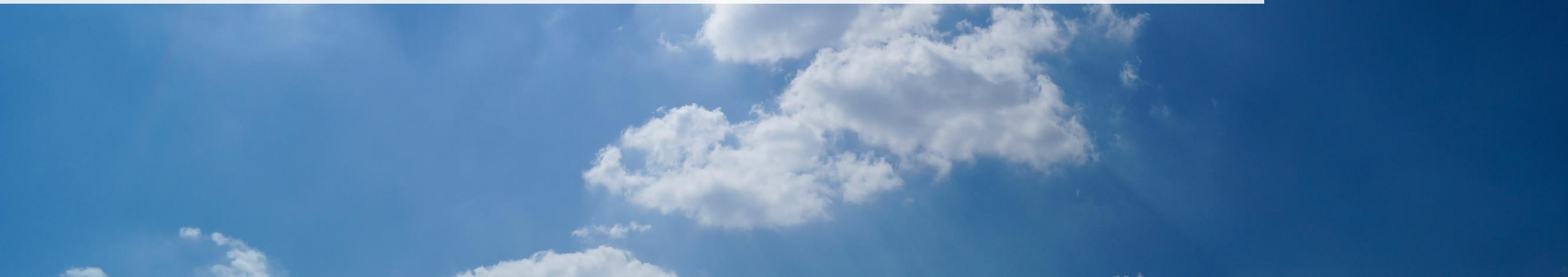
Unique-Path Identity Based Encryption With Applications to Strongly Secure Messaging



