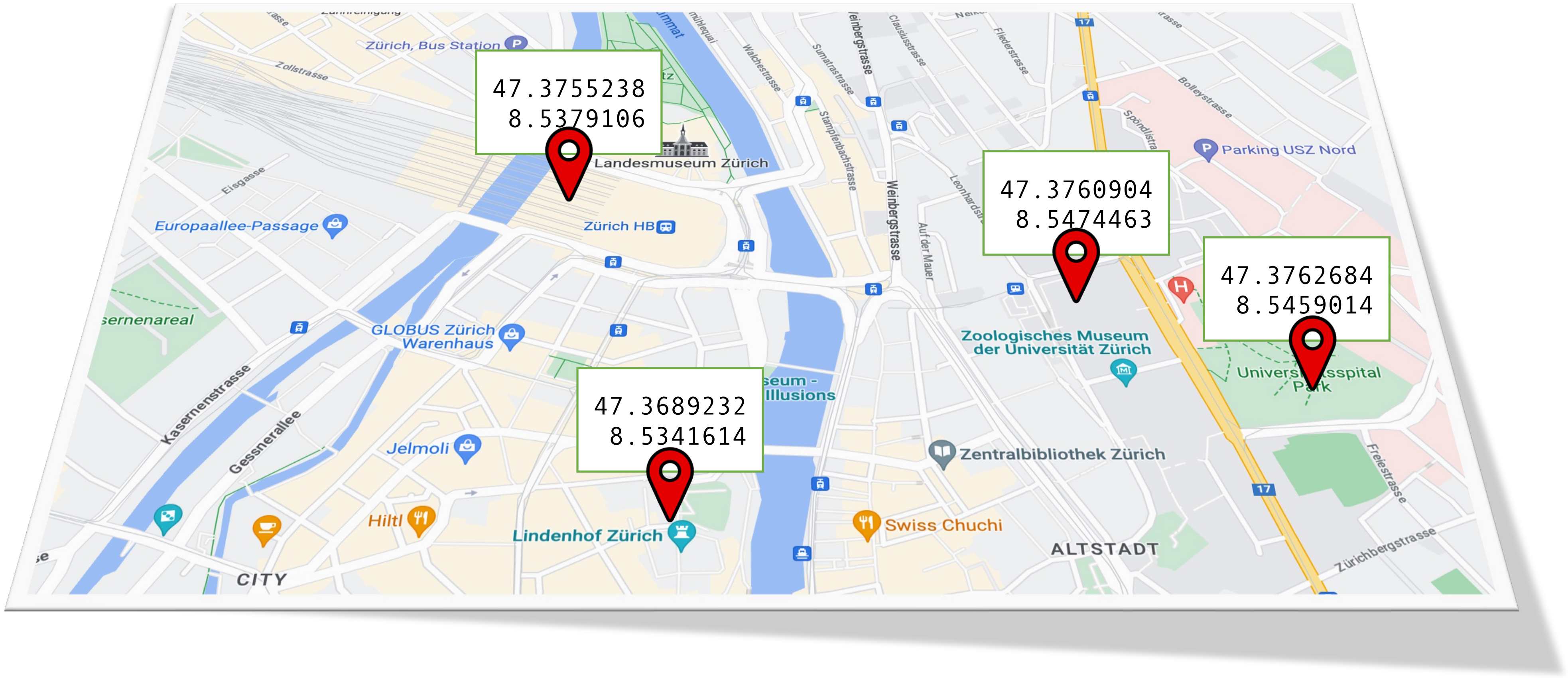
Multidimensional Approximate Agreement with Asynchronous Fallback

