Multi-Hop Fine-Grained Proxy Re-Encryption

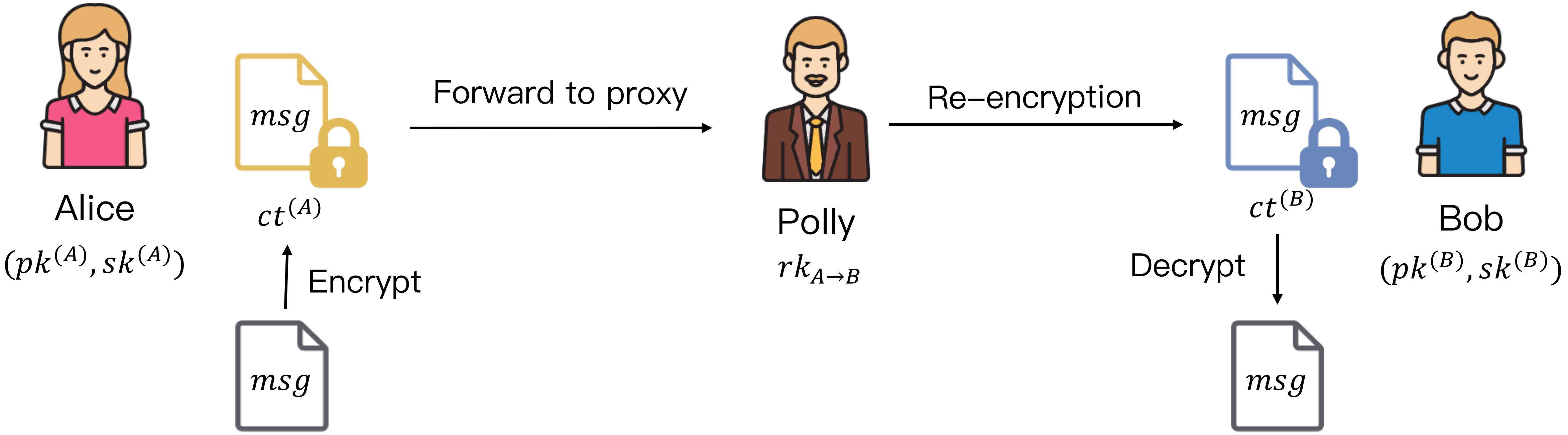
Yunxiao Zhou, Shengli Liu, Shuai Han

Shanghai Jiao Tong University

PKC 2024, Sydney, Australia

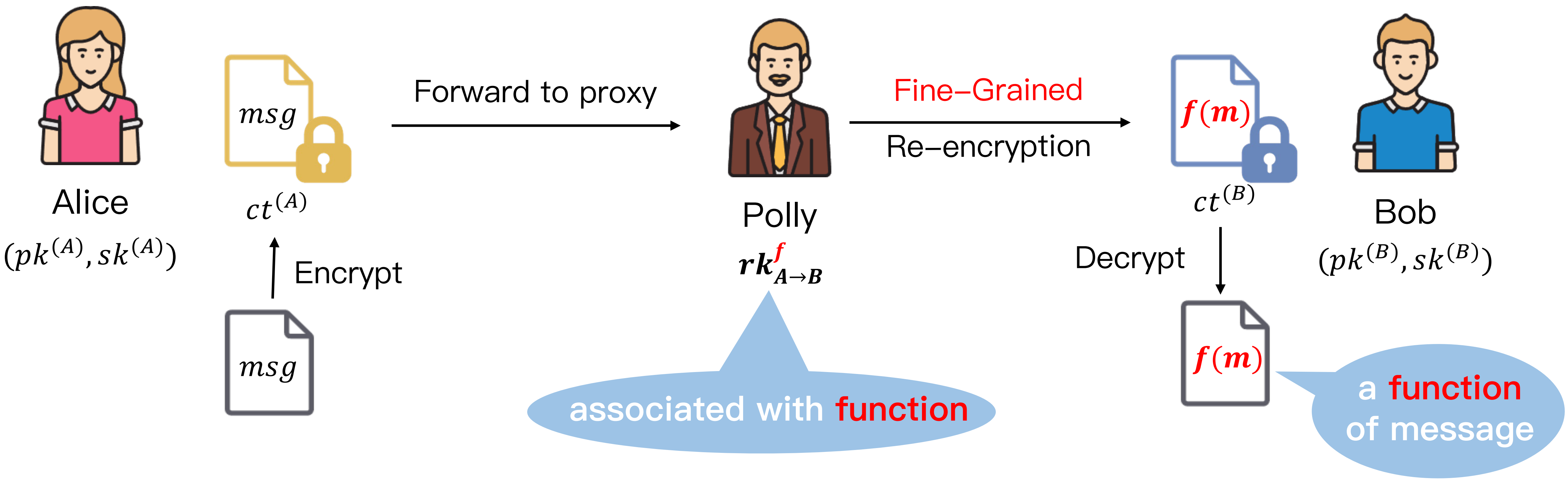
上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

Proxy Re–Encryption



Proxy Re–Encryption (PRE) is an **Extension** of Public Key Encryption (PKE). It allows **Alice** to allocate her **Decryption Right** to **Bob**, with the help of a proxy **Polly** that has a **Re–Encryption Key**.

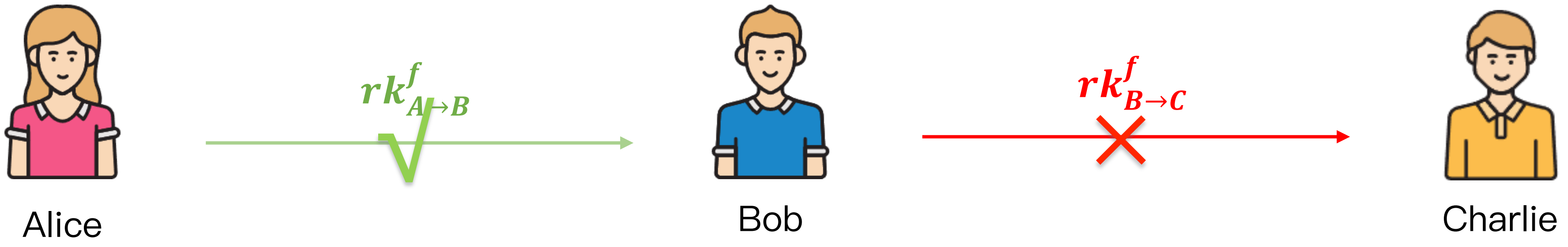
Fine–Grained Proxy Re–Encryption



Fine–Grained **Proxy Re–Encryption (FPRE)** was proposed in [ZLHZ23, AC], which supports more **flexible delegation**. Now Alice can distribute re–encryption key associated with a **function**.

