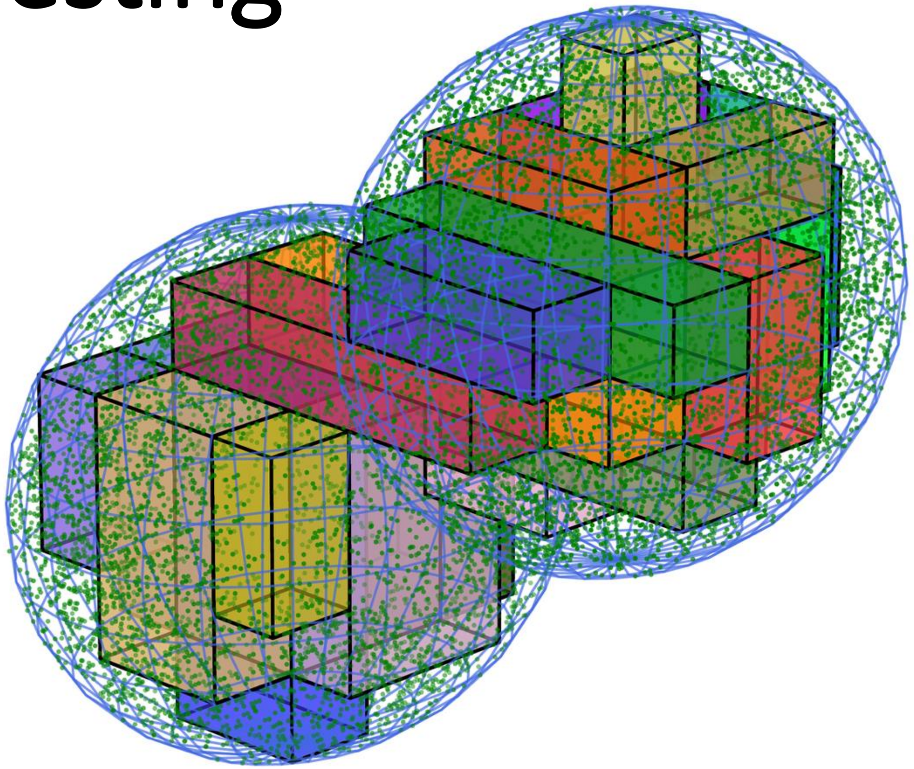
Swiss Crypto Day 2026

Zurich

Privacy-preserving Proximity Testing

from Geometric Fuzzy Matching



Florias Papadopoulos

University of St. Gallen

*This research is supported by armasuisse Science and Technology

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

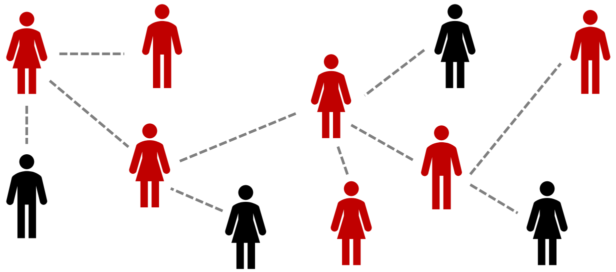
armasuisse Science and Technology
Cyber-Defence Campus

University of St.Gallen
Institute of Computer Science

Based on: *Privacy-preserving Proximity Testing from Geometric Fuzzy Matching*
F. Papadopoulos, I. Katis, K. Mitrokotsa (Published in ACM AsiaCCS 2026)

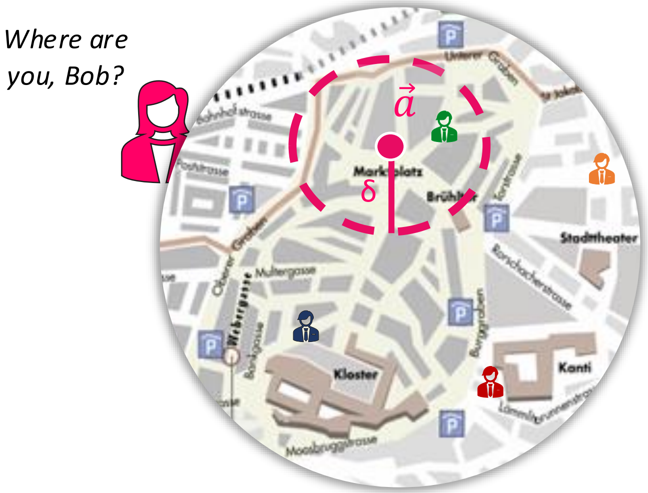
Scenarios Demanding Privacy in Proximity Testing

Contact Tracing

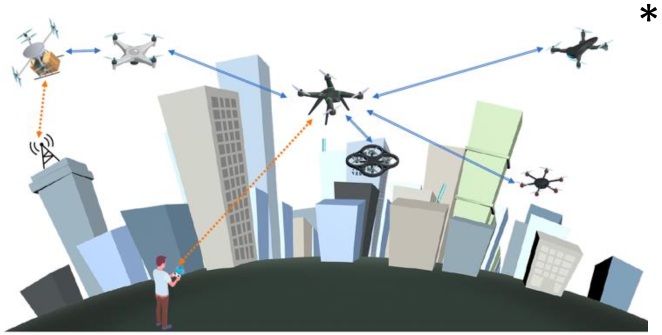


Privacy-preserving Ridesharing

Nearby friends' discovery



Drone Proximity & Collision Avoidance



*Tedeschi et al., ACSAC '23

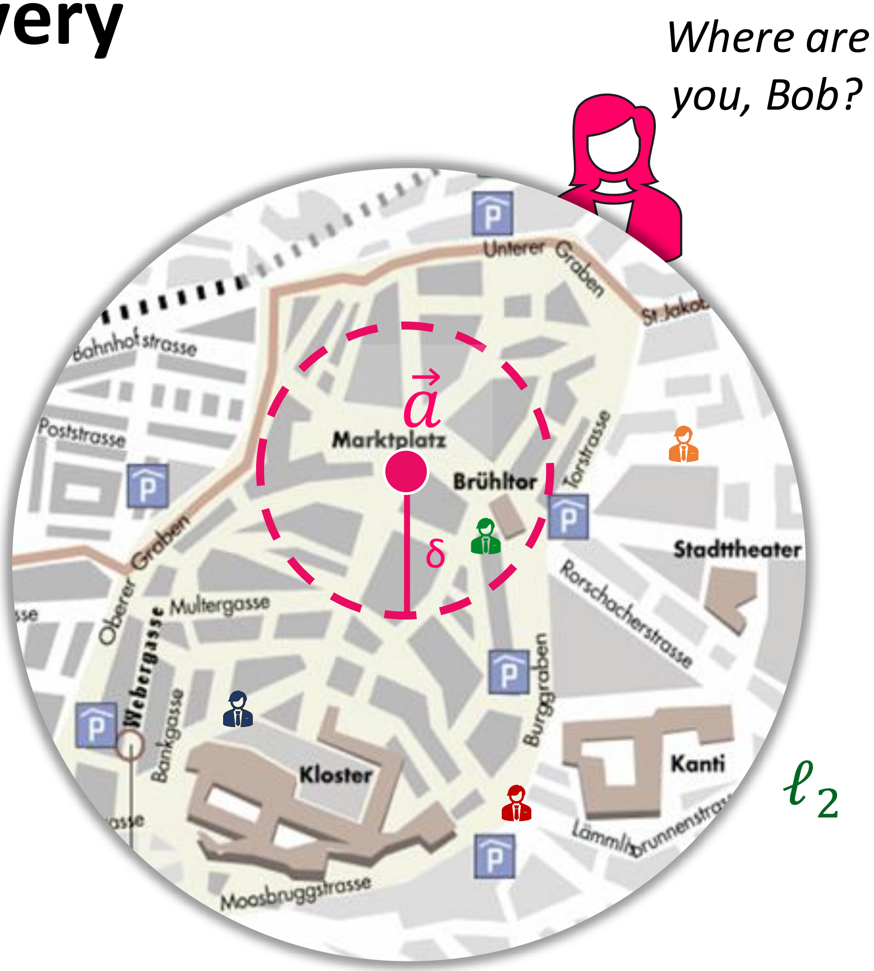
Nearby friends' discovery

- Current privacy-preserving methods

Have weak security models

Are inefficient

Rely on strong trust assumptions



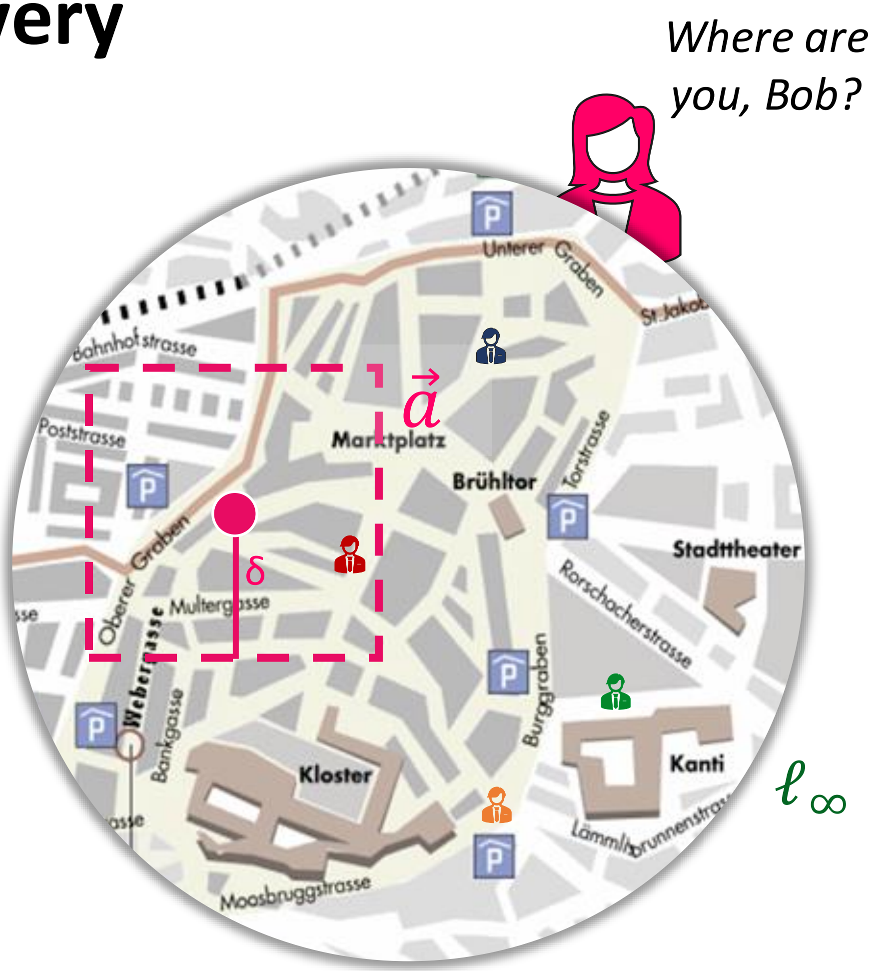
Nearby friends' discovery

- Current privacy-preserving methods

Have **weak** security models

Are **inefficient**

Rely on **strong trust** assumptions



- In practice, companies rely on insecure systems that **endanger user privacy and security**.

Nearby friends' discovery

- Current privacy-preserving methods

Have **weak** security models

Are **inefficient**

Rely on **strong trust** assumptions

- In practice, companies rely on insecure systems that **endanger user privacy and security**.

Where are you, Bob?

$dist?$

Efficient, privacy-preserving, and accurate proximity discovery at scale remains an **open problem**.