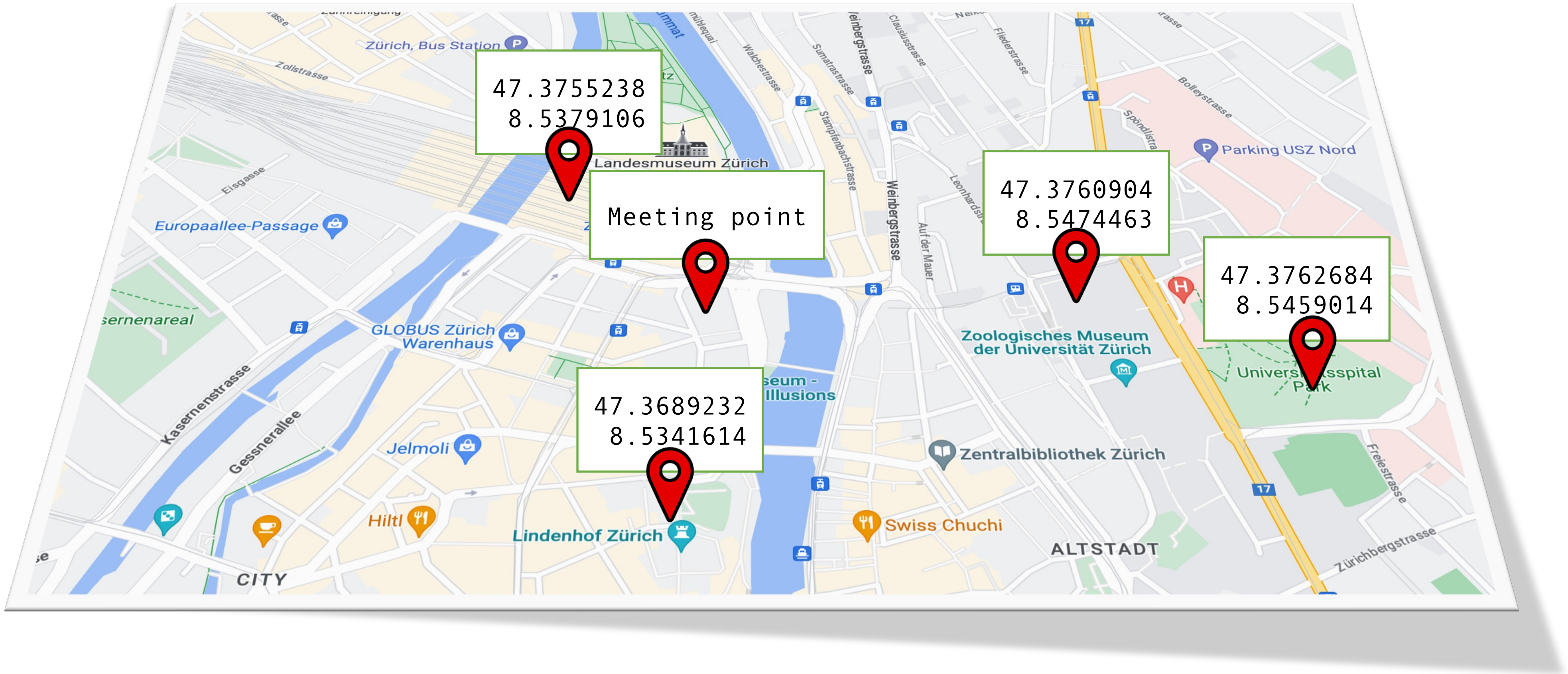
Diana Ghinea[1] Chen-Da Liu-Zhang[2] Roger Wattenhofer[1]

