2023 - AIP - **928-BA9** - Shuffle-based Private Set Union: Faster and More Secure - jia168@purdue.edu - Yanxue Jia

CERIAS

The Center for Education and Research in Information Assurance and Security

Shuffle-based Private Set Union: Faster and More Secure

Yanxue Jia, Shi-Feng Sun, Hong-Sheng Zhou, Jiajun Du, Dawu Gu

Presented in USENIX Security 2022

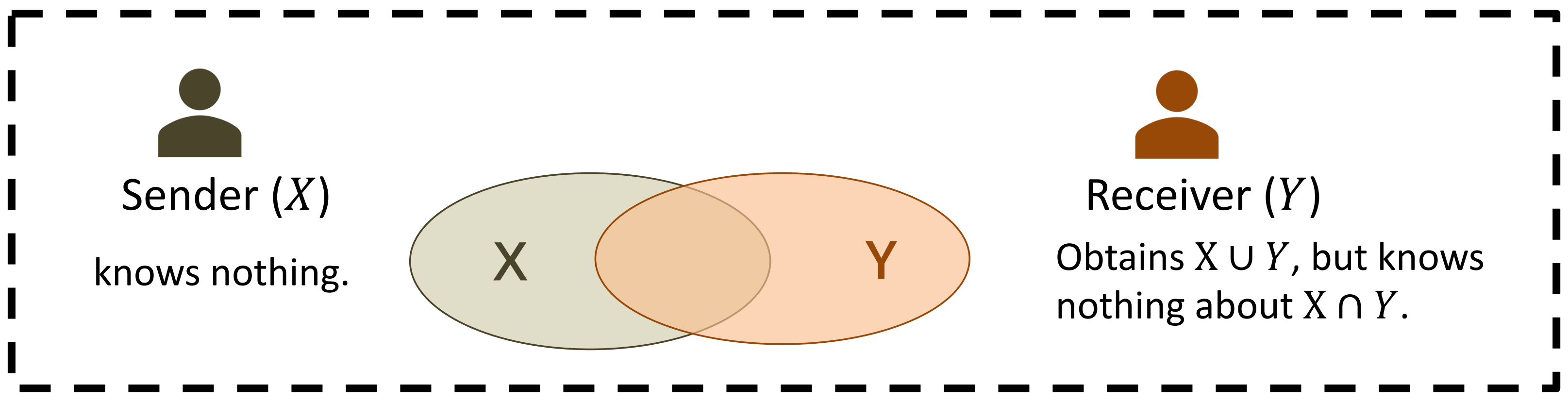
Abstract

- Designed two faster and more secure PSU protocols;
- Proposed and designed a generalized Reversed Private Membership Test (g-RPMT);
- Pointed out a security issue in the protocol of [KRTW19] and avoided it in our protocol.

	Runtime (in seconds)	Communication (in MB)
[KRTW19]	263.476	2470.11
Ours	48.703	1338.79

$|X| = |Y| = 2^{20}$ **in LAN setting.**

[KRTW19] Vladimir Kolesnikov, Mike Rosulek, Ni Trieu, and Xiao Wang. Scalable private set union from symmetric-key techniques. In Steven D. Galbraith and Shiho Moriai, editors, ASIACRYPT 2019, Part II, volume 11922 of LNCS, pages 636–666.



Sender (X)

knows nothing.

Receiver (Y)

Obtains $X \cup Y$, but knows nothing about $X \cap Y$.