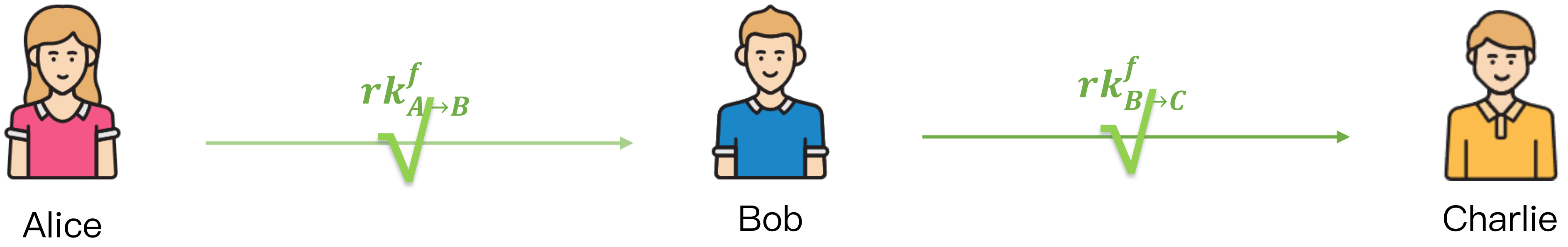
Single–Hop VS. Multi–Hop

Single–Hop FPRE



In a single–hop FPRE, the ciphertext can be re–encrypted only **once.**

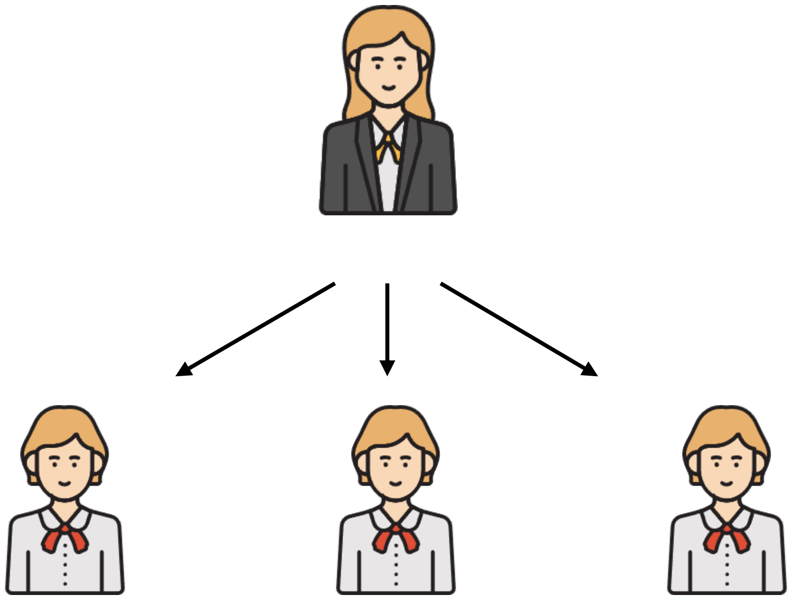
Multi–Hop FPRE



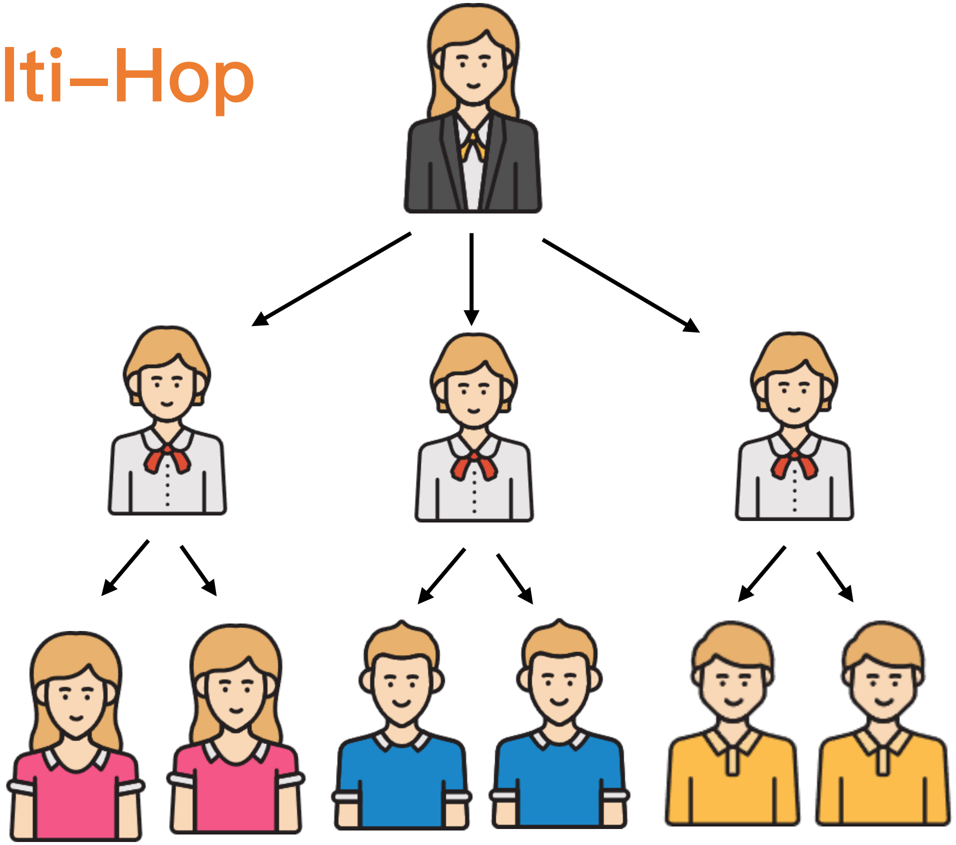
In a multi–hop FPRE, the ciphertext can be re–encrypted **multiple times.**

Single-Hop VS. Multi-Hop

Single-Hop

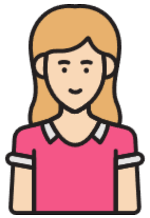


Multi-Hop



Single-hop FPRE supports only single-level delegation while multi-hop FPRE can support **multi-level delegation**.

Security Model: CPA for multi-hop FPRE



$(pk^{(A)}, sk^{(A)})$

$(pk^{(B)}, sk^{(B)})$

$(pk^{(C)}, sk^{(C)})$

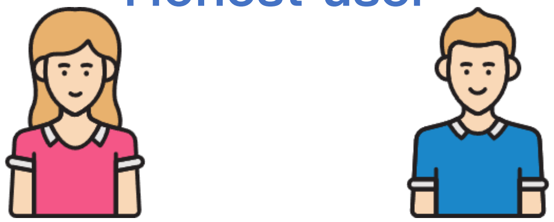
FPRE considers a multi-user setting.

Security Model: CPA for multi-hop FPRE

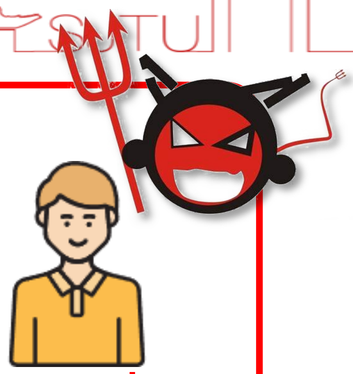
$(pk^{(A)}, sk^{(A)})$ $(pk^{(B)}, sk^{(B)})$ $(pk^{(C)}, sk^{(C)})$

FPRE considers a multi-user setting.

Honest user



$(pk^{(A)}, sk^{(A)})$ $(pk^{(B)}, sk^{(B)})$



Corrupted user

$(pk^{(C)}, sk^{(C)})$

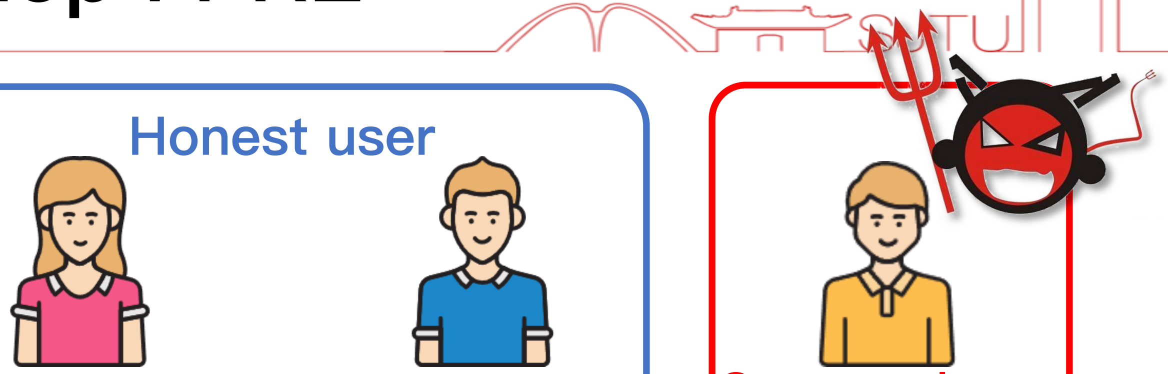
The adversary can corrupt some users and obtain their secret key.

Security Model: CPA for multi-hop FPRE

$(pk^{(A)}, sk^{(A)})$ $(pk^{(B)}, sk^{(B)})$ $(pk^{(C)}, sk^{(C)})$

FPRE considers a multi-user setting.