Eurocrypt 2023

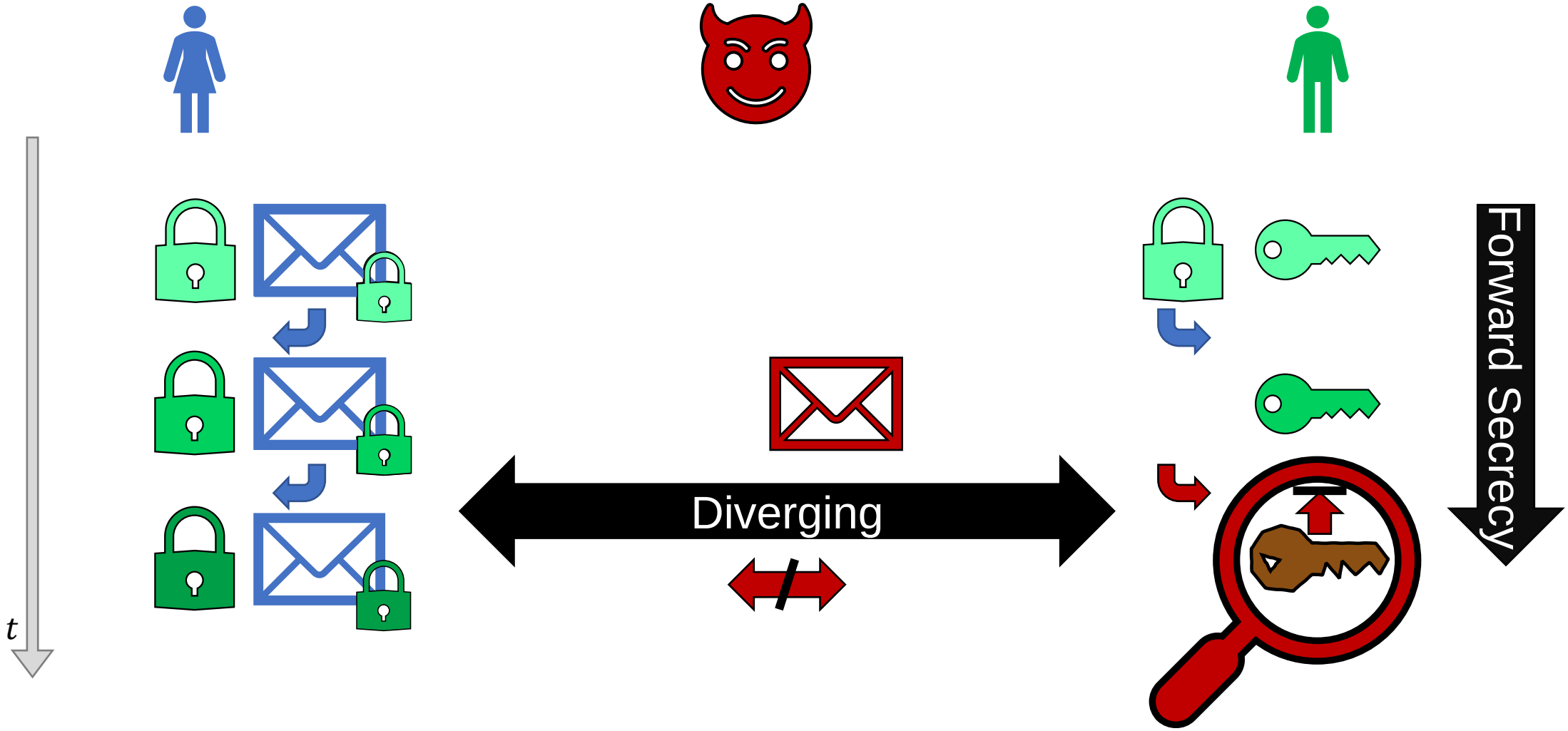
February 23

Real-World Cryptography Group
FAU Erlangen-Nürnberg, Germany

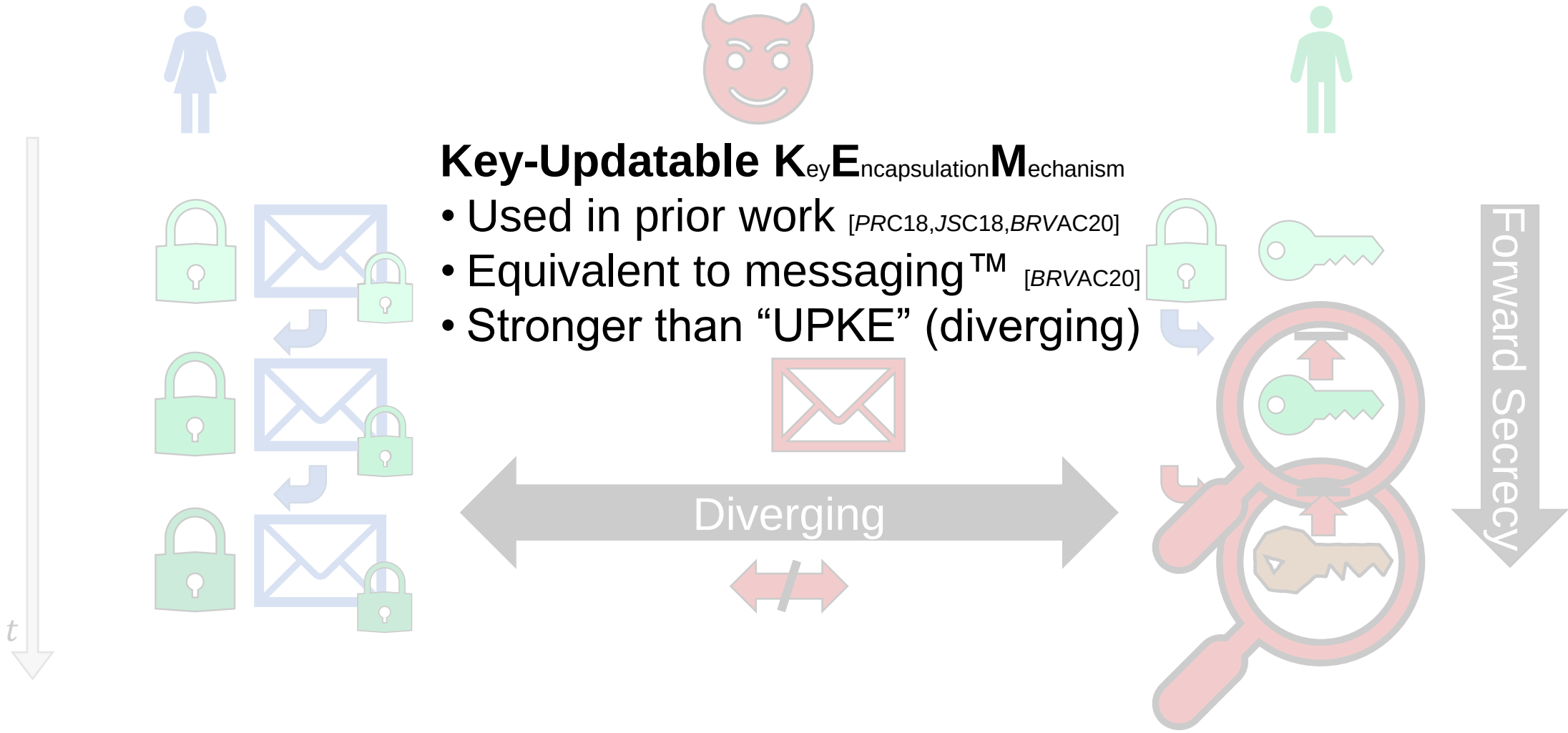
AIT Austrian Institute of Technology, Austria

