

# New Framework for Structure-Aware PSI From Distributed Function Secret Sharing

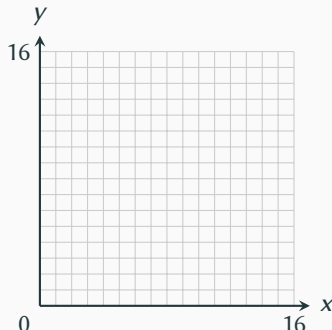
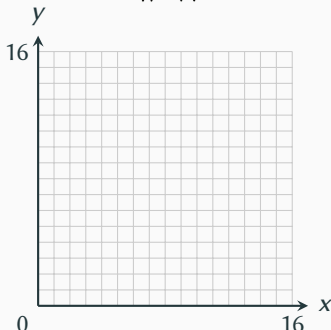
---

Dung Bui, Gayathri Garimella, Peihan Miao, **Phuoc Pham**

Asiacrypt 2025

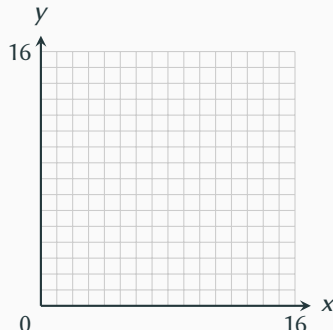
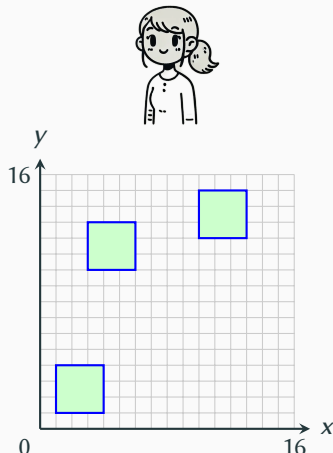
# Private Set Intersection

- Alice has a set of points  $x \in (\{0, 1\}^u)^d$  in  $d$ -dimensional space.
- Bob has a set of points  $y \in (\{0, 1\}^u)^d$  in  $d$ -dimensional space.
- Each ball has *diameter*  $\delta$ .



# Structure-Aware Private Set Intersection

- Alice has a set of  $L_\infty$  balls  $\mathcal{B}_x \subseteq (\{0, 1\}^u)^d$  in  $d$ -dimensional space.
- Bob has a set of points  $y \in (\{0, 1\}^u)^d$  in  $d$ -dimensional space.
- Each ball has *diameter*  $\delta$ .



- Structure-aware PSI was proposed by [GRS22] for  $L_\infty$  metric, introducing the framework:  
Spatial Hashing  $\rightarrow$  Function Secret Sharing  $\rightarrow$  Matching

- Structure-aware PSI was proposed by [GRS22] for  $L_\infty$  metric, introducing the framework:  
Spatial Hashing  $\rightarrow$  Function Secret Sharing  $\rightarrow$  Matching
- [GRS23] upgrades the protocol to malicious security.
- [GGM24] improve spatial hashing, and introduces trade-offs between computation and communication.

## Related Works

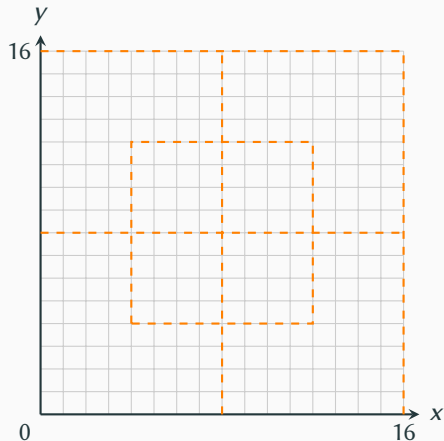
- Structure-aware PSI was proposed by [GRS22] for  $L_\infty$  metric, introducing the framework:

Spatial Hashing  $\rightarrow$  Function Secret Sharing  $\rightarrow$  Matching

- [GRS23] upgrades the protocol to malicious security.
- [GGM24] improve spatial hashing, and introduces trade-offs between computation and communication.
- [vBP24, GQL<sup>+</sup>24] generalizes the approach into *fuzzy map*, using Homomorphic Encryption, and support more distance metrics:  $L_p$  and Hamming distance.
- [ZCC<sup>+</sup>25, vBP25] replaces HE with symmetric key techniques, [PST<sup>+</sup>25] introduces distance-aware OT, to improve fuzzy maps efficiency.

