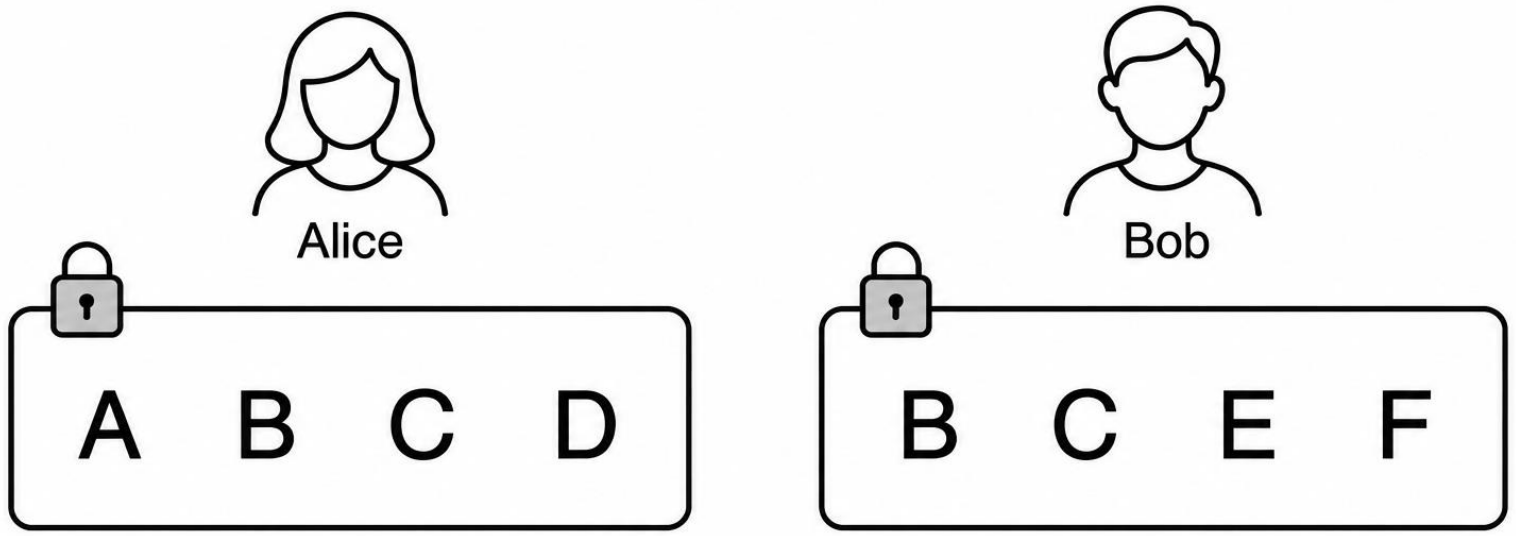
Post-Quantum
Private Set Intersection for Small Sets

Junxin Liu, Oregon State University

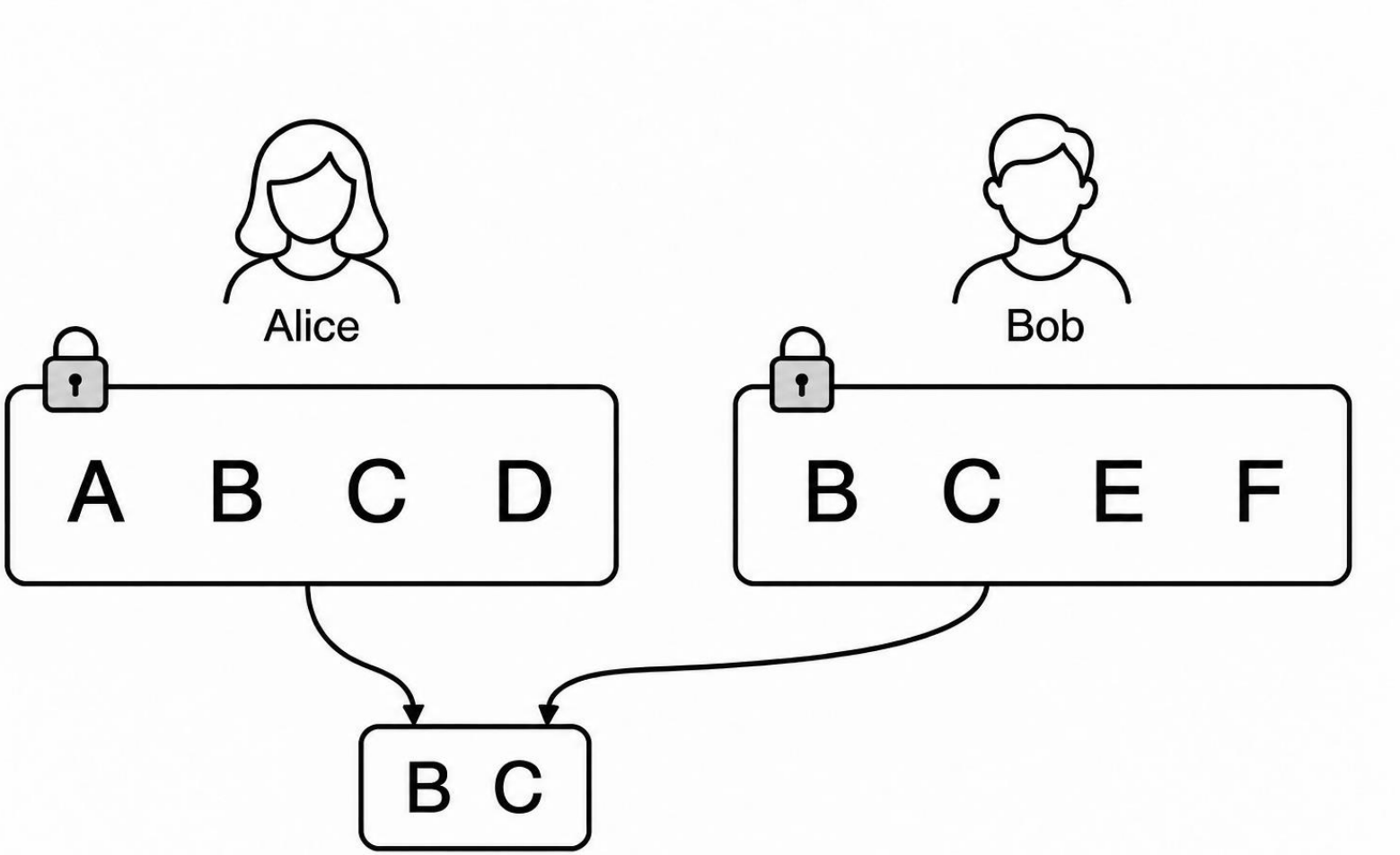
Joint Work with: Mike Rosulek(OSU), Ni Trieu(ASU)