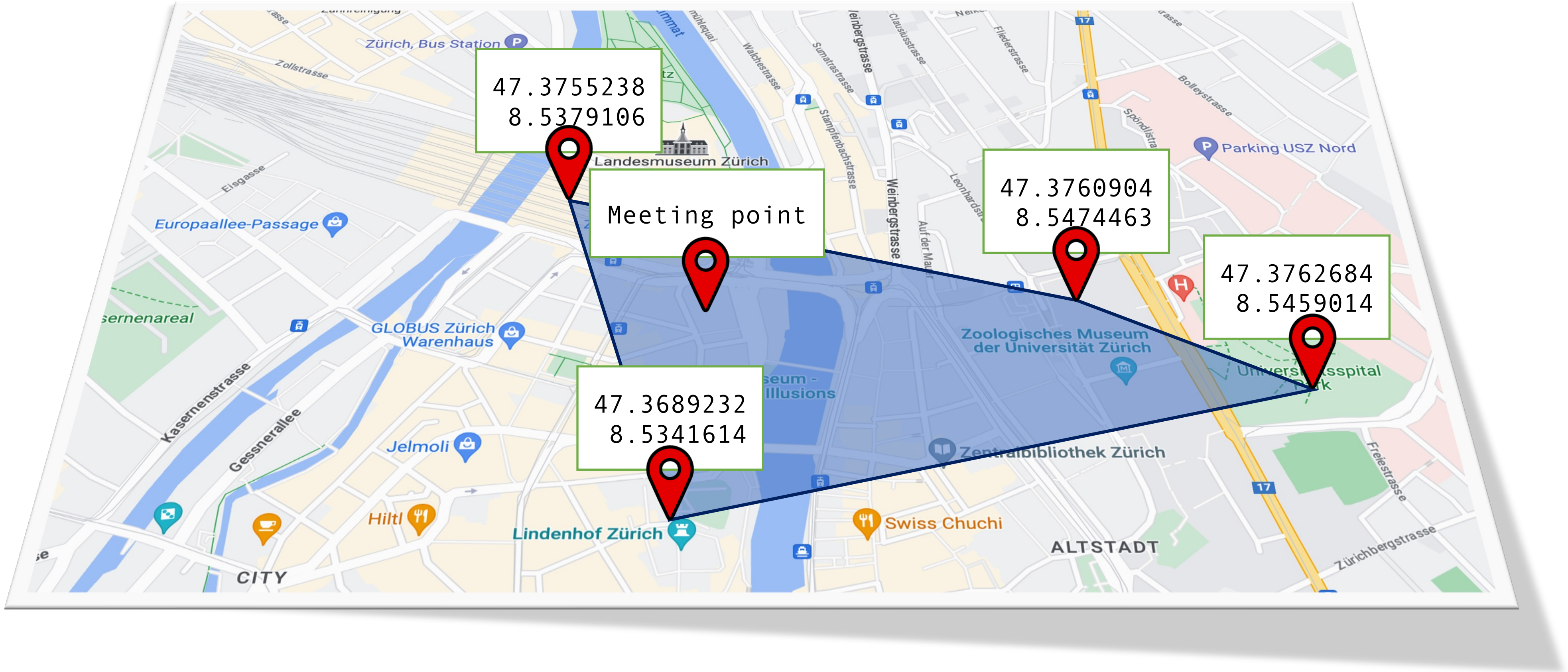
[1]ETH Zürich

[2]NTT Research

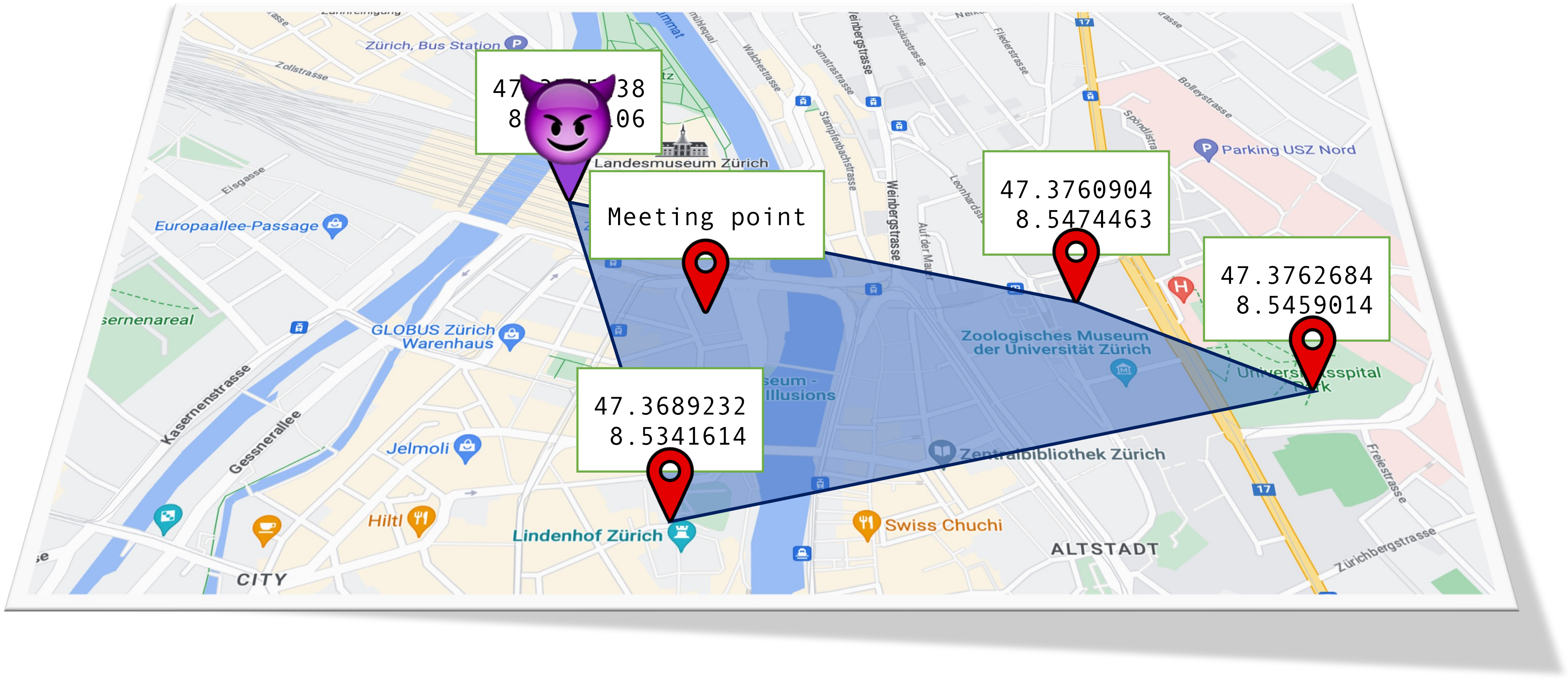


47.3755238
8.5379106
47.3760904
8.5474463
47.3762684
8.5459014
47.3689232
8.5341614
Zürich, Bus Station
Zollstrasse
Landesmuseum Zürich
Zürich HB
Eisgasse
Europaallee-Passage
GLOBUS Zürich Warenhaus
Kasernenstrasse
Gessnerallee
Jelmoli
Hiltl
Lindenhof Zürich
CITY
Swiss Chuchi
ALTSTADT
Zentralbibliothek Zürich
Zoologisches Museum der Universität Zürich
Parking USZ Nord
Bolleystrasse
Weinbergstrasse
Zürichbergstrasse

