrm{FPriv}(fk_{\boldsymbol{y}}, c) = \langle \Lambda_{sk}(c), \boldsymbol{y} \rangle$, where $fk_{\boldsymbol{y}} = \mu(sk, \boldsymbol{y})$



Properties of TL-IP-HPS: Multi-Key-Extracting

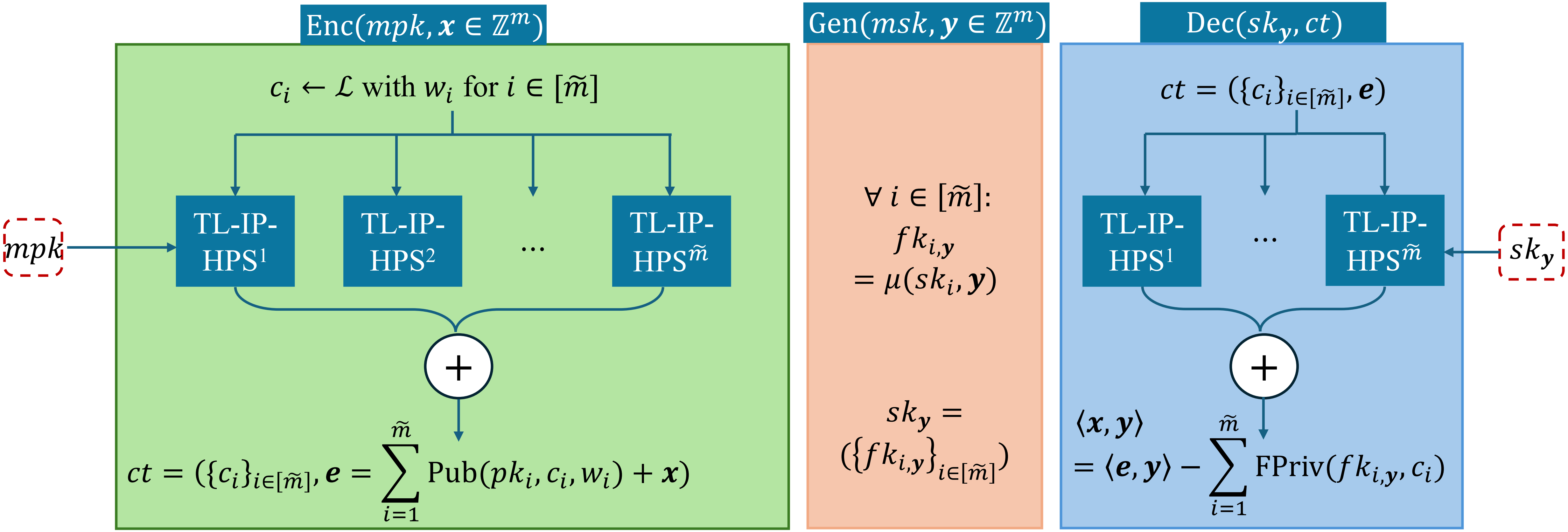


Generic Construction of Tightly Secure IPFE from TL-IP-HPS

Generic Construction

Parameterized by a chosen constant L, we construct tightly secure IPFE from $\tilde{m} = \frac{m}{L}$ copies of TL-IP-HPS:

- $pp \leftarrow \text{Setup}$
- For $i \in [\tilde{m}]$: $sk_i \leftarrow \mathcal{SK}$, $pk_i \leftarrow \alpha(sk_i)$; $msk := \{sk_i\}_{i\in[\tilde{m}]}$, $mpk := (pp, \{pk_i\}_{i\in[\tilde{m}]})$