PPPT from Geometric Fuzzy Matching

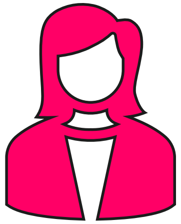
Related work on Fuzzy Matching

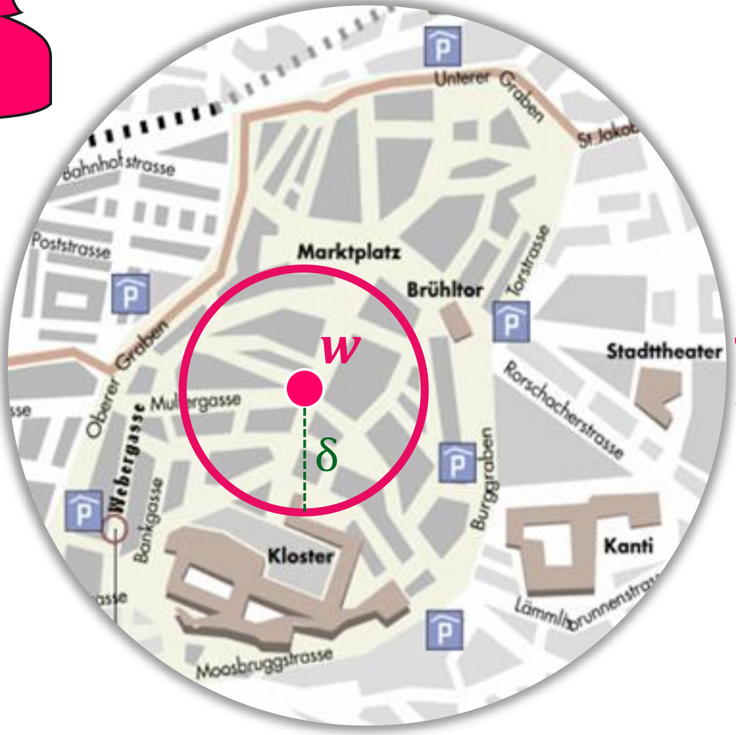
Geometric Fuzzy Matching

Applications of GFM

Related Work on Fuzzy Matching

Fuzzy Matching





$w \in \mathbb{Z}^d$

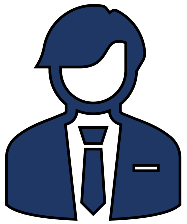
FM

$1\ or\ 0$

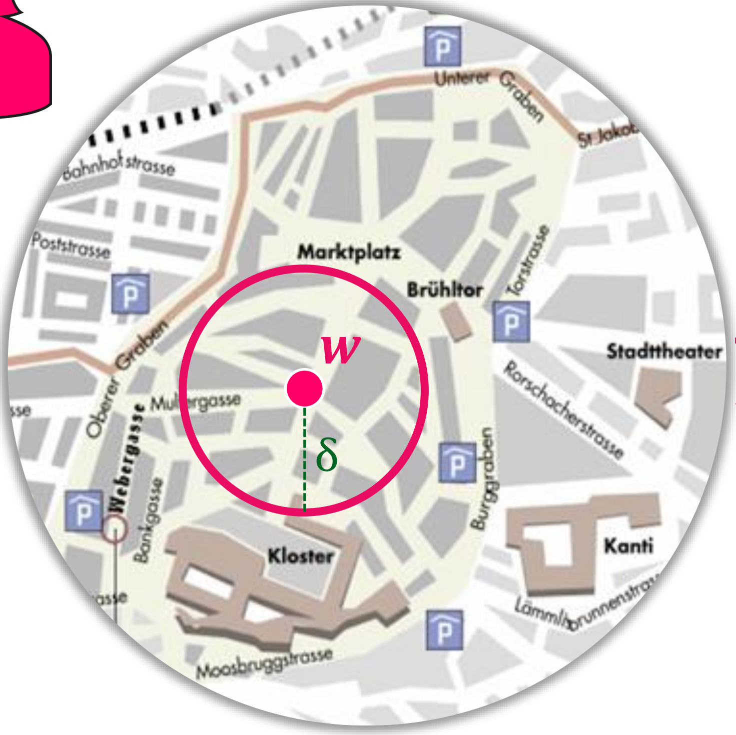
$q \in \mathbb{Z}^d$

δ: threshold

$dist(\cdot,\cdot)$: distance function



Fuzzy Matching



$\boldsymbol{w} \in \mathbb{Z}^{\boldsymbol{d}}$ → **FM** ← $\boldsymbol{q} \in \mathbb{Z}^{\boldsymbol{d}}$

$1 \; or \; 0$

δ: threshold

$dist(\cdot,\cdot)$: distance function

$\boxed{\ell_\infty}$

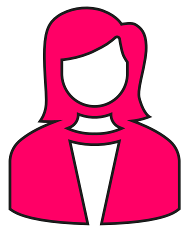
$$dist_\infty(\boldsymbol{w},\boldsymbol{q}) = \max_i(|w_i - q_i|)$$

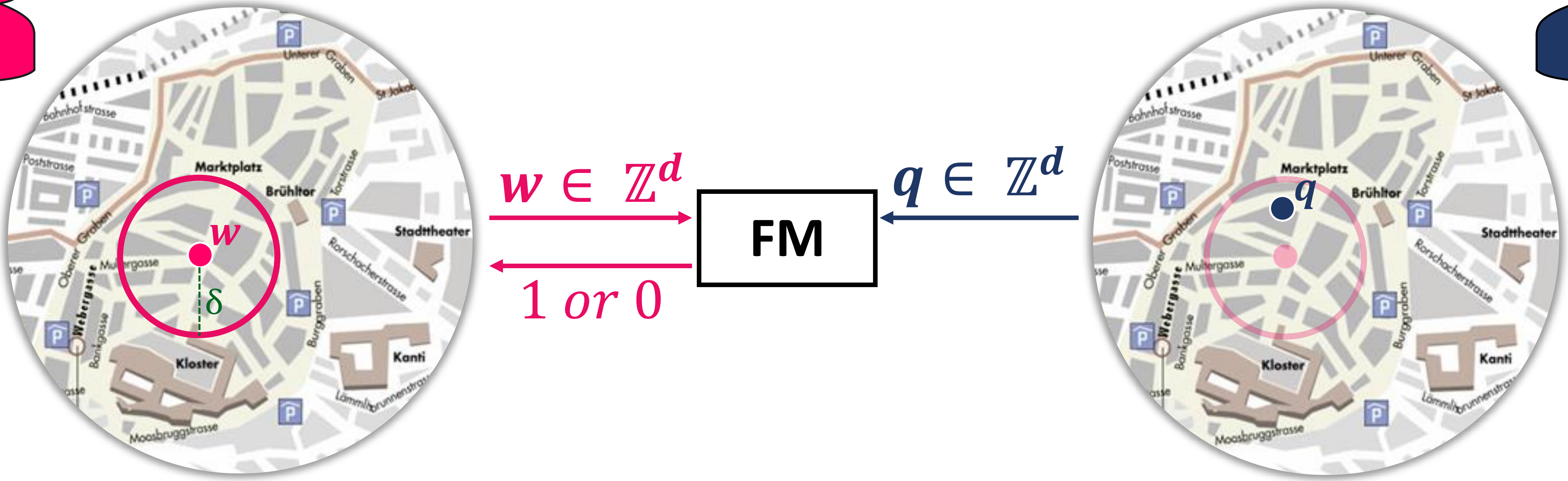
Hamming

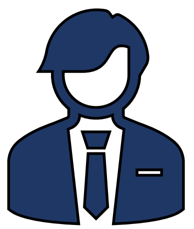
$\boxed{\ell_\mathrm{p}}$

$$dist_\mathrm{p}(\boldsymbol{w},\boldsymbol{q}) = \left(\sum_{i=1}^{n} |w_i - q_i|^\mathrm{p}\right)^{1/\mathrm{p}}$$

Fuzzy Matching

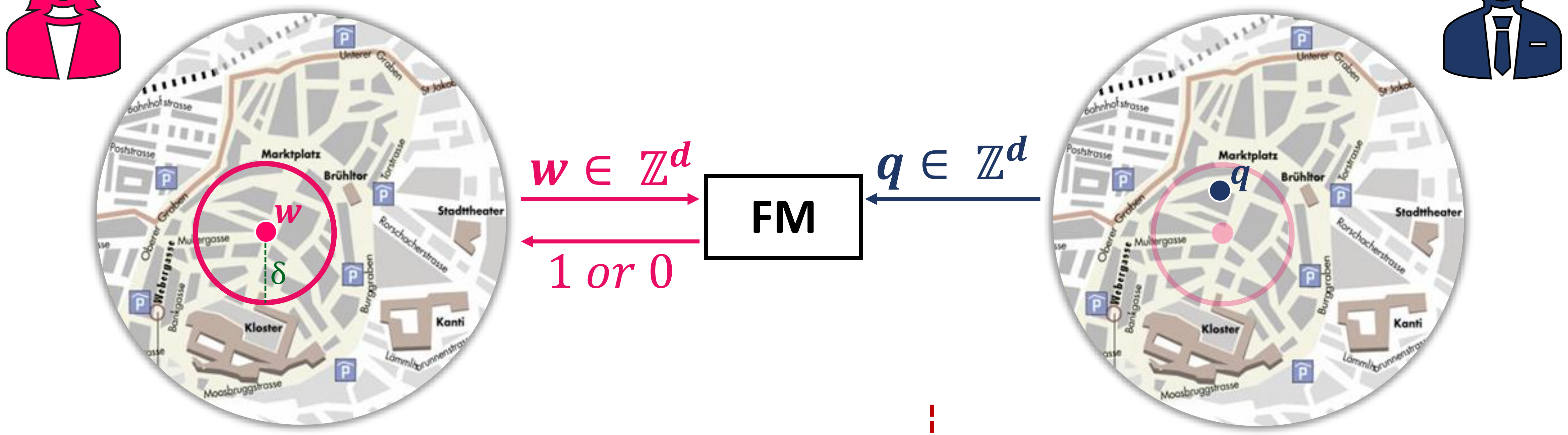






	[UCK+21] USENIX	[GRS22] CRYPTO	[CFR23] USENIX	[vBP24] EUROCRYPT	[GQL+24] ASIACRYPT	[vBP25] ASIACRYPT	[SPK+25] IEEE Access	[PST+25] CCS	[DZL25] CCS
dist	Hamming	ℓ_∞	Hamming, ℓ_1 $(d=1)$	$\ell_{p,\, p\in[1,\infty)}$	Hamming, $\ell_{p,\, p\in[1,\infty)}$	$\ell_{p,\, p\in[1,\infty)}$	Cosine Similarity	ℓ_∞, ℓ_1, $\ell_2(d=2)$	$\ell_{p,\, p\in[1,\infty)}$

Fuzzy Matching

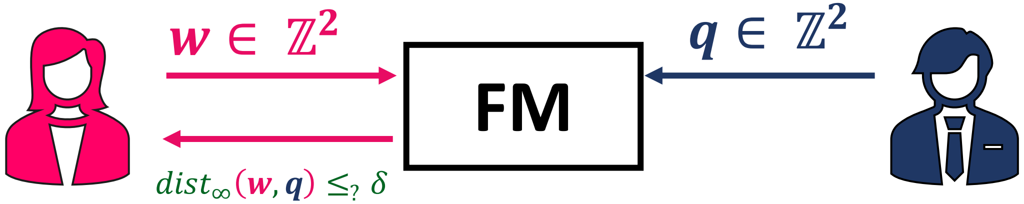


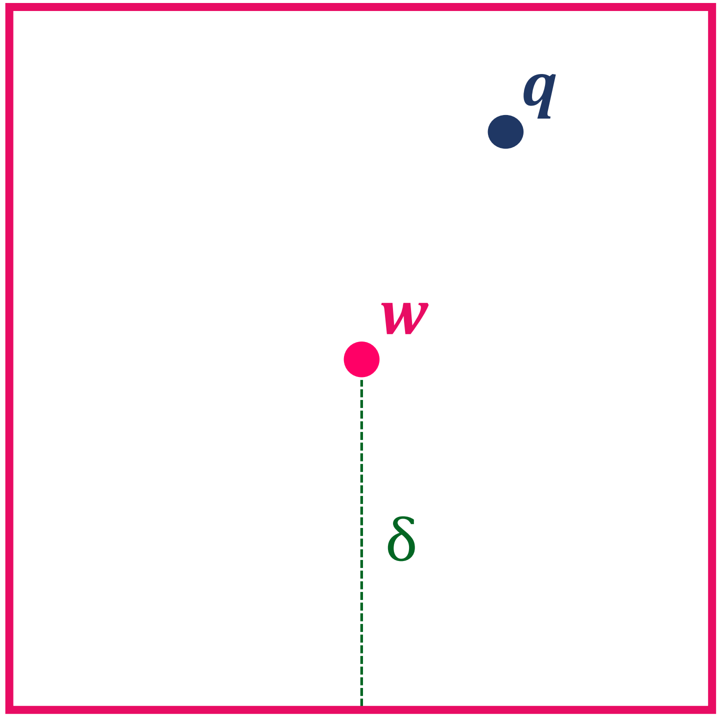
focus was fuzzy PSI* | concurrent/later work