Applications:

Joint IP Blacklist

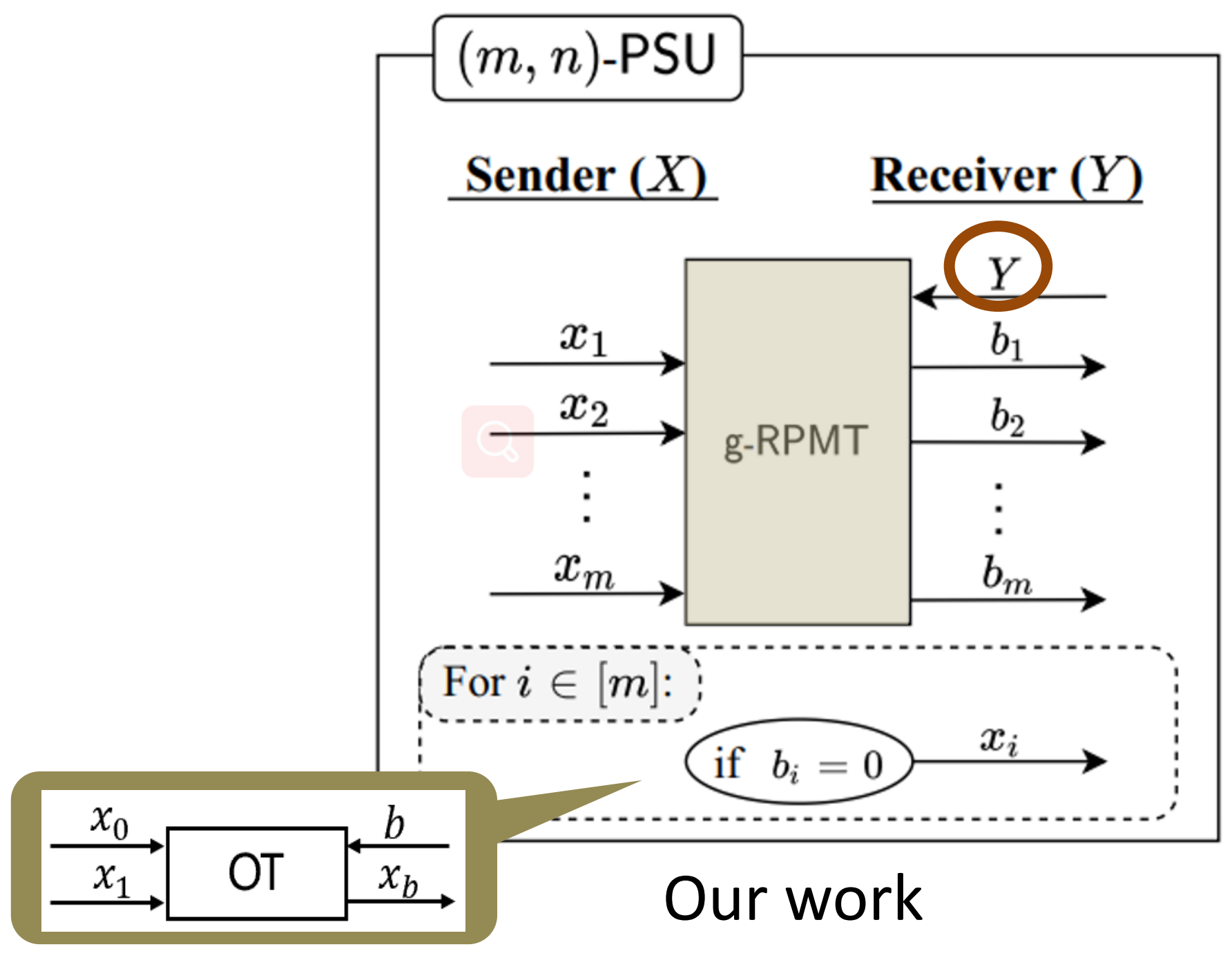
Privacy-preserving Database

Joint Patient List