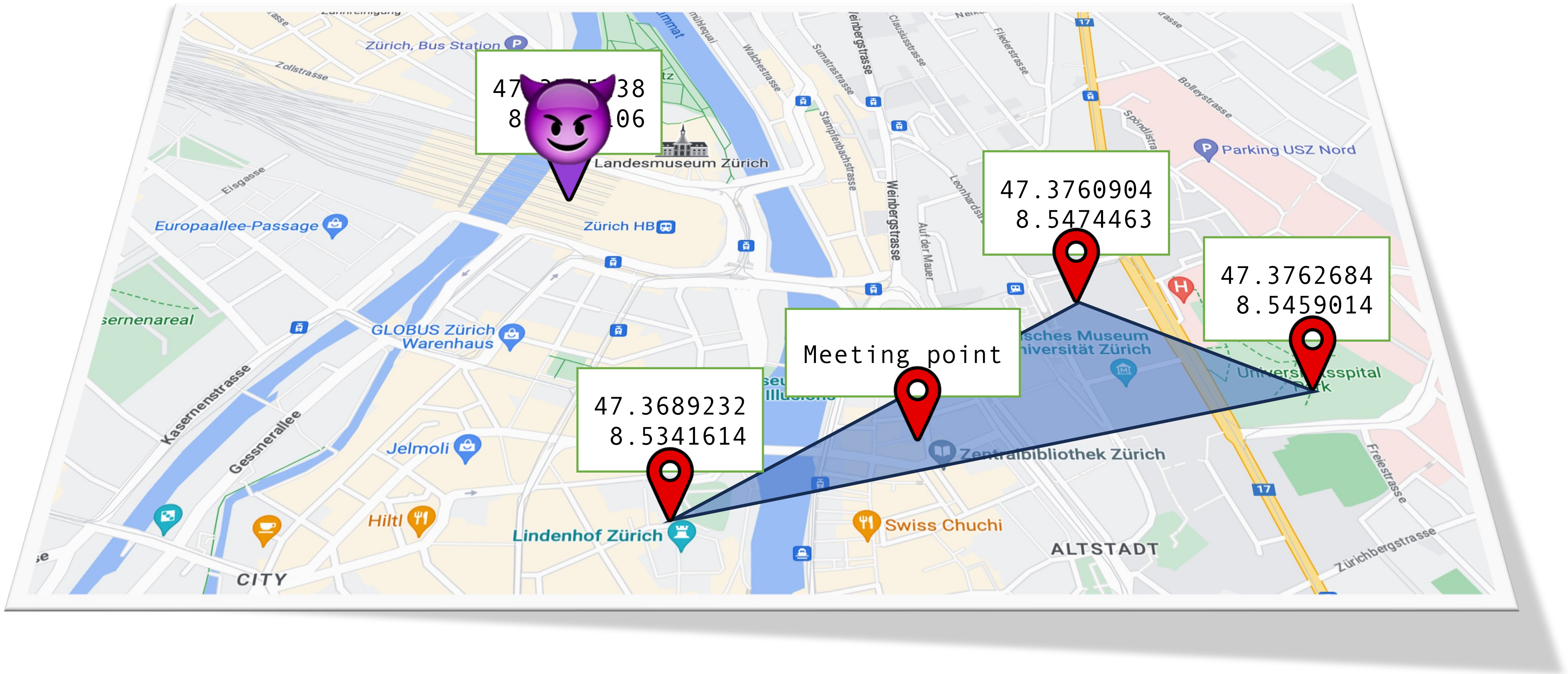

47.3755238
8.5379106
Meeting point
47.3760904
8.5474463
47.3762684
8.5459014
47.3689232
8.5341614
Zürich, Bus Station
Landesmuseum Zürich
Europaallee-Passage
GLOBUS Zürich Warenhaus
Jelmoli
Hiltl
Lindenhof Zürich
Swiss Chuchi
Zentralbibliothek Zürich
Zoologisches Museum der Universität Zürich
Parking USZ Nord
ALTSTADT
CITY
Kasernenstrasse
Gessnerallee
Weinbergstrasse
Zürichbergstrasse