	~~[UCK+21] USENIX~~	~~[GRS22] CRYPTO~~	~~[CFR23] USENIX~~	[vBP24] EUROCRYPT	~~[GQL+24] ASIACRYPT~~	~~[vBP25] ASIACRYPT~~	~~[SPK+25] IEEE Access~~	~~[PST+25] CCS~~	~~[DZL25] CCS~~
dist	~~Hamming~~	~~ℓ_∞~~	~~Hamming, ℓ_1 $(d=1)$~~	$\ell_{p,\, p\in[1,\infty)}$	~~Hamming, $\ell_{p,\, p\in[1,\infty)}$~~	~~$\ell_{p,\, p\in[1,\infty)}$~~	~~Cosine Similarity~~	~~$\ell_\infty, \ell_1, \ell_2 (d=2)$~~	~~$\ell_{p,\, p\in[1,\infty)}$~~

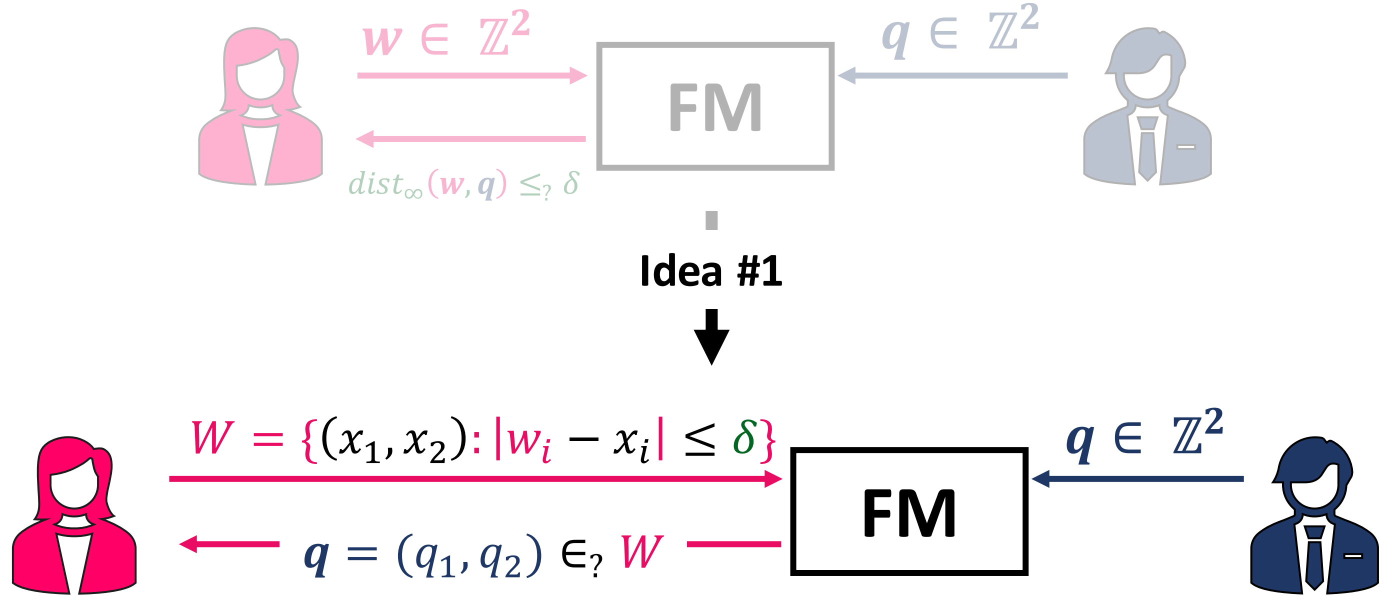
*Private Set Intersection (PSI)