NIST WPEC, Oct 2026

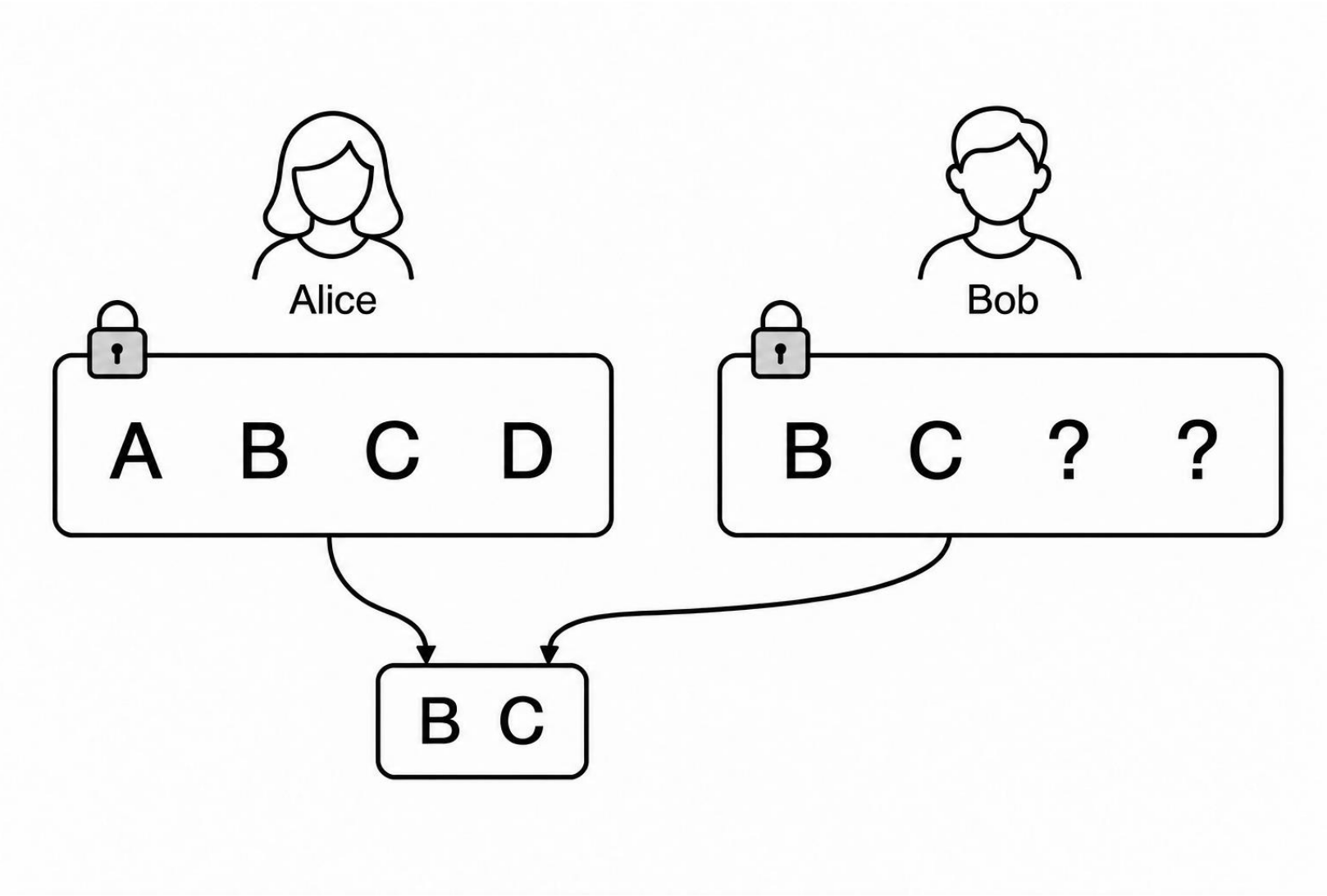
What is **Private Set Intersection** (**PSI**)



What is **Private Set Intersection** (**PSI**)



What is **Private Set Intersection** (**PSI**)



PSI Example: Private device enrollment (ChromeOS)



Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Protecting your device information with Private Set Membership

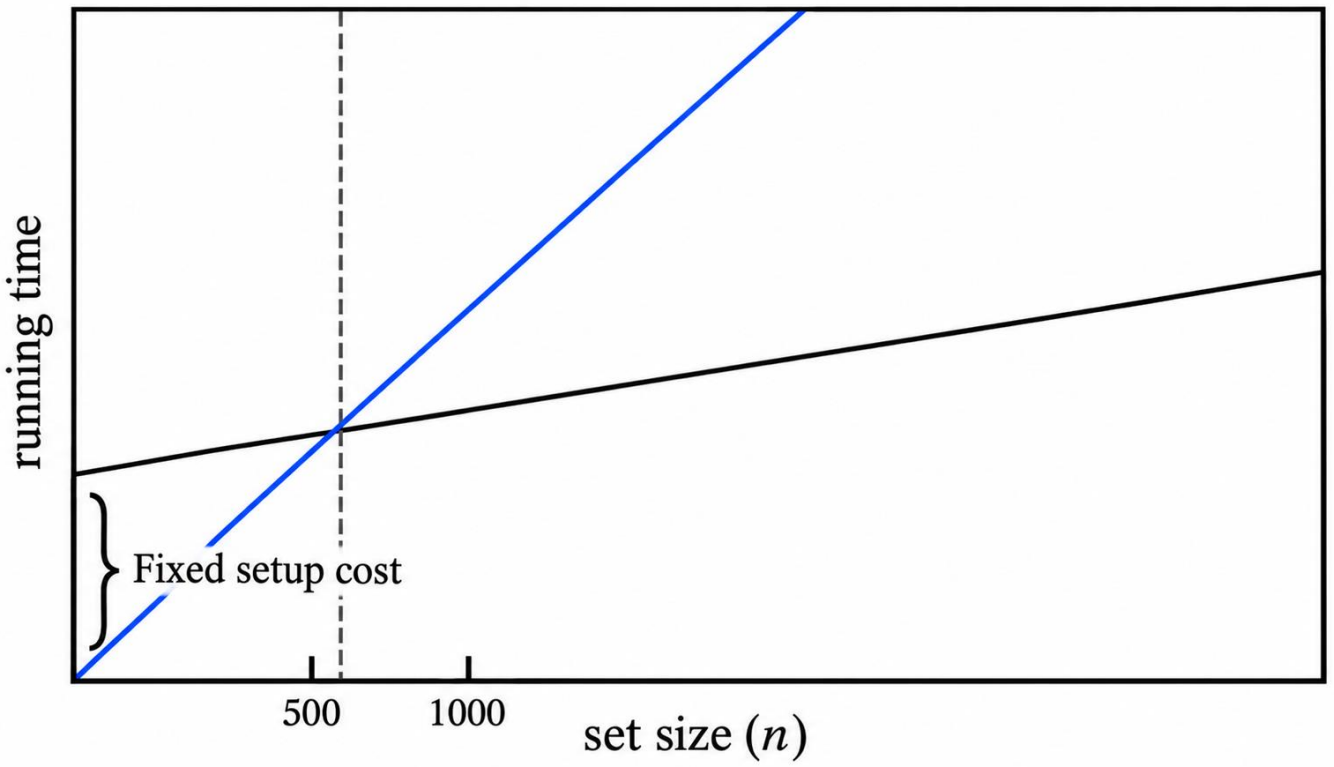
October 28, 2021

Posted by Kevin Yeo and Sarvar Patel, Private Computing Team

$$\underbrace{\{\text{device ID}\}}_{\text{Chromebook}} \cap \underbrace{\{\text{enterprise-enrolled device IDs}\}}_{\text{Google}}$$

KA vs. OT-based PSI

(Key Agreement) (Oblivious Transfer)