Honest user



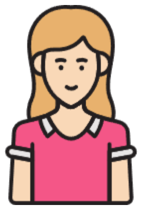
$(pk^{(A)}, sk^{(A)})$ $(pk^{(B)}, sk^{(B)})$

Corrupted user

$(pk^{(C)}, sk^{(C)})$

The adversary can corrupt some users and obtain their secret key.

Challenge user



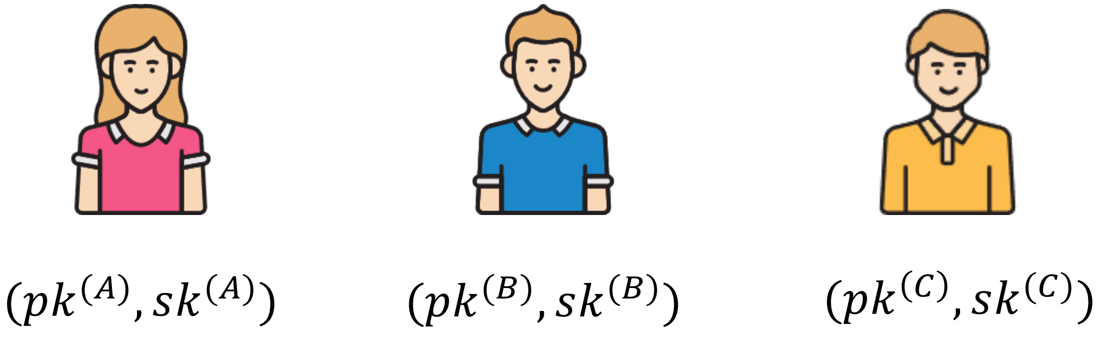
$('Alice', m_0, m_1)$

$ct^* \leftarrow Enc(pk^{(A)}, m_b)$

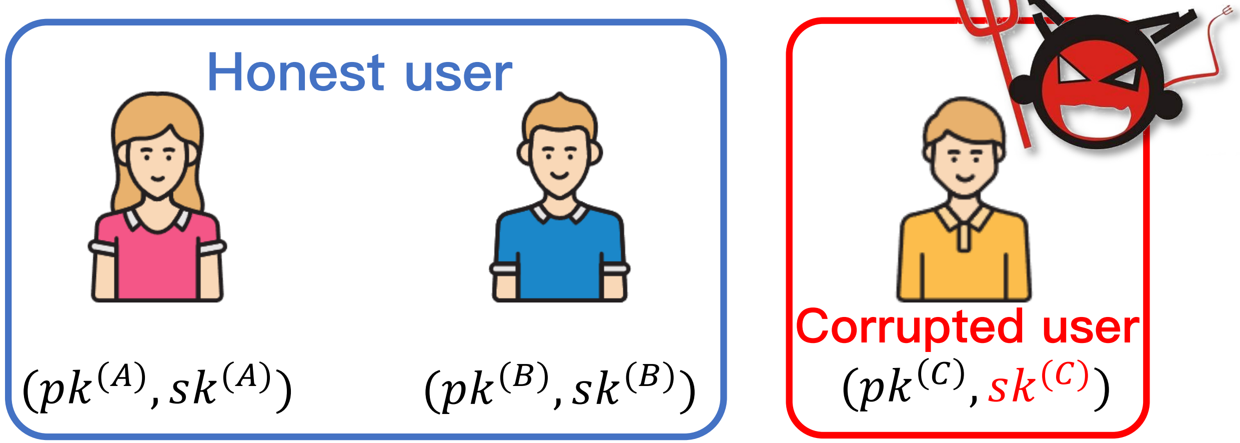
$(pk^{(A)}, sk^{(A)})$

The adversary wants to distinguish the challenge ciphertext encrypts m_0 or m_1

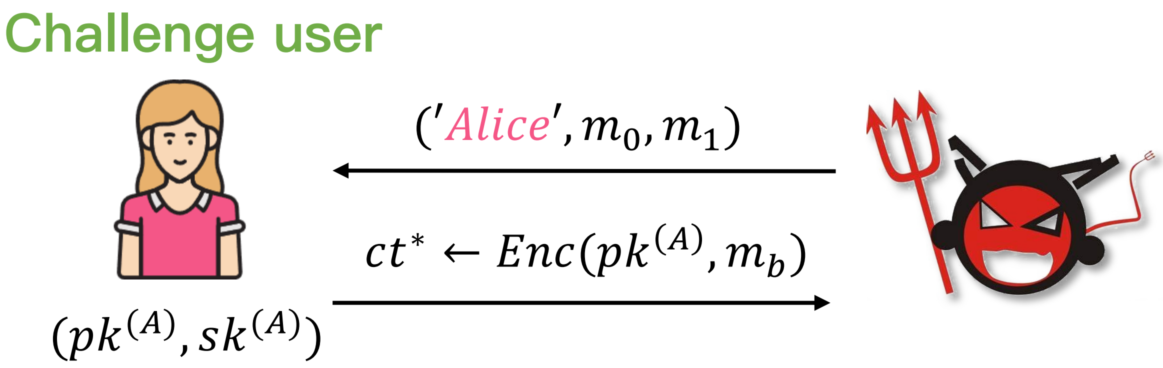
Security Model: CPA for multi-hop FPRE



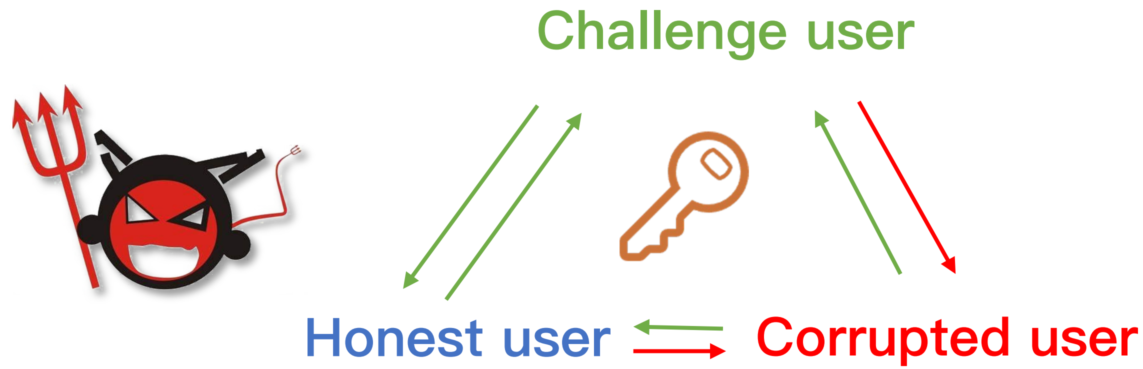
FPRE considers a multi-user setting.



The adversary can corrupt some users and obtain their secret key.