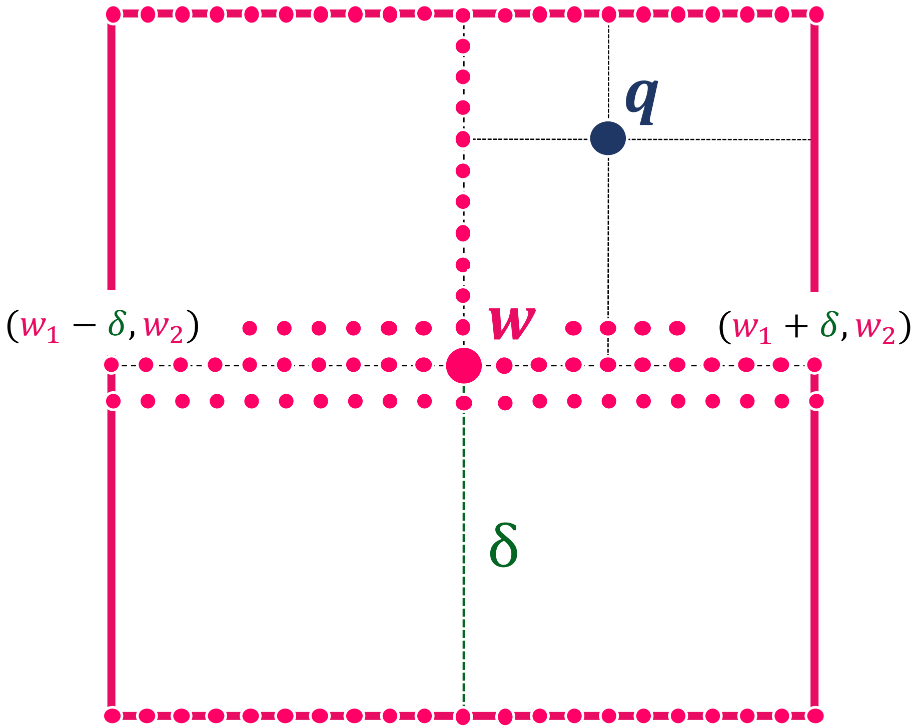
Fuzzy Matching for ℓ_∞



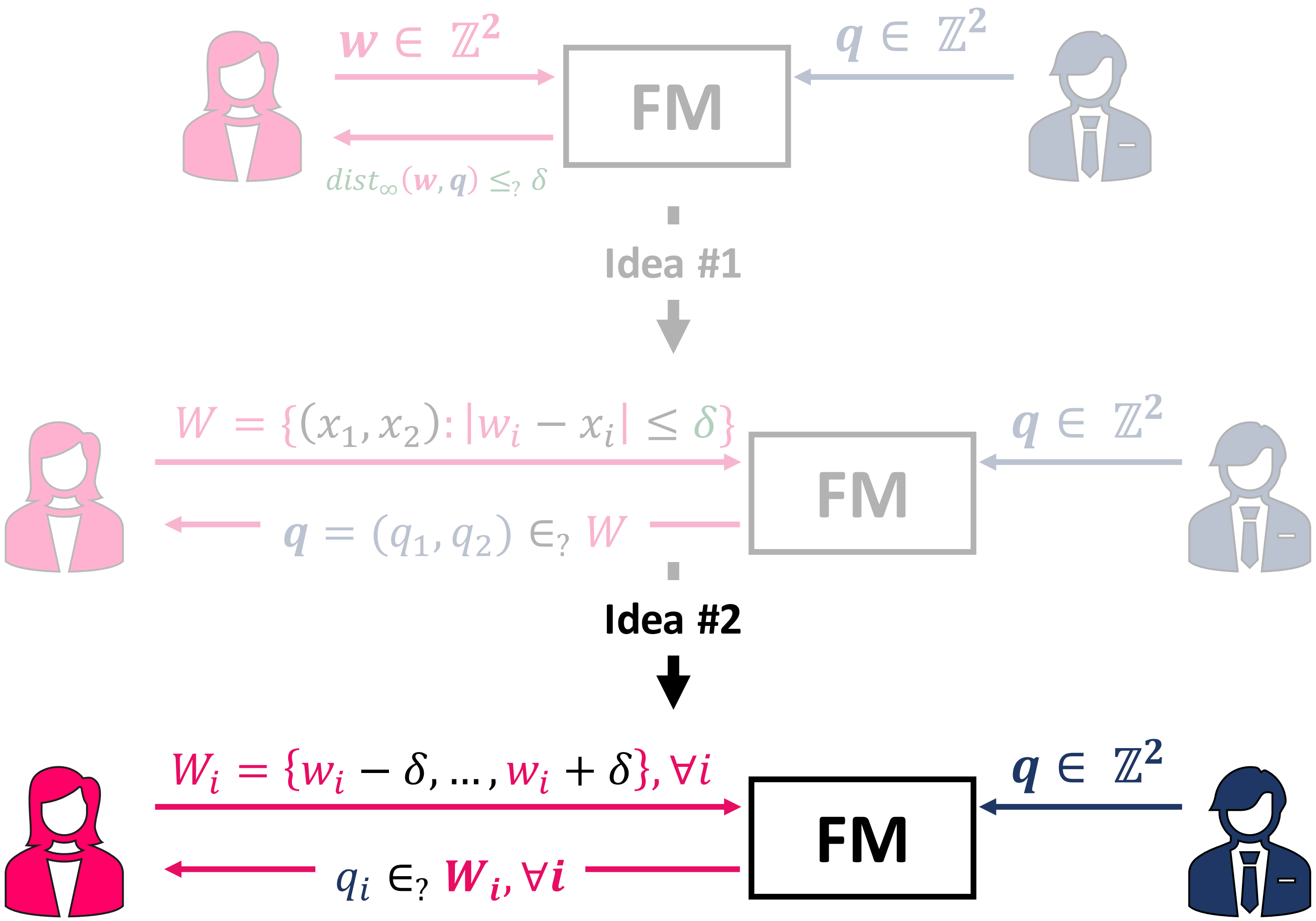


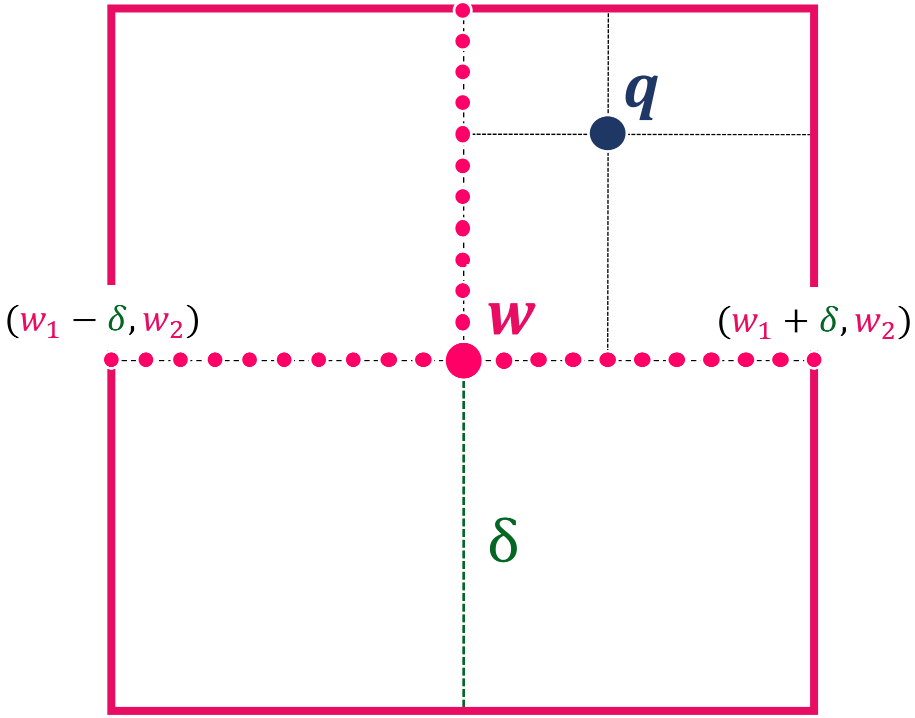
Fuzzy Matching for ℓ_∞



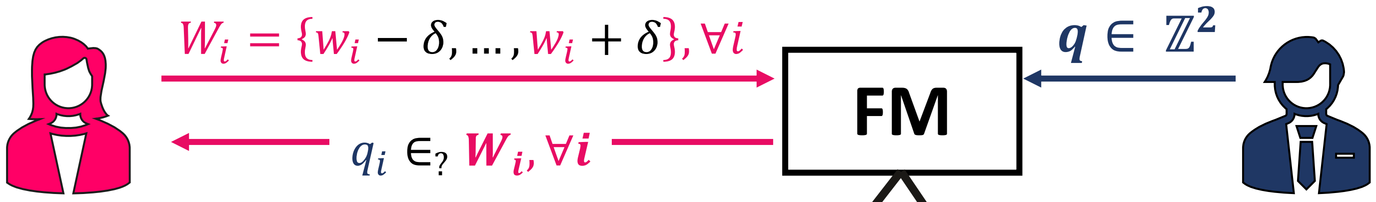


Fuzzy Matching for ℓ_∞





Fuzzy Matching for $\ell_{p,\, p \in [1,\infty]}$ (from [vBP24])



Additive Homomorphic Encryption

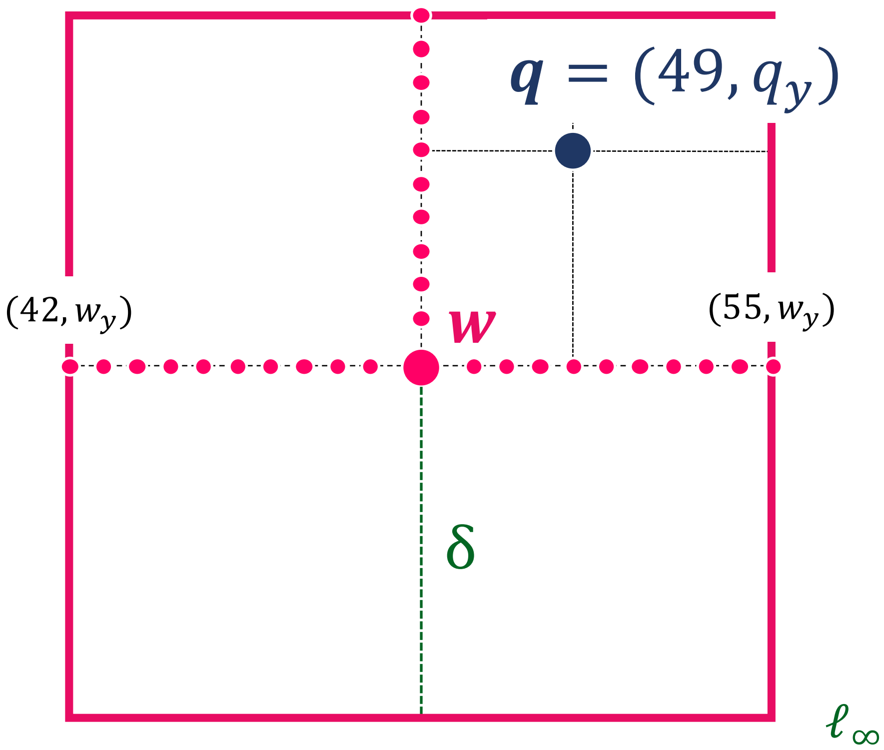
	ℓ_∞	$\ell_{p, p \in [1,\infty)}$
Total Comm.:	$\sim O(\delta d)$	$\sim O(\delta d + \underline{\delta^{p}})$
Alice's Comp.:	$\sim O(\delta d)$	$\sim O(\delta d)$
Bob's Comp.:	$\sim O(d)$	$\sim O(d + \underline{\delta^{p}})$

Geometric Fuzzy Matching

(Geometric) Fuzzy Matching for ℓ_∞ (GFM$_\infty$)

Goal: Get more efficient Fuzzy Matching for the ℓ_∞ distance.

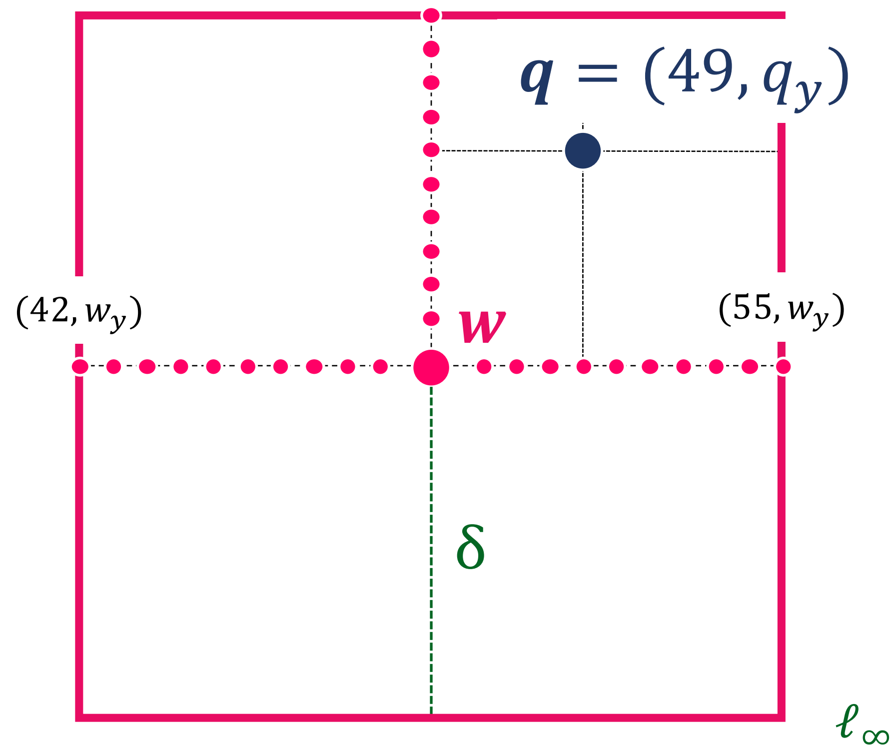
How?



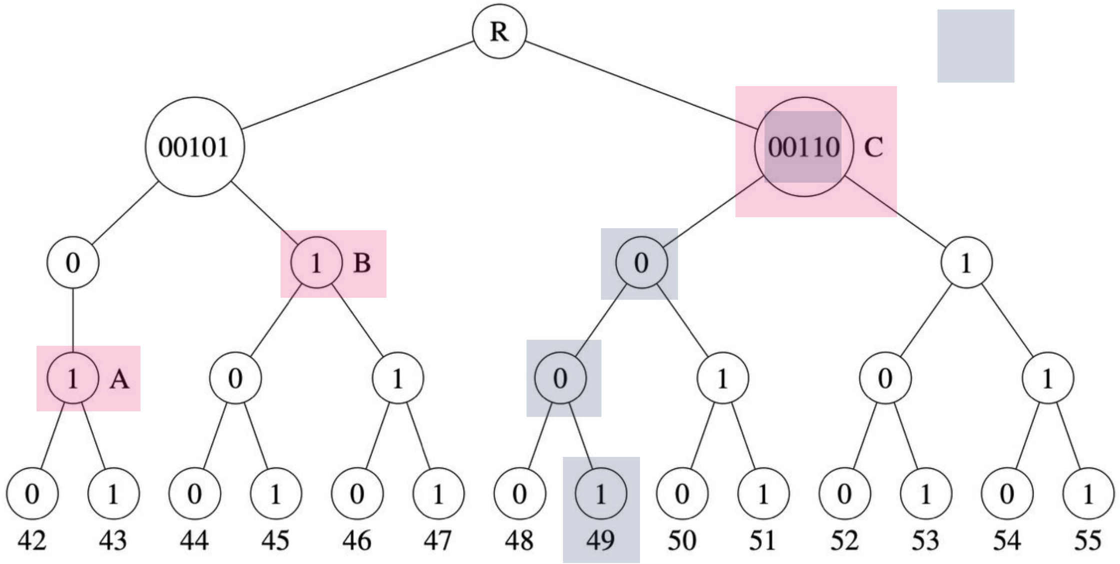
(Geometric) Fuzzy Matching for ℓ_∞ (GFM$_\infty$)

Goal: Get more efficient Fuzzy Matching for the ℓ_∞ distance.

How? FM from [VP24] **+ Distance-Aware Set Augmentation** technique [CRS23]



Represent interval $[w-\delta, w+\delta]$ with $O(\log\delta)$ strings



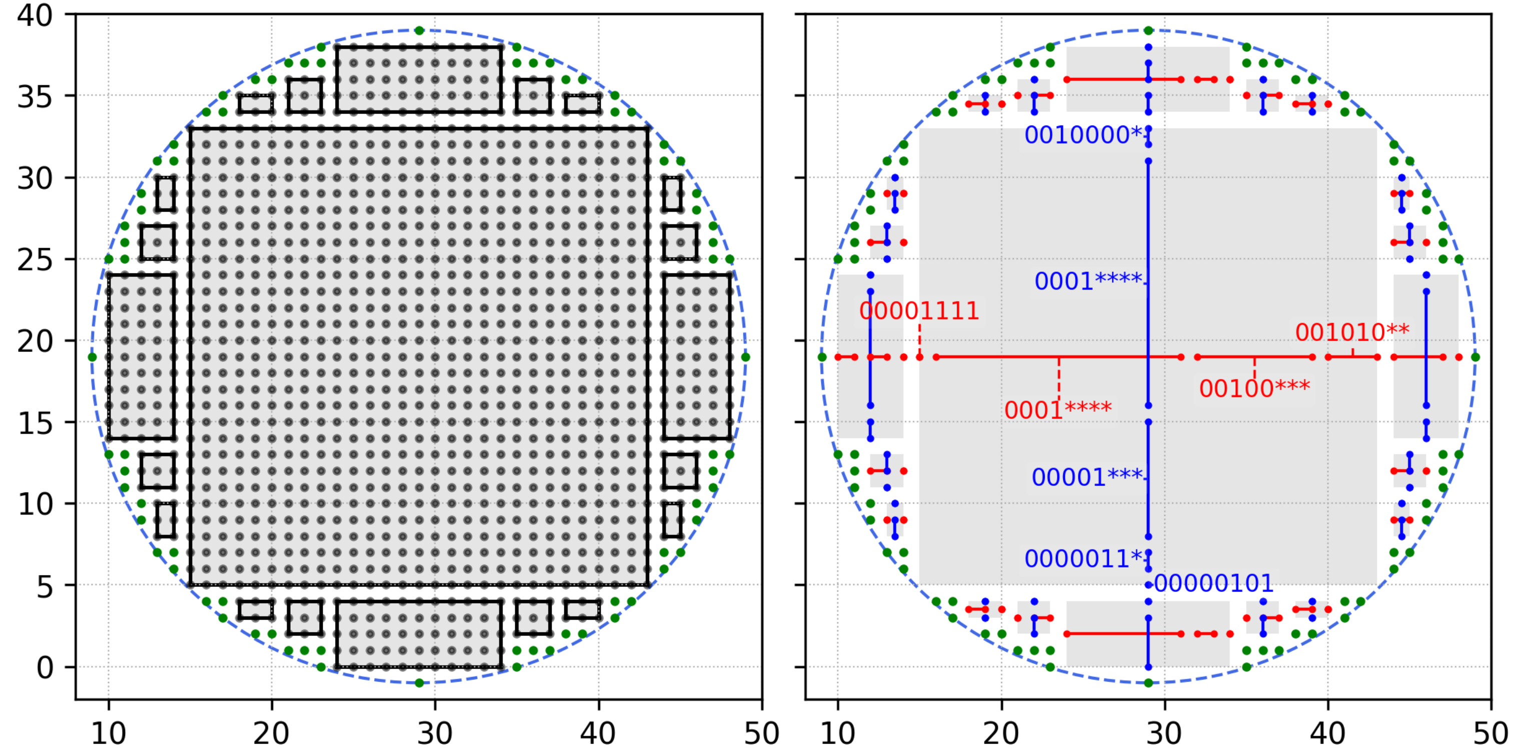
$[42,55] \leftrightarrow \{0010101*, 001011**, 00110***\}$

$49 \leftrightarrow \{00110001, 0011000*, 001100**, 00110***, 0011****\}$

Geometric Fuzzy Matching

Goal: Think geometrically! Get expressive Fuzzy Matching for any region.