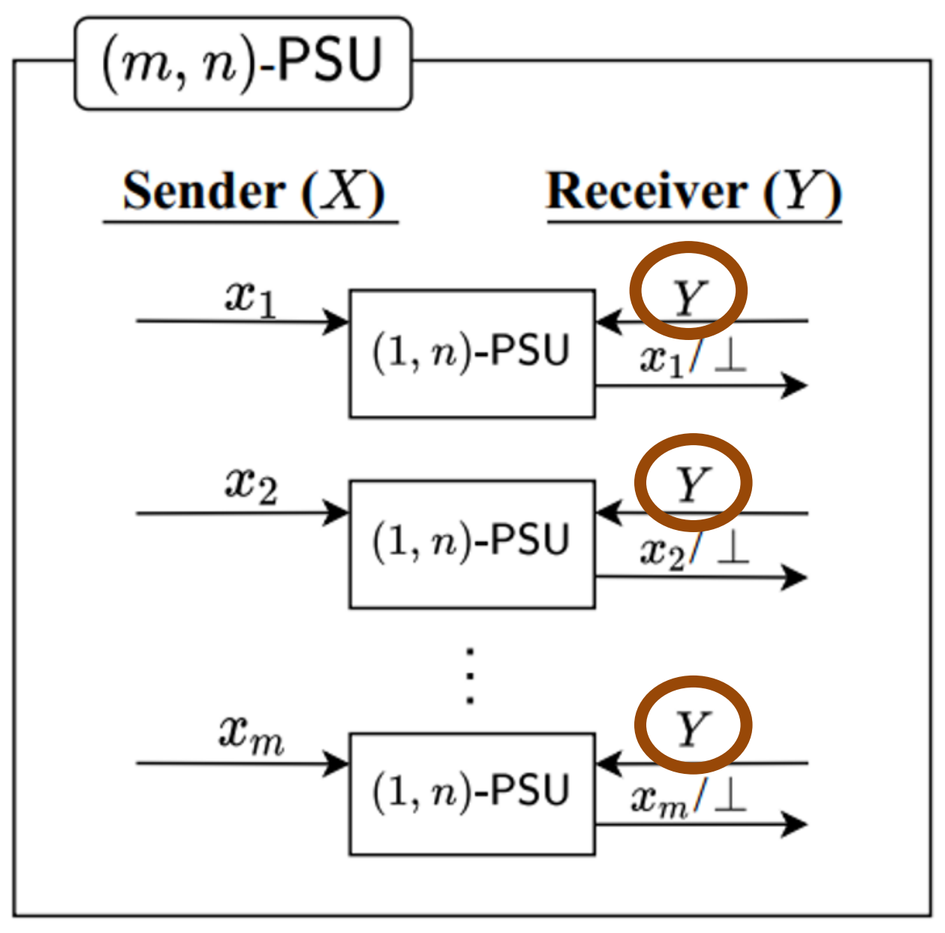
…

Design Framework

- To avoid splitting set Y;
- To guarantee that set Y only needs to be processed once.