KA-based

- $O(n)$ KEM pub-key ops

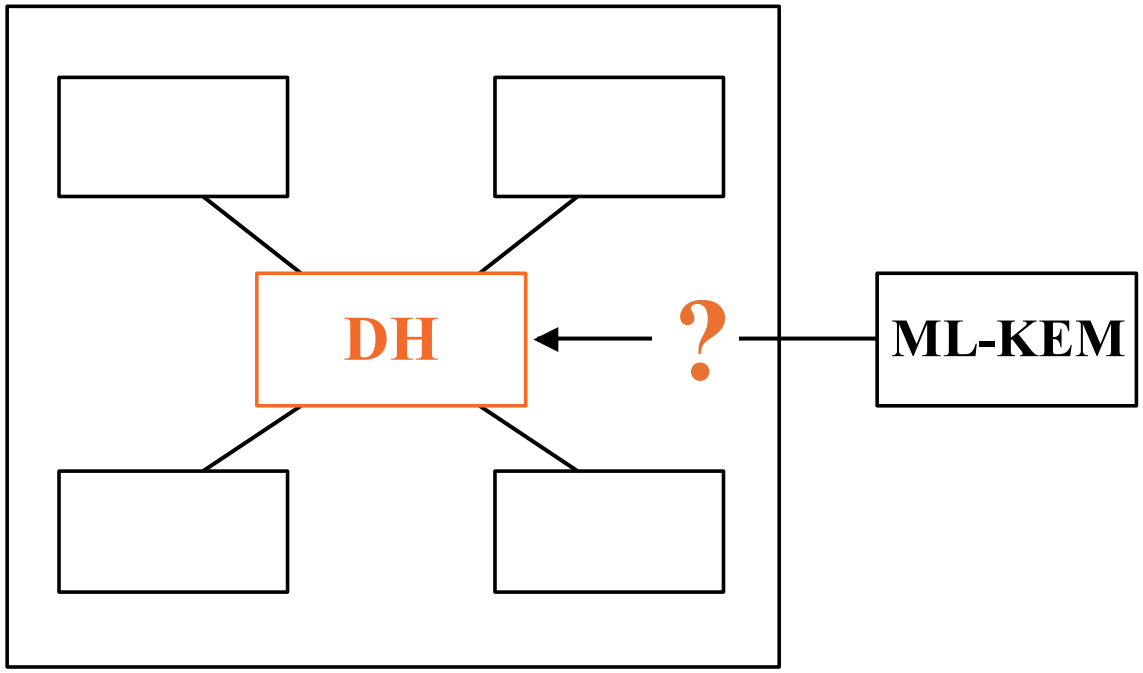
OT-based

- Fixed number of OTs setup
- $O(n)$ symm-key ops

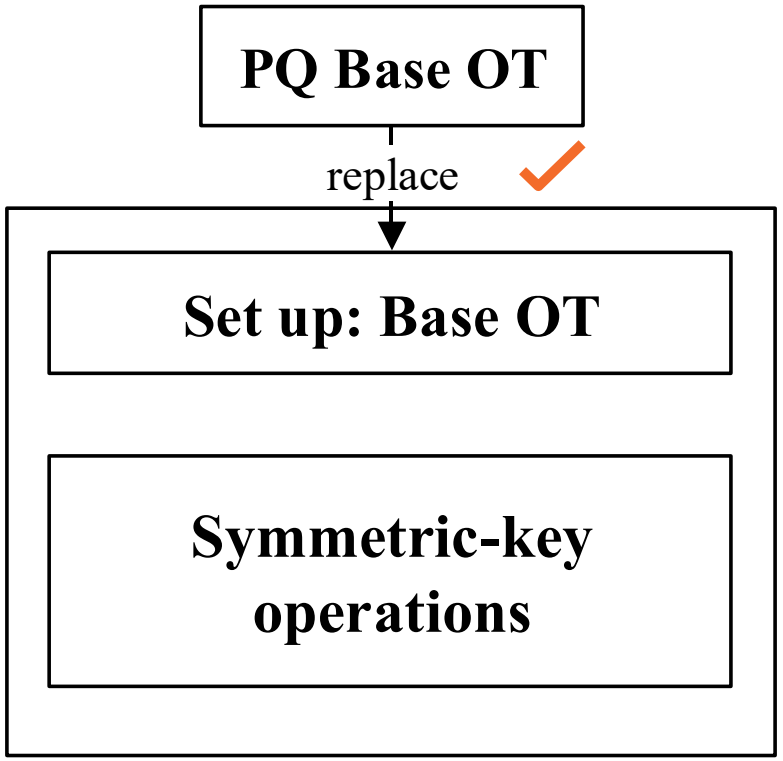
Are PSI protocols ready for the post-quantum future?

In the Post-Quantum future

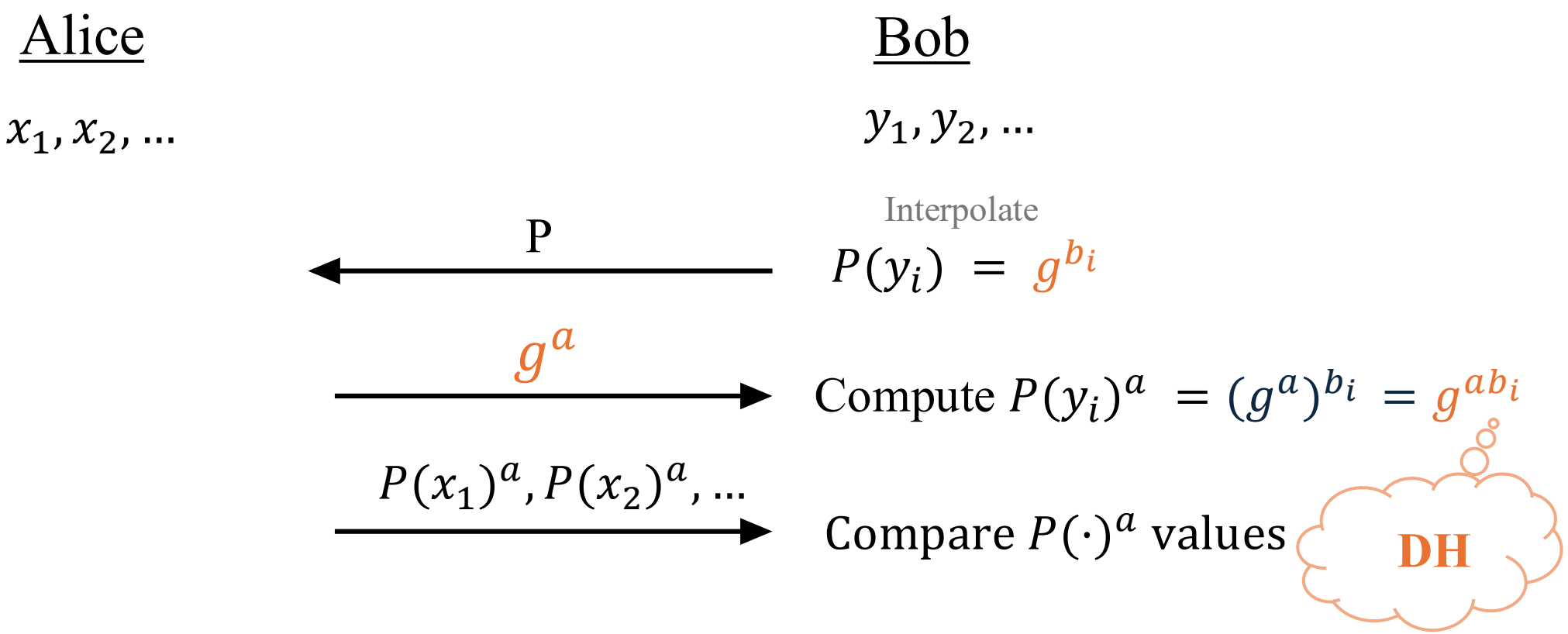
KA-based



OT-based



State of the Art KA-based PSI: [RT21]