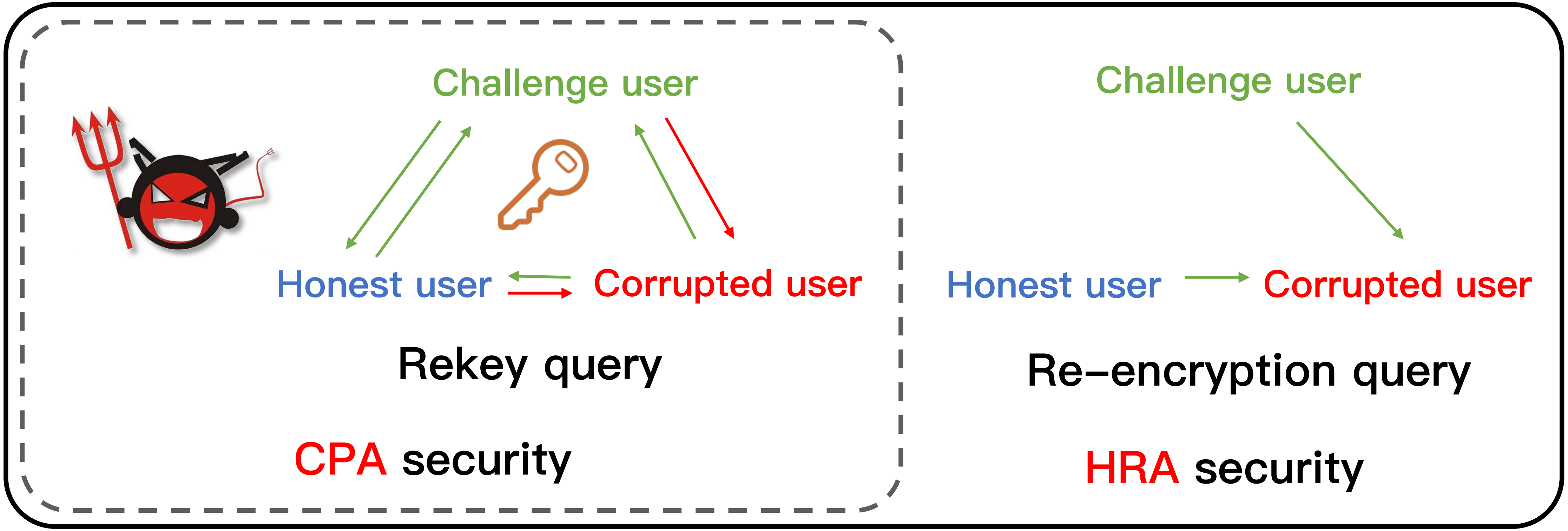
The adversary wants to distinguish the challenge ciphertext encrypts m_0 or m_1



The adversary can obtain rekeys that does not lead to trivial attack.

Security Model: HRA for multi-hop FPRE

IND security against **honest-re-encryption attack (HRA),** proposed in [Cohen19, PKC], allows the adversary to query honest re-encryptions from honest user (including challenger user) to corrupted user.



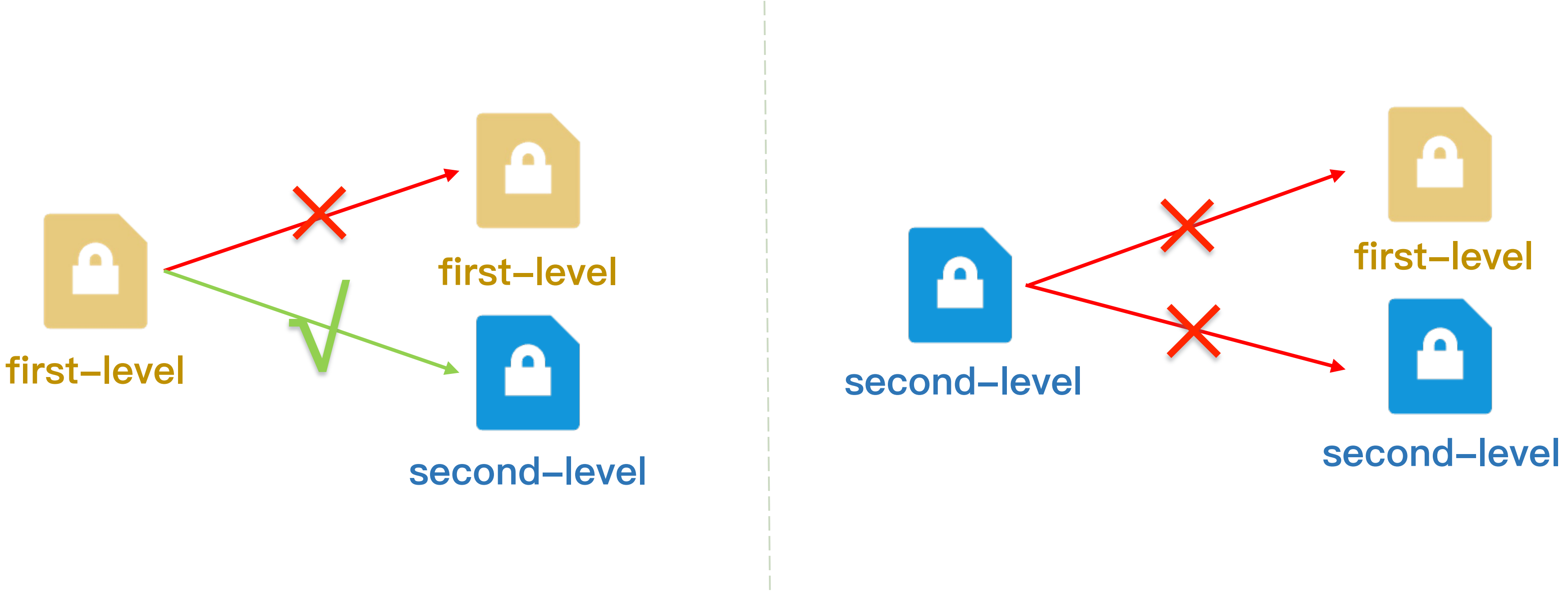
Contribution

- **Formal Definitions for Multi-Hop Fine-Grained PRE and Its Securities.**
  - Formalize the security properties like CPA, HRA, IND, wKP, SH, UNID, CUL for multi-hop FPRE and show **relations** among them.
- Generic Framework **for Achieving CPA and HRA Security for Multi-Hop FPRE.**
- **Construction of Multi-Hop FPRE from LWE.**
  - ✓ **with adaptive HRA security.**

Contents

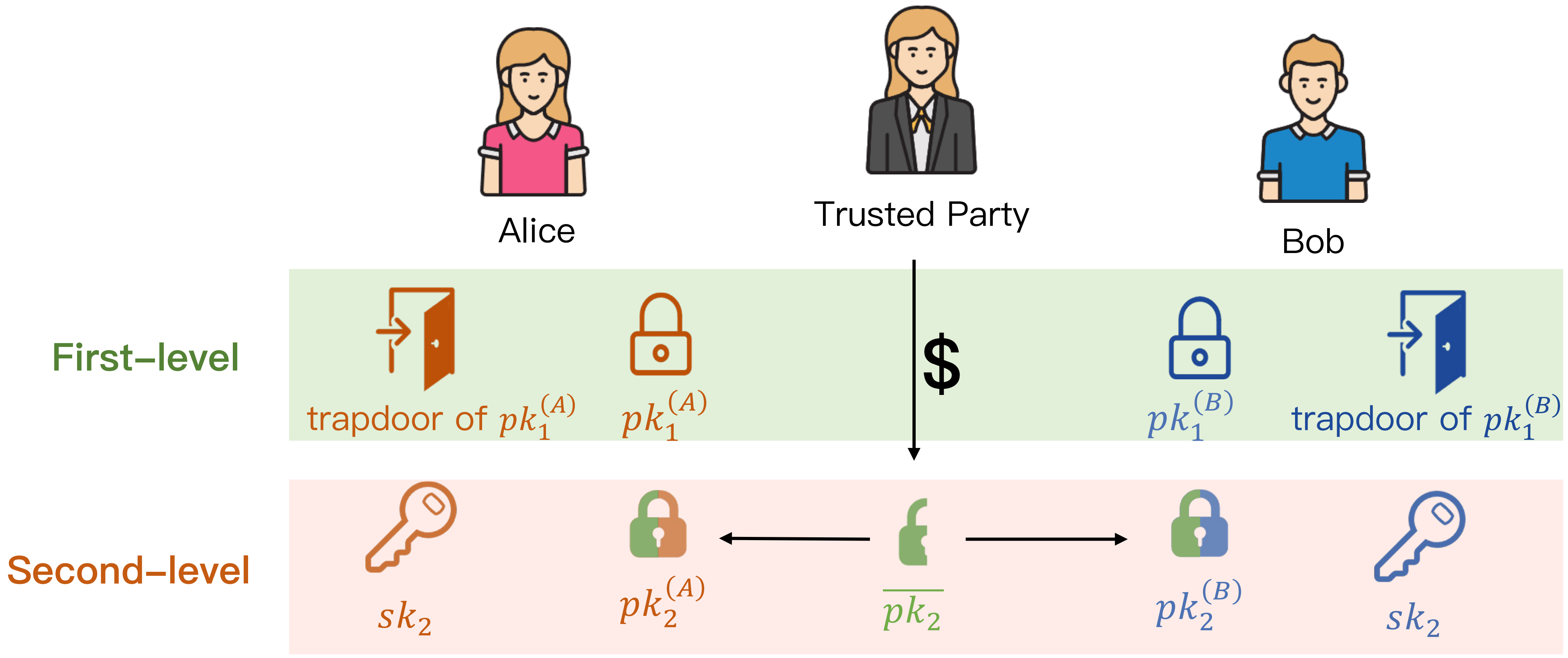
Recap：Single-hop FPRE in [ZLHZ23]

The scheme in [ZLHZ23, AC] has **two levels** of ciphertext, the first-level ciphertext can be re-encrypted but the second-level ciphertext cannot, and thus only achieves **single-hop** FPRE.