Proof Strategy I: Trigger co-Hash via Functional Smoothness

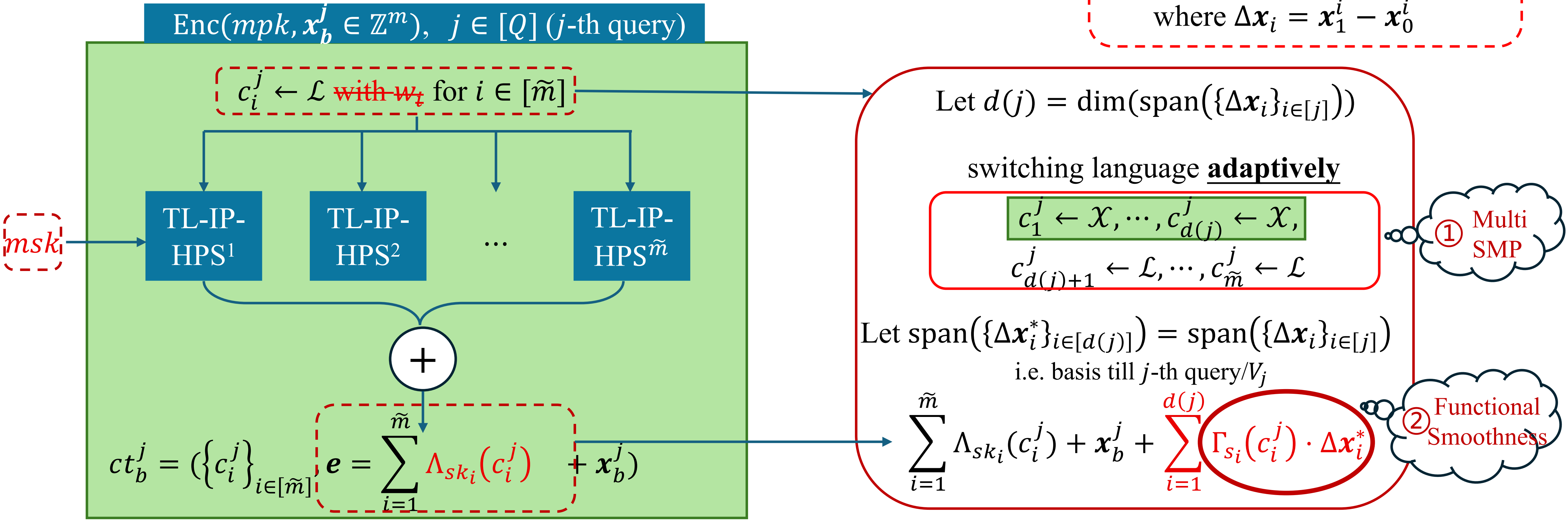
Security analysis:

- Game 1: switch from public evaluation to private evaluation ($\mathrm{Pub}(pk_i, c_i, w_i) \to \Lambda_{sk_i}(c_i)$)
- Game 2: adaptively trigger co-Hash according to the queries of $O_{enc}(\boldsymbol{x}_0^j, \boldsymbol{x}_1^j)$
  - ① Do preparation by **switching language adaptively**
  - ② **Adaptively trigger co-hash** functions

Fact: Let $V_j = \mathrm{span}(\{\Delta \boldsymbol{x}_i\}_{i\in[j]})$

then $\boldsymbol{x}_0^j + V = \boldsymbol{x}_1^j + V$

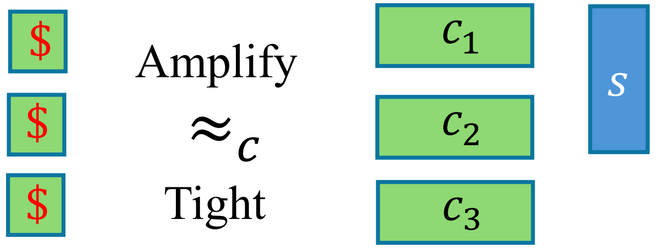
where $\Delta \boldsymbol{x}_i = \boldsymbol{x}_1^i - \boldsymbol{x}_0^i$



Proof Strategy II: Amplification via Multi-Key Extraction

- Game 3: further **amplify co-Hash functions to uniformly random values**!