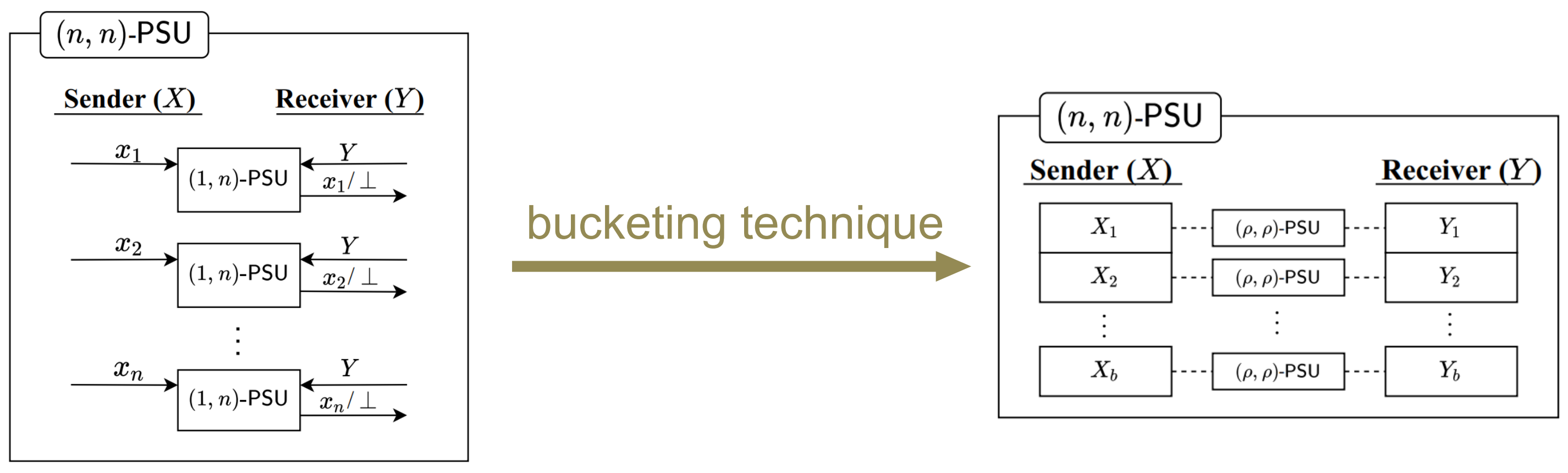


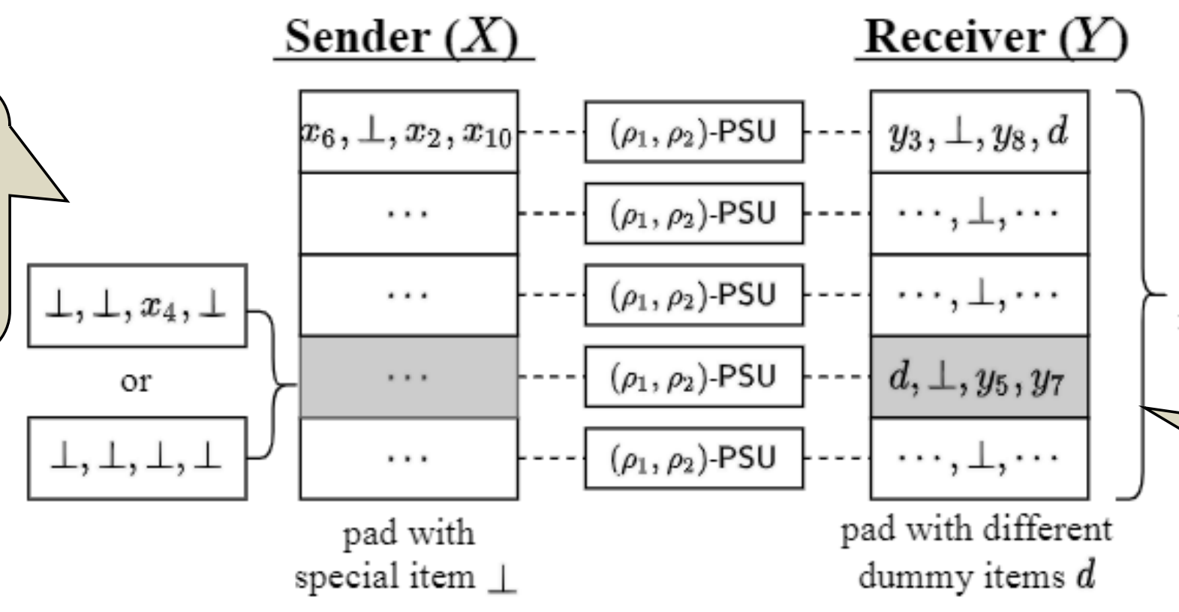
Our work



[KRTW19]

Security Issue in [KRTW19]




Sender (X)
Receiver (Y)
$x_6, \perp, x_2, x_{10}$
(ρ_1, ρ_2)-PSU
$y_3, \perp, y_8, d$
$\cdots$
$\cdots, \perp, \cdots$
$d, \perp, y_5, y_7$
$\perp, \perp, x_4, \perp$
or
$\perp, \perp, \perp, \perp$
add a special item $\perp$ to each bin
pad with special item $\perp$
pad with different dummy items d