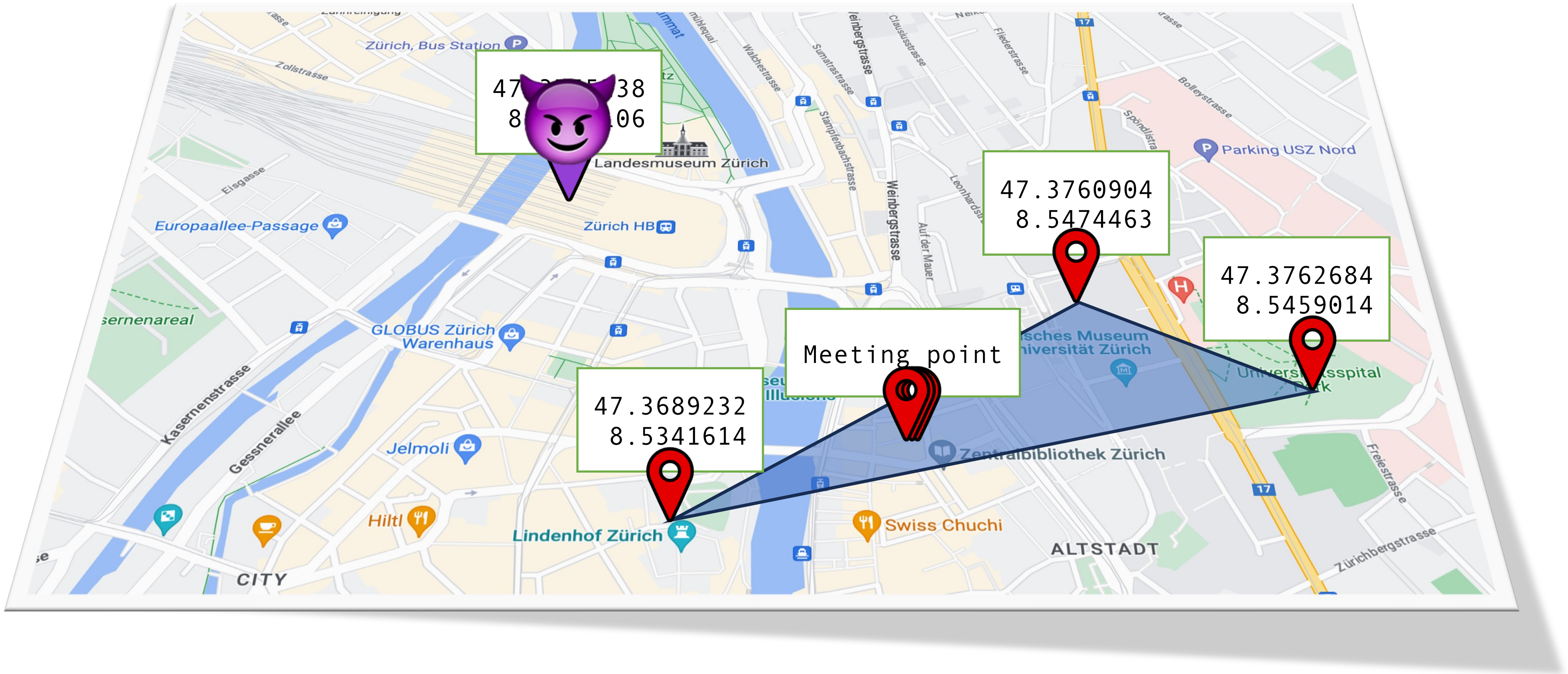
47.3755238
8.5379106
Meeting point
47.3760904
8.5474463
47.3762684
8.5459014
47.3689232
8.5341614
Zürich, Bus Station
Zollstrasse
Landesmuseum Zürich
Europaallee-Passage
GLOBUS Zürich
Warenhaus
Jelmoli
Hiltl
Lindenhof Zürich
Swiss Chuchi
Zentralbibliothek Zürich
Zoologisches Museum
der Universität Zürich
Parking USZ Nord
ALTSTADT
CITY
Kasernenstrasse
Gessnerallee
Weinbergstrasse
Zürichbergstrasse
Freiestrasse