Paul Rösler, Daniel Slamanig, Christoph Striecks

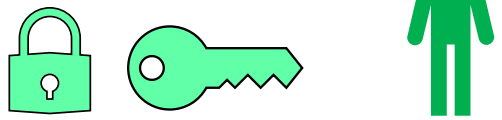
Messaging with Key Updates



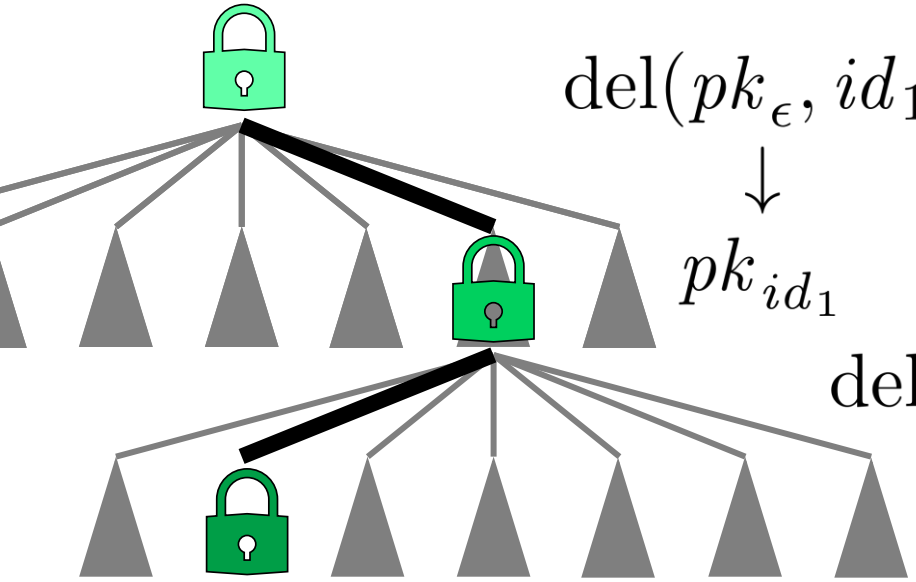
Messaging with Key Updates



KU-KEM from Unique-Path IBE



$(pk_\epsilon, sk_\epsilon) \leftarrow \text{gen}$



$\text{del}(pk_\epsilon, id_1)$

$\downarrow$

pk_{id_1}

$\text{del}(pk_{id_1}, id_2)$

$\downarrow$

$pk_{id_1 \| id_2}$

$\text{enc}(pk_{id_1 \| id_2}) \rightarrow (k, c)$

$\text{del}(sk_\epsilon, id_1)$

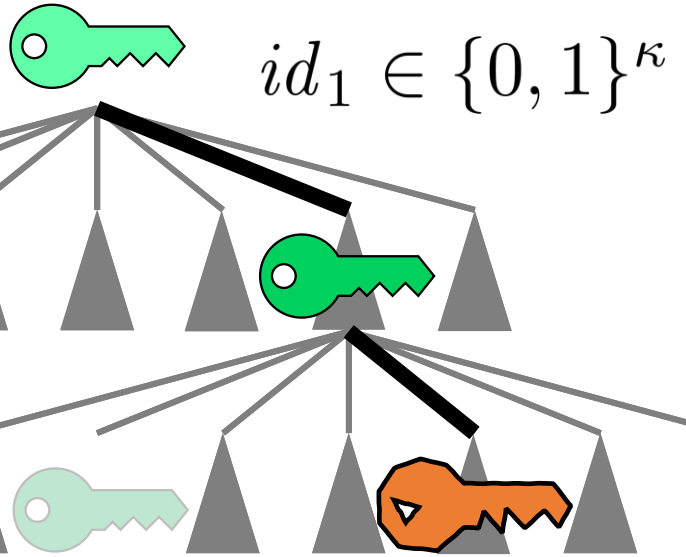
$\downarrow$

sk_{id_1}

$\text{del}(sk_{id_1}, \boldsymbol{id'})$

$\downarrow$

$sk_{id_1 \| \boldsymbol{id'}}$



$id_1 \in \{0,1\}^\kappa$

$\text{dec}(sk_{id_1 \| \boldsymbol{id'}}, c) \rightarrow$ 

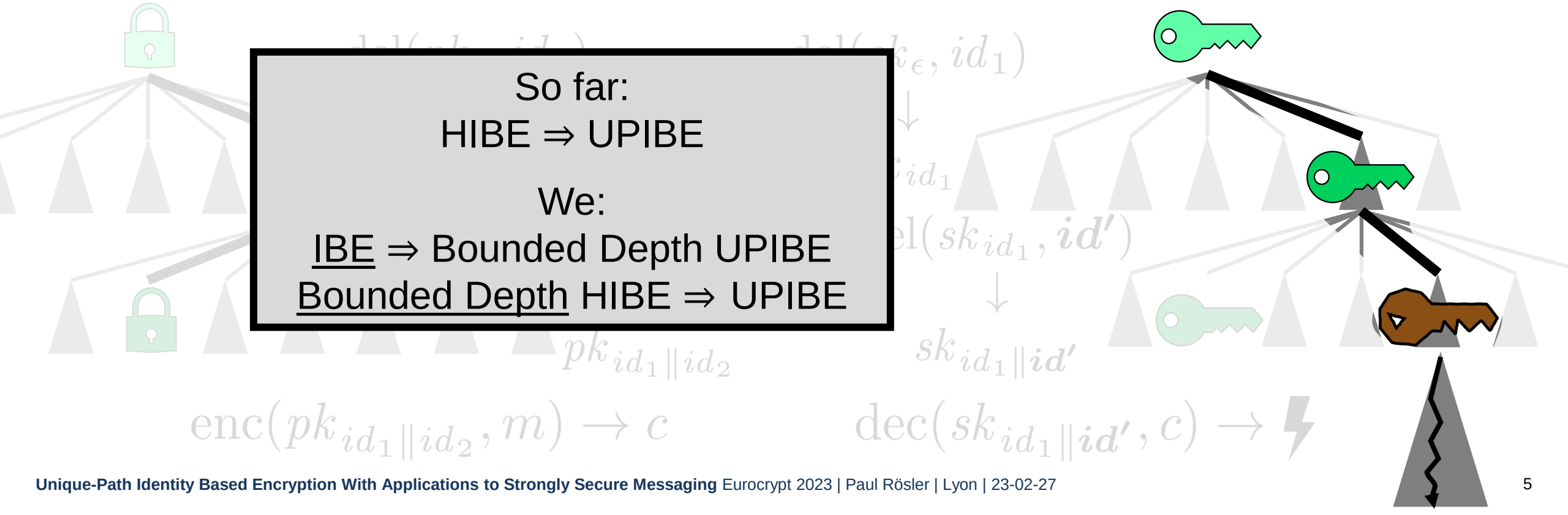
KU-KEM from Unique-Path IBE

Unique-Path Identity**B**ased**E**ncapsulation

- The same as **Hierarchical IBE**
- Only one delegation per secret key
  → *Unique* secret-key *path*

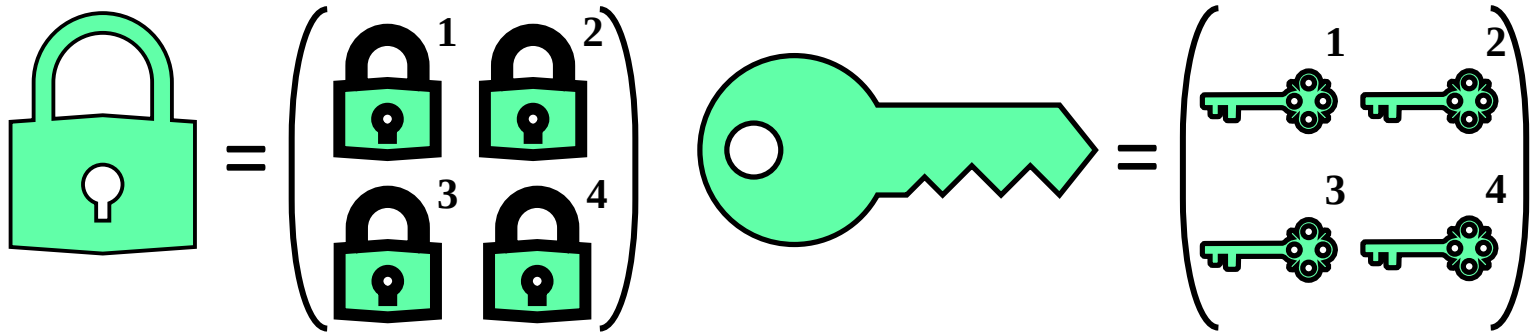
So far:
HIBE ⇒ UPIBE

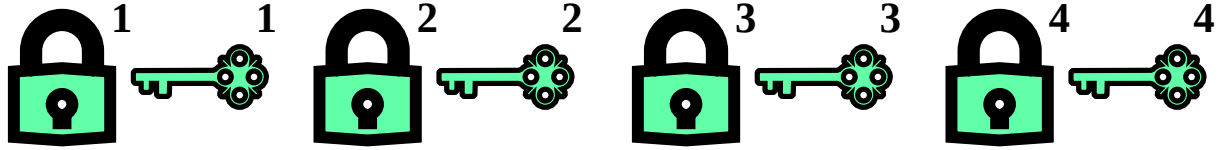
We:
IBE ⇒ Bounded Depth UPIBE
Bounded Depth HIBE ⇒ UPIBE