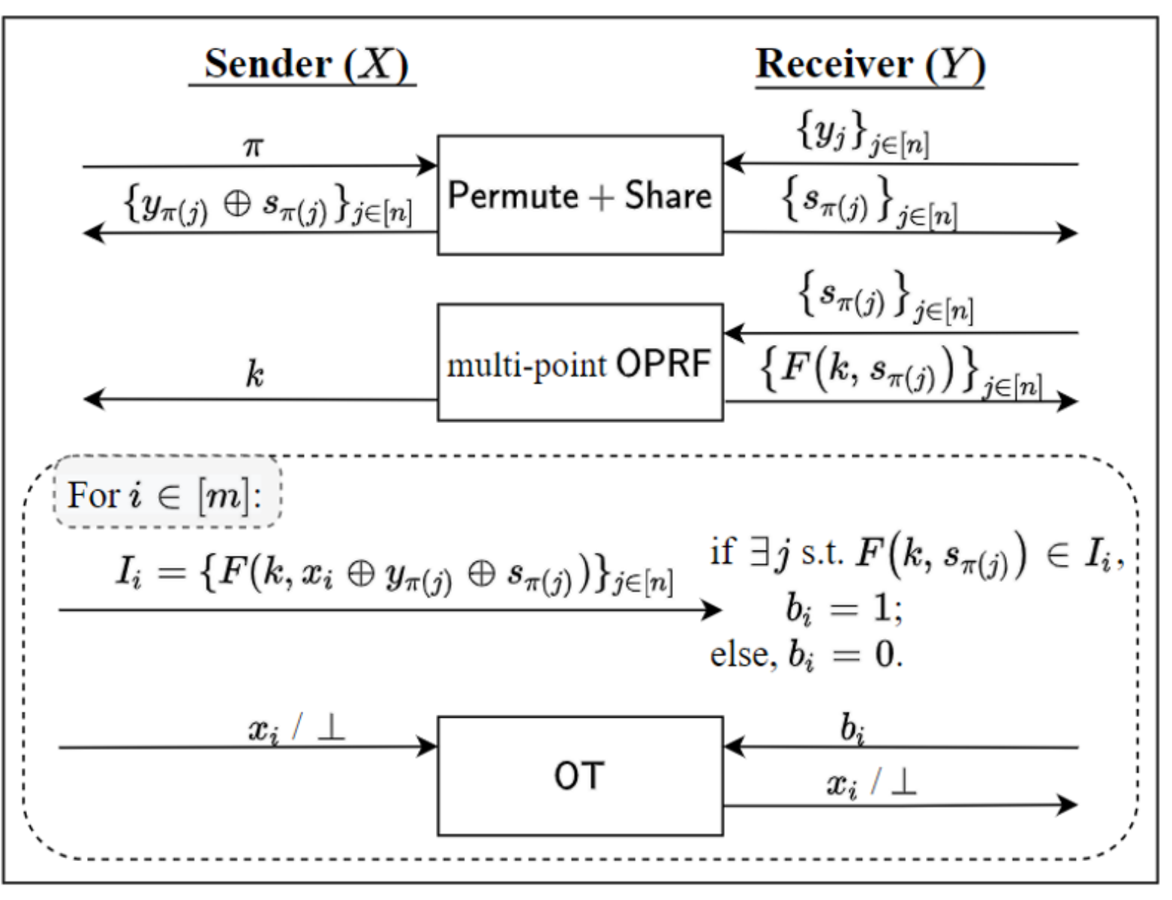
This case happens with a high probability.

The receiver may know which subsets have items in $X \cap Y$, which is not allowed in PSU.