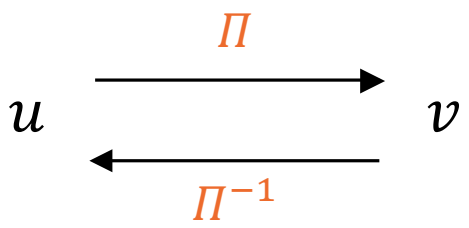
Match: $x_j = y_i \implies P(x_j)^a = (g^a)^{b_i}$

No match: $x_j \notin Y \implies P(x_j)^a$ *look random to Bob*

?

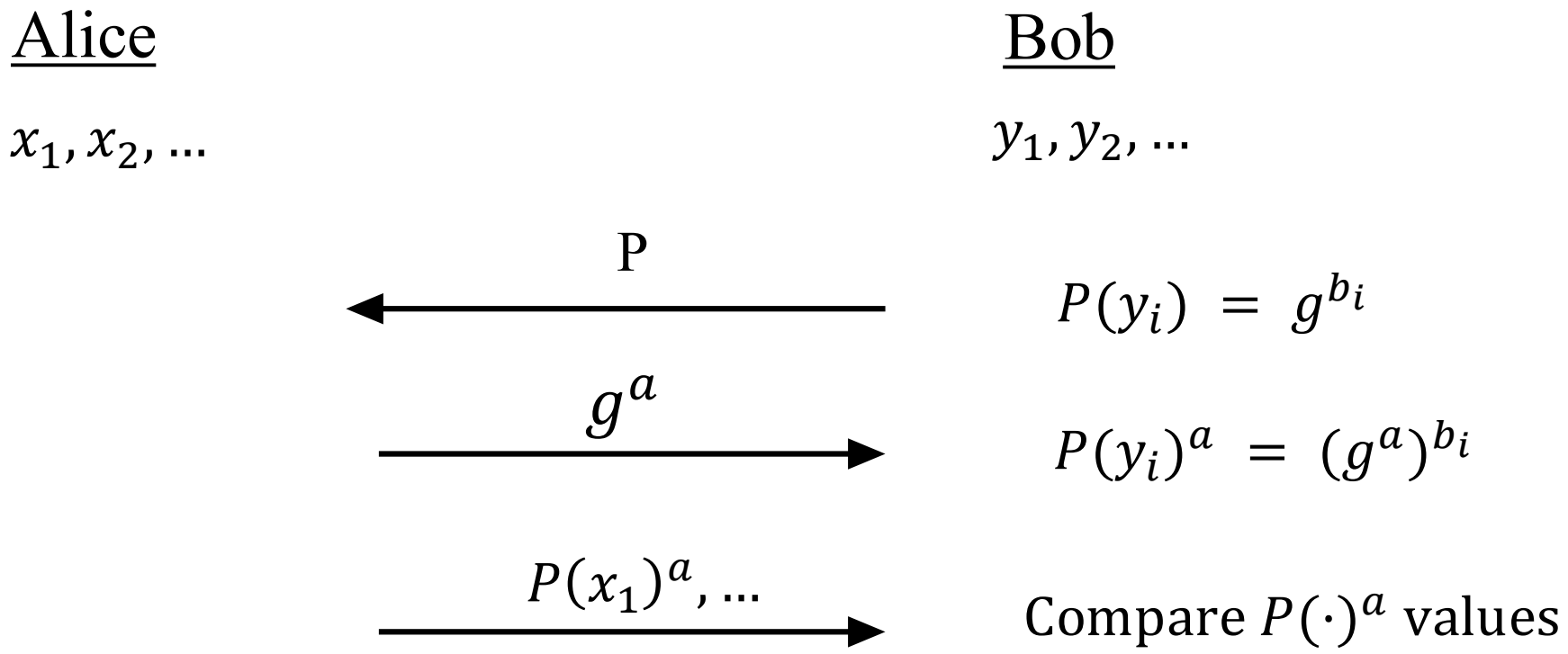
Missing details from [RT21]

Ideal permutation Π: a pulicly accessible uniformly random bijection.

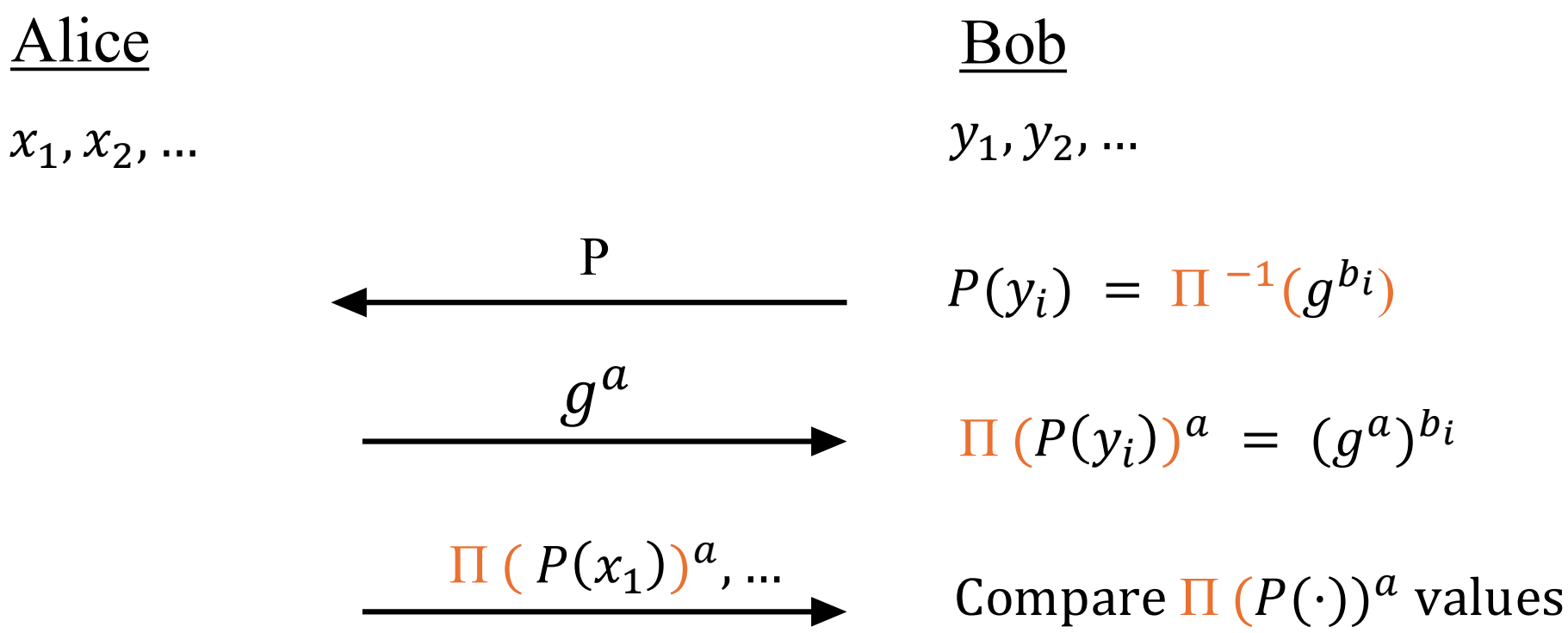


	With **ideal permutation:**
Bob encodes	
$P(y_i) = g^{b_i}$	$P(y_i) = \Pi^{-1}(g^{b_i})$
Alice evaluates	
$P(x)^a$	$\Pi(P(x))^a$