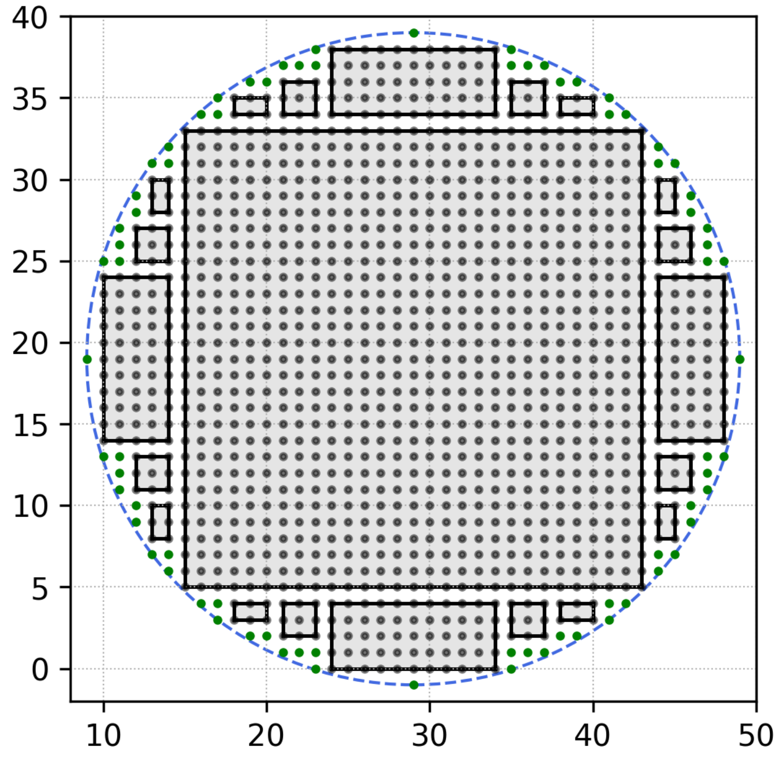
How? GFM_∞ + Partitioning Algorithms

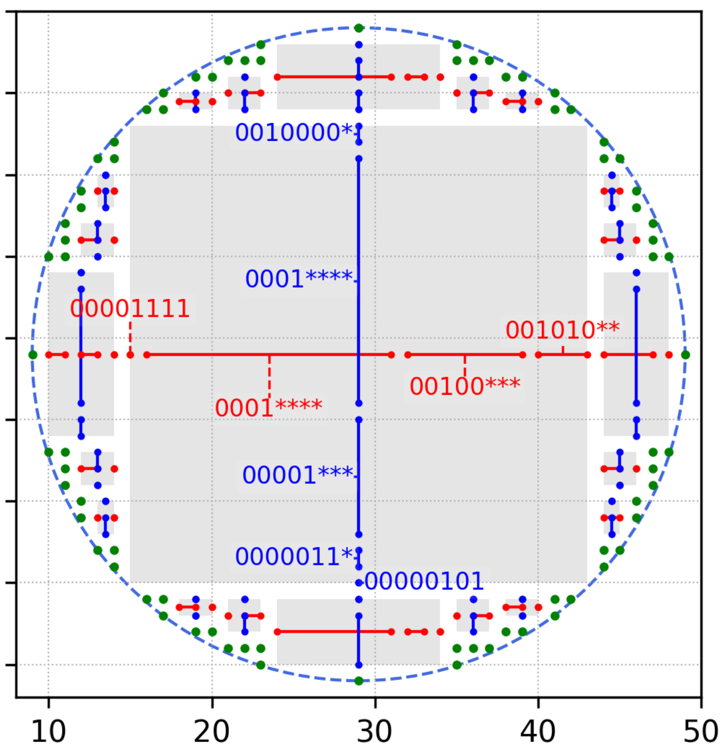


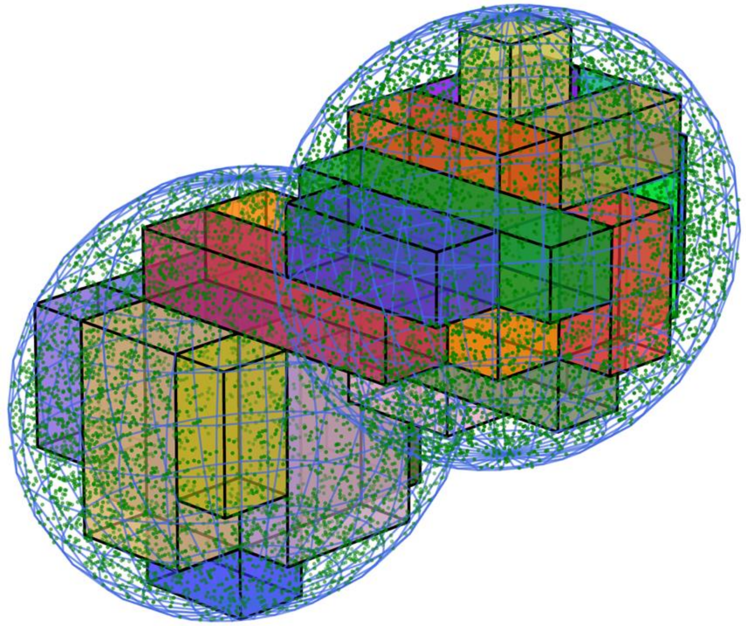
Geometric Fuzzy Matching

Goal: Think geometrically! Get expressive Fuzzy Matching for any region.

How? GFM_{∞} + Partitioning Algorithms







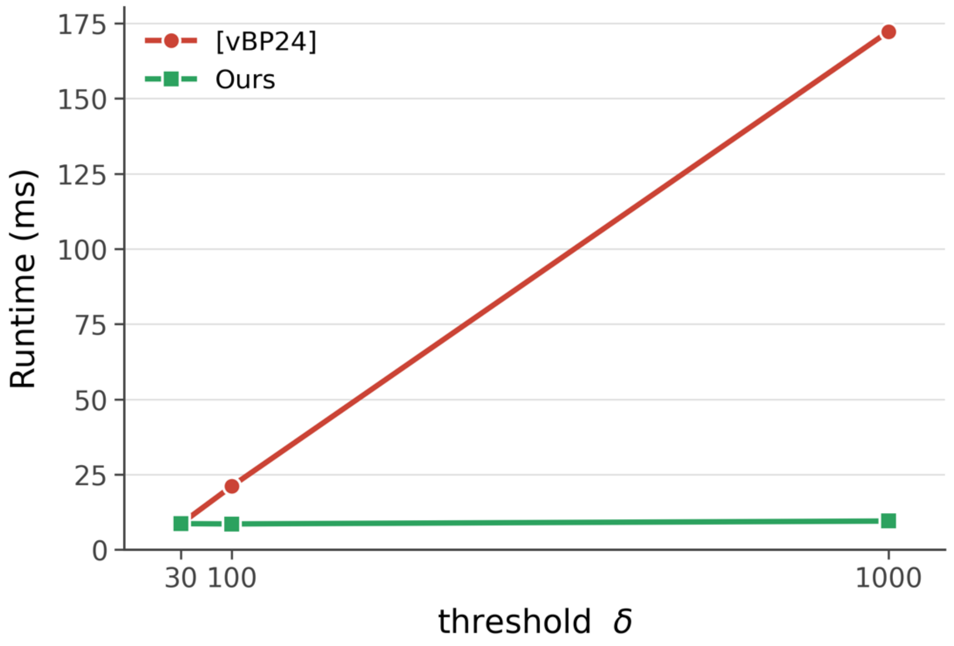
GFM$_\infty$ – Complexities & Comparison

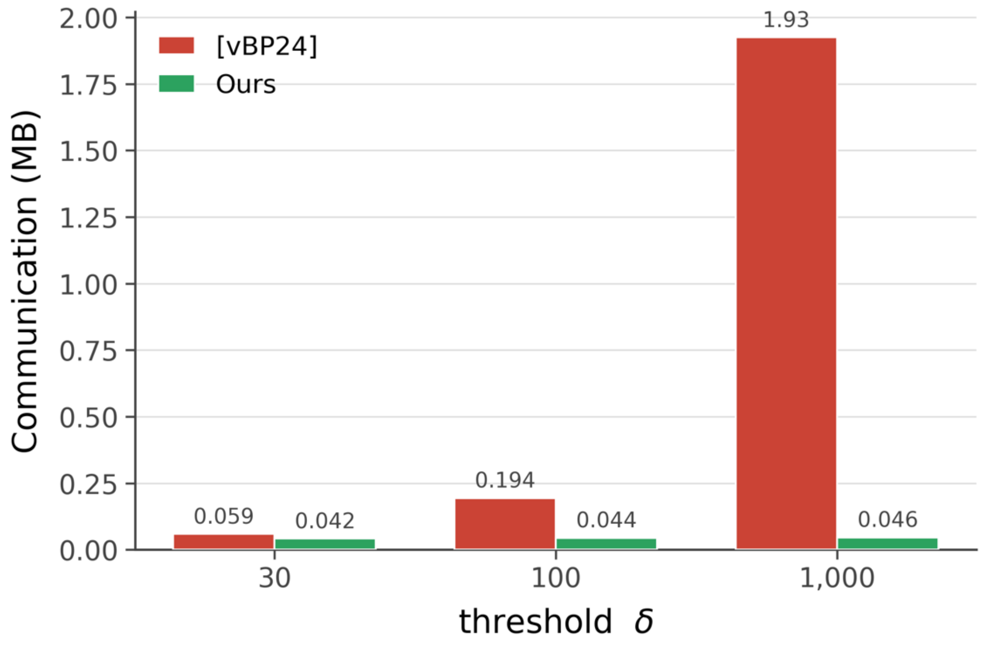
ℓ_∞	Total Communication	Receiver's Computations	Sender's Computations
[vBP24]	$O(\delta d)$	$O(\delta d)$	$O(d)$
Ours	$O(2\delta \log \delta + \log^{d} \delta)$	$O(2\delta \log \delta + \log^{d} \delta)$	$O(d \log^{d} \delta)$

GFM_∞ – Complexities & Comparison

ℓ_∞	Total Communication	Receiver's Computations	Sender's Computations
[vBP24]	$O(\delta d)$	$O(\delta d)$	$O(d)$
Ours	$O(2\delta \log \delta + \log^{d} \delta)$	$O(2\delta \log \delta + \log^{d} \delta)$	$O(d \log^{d} \delta)$