Two PSU Protocols

Π_{PSU}^{R} by Shuffling Set Y $(X = Y, X \gg Y)$

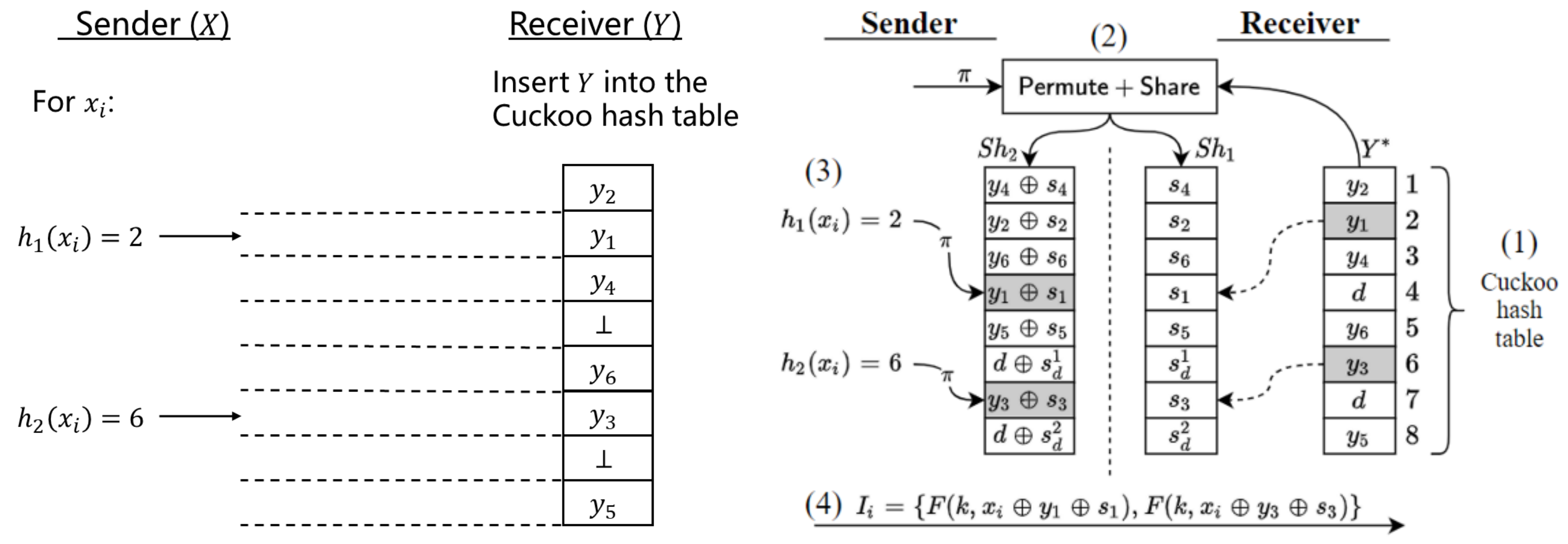
Basic scheme


Sender (X)
Receiver (Y)
π
Permute + Share
$\{y_j\}_{j\in[n]}$
$\{y_{\pi(j)} \oplus s_{\pi(j)}\}_{j\in[n]}$
$\{s_{\pi(j)}\}_{j\in[n]}$
multi-point OPRF
k
$\{F(k, s_{\pi(j)})\}_{j\in[n]}$
For $i \in [m]$:
$I_i = \{F(k, x_i \oplus y_{\pi(j)} \oplus s_{\pi(j)})\}_{j\in[n]}$
if $\exists j$ s.t. $F(k, s_{\pi(j)}) \in I_i$, $b_i = 1$; else, $b_i = 0$.
$x_i / \perp$
OT
b_i