More accurate picture of [RT21]

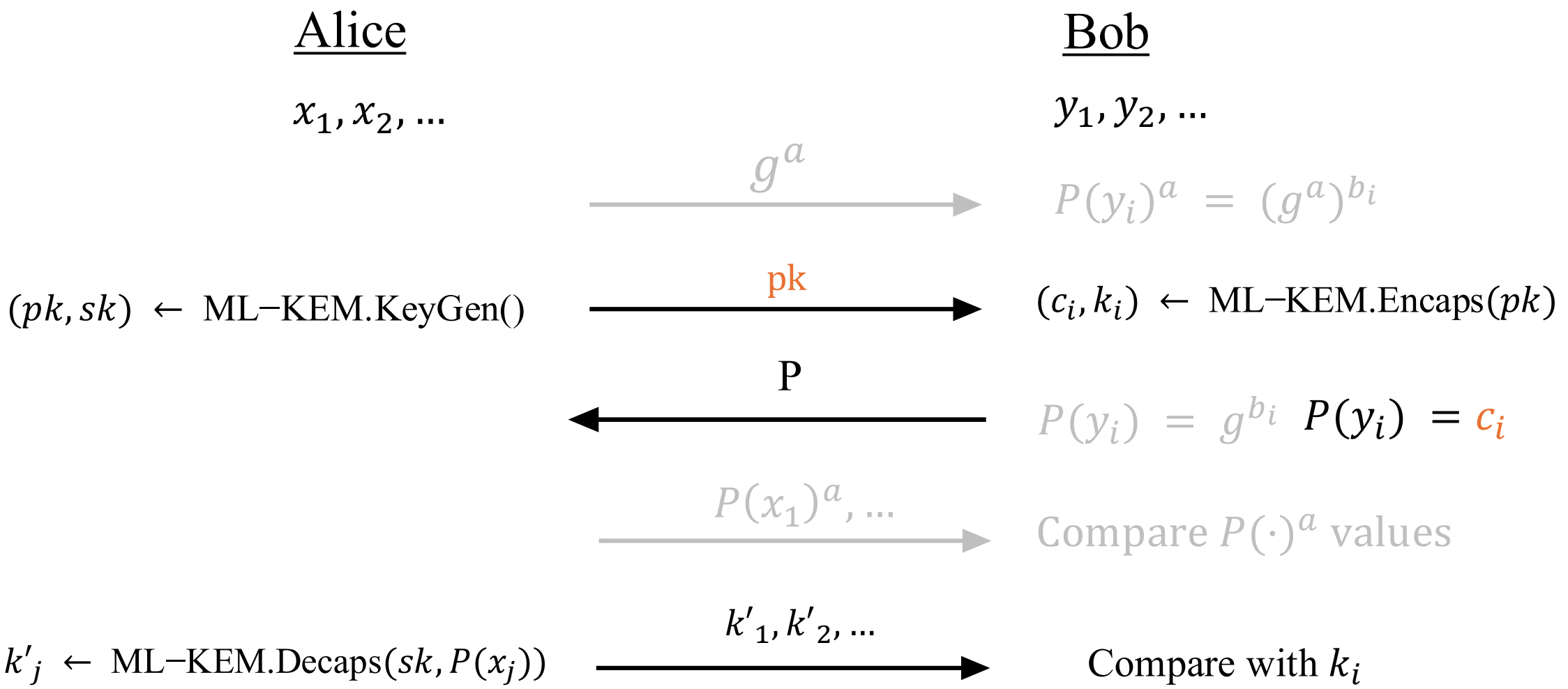


More accurate picture of [RT21]

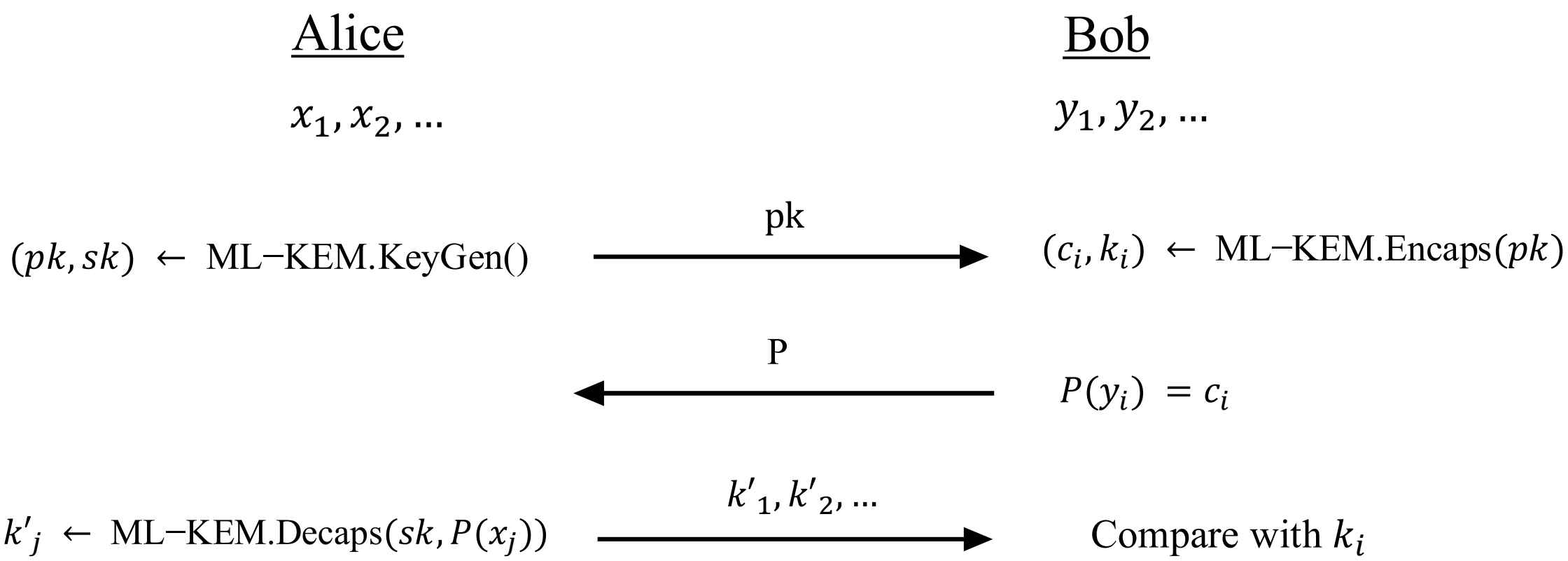


Can we just replace DH with ML-KEM?