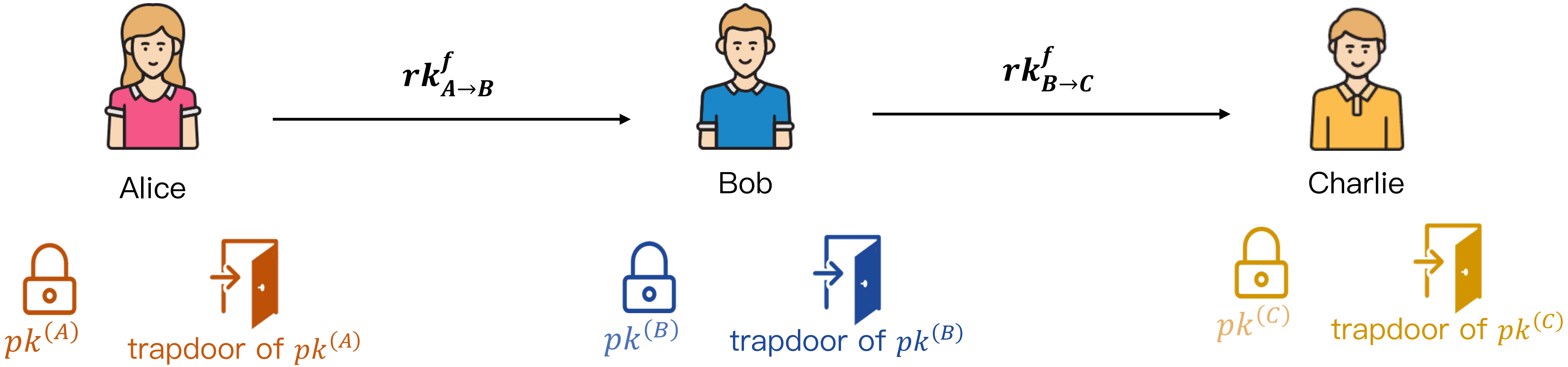
Recap：Single-hop FPRE in [ZLHZ23]

In [ZLHZ23], the public key of each user is consist of **two parts**. The second public key of each user contains a **random part** picked by a **trusted party**, this **is necessary to** the proof of their adaptive security!



To Achieve Multi-Hop FPRE

Multi-Hop FPRE implicitly requires that **the ciphertexts of all levels should be similar** (since one ciphertext can be re-encrypted multiple times !)



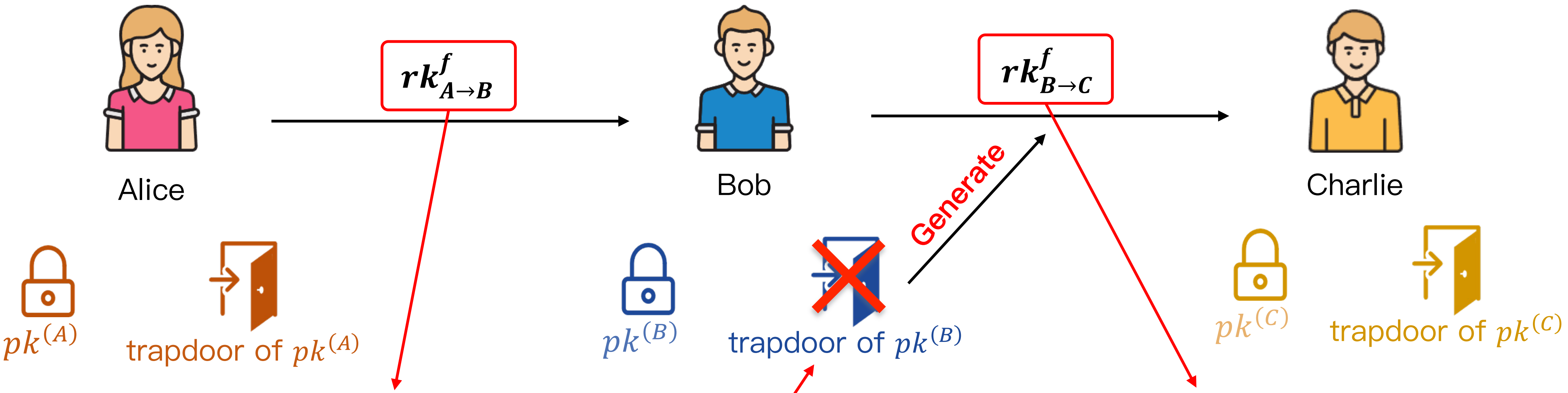
In our multi-hop FPRE scheme, each user only has **one pair** of **public/secret key**.

And the trusted party is **not required** anymore.

Troubles in proving Adaptive Security

However, we note that:

One level ciphertext is hard to achieve **adaptive security.**

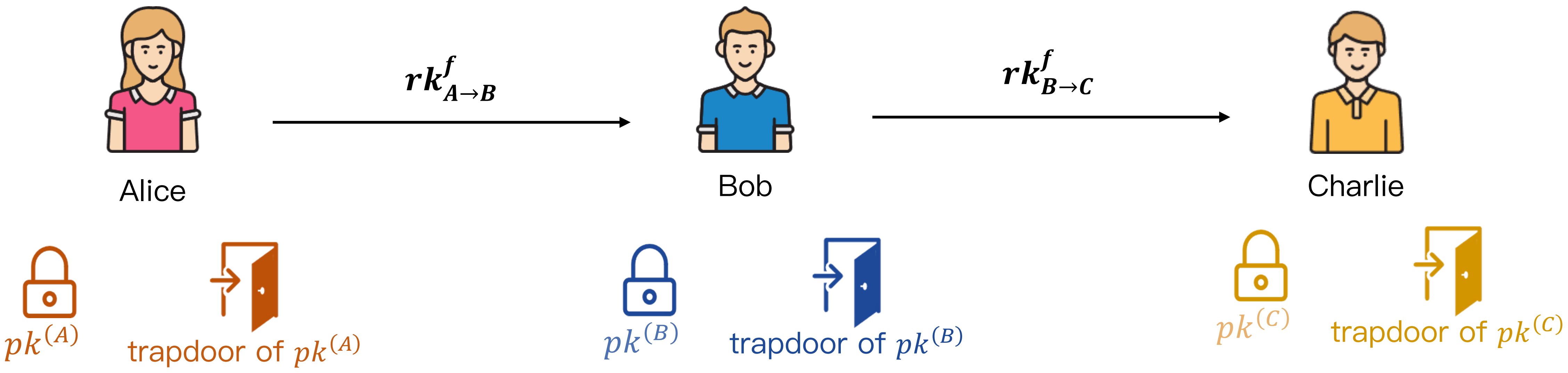


To simulate rekey, we will embed **LWE problem** on $pk^{(B)}$, and this causes that the **trapdoor is unknown** to us !

Adversary might then query re-key from **Bob** to **Charlie** and it is hard to reply without the **trapdoor** of **Bob**!