Fact: Let $V = \mathrm{span}(\{\Delta \boldsymbol{x}_i\}_{i\in[j]})$ then $\boldsymbol{x}_0^j + V = \boldsymbol{x}_1^j + V$



Let $d(j) = \dim(\mathrm{span}(\{\Delta \boldsymbol{x}_i\}_{i\in[j]}))$

switching language adaptively

$c_1^j \leftarrow \mathcal{X}, \cdots, c_{d(j)}^j \leftarrow \mathcal{X},$

$c_{d(j)+1}^j \leftarrow \mathcal{L}, \cdots, c_{\widetilde{m}}^j \leftarrow \mathcal{L}$

Let $\mathrm{span}(\{\Delta \boldsymbol{x}_i^*\}_{i\in[d(j)]}) = \mathrm{span}(\{\Delta \boldsymbol{x}_i\}_{i\in[j]})$

$$\sum_{i=1}^{\widetilde{m}} \Lambda_{sk_i}(c_i^j) + \boldsymbol{x}_b^j + \sum_{i=1}^{d(j)} \Gamma_{s_i}(c_i^j)\cdot \Delta \boldsymbol{x}_i^*$$

③ Multi-key Extracting

$$\sum_{i=1}^{\widetilde{m}} \Lambda_{sk_i}(c_i^j) + \boldsymbol{x}_b^j + \sum_{i=1}^{d(j)} \$ \cdot \Delta \boldsymbol{x}_i^*$$

If $d(j) \le \widetilde{m}$, $\sum_{i=1}^{d(j)} \$ \cdot \Delta \boldsymbol{x}_i^*$ perfectly hides $\boldsymbol{x}_b^j$

Problem: what if $d(j) > \widetilde{m}$?

Proof Strategy III: Iterative Language Switching

Problem: what if $d(j) > \tilde{m}$?

Suppose $\underline{k \cdot \tilde{m} \le d(j) < (k+1) \cdot \tilde{m}}$ for some $\underline{k}$

First round of language switching via Proof Strategy I & II

$$c_1^j \leftarrow \mathcal{X}, \cdots, \cdots, c_{\tilde{m}}^j \leftarrow \mathcal{X}$$

$$\sum_{i=1}^{\tilde{m}} \Lambda_{sk_i}(c_i^j) + \boldsymbol{x}_b^j + \sum_{i=1}^{\tilde{m}} \$ \cdot \Delta \boldsymbol{x}_i^*$$

Second round of language switching via Proof Strategy I & II

$$c_1^j \leftarrow \mathcal{X}, \cdots, \cdots, c_{\tilde{m}}^j \leftarrow \mathcal{X}$$

$$\sum_{i=1}^{\tilde{m}} \Lambda_{sk_i}(c_i^j) + \boldsymbol{x}_b^j + \sum_{i=1}^{\tilde{m}} \$ \cdot \Delta \boldsymbol{x}_i^* + \sum_{i=1}^{\tilde{m}} \$ \cdot \Delta \boldsymbol{x}_{\tilde{m}+i}^*$$

⋮

$(k+1)$-th round of language switching via Proof Strategy I & II

$$c_1^j \leftarrow \mathcal{X}, \cdots, \cdots, c_{d(j)-k\cdot\tilde{m}}^j \leftarrow \mathcal{X}, \quad c_{d(j)-k\cdot\tilde{m}+1}^j \leftarrow \mathcal{L}, \cdots, c_{\tilde{m}}^j \leftarrow \mathcal{L}$$

$$\sum_{i=1}^{\tilde{m}} \Lambda_{sk_i}(c_i^j) + \boldsymbol{x}_b^j + \sum_{i=1}^{\tilde{m}} \$ \cdot \Delta \boldsymbol{x}_i^* + \sum_{i=1}^{\tilde{m}} \$ \cdot \Delta \boldsymbol{x}_{\tilde{m}+i}^* + \cdots + \sum_{i=1}^{d(j)-k\cdot\tilde{m}} \$ \cdot \Delta \boldsymbol{x}_{k\cdot\tilde{m}+i}^*$$

$\sum_{i=1}^{d(j)} \$ \cdot \Delta \boldsymbol{x}_i^*$

After $k+1$ iterations, we extract enough entropy $\sum_{i=1}^{d(j)} \$ \cdot \Delta \boldsymbol{x}_i^*$ to hide $\boldsymbol{x}_b^j$

Instantiation from LWE

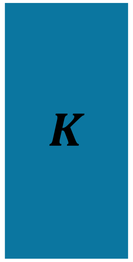
Probabilistic TL-IP-HPS (following [HLW+23, C])

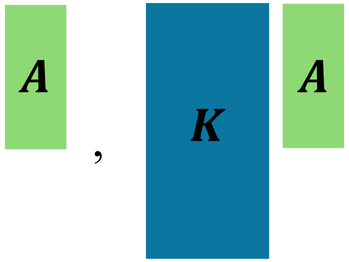
LWE assumption does not result in exact evaluation.
Need **adapting** TL-IP-HPS to allow for **approximate evaluation**.