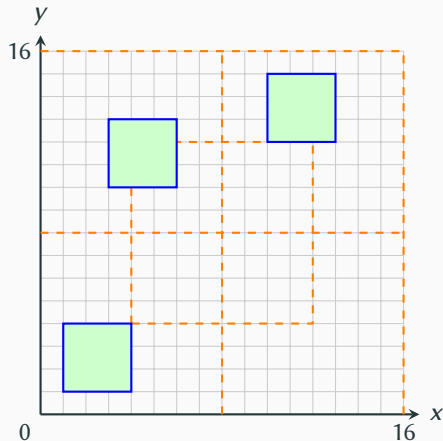
# Spatial Hashing

- The space contains (can be overlapped) *mini-universes*.
- Each mini-universe has side length  $u \geq 2\delta$ .



# Spatial Hashing and Input Assumption

- The space contains (can be overlapped) *mini-universes*.
- Each mini-universe has side length  $u \geq 2\delta$ .
- Each  $L_\infty$  ball is fully contained in a unique mini-universe.

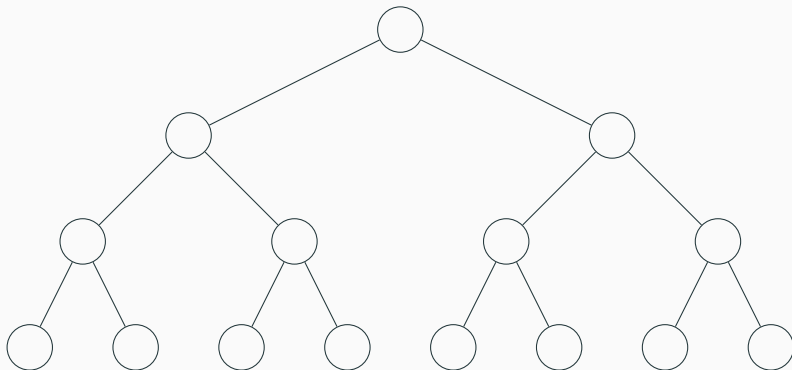




# Results Analysis

## Matching Phase:

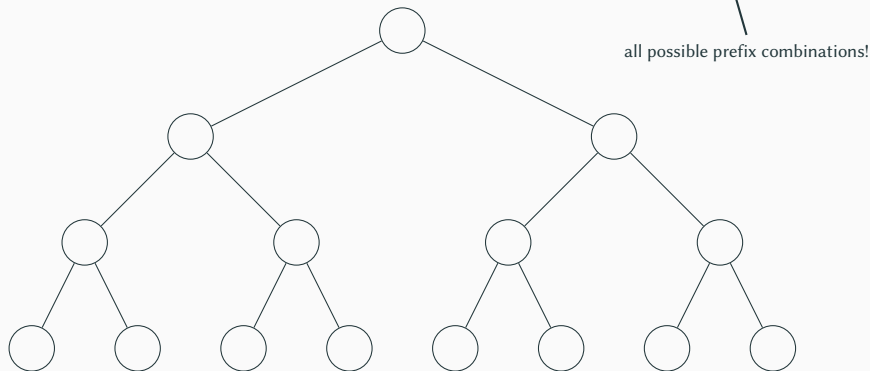
- All related works (including ours) use tree-searching technique to find matching elements.
- Total sender communication - receiver computation cost is  $O(u^d)$ .



# Results Analysis

## Matching Phase:

- All related works (including ours) use tree-searching technique to find matching elements.
- Total sender communication - receiver computation cost is  $O(u^d)$ .



# Results Analysis

## Matching Phase:

- All related works (including ours) use tree-searching technique to find matching elements.
- Total sender communication - receiver computation cost is  $O(u^d)$ .

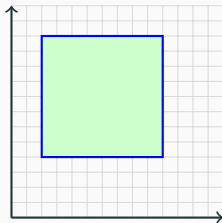
## Fuzzy Map:

- The fuzzy map step in [vBP25, ZCC<sup>+</sup>25, PST<sup>+</sup>25] has communication complexity depends *linearly* on  $u \approx \delta$  (the distance).
- Function Secret Sharing in [GGM24] has comm.  $O(\kappa^2 \cdot N_A \cdot \log \delta \cdot d)$ .
- **This work:** Communication  $O(\kappa \cdot N_A \cdot \log \delta \cdot d)$ .