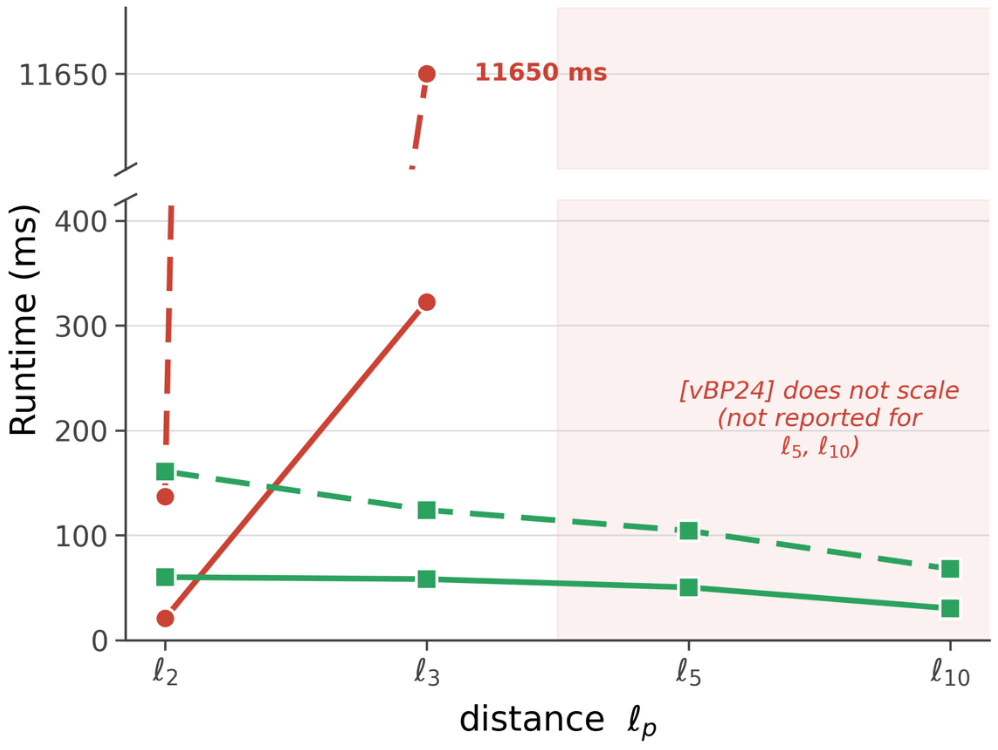
$\boldsymbol{d = 2}$

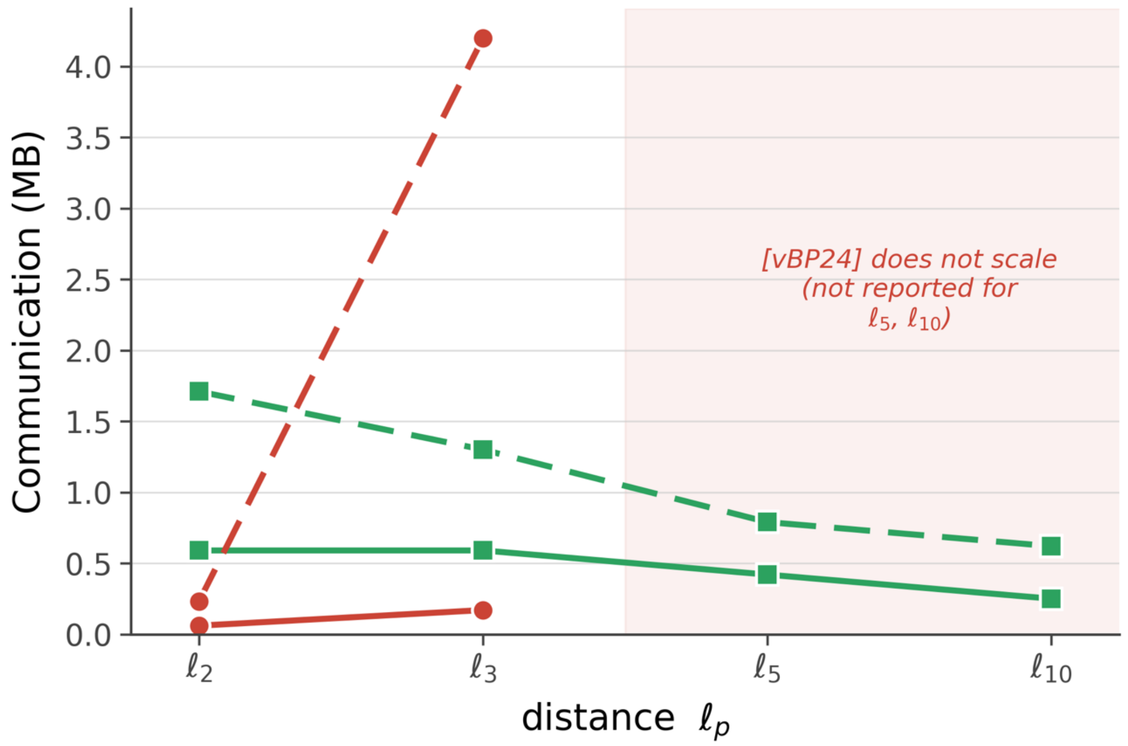




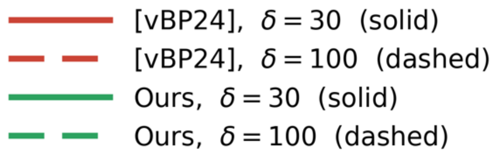
GFM – Complexities & Comparison

$d = 2$





- Benchmarks for ℓ_p are representative of our framework's behavior across different geometric regions.



Nearby Friends' Discovery

Geometric Fuzzy Matching

Nearby Friends' Finder from GFM

DEMO 01

L_2 Distance Proximity

Alice sets her location and a matching radius δ. She sends Msg_1. Bob places himself and sees δ around him. Protocol reveals only inside/outside.

`Our Partitioner algorithm`

DEMO 02

2D Polygon Region

Alice draws any region on a map. Bob's point is tested privately. Draw any shape, drag Bob live.