Meeting point
47.3760904
8.5474463
47.3762684
8.5459014
47.3689232
8.5341614
Zürich, Bus Station
Zollstrasse
Landesmuseum Zürich
Europaallee-Passage
GLOBUS Zürich Warenhaus
Jelmoli
Hiltl
Lindenhof Zürich
Swiss Chuchi
Zentralbibliothek Zürich
Zoologisches Museum der Universität Zürich
Parking USZ Nord
ALTSTADT
CITY
Kasernenstrasse
Gessnerallee
Weinbergstrasse
Zürichbergstrasse
Bolleystrasse



47.3760904
8.5474463
47.3762684
8.5459014
Meeting point
47.3689232
8.5341614
Zürich, Bus Station
Zollstrasse
Landesmuseum Zürich
Eisgasse
Europaallee-Passage
Zürich HB
GLOBUS Zürich
Warenhaus
Kasernenstrasse
Gessnerallee
Jelmoli
Hiltl
Lindenhof Zürich
CITY
Swiss Chuchi
ALTSTADT
Zentralbibliothek Zürich
Parking USZ Nord
Bolleystrasse
Weinbergstrasse
Freiestrasse
Zürichbergstrasse



47.3760904
8.5474463
47.3762684
8.5459014
Meeting point
47.3689232
8.5341614
Zürich, Bus Station
Landesmuseum Zürich
Zürich HB
Europaallee-Passage
GLOBUS Zürich Warenhaus
Jelmoli
Hiltl
Lindenhof Zürich
Swiss Chuchi
Zentralbibliothek Zürich
ALTSTADT
CITY
Parking USZ Nord
Kasernenstrasse
Gessnerallee
Weinbergstrasse
Zürichbergstrasse

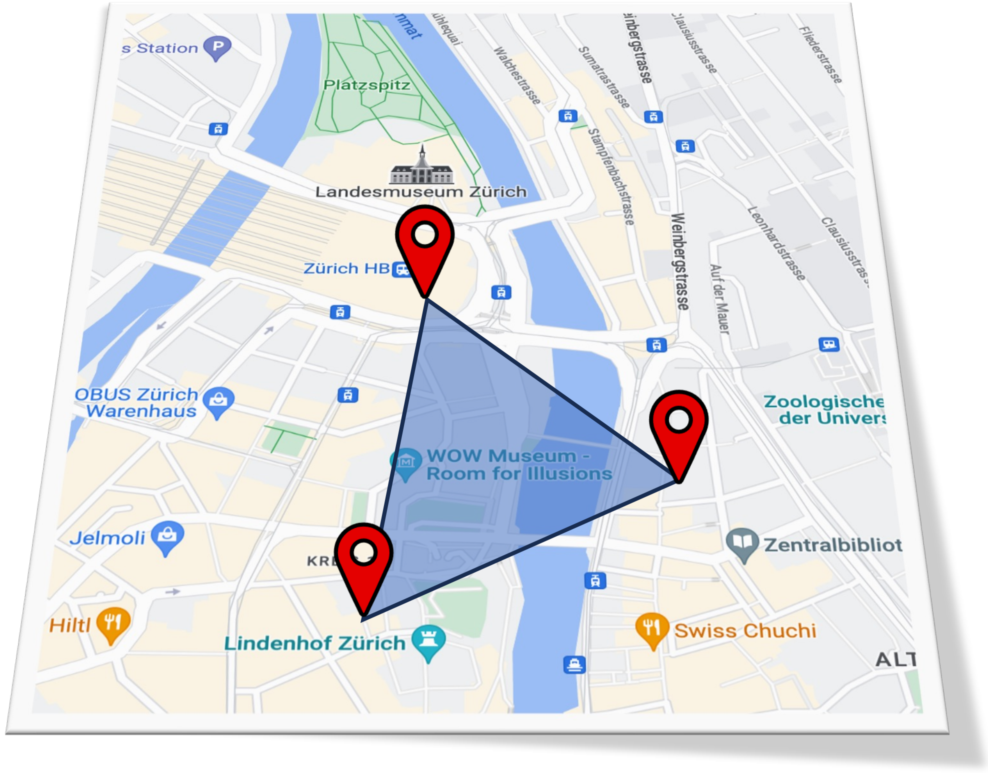
Multidimensional Approximate Agreement (***D-AA***)