(Ideal Permutation is omitted in all future slides)

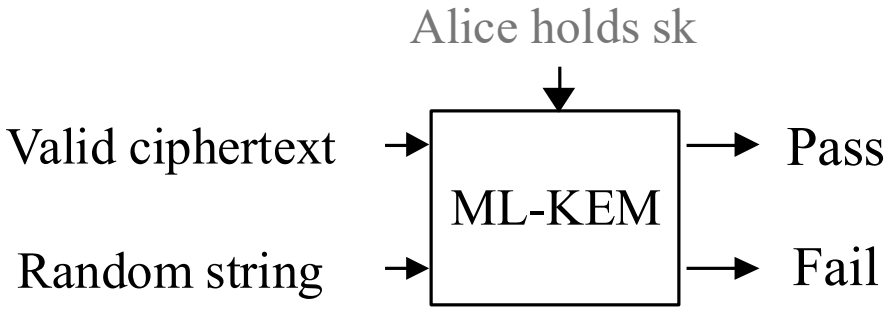


Can we just replace DH with ML-KEM?



Can we just replace DH with ML-KEM?

Challenge #1: Weird Security Property



Ciphertexts must look random

Even to Alice who has *sk*

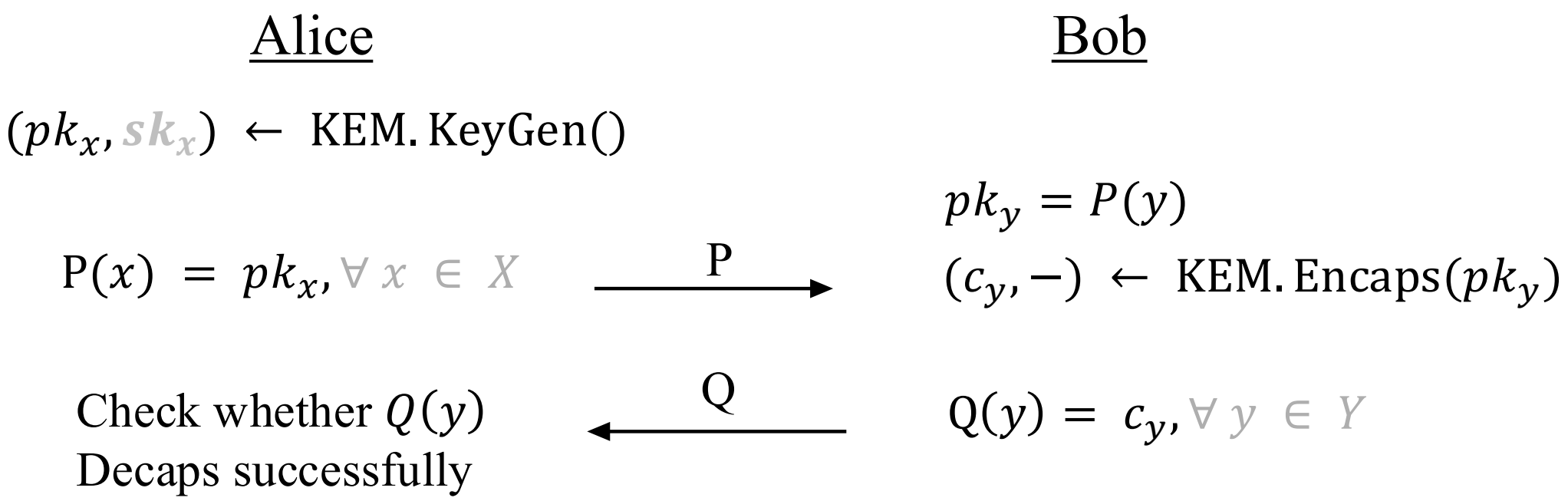
Challenge #2: Ultra-wide Permutation

(Elliptic-curve) DH → 256 bits

= 32 bytes

ML-KEM → 800–1,600 bytes

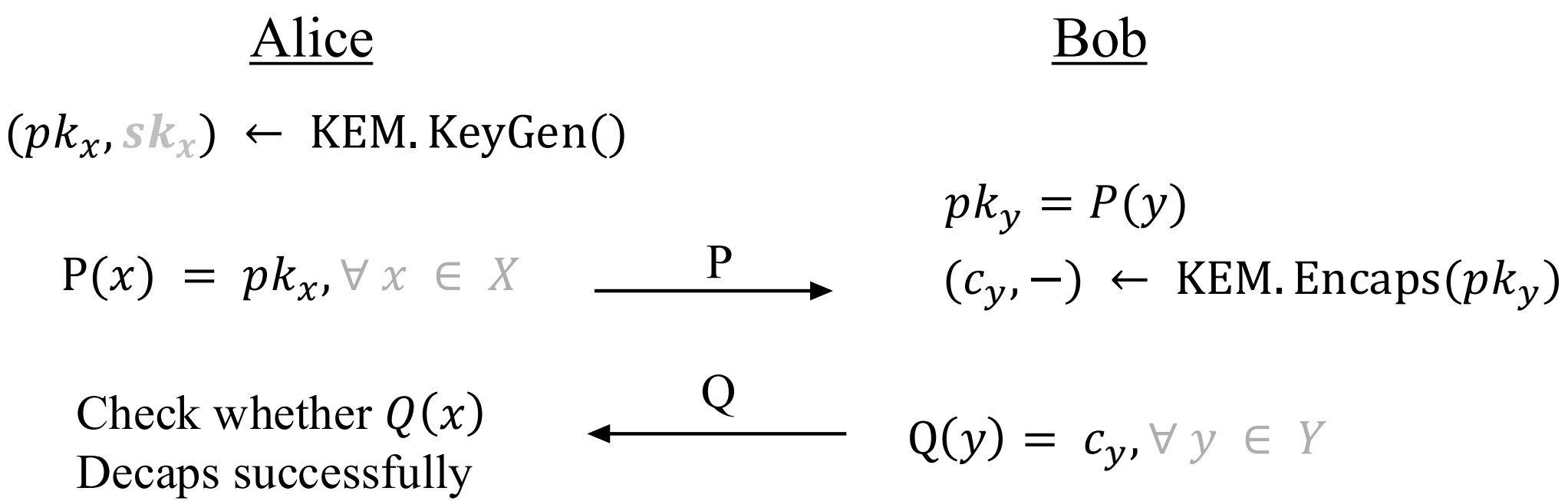
Our Modification to RT21



$y \in X \cap Y \Longrightarrow P(y) = pk_x$, $\quad$ Decaps$(sk_x, Q(y) = c_y) \neq \perp$

$y \in Y \setminus X \Longrightarrow P(y) =?$, $\quad$ Decaps$(sk_x, Q(y) =?) = \perp$

Our Modification to RT21



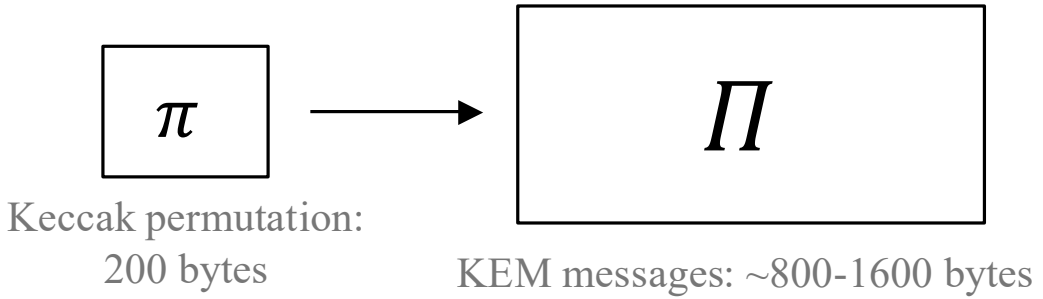
Theorem. Our variant of RT21 is secure assuming a CPA-secure KEM.