## Secret Sharing $L_\infty$ ball

- For center  $(x_1, \dots, x_d)$ , we want to secret share this huge  $L_\infty$  ball:

$$[x_1 - \delta, x_1 + \delta] \times [x_2 - \delta, x_2 + \delta] \times \dots \times [x_n - \delta, x_n + \delta]$$



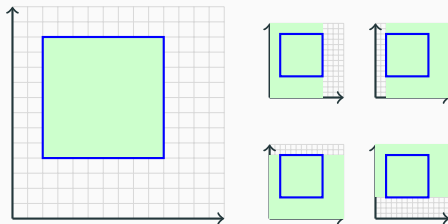
## Secret Sharing $L_\infty$ ball

- For center  $(x_1, \dots, x_d)$ , we want to secret share this huge  $L_\infty$  ball:

$$[x_1 - \delta, x_1 + \delta] \times [x_2 - \delta, x_2 + \delta] \times \dots \times [x_n - \delta, x_n + \delta]$$

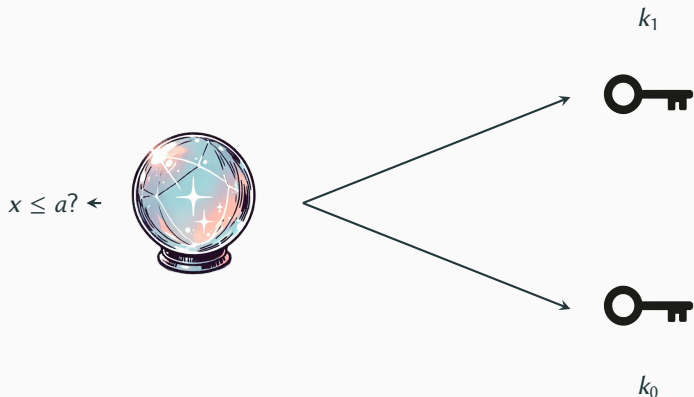
- We can secret share each dimension separately, then AND the results.

$$y_1 \geq x_1 - \delta \quad \wedge \quad y_1 \leq x_1 + \delta \quad \wedge \quad \dots \quad \wedge \quad y_d \geq x_d - \delta \quad \wedge \quad y_d \leq x_d + \delta$$



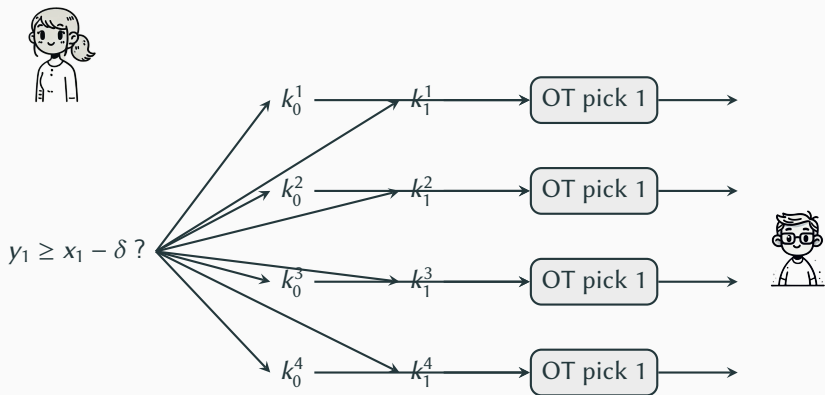
## Primitive: Function Secret Sharing (FSS)

- FSS was introduced in [BGI15], allowing to secret share a function  $f$  between multiple parties.
- For domain bit length  $u$ , security parameter  $\kappa$ , payload bit length  $v$ , the key size is  $O(u \cdot (\kappa + v))$  bits.



## Function Secret Sharing in [GGM24]

- Alice prepares  $O(\kappa)$  FSS keys pairs with *binary output* (in / out?) for each inequality check.
- Alice and Bob runs 1-out-of-2 OTs, for Bob to learn either  $k_0^i$  or  $k_1^i$  for each inequality check.
- If the inequality check succeeds, for any of  $\kappa$  key pairs, the evaluations would be equal.