Building UPIBE: Bounded Depth q

$$(pk_\epsilon, sk_\epsilon) \leftarrow \mathrm{gen}_{\mathrm{UI}}$$

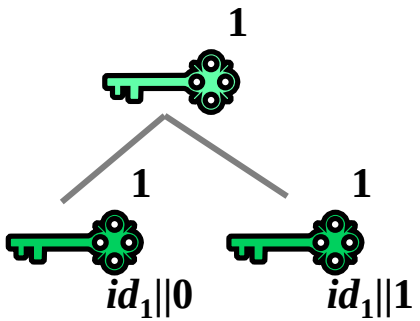


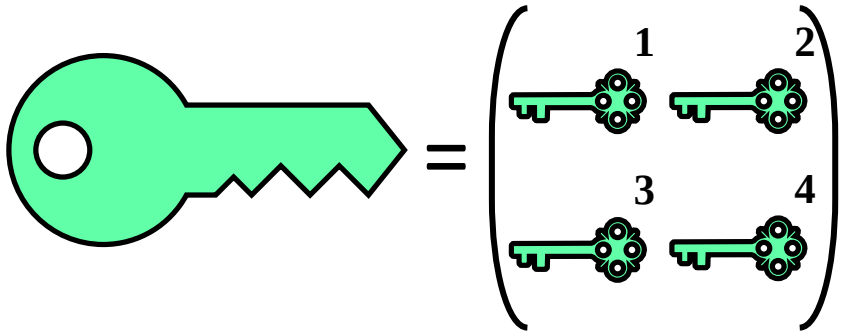


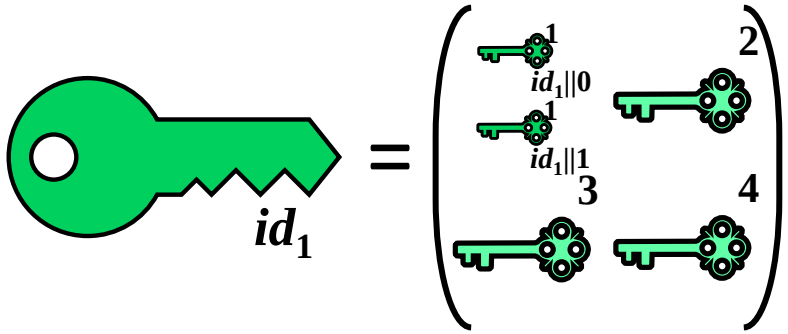
1 IBE Key Pair
per UPIBE depth

Building UPIBE: Bounded Depth q

$$sk_{id||id^*} \leftarrow \mathrm{del}_{\mathrm{UI}}(sk_{id}, id^*)$$

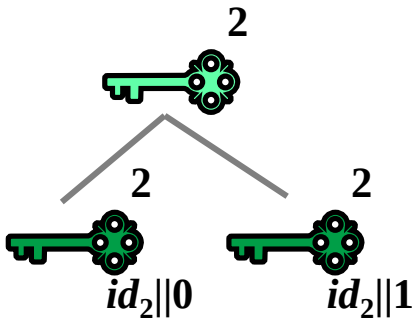