Probabilistic TL-IP-HPS

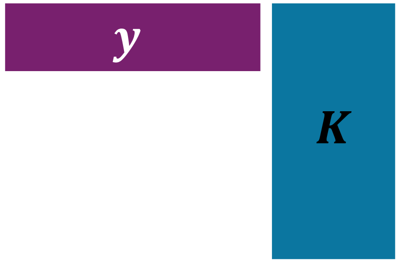
Correctness: $\text{Pub}(pk, c, w) = \text{Priv}(sk, c)$	→	Statistical evaluation Ind: $\text{Pub}(pk, c, w) \approx_s \text{Priv}(sk, c)$
Functional correctness	→	Functional correctness
Deterministic algorithms co-Hash, Priv, Pub	→	Probabilistic algorithms co-Hash, Priv, Pub
Functional smoothness	→	Functional smoothness

TL-IP-HPS from LWE

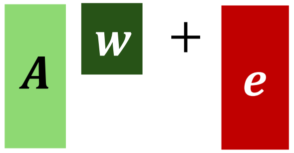
- $\boldsymbol{A} =$  $\leftarrow \mathbb{Z}_q^{l\times n}$
- $sk = \boldsymbol{K} =$  $\leftarrow \chi_K^{m\times l}$
- $pk = (\boldsymbol{A}, \boldsymbol{P} \coloneqq \boldsymbol{K}\boldsymbol{A})$



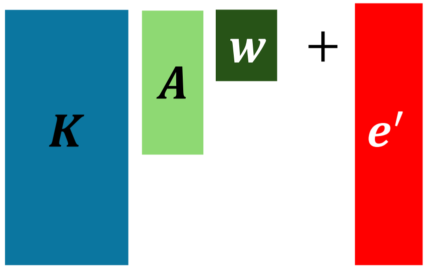
- $fk_{\boldsymbol{y}} = \boldsymbol{y}^T\boldsymbol{K}, \boldsymbol{y} \in \mathbb{Z}^m$



- $\boldsymbol{c} = \boldsymbol{A}\boldsymbol{w} + \boldsymbol{e}$

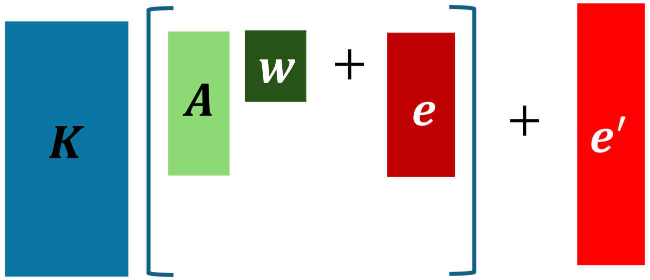


- $\mathrm{Pub}(pk, \boldsymbol{c}, \boldsymbol{w}) = \boldsymbol{P}\boldsymbol{w} + \boldsymbol{e}'$

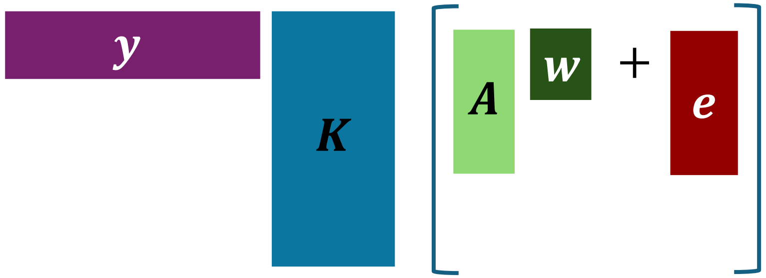


Big noise
(smudging)