Consider some $\mathcal{E} > 0$, and a setting of n parties holding inputs in $\mathbb{R}^D$.

Even when t of the n parties are Byzantine, honest parties obtain:

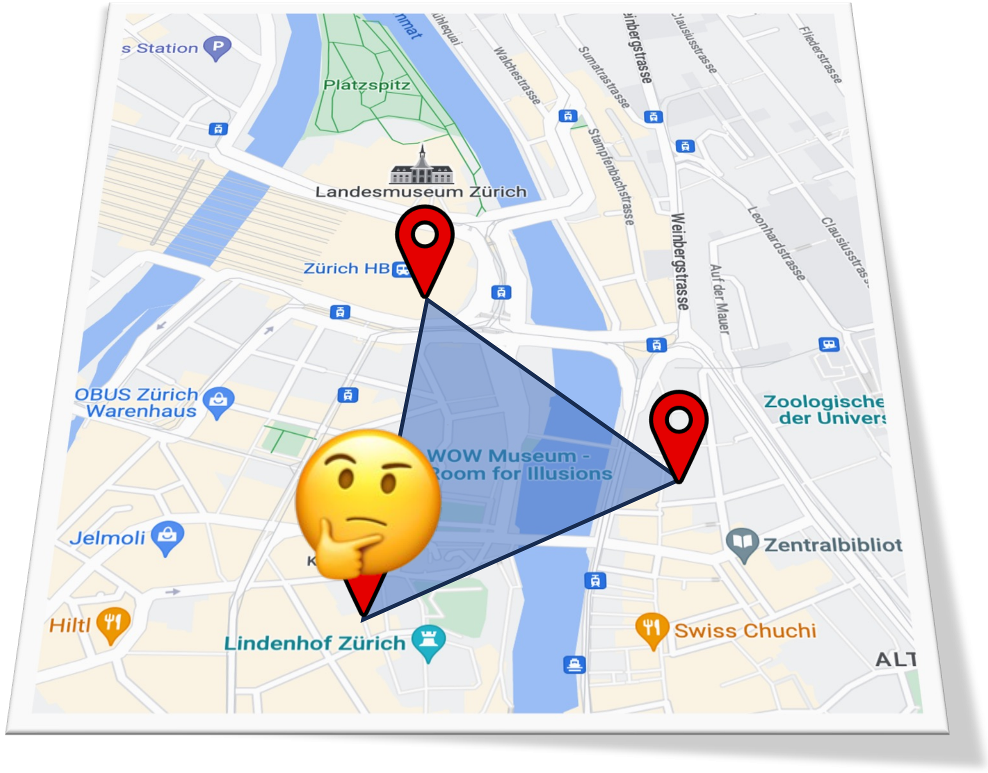
- $\mathcal{E}$-close outputs in $\mathbb{R}^D$ ($\mathcal{E}$-*Agreement*).
- That are in the convex hull of their inputs (*Validity*).

How many corruptions can be tolerated?