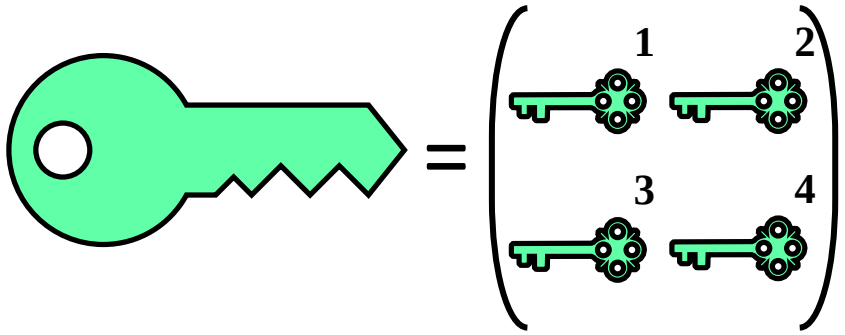


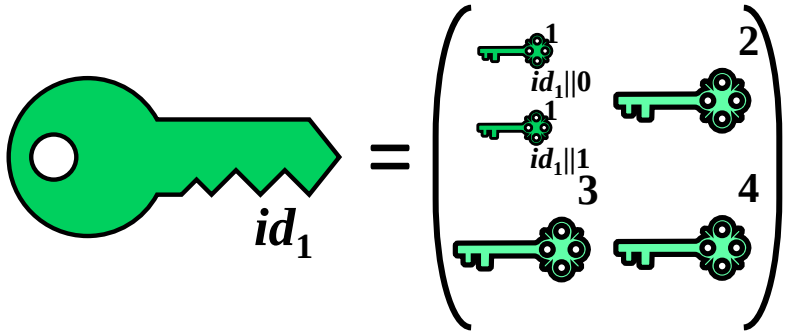


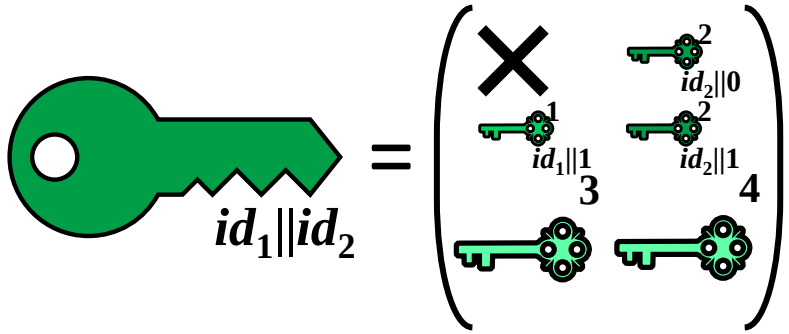
Building UPIBE: Bounded Depth q

$$sk_{id||id^*} \leftarrow \mathrm{del}_{\mathrm{UI}}(sk_{id}, id^*)$$



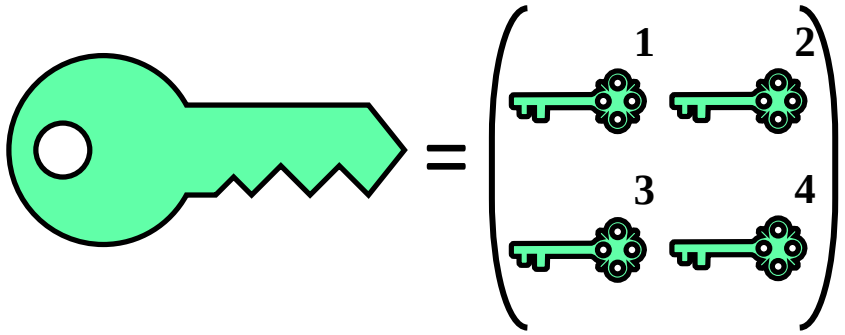


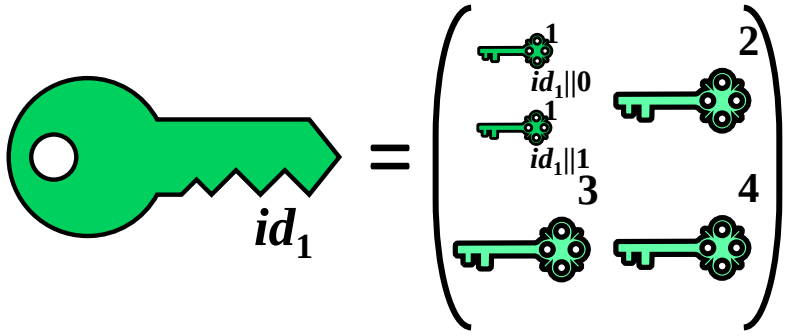


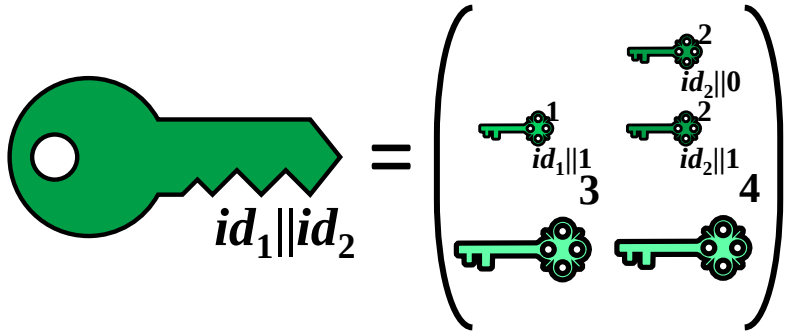


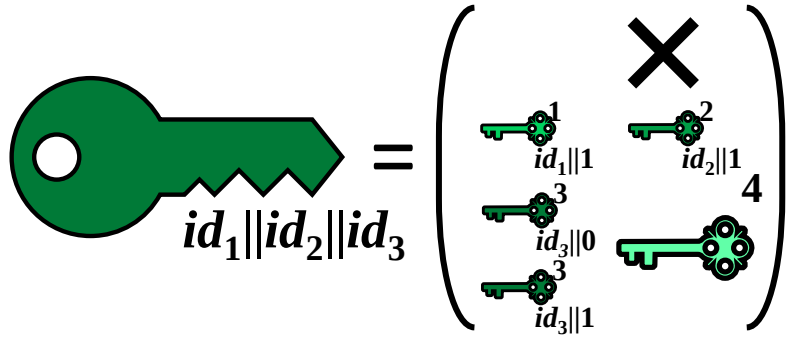
Building UPIBE: Bounded Depth q