Disclaimer: classical adversaries, using post-quantum primitives

Challenge #2: Ultra-wide Ideal Permutation

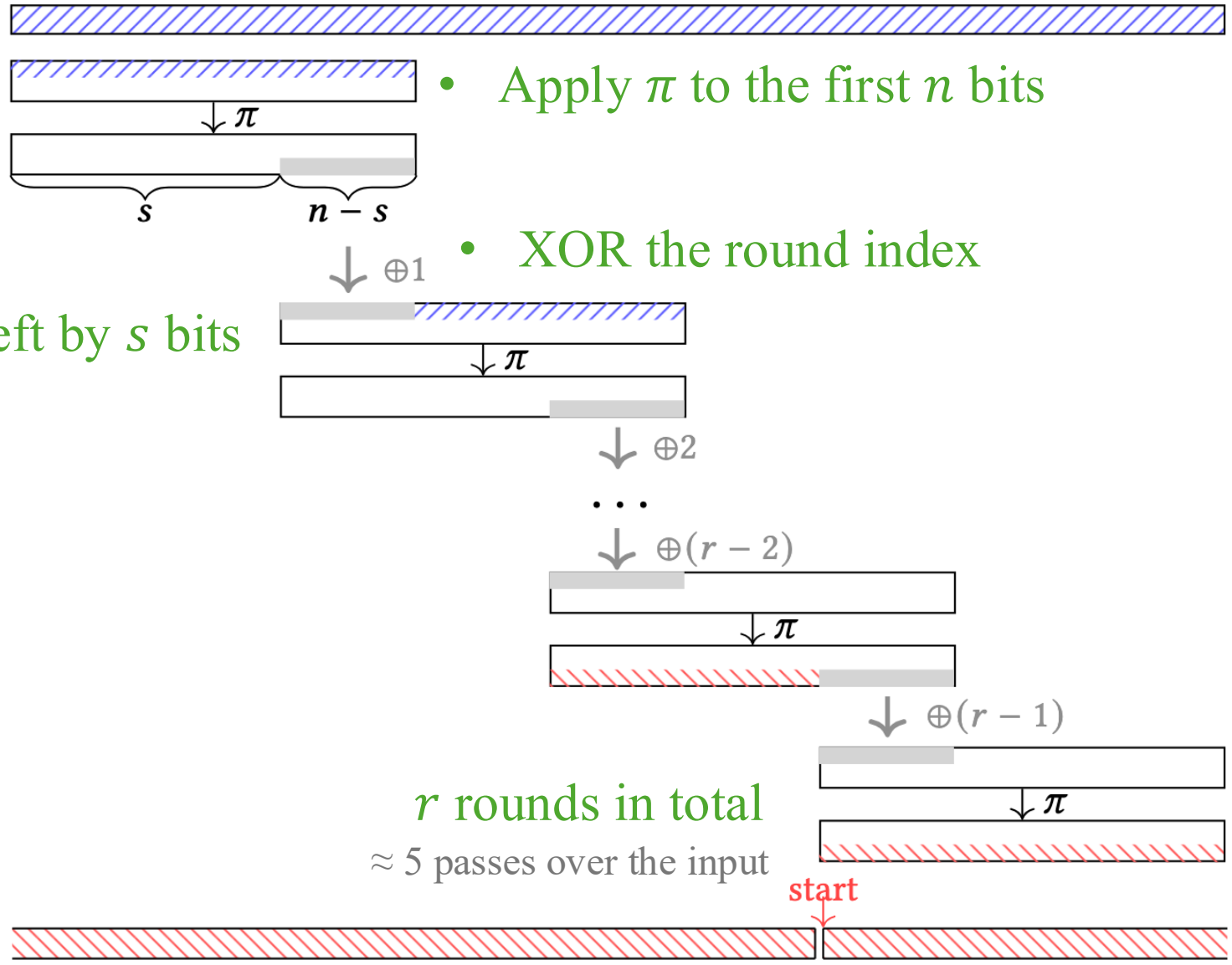
ML-KEM pk/ctxt are ***800-1600 bytes***

→ Our construction built **directly** on small ideal permutation (like Keccak)



Our Construction of Ultra-wide Permutation

- Input X



- Apply π to the first n bits
- XOR the round index

Shift left by s bits

r rounds in total

≈ 5 passes over the input

- Output Y

Our Construction of Ultra-wide Permutation

Theorem:

