

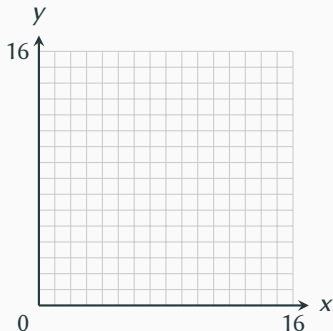
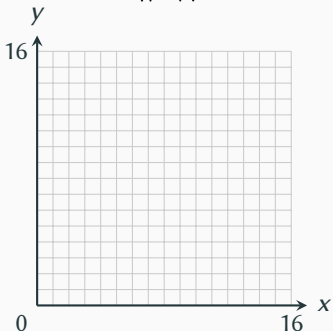
New Framework for Structure-Aware PSI From Distributed Function Secret Sharing

Dung Bui, Gayathri Garimella, Peihan Miao, Phuoc Pham

Asiacrypt 2025

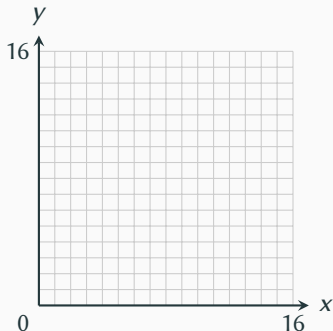
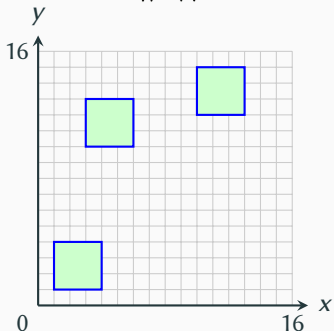
Private Set Intersection

- 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* δ .



Structure-Aware Private Set Intersection

- Alice has a set of L_∞ 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* δ .



Related Works

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

Spatial Hashing \rightarrow Function Secret Sharing \rightarrow Matching

Related Works

- Structure-aware PSI was proposed by [GRS22] for L_∞ 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

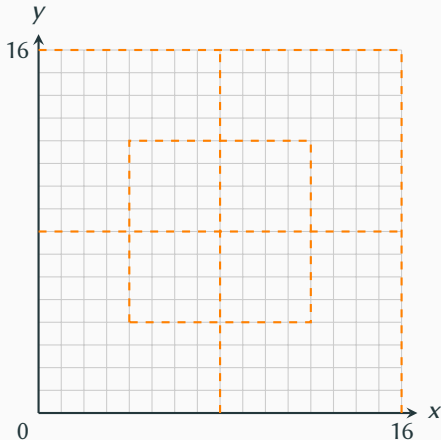
- Structure-aware PSI was proposed by [GRS22] for L_∞ metric, introducing the framework:

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⁺24] generalizes the approach into *fuzzy map*, using Homomorphic Encryption, and support more distance metrics: L_p and Hamming distance.
- [ZCC⁺25, vBP25] replaces HE with symmetric key techniques, [PST⁺25] introduces distance-aware OT, to improve fuzzy maps efficiency.

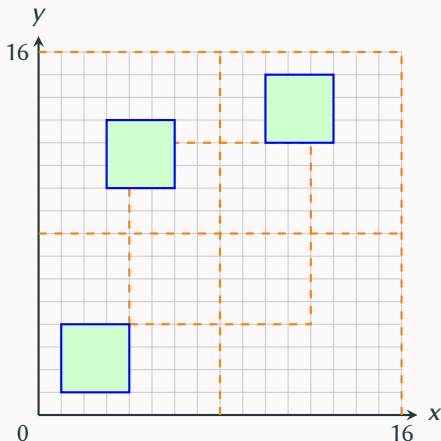
Spatial Hashing

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



Spatial Hashing and Input Assumption

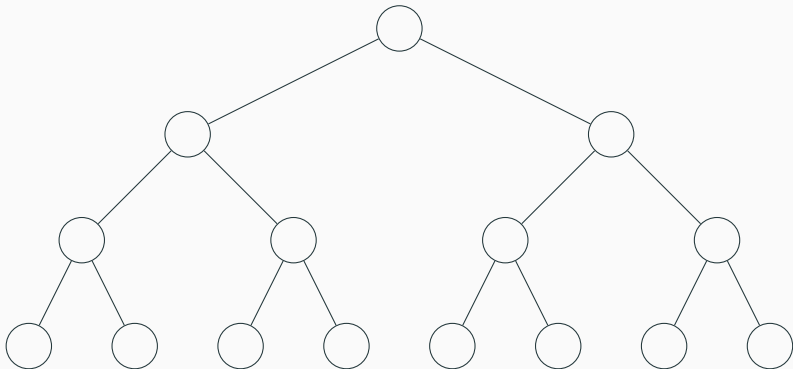
- The space contains (can be overlapped) *mini-universes*.
- Each mini-universe has side length $u \geq 2\delta$.
- Each L_∞ ball is fully contained in a unique mini-universe.