- $\mathrm{Priv}(sk, \boldsymbol{c}) = \boldsymbol{K}\boldsymbol{c} + \boldsymbol{e}'$



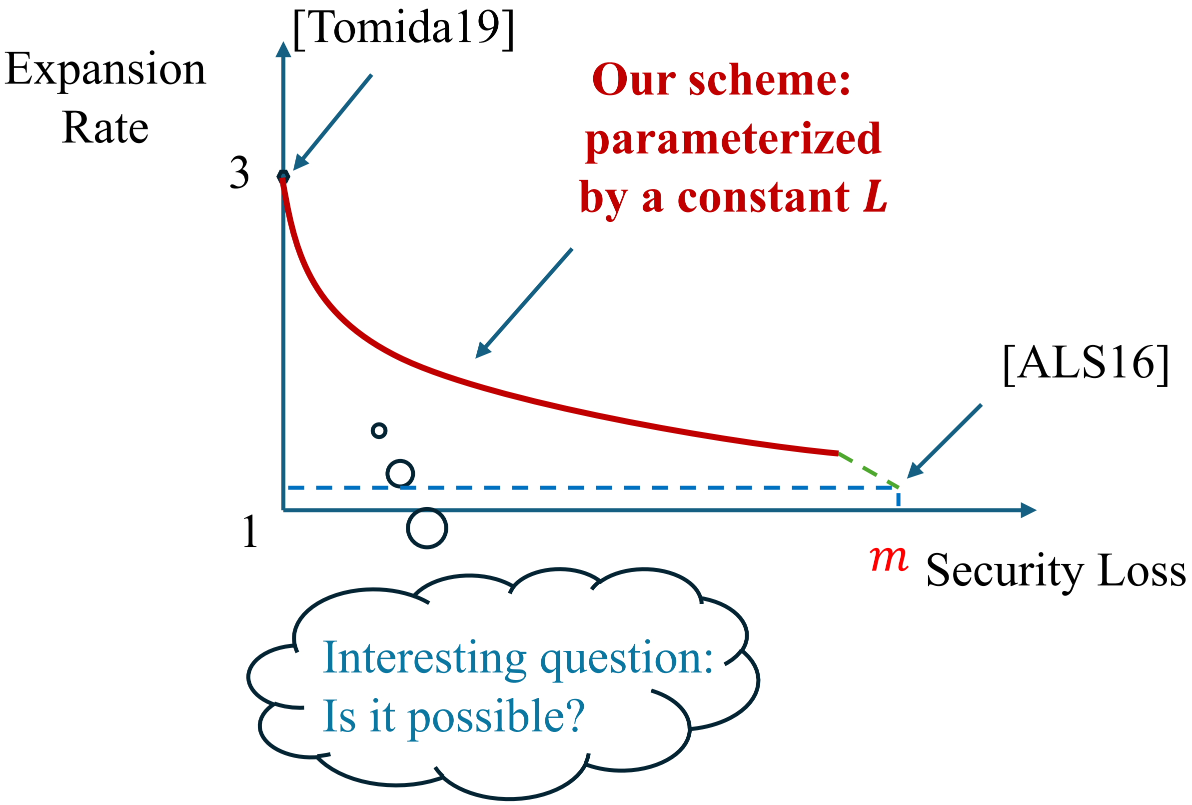
- $\mathrm{FPriv}(fk_{\boldsymbol{y}}, \boldsymbol{c})$
  $= (\boldsymbol{y}^T\boldsymbol{K}) \cdot \boldsymbol{c}$



- ➢ Statistical evaluation Ind: due to smudging
- ➢ Functional Correctness
- ➢ Functional Smoothness: fine-grained statistical analysis of discrete Gaussians
- ➢ Multi-key-extracting: tight reductions from LWE to Multi-instance LWE

Conclusion

- A unified framework for tightly secure IPFE from TL-IP-HPS:
  Compact design & Economic proof strategy
  - *More compact* tightly secure DDH-based IPFE:
    Solving Tomida's problem
  - the *first* tightly secure DCR-based IPFE
  - the *first* tightly secure LWE-based IPFE
- Byproduct: tighter security loss for [ALS16]



Thanks! Questions?

Email: tcs.hongxu.yi@gmail.com