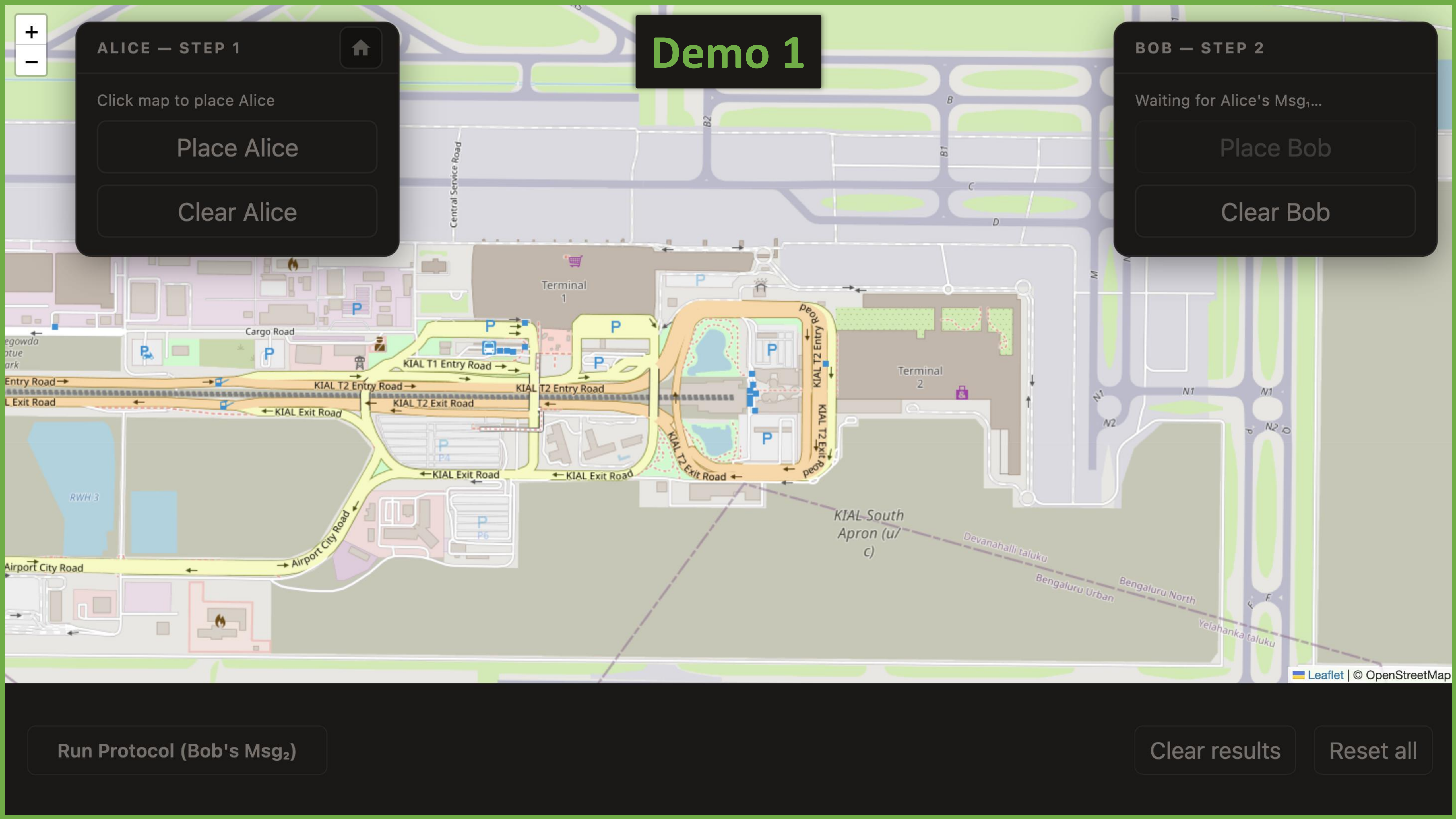
`Our Partitioner algorithm`

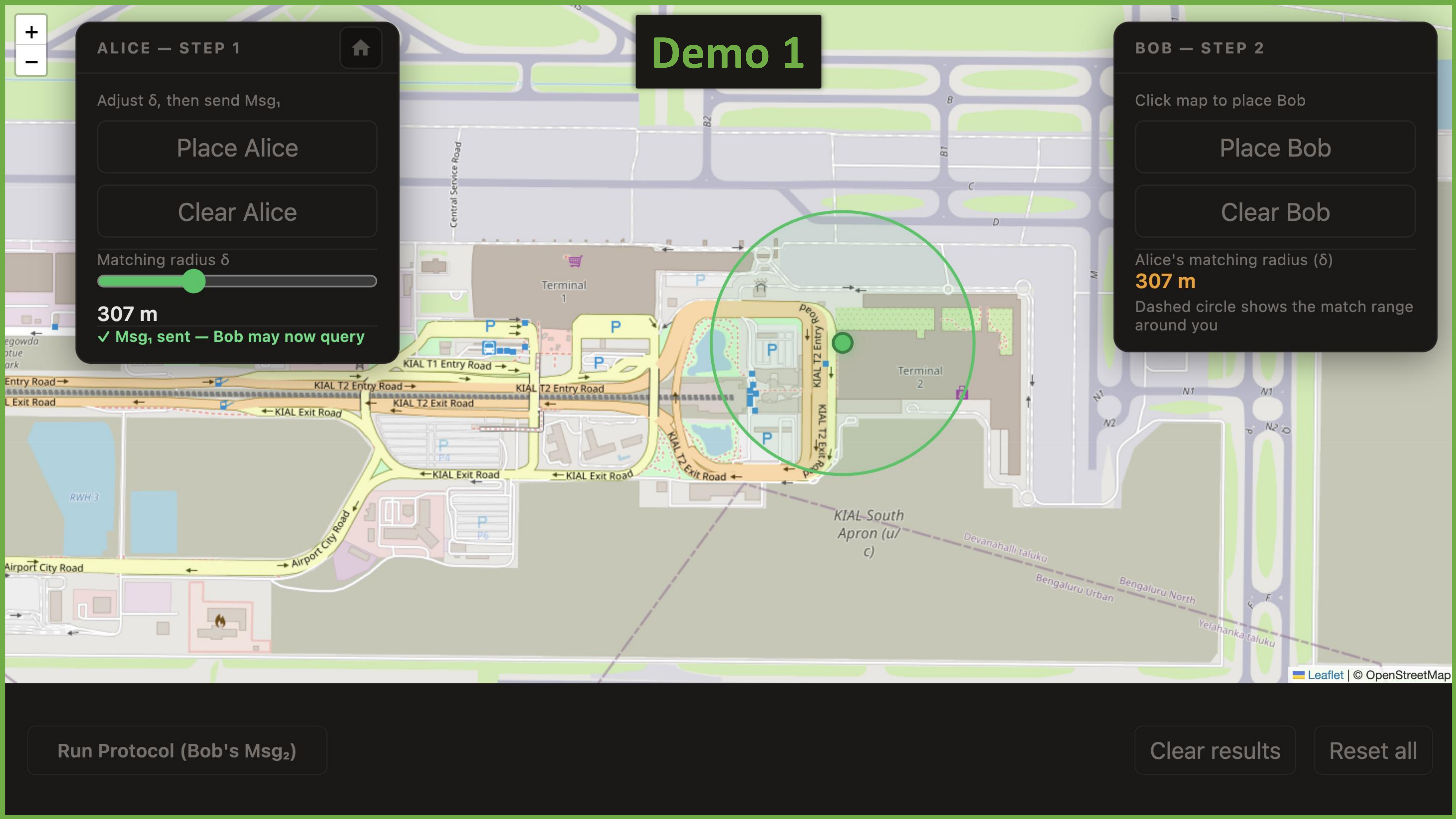
DEMO 03

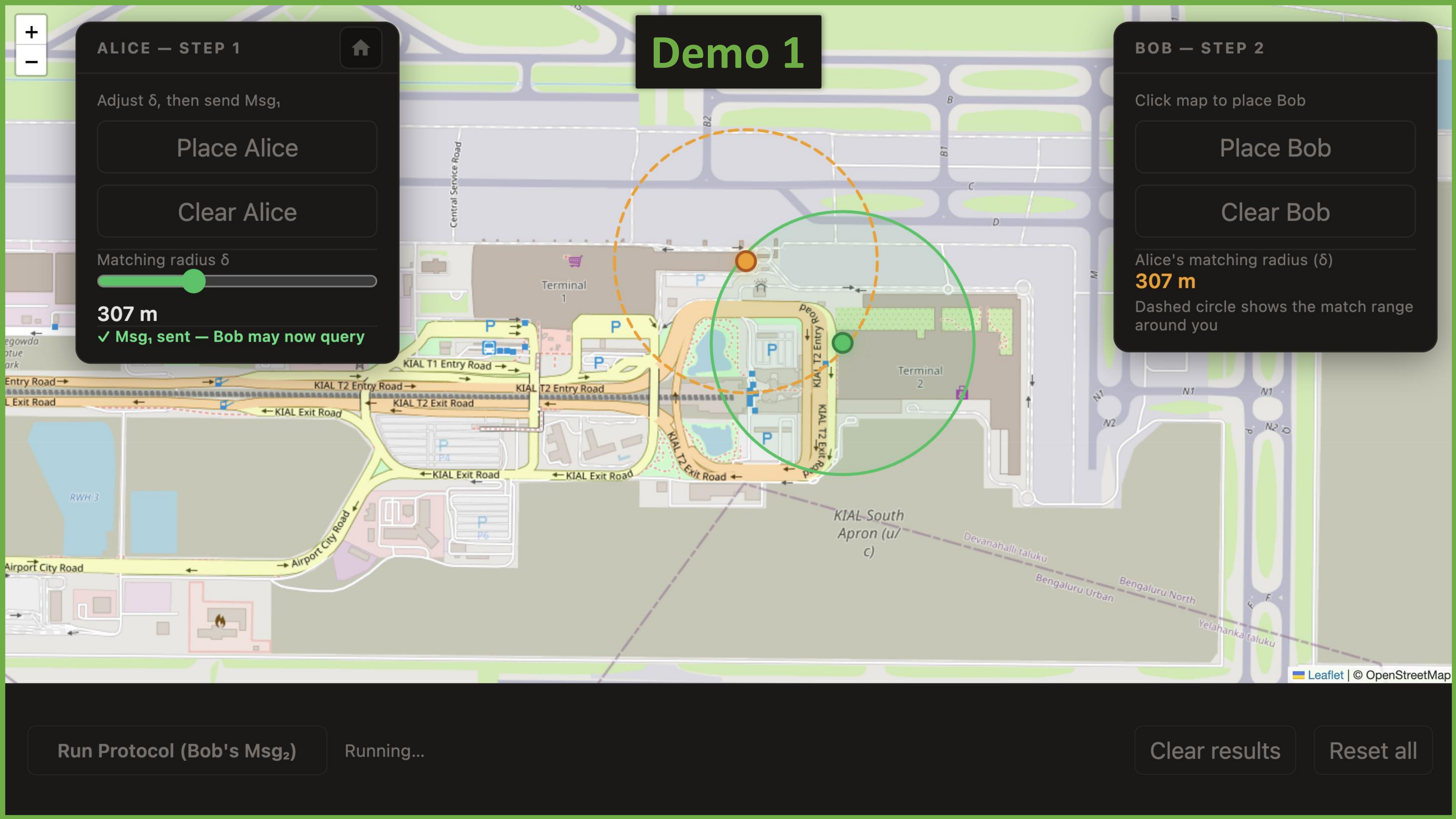
3D Building (Indoor)

Alice authorizes a full floor of Skybridge Campus. Bob is placed in any room.

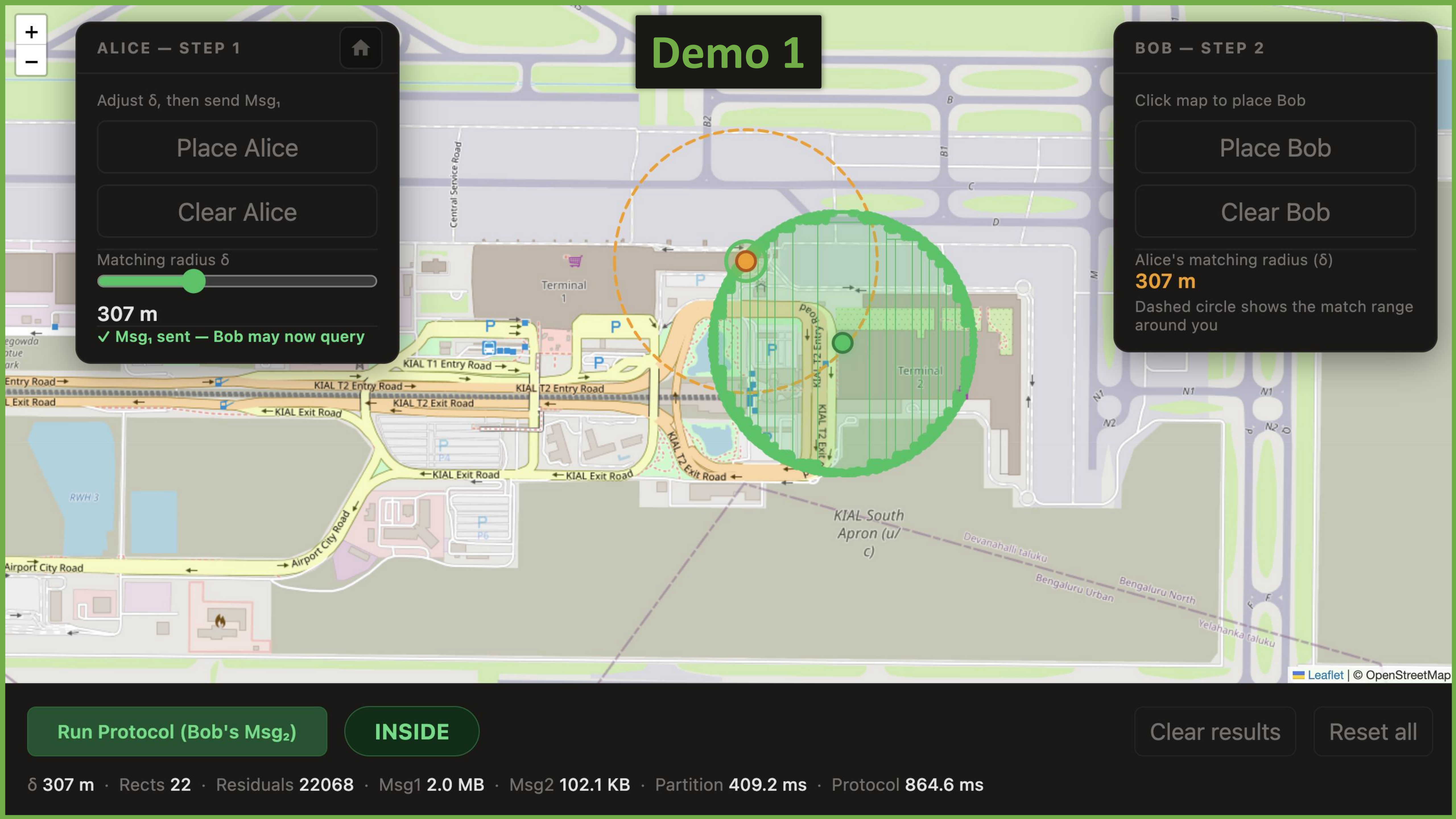
`Composite hyperrectangle region (Holub et al.)`