Results Analysis

Matching Phase:

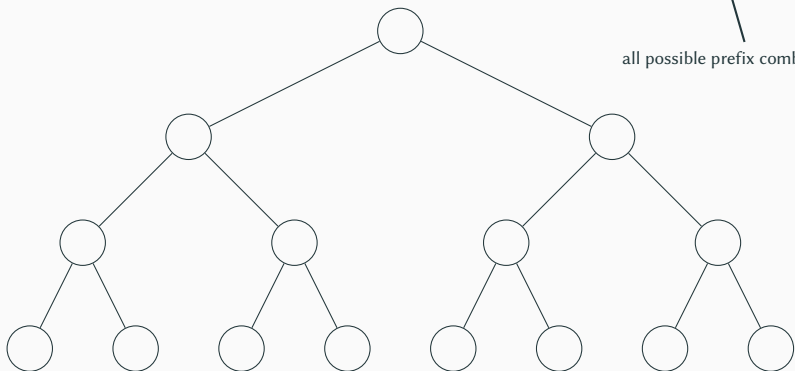
- All related works (including ours) use tree-searching technique to find matching elements.
- Total sender communication - receiver computation cost is $O(u^d)$.



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 $O(u^d)$.

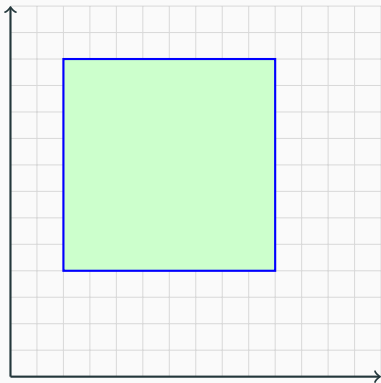
Fuzzy Map:

- The fuzzy map step in [vBP25, ZCC⁺25, PST⁺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_∞ ball

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

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



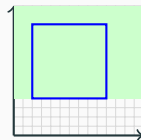
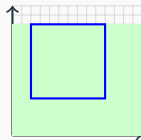
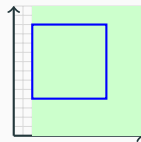
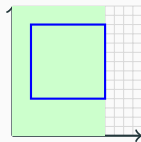
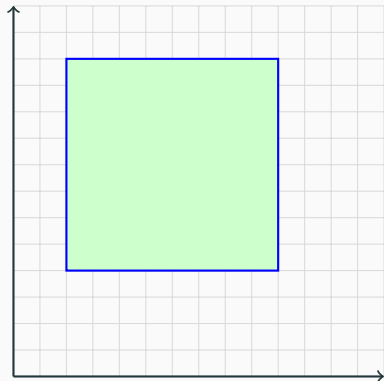
Secret Sharing L_∞ ball

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

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

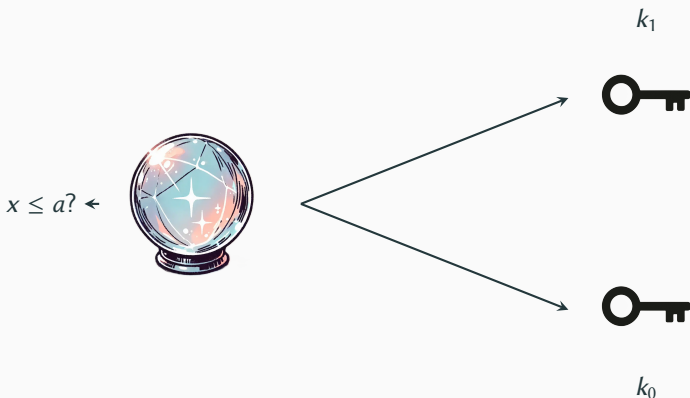
- We can secret share each dimension separately, then AND the results.

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



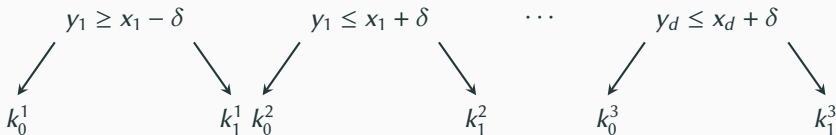
Primitive: Function Secret Sharing (FSS)

- FSS was introduced in [BGI15], allowing to secret share a function f between multiple parties.
- For domain bit length u , security parameter κ , 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 dimension.

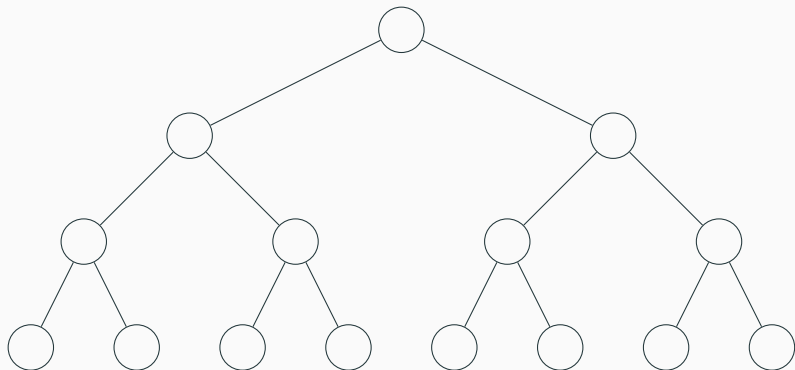


Why do we need κ key pair?

Critical Prefix

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

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



Trade-off in Tree Search

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

Analysis

Input Assumptions

- Disjoints balls
- Disjoint projection
- At least one dimension being 2δ far away from others

Input Assumptions

- Disjoint balls
- Disjoint projection
- At least one dimension being 2δ 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.