$$sk_{id||id^*} \leftarrow \mathrm{del}_{\mathrm{UI}}(sk_{id}, id^*)$$



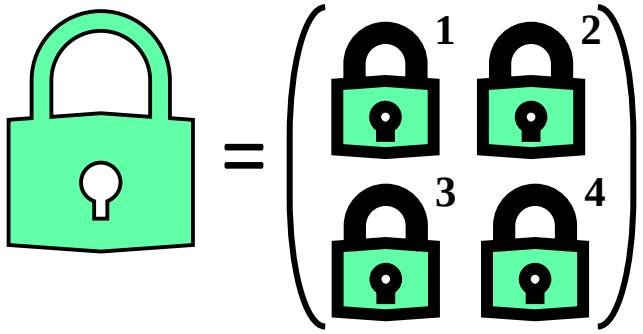




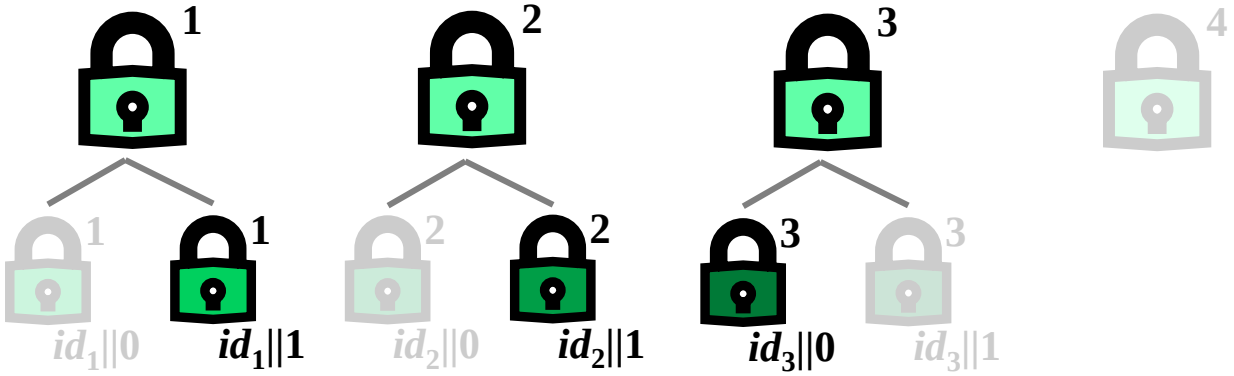


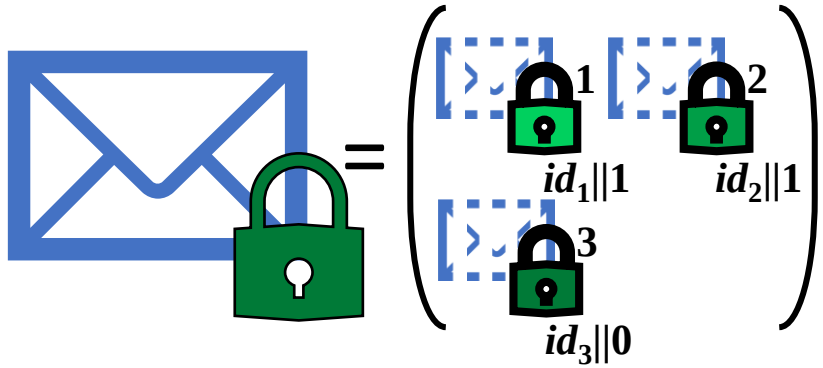
Building UPIBE: Bounded Depth q

$$(k, c) \leftarrow \mathrm{enc}_{\mathrm{UI}}(pk, id_1 \| .. \| id_l)$$



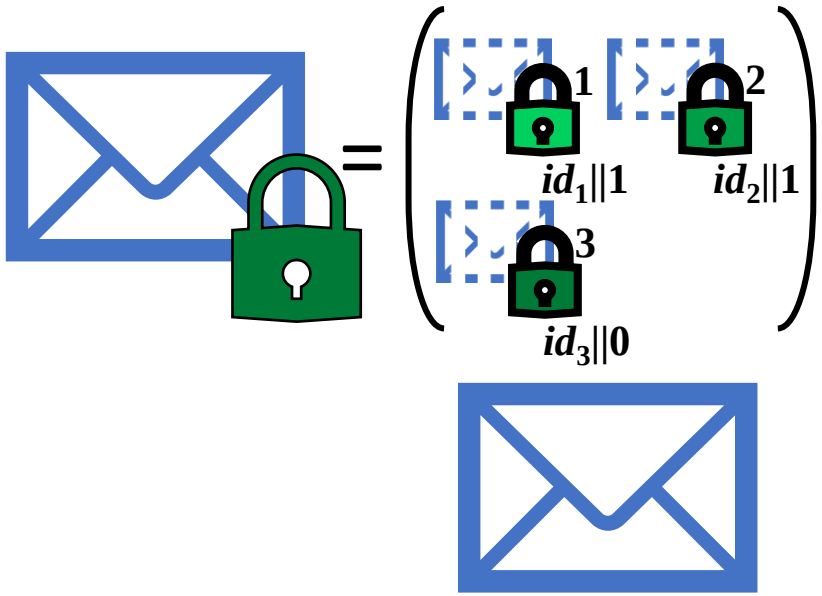
$$id = id_1 \| id_2 \| id_3$$

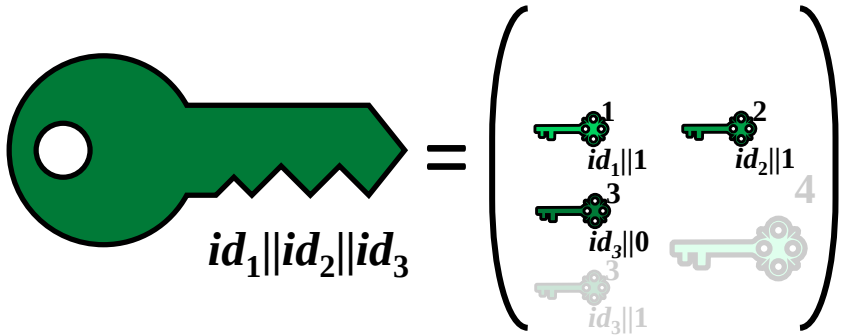