$\pi : \{0,1\}^n \rightarrow \{0,1\}^n$

Ideal n-bit permutation

Our construction →

$\Pi : \{0,1\}^N \rightarrow \{0,1\}^N$

Indifferentiable from N-bit ideal permutation

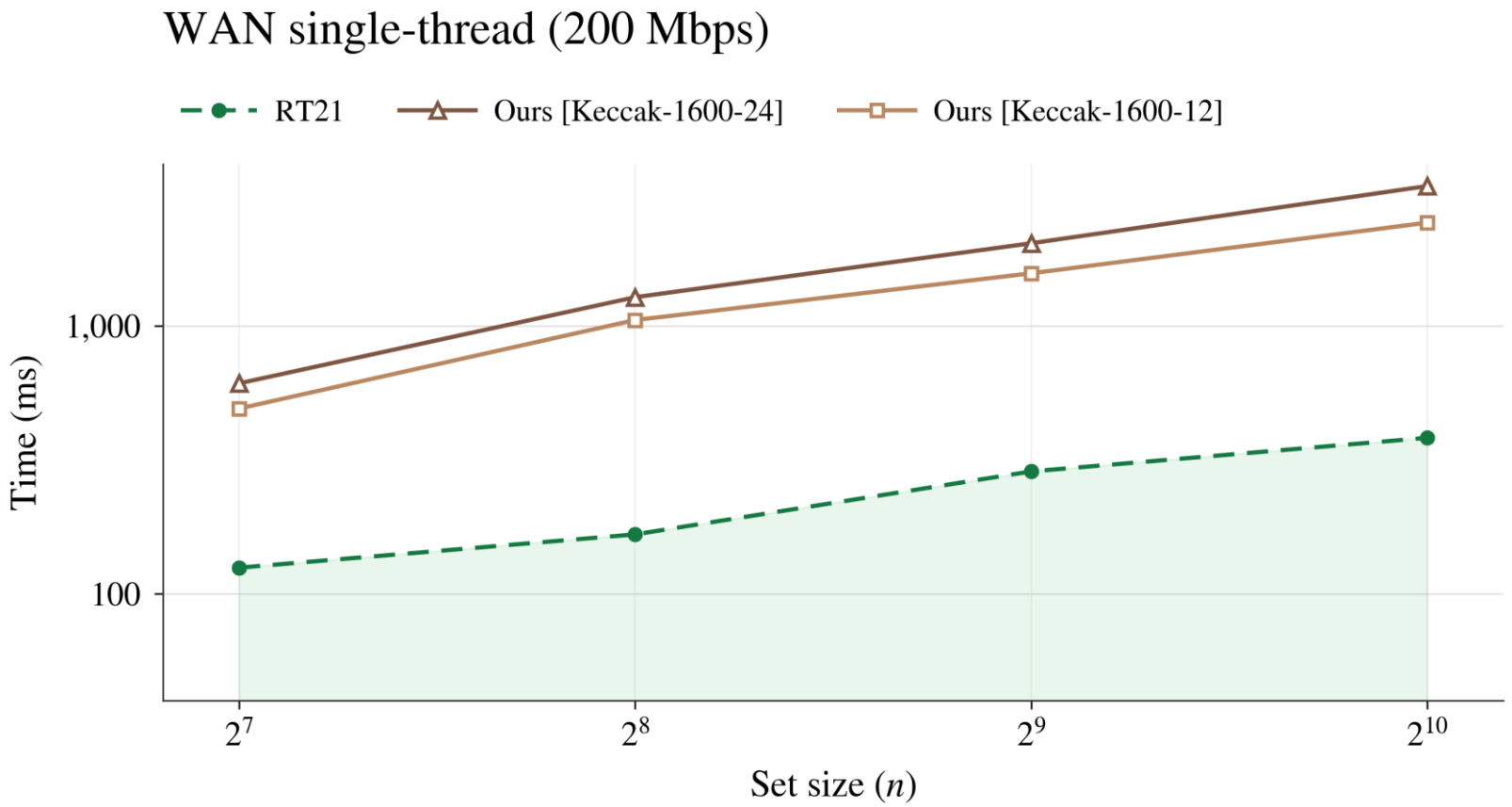
(**Indifferentiable:** Secure to replace the Ideal Permutation with our construction)

How much more expensive compared to Non-PQ PSI(RT21)?

Total communication (KiB)

Protocol	$n = 2^7$	$n = 2^8$	$n = 2^9$	$n = 2^{10}$	
RT21	8.04	16.04	32.04	64.04	
Ours	**225.00**	**428.12**	**856.25**	**1712.50**	~27×

How much more expensive compared to Non-PQ PSI(RT21)?



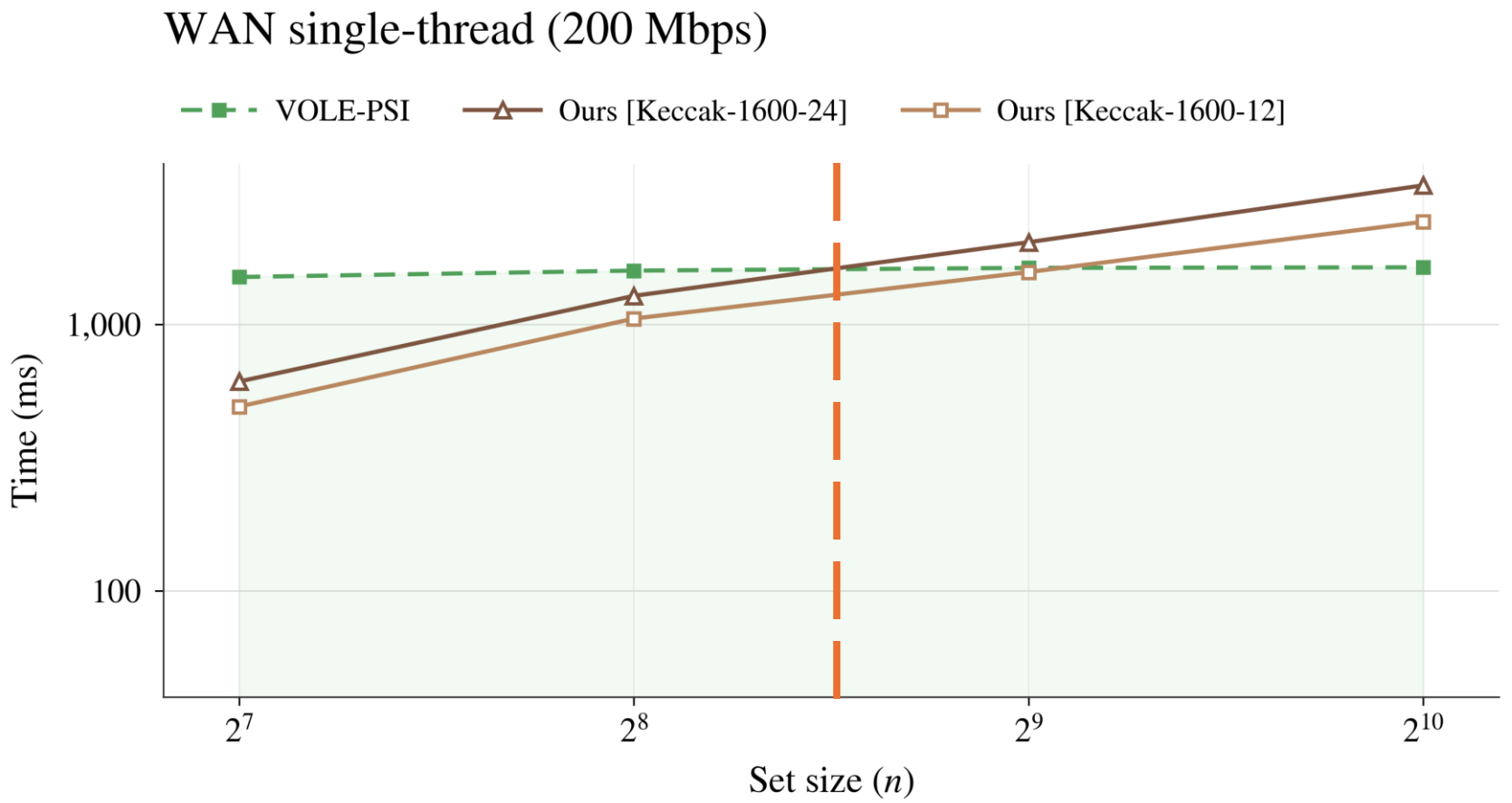
~8x slower

Compare to OT-based PSI

Total communication (KiB)

Protocol	$n = 2^7$	$n = 2^8$	$n = 2^9$	$n = 2^{10}$
(Rindal & Schoppmann, EUROCRYPT 2021.) VOLE-PSI [PQ OTs]	1117.36	1121.14	1138.69	1163.03
Ours	**225.00**	**428.12**	**856.25**	**1712.50**

Compare to OT-based PSI



How much more expensive is **PQ**-KEM in PSI?

Observation:

Larger ML-KEM public keys and ciphertexts increases Communication

The main computation overhead comes from the permutation

→ Keccak inverse is slow

Future Work

- Computation: A faster ultra-wide-block ideal permutation
- Security: Prove security of the PSI protocol against quantum attackers
  - Challenge: How to extract things from the adversary in quantum ideal permutation model?
- Communication: Let one party send only 1 ML-KEM item instead of n
  - Each party sends n ML-KEM items in our protocol
  - But Alice sends 1 DH item in RT21