For each $x_i \in X$, generate a I_i

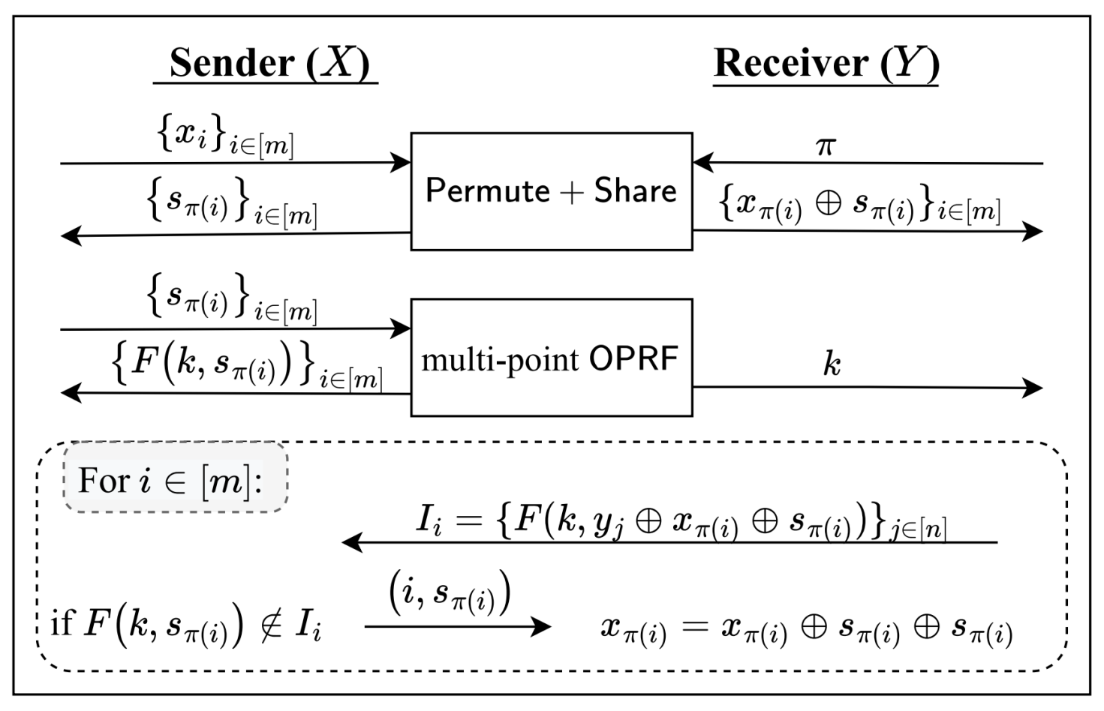
Computation and communication costs are both $O(mn)$!