Building UPIBE: Bounded Depth q

$$k \leftarrow \mathrm{dec}_{\mathrm{UI}}(sk, c)$$

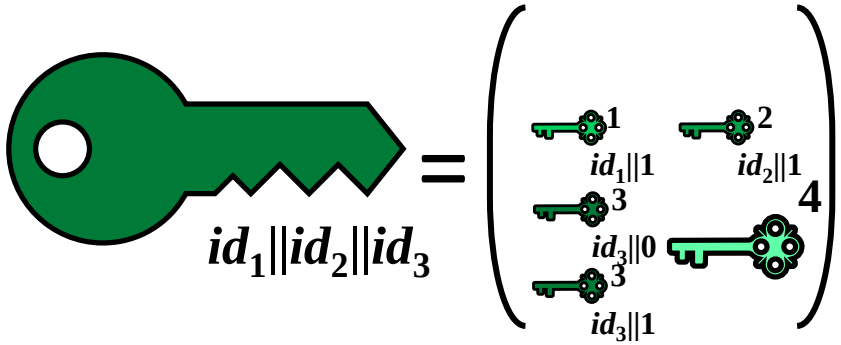


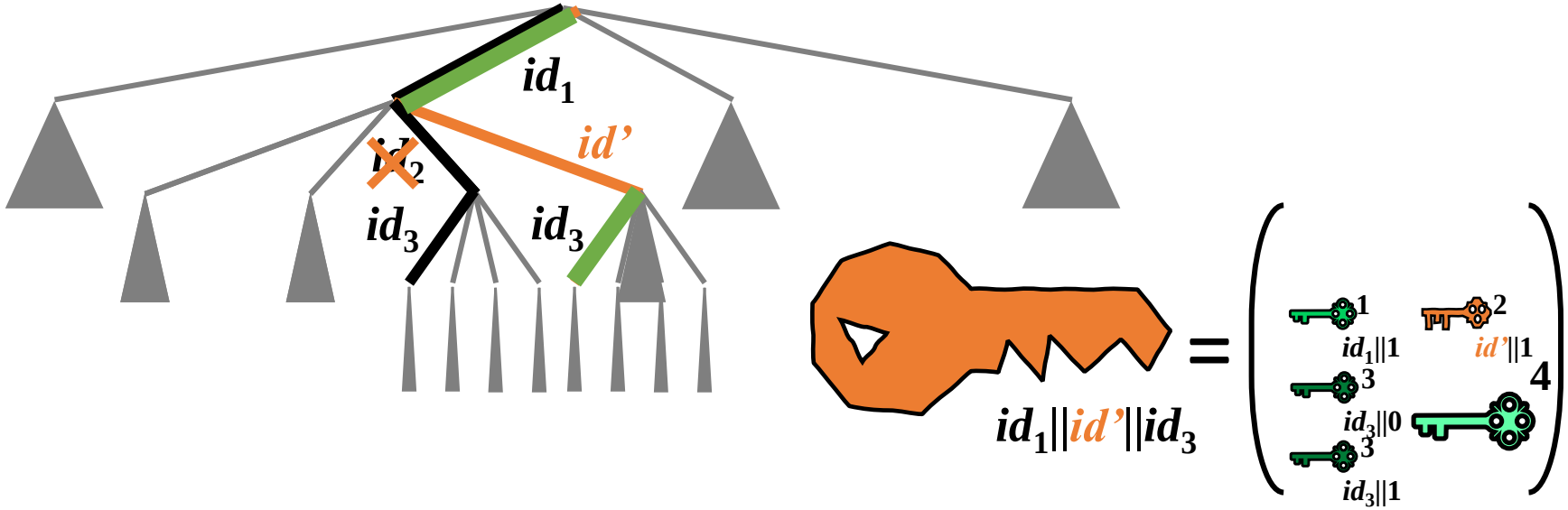


Building UPIBE: Bounded Depth q

Why 1 IBE instance per depth?

→ No Compilation





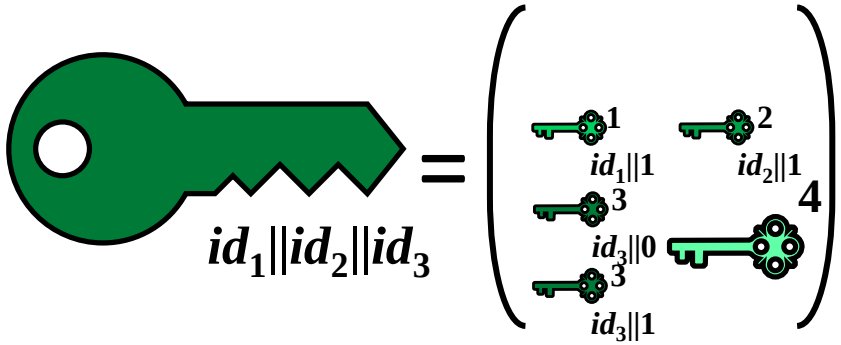
Building UPIBE: Bounded Depth q

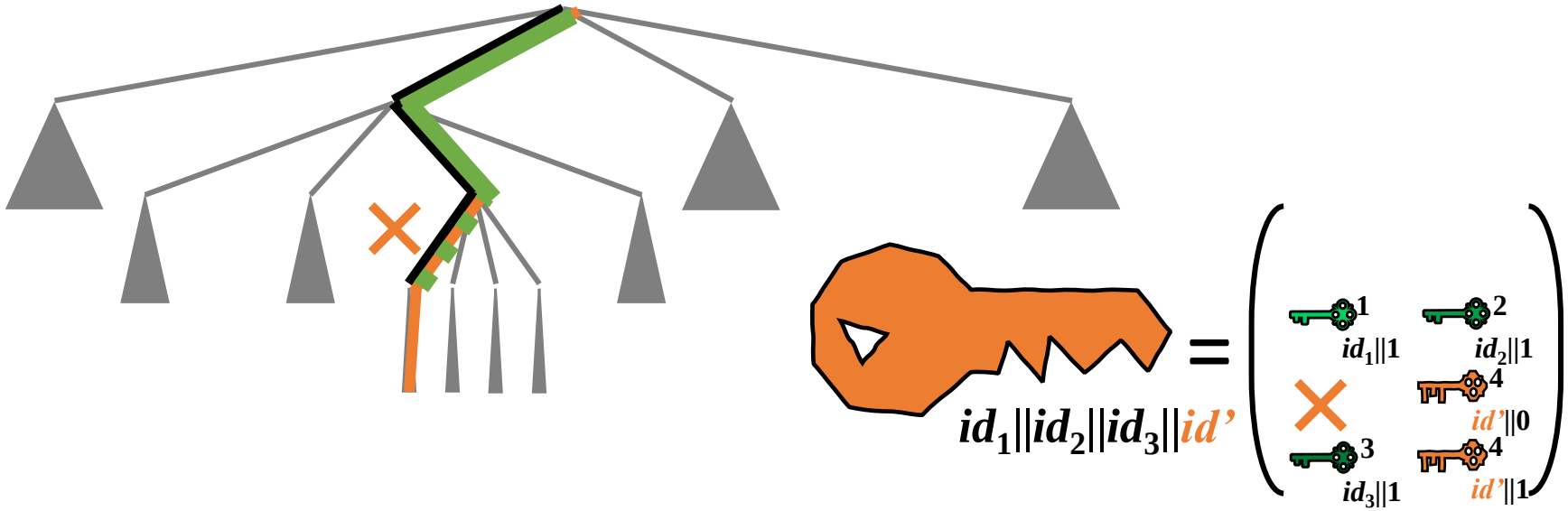
Why 1 IBE instance per depth?