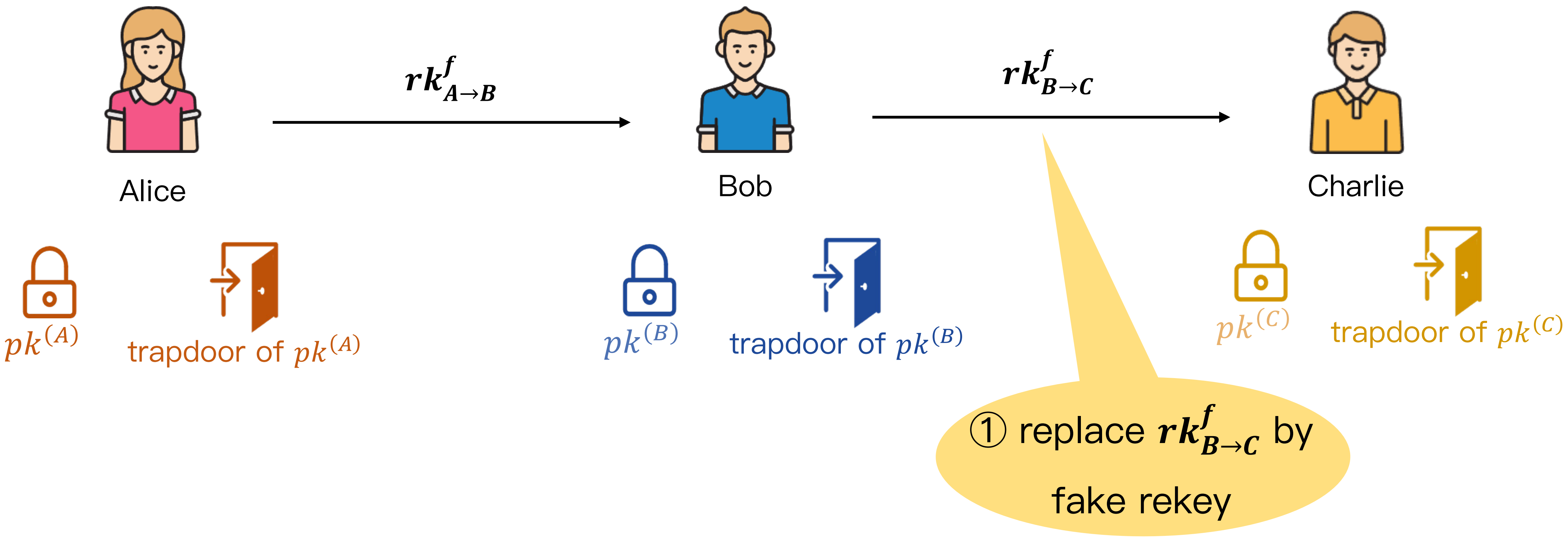
Step 1: Proving Selective Security

In a selective model, we can substitute real rekeys by simulated rekeys from bottom (**users that never generate rekeys**) the top (**challenge user**).



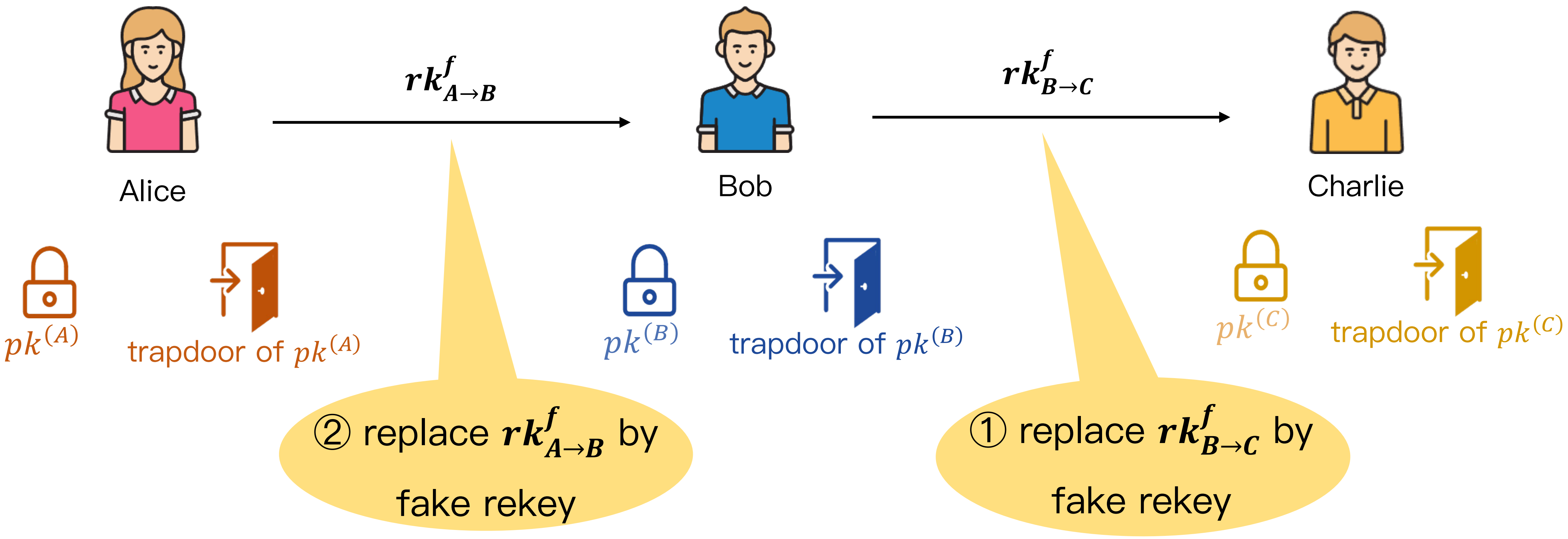
Step 1: Proving Selective Security

In a selective model, we can substitute real rekeys by simulated rekeys from bottom (**users that never generate rekeys**) the top (**challenge user**).



Step 1: Proving Selective Security

In a selective model, we can substitute real rekeys by simulated rekeys from bottom (**users that never generate rekeys**) the top (**challenge user**).



Note that after ①, trapdoor of $pk^{(B)}$ is **not needed** and thus ② is OK.

Step 2: Selective security to Adaptive security

- [JKKKPW17, C] introduces a framework that raises **selective security to adaptive security** when the security reduction is like a pebbling game.

- [FKKP19, PKC] first introduces this framework to **(standard) PRE** scheme and deeply discussed the **adaptive security** of PRE.

- We extend the framework of [JKKKPW17, C] and the techniques of [FKKP19, PKC] to **multi-hop FPRE setting**.

Extending IND and wKP to mFPRE

[FKKP19, PKC] shows that adaptive **CPA security** is implied by **IND security** and **wKP security**. We first introduces these two notion in FPRE setting.

Indistinguishability (IND)

Enc($pk^{(i)}, m_0, v$) $\approx$ Enc($pk^{(i)}, m_1, v$)

IND security considers the **indistinguishability** of ciphertexts at all levels **without** providing **any rekey or re-encryption oracle.**

Weakly Key-Privacy (wKP)

$rk^{f}_{A\to B}$ $\approx$ $\widetilde{rk^{f}_{A\to B}}$

Real rekey — **Simulated rekey**

wKP security considers the **indistinguishability** of rekey pairs **without** providing **any secret keys of associated users.**

IND security of our construction

The basic PKE scheme of our construction is Dual Regev encryption [Regev05, STOC].

The public key of user i is set as a **matrix** $\boldsymbol{A}^{(i)}$ where $\mathbf{A}^{(i)} = \begin{pmatrix} \overline{\mathbf{A}}^{(i)} \\ \underline{\mathbf{A}}^{(i)} \end{pmatrix}$

To encrypt a message $\boldsymbol{m} \in \{0,1\}^{\ell}$, the algorithm works as follows.

$$ct^{(i)} = \boxed{\mathbf{A}^{(i)}\mathbf{s} + \mathbf{e}} + \boxed{\begin{pmatrix} \mathbf{0} \\ \lfloor q/2 \rfloor \mathbf{m} \end{pmatrix}} = \begin{pmatrix} \overline{\mathbf{A}}^{(i)}\mathbf{s} + \mathbf{e}_1 \\ \underline{\mathbf{A}}^{(i)}\mathbf{s} + \mathbf{e}_2 + \lfloor q/2 \rfloor \cdot \mathbf{m} \end{pmatrix}$$

LWE instance

message

Thus the **IND security** comes from the LWE assumption.

wKP security of our construction

The key part of **re-encryption key** of our scheme is a matrix **R** sampled by **pre-image sampling** algorithm [GPV08, STOC] such that

$$\mathbf{R}\overline{\mathbf{A}}^{(i)} = \mathbf{A}^{(j)}\mathbf{S} + \mathbf{E} - \begin{pmatrix} \mathbf{0} \\ \mathbf{M}_1 \end{pmatrix} \underline{\mathbf{A}}^{(i)}$$

LWE instance $\approx$

random

Under the LWE assumption, the **right-side** of the equation is **close to random** and consequently, the pre-image R of a random matrix is close to random!