Optimization

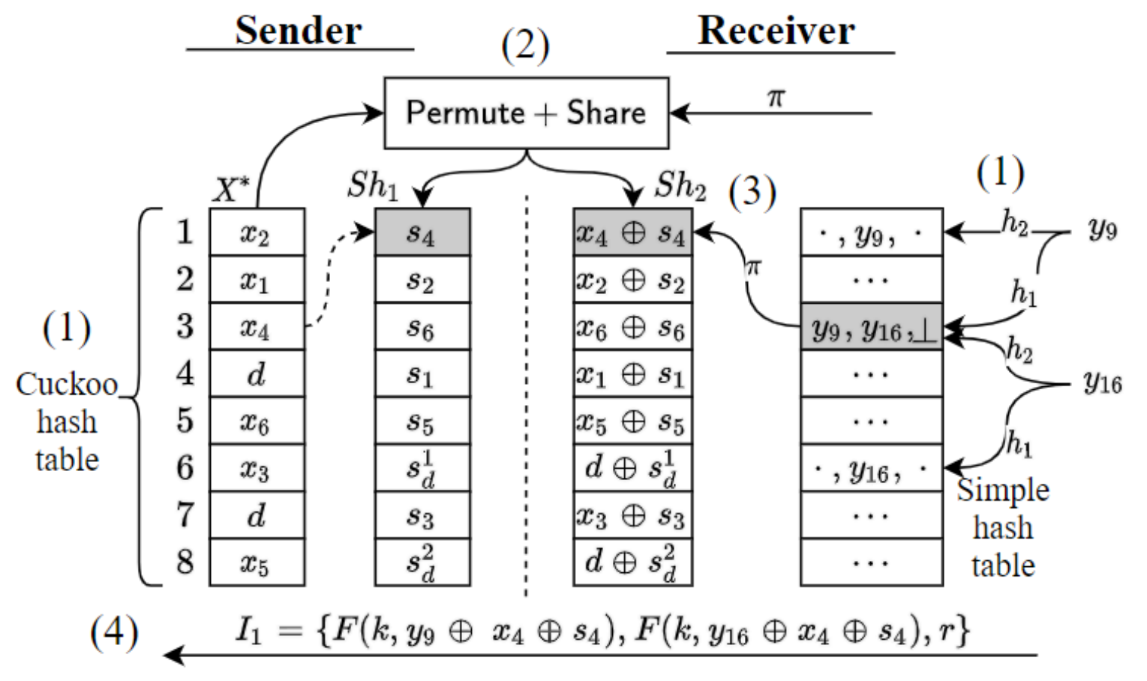


Π_{PSU}^{S} by Shuffling Set X $(X \ll Y)$

Basic scheme


Sender (X)
Receiver (Y)
$\{x_i\}_{i\in[m]}$
Permute + Share
π
$\{s_{\pi(i)}\}_{i\in[m]}$
$\{x_{\pi(i)} \oplus s_{\pi(i)}\}_{i\in[m]}$
multi-point OPRF
$\{F(k, s_{\pi(i)})\}_{i\in[m]}$
k
For $i \in [m]$:
$I_i = \{F(k, y_j \oplus x_{\pi(i)} \oplus s_{\pi(i)})\}_{j\in[n]}$
if $F(k, s_{\pi(i)}) \notin I_i$
$(i, s_{\pi(i)})$
$x_{\pi(i)} = x_{\pi(i)} \oplus s_{\pi(i)} \oplus s_{\pi(i)}$

Optimization



Performance

		Protocol	2^{8}	2^{10}	2^{12}	2^{14}	2^{16}	2^{18}	2^{20}	2^{22}
Time (s)	WAN	[18]	1.064	1.379	2.164	5.326	17.541	86.358	333.073	1459.539
		$\Pi_{\mathrm{PSU}}^{\mathrm{R}}$	**0.671**	**0.892**	**1.132**	**1.778**	**4.412**	**16.104**	**67.756**	**341.758**
		$\Pi_{\mathrm{PSU}}^{\mathrm{S}}$	0.712	0.993	1.238	2.214	6.233	22.78	102.039	458.731
	LAN	[18]	0.578	0.69	1.278	3.551	13.285	69.19	263.476	1191.703
		$\Pi_{\mathrm{PSU}}^{\mathrm{R}}$	**0.265**	**0.308**	**0.412**	**0.87**	**2.702**	**10.751**	**48.703**	**251.091**
		$\Pi_{\mathrm{PSU}}^{\mathrm{S}}$	0.274	0.32	0.434	1.051	3.452	13.382	60.16	279.97
Comm.(MB)		[18]	0.41	1.86	7.72	31.8	131.17	600.62	2470.11	10233.28
		$\Pi_{\mathrm{PSU}}^{\mathrm{R}}$	**0.22**	**0.814**	**3.576**	**15.848**	**70.198**	**307.192**	**1338.79**	**5779.599**
		$\Pi_{\mathrm{PSU}}^{\mathrm{S}}$	0.376	1.554	7.019	31.381	140.604	617.654	2725.932	11746.69

Table 5. Comparisons of total runtime (in seconds) and communication (in MB) between $\Pi_{\mathrm{PSU}}^{\mathrm{R}}$, $\Pi_{\mathrm{PSU}}^{\mathrm{S}}$ and [18] with a single thread in WAN/LAN settings where $n_1 = n_2 = n$. Best results are marked in bold.

PURDUE UNIVERSITY Discovery Park

CERIAS