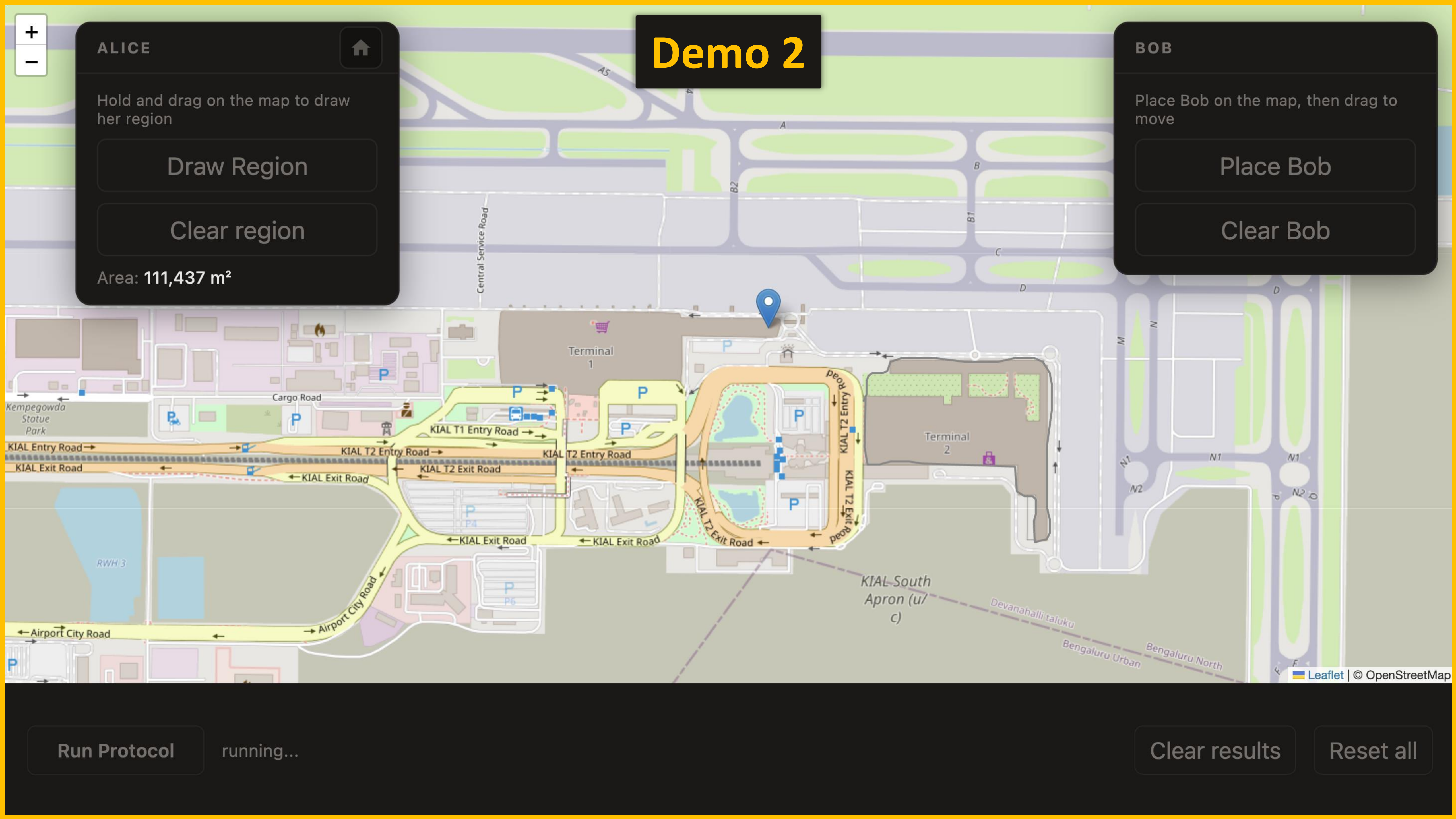

Demo 1
ALICE — STEP 1
Click map to place Alice
Place Alice
Clear Alice
BOB — STEP 2
Waiting for Alice's Msg$_1$...
Place Bob
Clear Bob
Terminal 1
Terminal 2
Cargo Road
Central Service Road
KIAL T1 Entry Road
KIAL T2 Entry Road
KIAL T2 Exit Road
KIAL Exit Road
Entry Road
Exit Road
Airport City Road
RWH 3
KIAL South Apron (u/c)
Devanahalli taluku
Bengaluru Urban
Bengaluru North
Yelahanka taluku
Leaflet | © OpenStreetMap
Run Protocol (Bob's Msg$_2$)
Clear results
Reset all

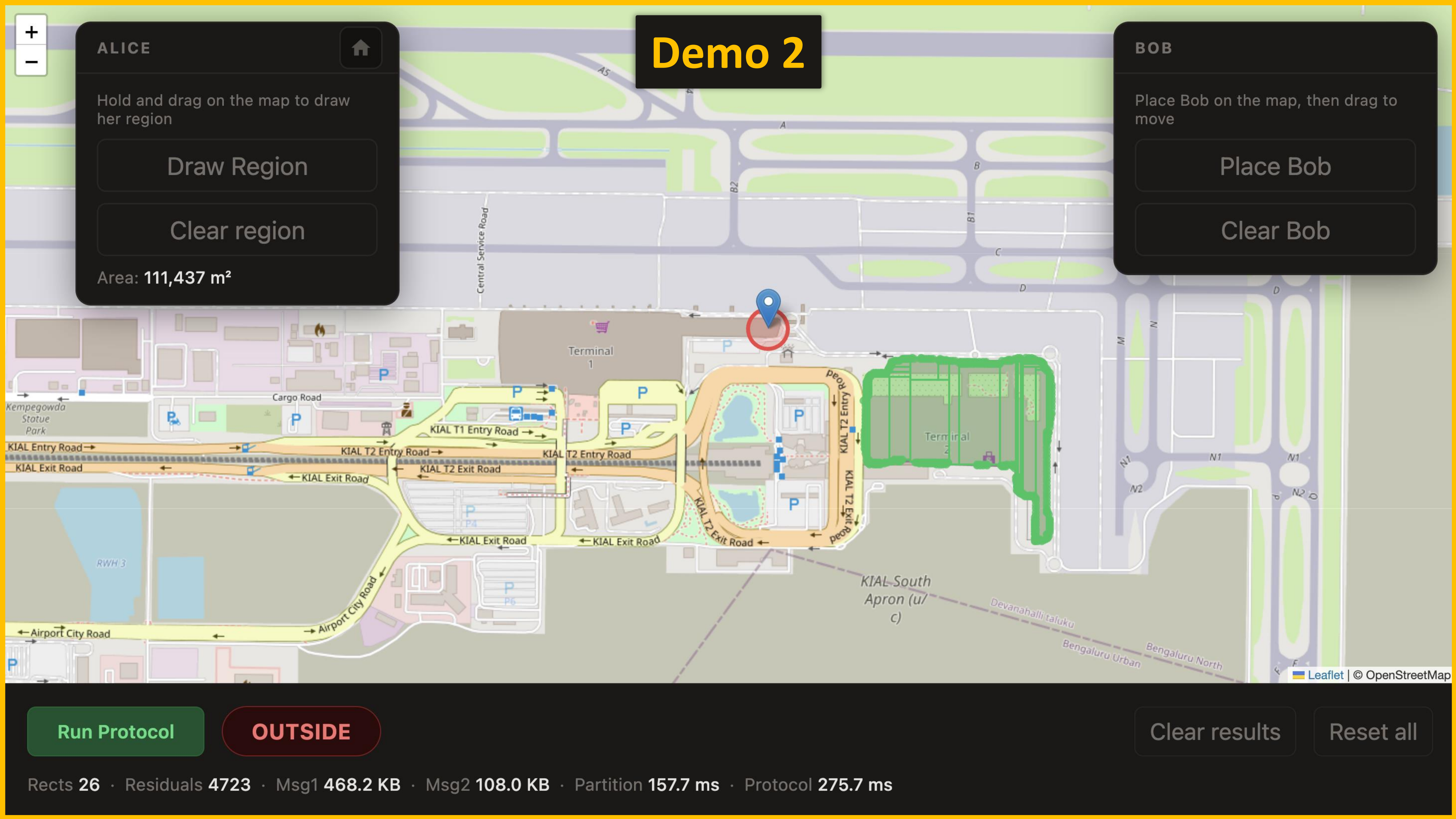

Demo 1
ALICE — STEP 1
Adjust δ, then send Msg₁
Place Alice
Clear Alice
Matching radius δ
307 m
✓ Msg₁ sent — Bob may now query
BOB — STEP 2
Click map to place Bob
Place Bob
Clear Bob
Alice's matching radius (δ)
307 m
Dashed circle shows the match range around you
Terminal 1
Terminal 2
KIAL South Apron (u/c)
Run Protocol (Bob's Msg₂)
Clear results
Reset all
Leaflet | © OpenStreetMap



Demo 1
ALICE — STEP 1
Adjust δ, then send Msg₁
Place Alice
Clear Alice
Matching radius δ
307 m
✓ Msg₁ sent — Bob may now query
BOB — STEP 2
Click map to place Bob
Place Bob
Clear Bob
Alice's matching radius (δ)
307 m
Dashed circle shows the match range around you
Terminal 1
Terminal 2
KIAL T1 Entry Road
KIAL T2 Entry Road
KIAL T2 Exit Road
KIAL Exit Road
KIAL T2 Entry Road
KIAL T2 Exit Road
Central Service Road
Airport City Road
KIAL South Apron (u/c)
Devanahalli taluku
Bengaluru Urban
Bengaluru North
Yelahanka taluku
RWH 3
Leaflet | © OpenStreetMap
Run Protocol (Bob's Msg₂)
Running...
Clear results
Reset all


Demo 1
ALICE — STEP 1
Adjust δ, then send Msg₁
Place Alice
Clear Alice
Matching radius δ
307 m
✓ Msg₁ sent — Bob may now query
BOB — STEP 2
Click map to place Bob
Place Bob
Clear Bob
Alice's matching radius (δ)
307 m
Dashed circle shows the match range around you
Terminal 1
Terminal 2
KIAL T1 Entry Road
KIAL T2 Entry Road
KIAL T2 Exit Road
KIAL Exit Road
Central Service Road
Airport City Road
KIAL South Apron (u/c)
Devanahalli taluku
Bengaluru Urban
Bengaluru North
Yelahanka taluku
RWH 3
Leaflet | © OpenStreetMap
Run Protocol (Bob's Msg₂)
INSIDE
Clear results
Reset all
δ 307 m · Rects 22 · Residuals 22068 · Msg1 2.0 MB · Msg2 102.1 KB · Partition 409.2 ms · Protocol 864.6 ms


Demo 2
ALICE
Hold and drag on the map to draw her region
Draw Region
Clear region
Area: 111,437 m²
BOB
Place Bob on the map, then drag to move
Place Bob
Clear Bob
Run Protocol
running...
Clear results
Reset all
Terminal 1
Terminal 2
Cargo Road
Central Service Road
Kempegowda Statue Park
KIAL Entry Road
KIAL Exit Road
KIAL T1 Entry Road
KIAL T2 Entry Road
KIAL T2 Exit Road
Airport City Road
KIAL South Apron (u/c)
Devanahalli taluku
Bengaluru Urban
Bengaluru North
RWH 3
Leaflet | © OpenStreetMap


Demo 2
ALICE
Hold and drag on the map to draw her region
Draw Region
Clear region
Area: 111,437 m²
BOB
Place Bob on the map, then drag to move
Place Bob
Clear Bob
Terminal 1
Terminal 2
Cargo Road
Central Service Road
Kempegowda Statue Park
KIAL Entry Road
KIAL Exit Road
KIAL T1 Entry Road
KIAL T2 Entry Road
KIAL T2 Exit Road
Airport City Road
KIAL South Apron (u/c)
Devanahalli taluku
Bengaluru Urban
Bengaluru North
RWH 3
Leaflet | © OpenStreetMap
Run Protocol
OUTSIDE
Clear results
Reset all
Rects 26 · Residuals 4723 · Msg1 468.2 KB · Msg2 108.0 KB · Partition 157.7 ms · Protocol 275.7 ms

Demo 3
ALICE
Authorized floor -- all rooms included
Choose a floor...
No floor selected
BOB
Floor
Choose a floor...
Room (placed at center)
Select a floor first
No position set
Run Protocol
Clear & Reset


Demo 3
ALICE
Authorized floor -- all rooms included
F2
F2 -- 8 rooms -- 13,600 m²
BOB
Floor
Choose a floor...
Room (placed at center)
Select a floor first
No position set
Run Protocol
Clear & Reset


Demo 3
ALICE
Authorized floor -- all rooms included
F2
F2 -- 8 rooms -- 13,600 m²
BOB
Floor
F4
Room (placed at center)
Observatory B
F4 -- Observatory B
Run Protocol
Clear & Reset
OUTSIDE
Done.
Rects 3 · Residuals 0 · Msg1 11.7 KB · Msg2 27.6 KB · Partition 0 ms · Protocol 81 ms

Conclusion and Future Work

Efficient FM for ℓ_∞ in low dimensions

Novel partitioning algorithms

Our Results

Geometric Fuzzy Matching

new primitive for arbitrary geometric region membership

Privacy-Preserving Proximity Testing for complex layouts

Conclusion and Future Work

Our Results

Efficient FM for ℓ_∞ in low dimensions

Novel partitioning algorithms

Geometric Fuzzy Matching

new primitive for arbitrary geometric region membership

Privacy-Preserving Proximity Testing for complex layouts

Future Work

Dynamic environments for moving entities

Full hiding of *region layout* from the sender

Support for repeated queries

Conclusion and Future Work

Our Results

Efficient FM for ℓ_∞ in low dimensions — Novel partitioning algorithms

Geometric Fuzzy Matching

new primitive for arbitrary geometric region membership

Privacy-Preserving Proximity Testing for complex layouts

Future Work

Dynamic environments for moving entities

Full hiding of *region layout* from the sender

Support for repeated queries

Thank you!