SH: further to HRA security

HRA security is built from CPA security and **SH security.**

Source Hiding (SH)

Re-encryption →

level $v-1$	level v
$\text{Enc}(pk^{(i)}, m, v-1)$	$\text{FReEnc}(rk^{f}_{i\to j}, ct^{(i)}_{v-1}, v-1)$

ciphertexts with proxy relation

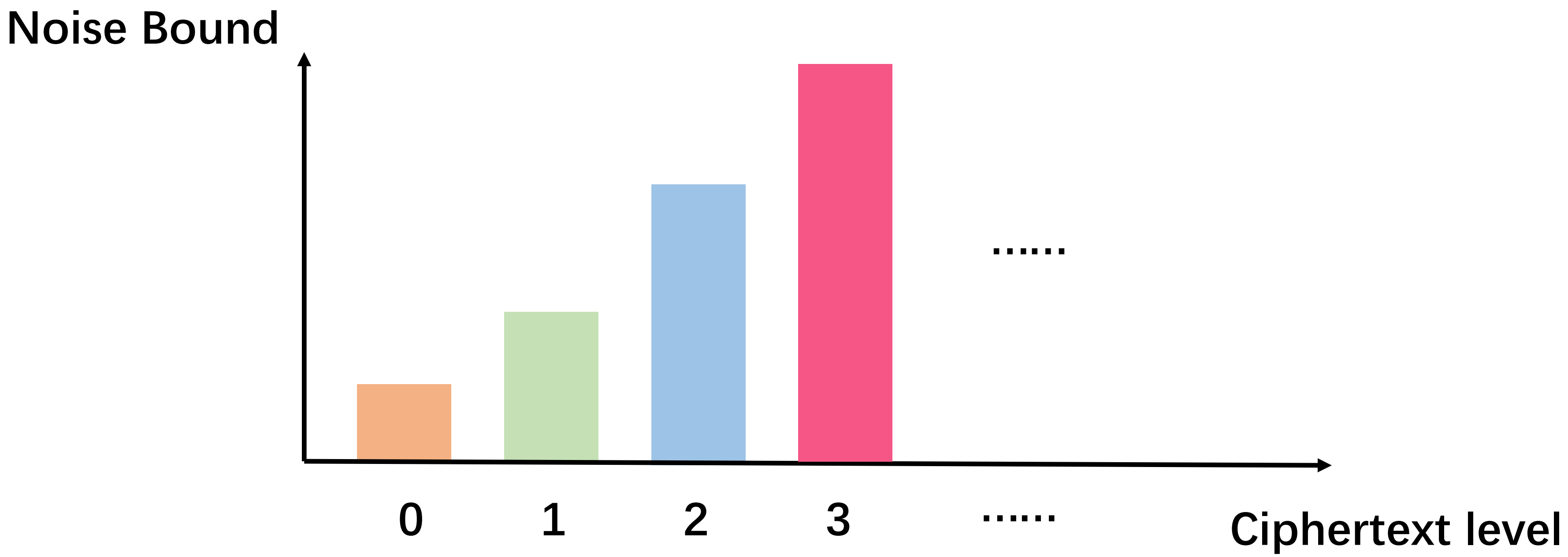
$\approx$

level $v-1$	level v
$\text{Enc}(pk^{(i)}, m, v-1)$	$\text{Enc}(pk^{(j)}, f(m), v)$

ciphertexts generated independently

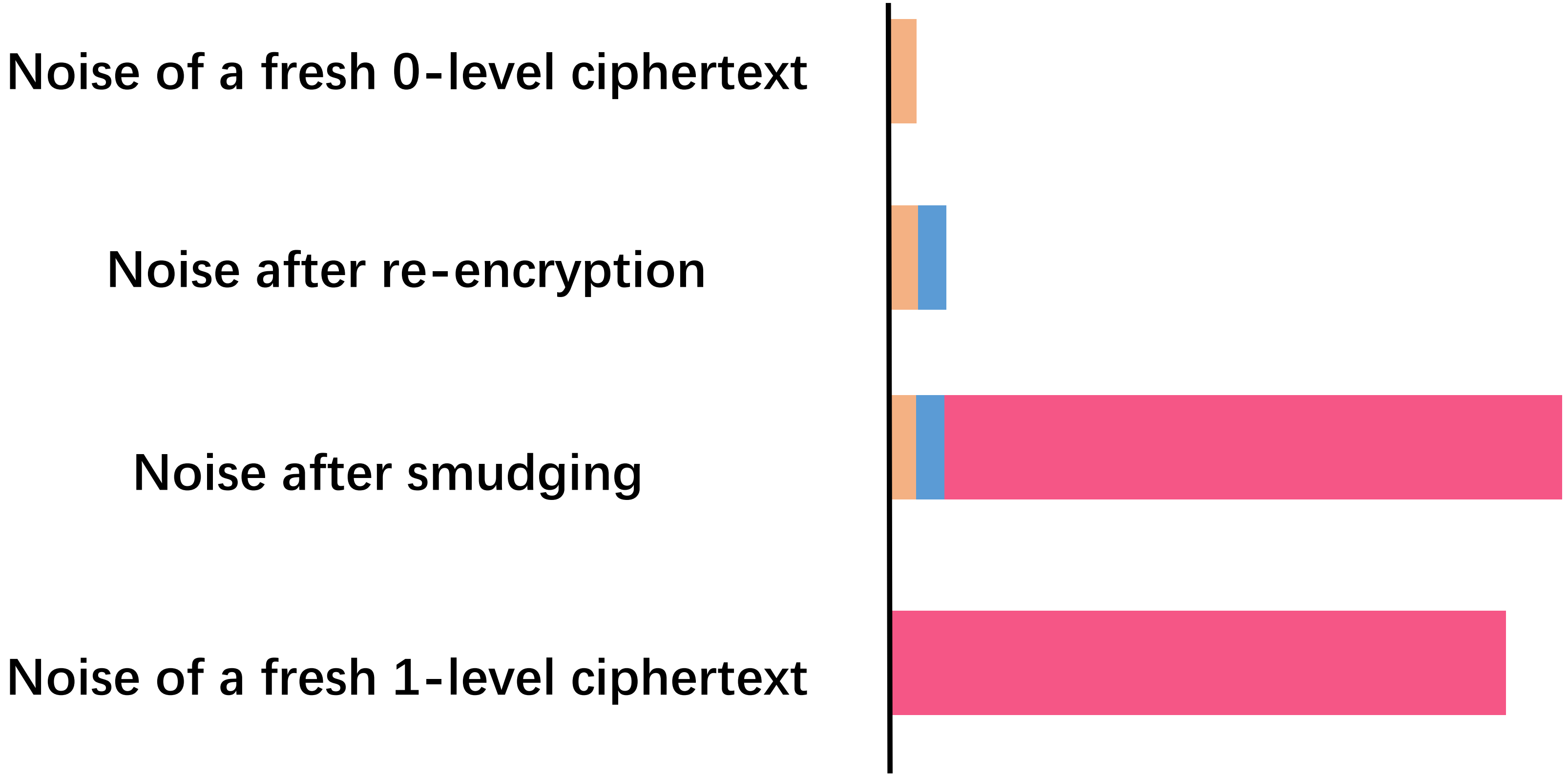
SH security implies that the adversary cannot tell a v–level ciphertext is generated by **re–encryption or encryption**, even the adversary obtains the rekey from user i to user j.