→ No Compilation

Why 2 delegations per instance?

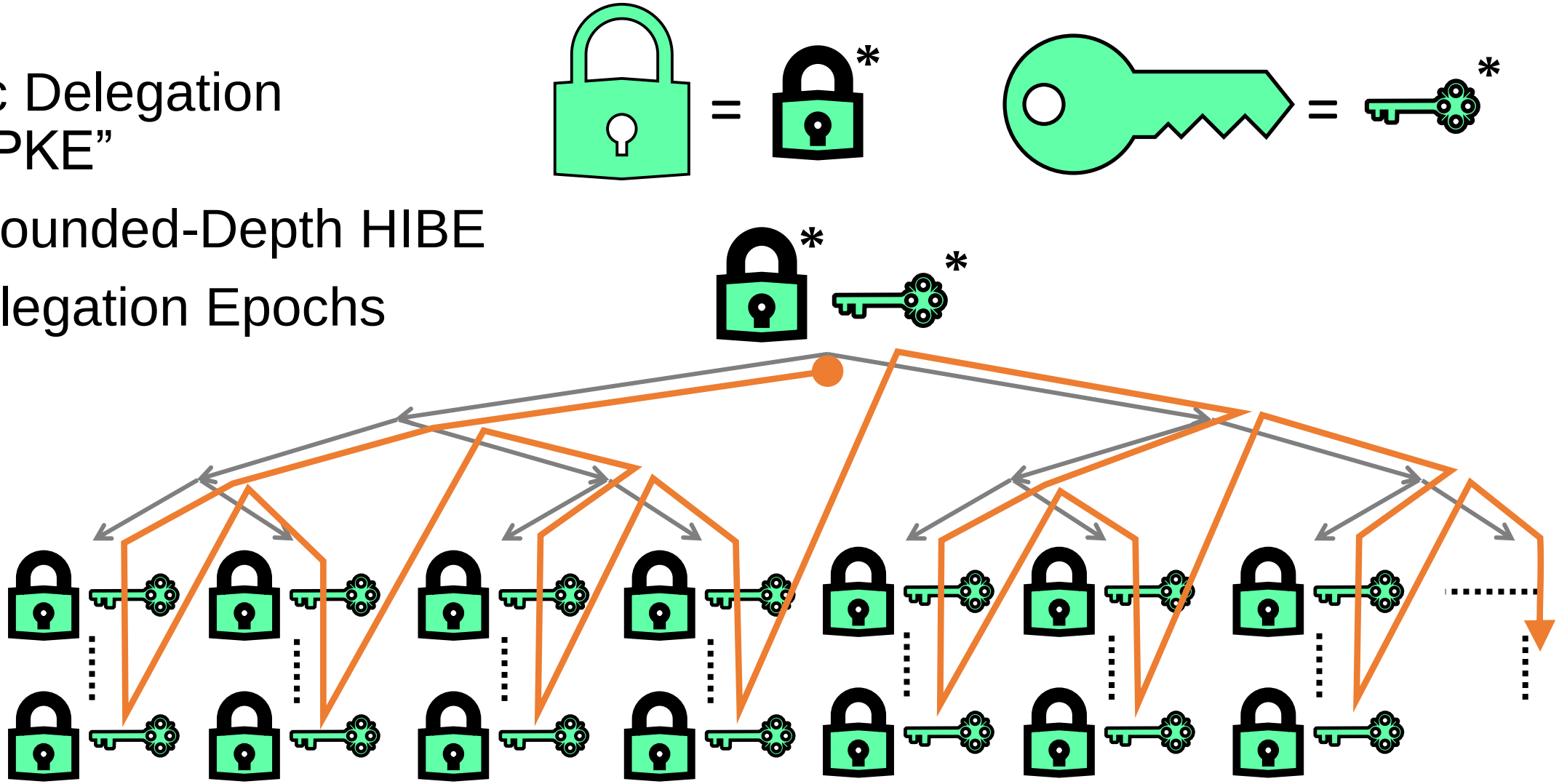
→ No Prefix





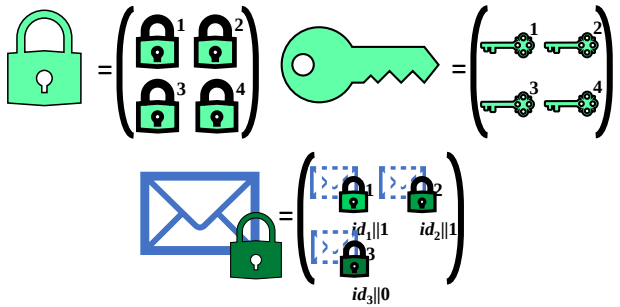
Building UPIBE: **Un**bounded Depth

- Dynamic Delegation via “FS-PKE”
- Single Bounded-Depth HIBE
- Multi-Delegation Epochs



Summary & Outlook

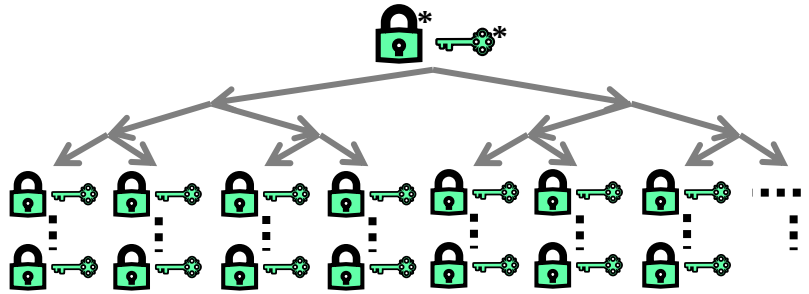
Bounded Depth UPIBE



- From 2-Bounded Collusion IBE
- From DDH: $|sk| = |c| = \mathcal{O}(1)$

$$|pk| = \mathcal{O}(q)$$

Unbounded Depth UPIBE



- From κ-Bounded Depth HIBE
- Using ROM from Selective

→ Exploit Structure to Aggregate?

ia.cr/2023/248