## Can we use only one key pair?

- Alice can prepare only one FSS key pair for each inequality check, with *longer payload*.
- This will also avoid dictionary attack from Bob.
- However, Alice can prepare malicious payload, which is undesirable.
- Nonetheless, the key size for one inequality check is improved:

$$O(\kappa \cdot u \cdot (\kappa + 1))$$



$$O(u \cdot (\kappa + \kappa))$$

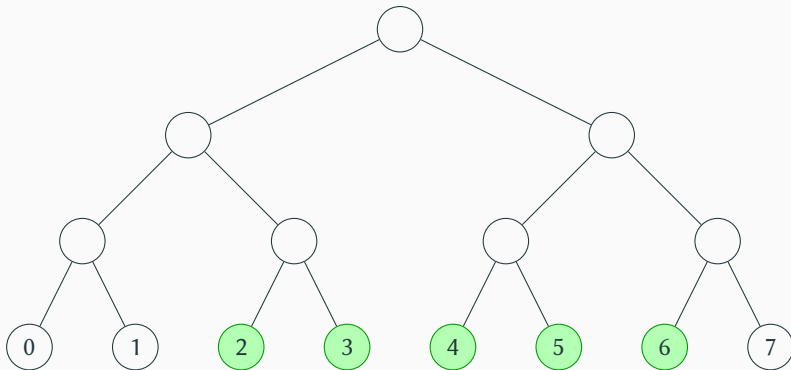




# Critical Prefix

- Each interval  $\mathcal{I}$  can be represented as set of *critical prefixes*  $\text{pref}_{\mathcal{I}}$ .

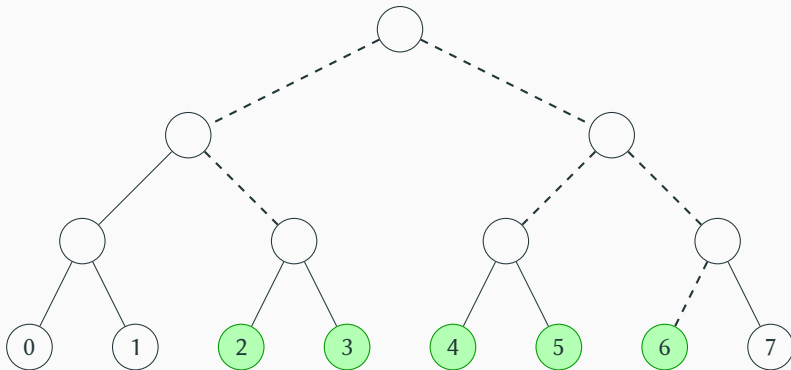
$$y \in \mathcal{I} \iff \text{exists prefix } p \prec y, p \in \text{pref}_{\mathcal{I}}$$



# Critical Prefix

- Each interval  $\mathcal{I}$  can be represented as set of *critical prefixes*  $\text{pref}_{\mathcal{I}}$ .

$$y \in \mathcal{I} \iff \text{exists prefix } p \prec y, p \in \text{pref}_{\mathcal{I}}$$



# Trade-off in Tree Search

- One way to make trade-off is by slicing the dimensions.

# Analysis

---

# Input Assumptions

- Disjoint balls
- Disjoint projection
- At least one dimension being  $2\delta$  far away from others

# Input Assumptions

- Disjoint balls
- Disjoint projection
- At least one dimension being  $2\delta$  far away from others

In this paper, we also assume that the distance is a power of 2, so  $\delta = 2^a$ .

# Experimental Results

- Only include our own results, don't need to compare with other works.
- Highlight the bottleneck is still the tree search.



# Open Questions

- Is there better, "flattened" tree search? The goal is to remove exponential dependency on  $d$ .

# References

-  Elette Boyle, Niv Gilboa, and Yuval Ishai.  
**Function secret sharing.**  
In *Annual international conference on the theory and applications of cryptographic techniques*, pages 337–367. Springer, 2015.
-  Gayathri Garimella, Benjamin Goff, and Peihan Miao.  
**Computation efficient structure-aware psi from incremental function secret sharing.**  
In *Annual International Cryptology Conference*, pages 309–345. Springer, 2024.
-  Ying Gao, Lin Qi, Xiang Liu, Yuanchao Luo, and Longxin Wang.  
**Efficient fuzzy private set intersection from fuzzy mapping.**  
In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 36–68. Springer, 2024.
-  Gayathri Garimella, Mike Rosulek, and Jaspal Singh.  
**Structure-aware private set intersection, with applications to fuzzy matching.**