SH security of our construction



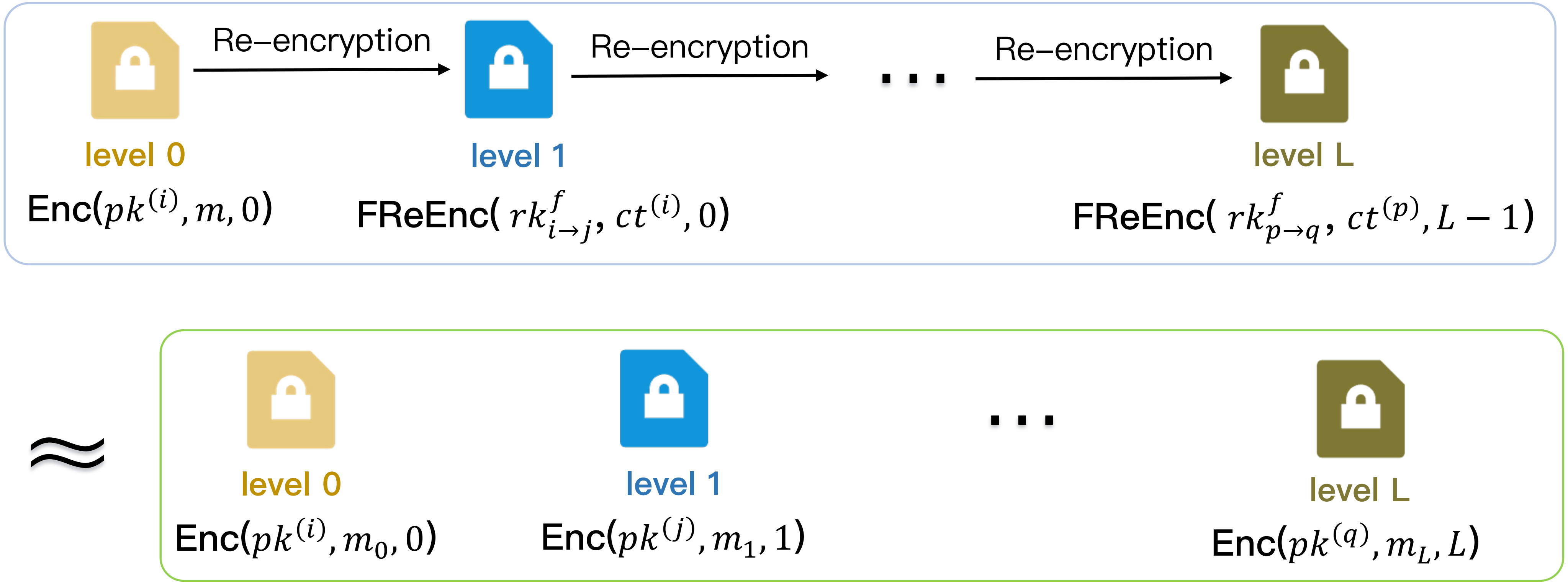
To achieve SH security, we set **noise bounds of different sizes for different levels of ciphertexts.**

SH security of our construction



After the transformation of public key, we uses a fresh ciphertext of **zero** at the **next level** to smudge the noise of the ciphertext, enabling the re-encrypted ciphertext is **statistically close to a fresh ciphertext at the next level.**

CUL Security for multi-hop FPRE

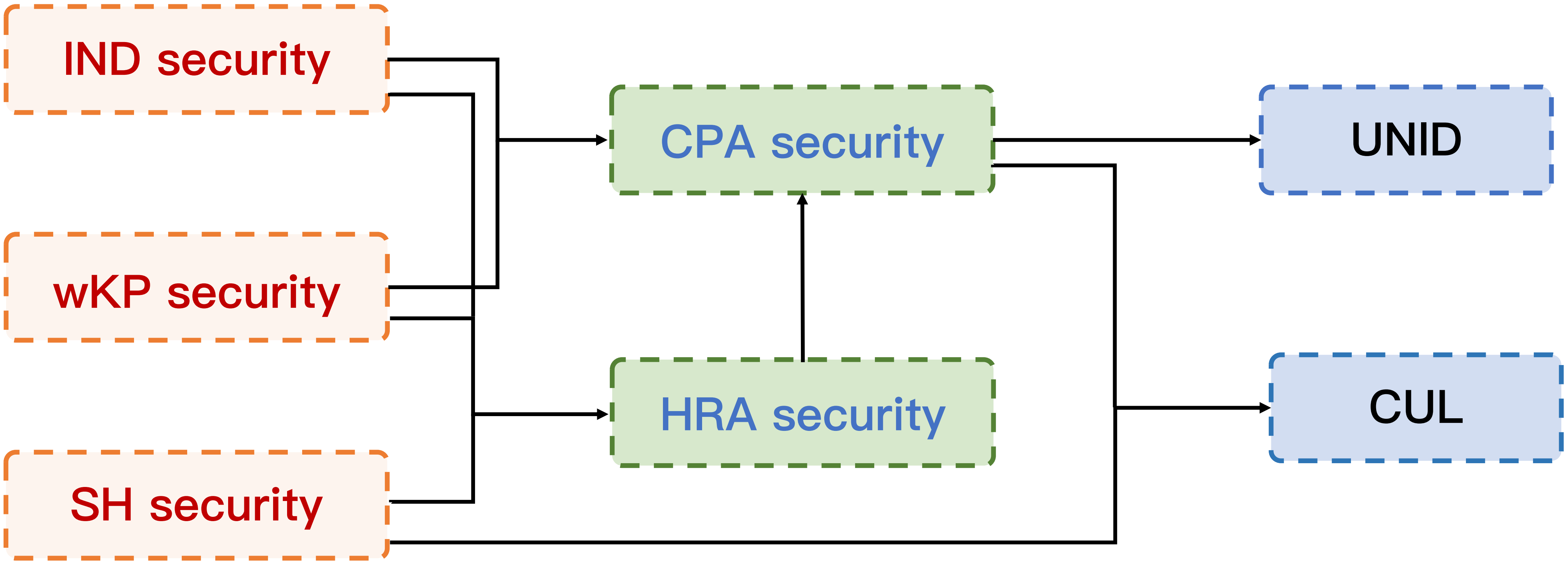


ciphertexts with proxy relation

ciphertexts generated independently

Ciphertext UnLinkability **(CUL)** is a security property that protects the **underlying proxy relationship.** We extends this property to multi-hop FPRE setting.

mFPRE: Security Relations



We formalize all above security properties (**IND, wKP, SH, CPA, HRA, UNID,CUL**) in multi-hop FPRE settings and establish **relations** among them by reduction.

Contents

Multi-hop FPRE Scheme: Comparison

Comparison of **multi-hop unidirectional** PRE schemes.

Scheme	Standard Model ?	Adaptive corruption?	Security	UNID	CUL	Assumption	Post Quantum?	Fine-Grained?	Maximum -hops
FL19	√	×	tbCCA	√	-	LWE	√	×	poly-log
LHAM20	√	×	CCA	√	-	iO	×	×	-
MPW23	√	×	HRA	√	-	DDH	×	×	unbound*
FKKP19+ CCLNX14	√	√	HRA	√	√	LWE	√	×	sub-linear
FKKP19+ Gen09	√	√	HRA	√	√	LWE over ideal lattice + circular security	√	×	-
Our Con 1	√	√	CPA	√	-	LWE	√	√	sub-linear
Our Con 2	√	√	HRA	√	√	LWE	√	√	sub-linear

Contribution

- **Formal Definitions for Multi-Hop Fine-Grained PRE and Its Securities.**
  - Formalize the security properties like CPA, HRA, IND, wKP, SH, UNID, CUL for multi-hop FPRE and show relations among them.
- **Generic Framework for Achieving CPA and HRA Security for Multi-Hop FPRE.**
- **Construction of Multi-Hop FPRE from LWE.**
  - ✓ **with adaptive HRA security and all above**

Thanks!   Questions?

ePrint: ia.cr/2024/055