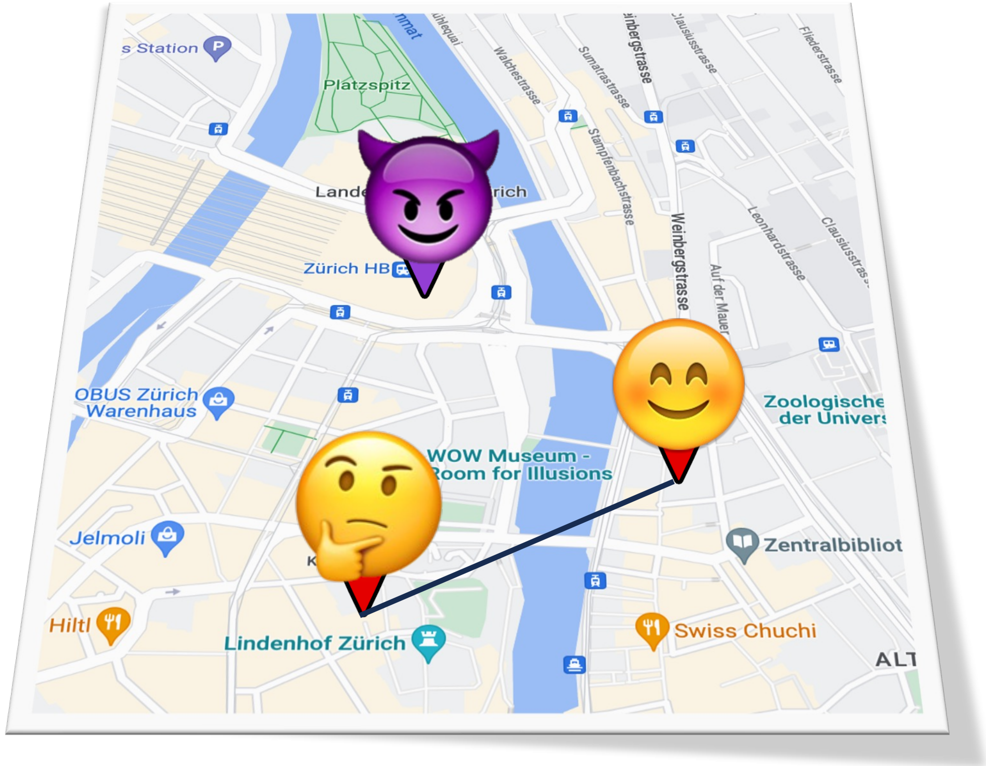
In $\mathbb{R}^2$, t $\geq n/3$ is too much.

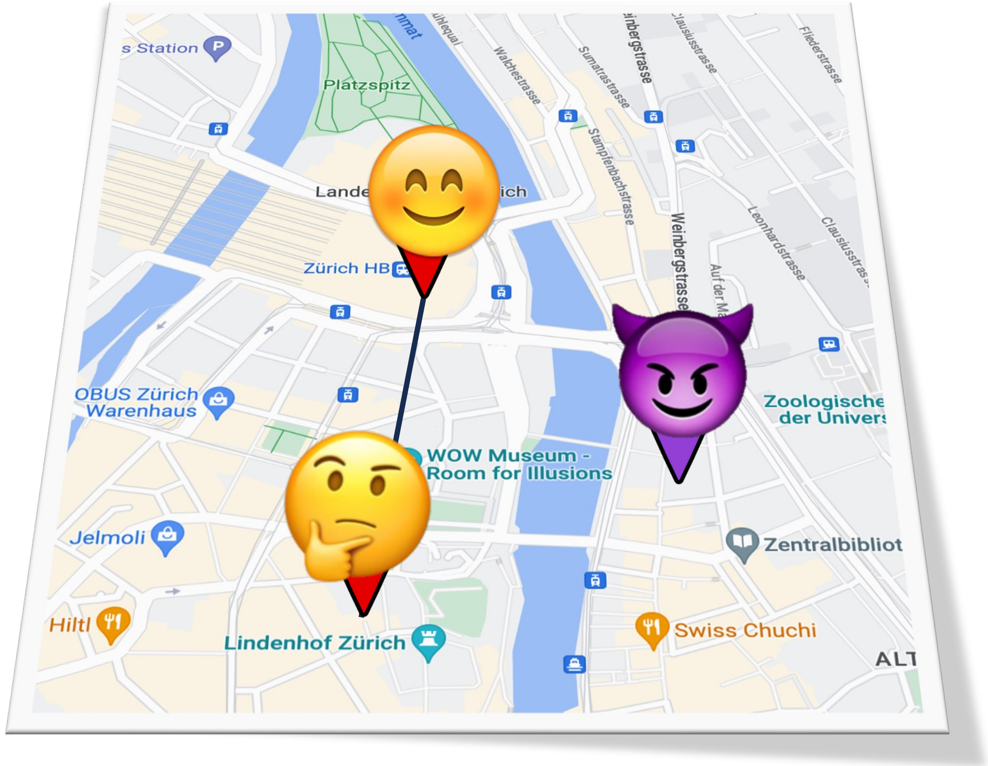
How many corruptions can be tolerated?



In $\mathbb{R}^2$, t $\geq n/3$ is too much.

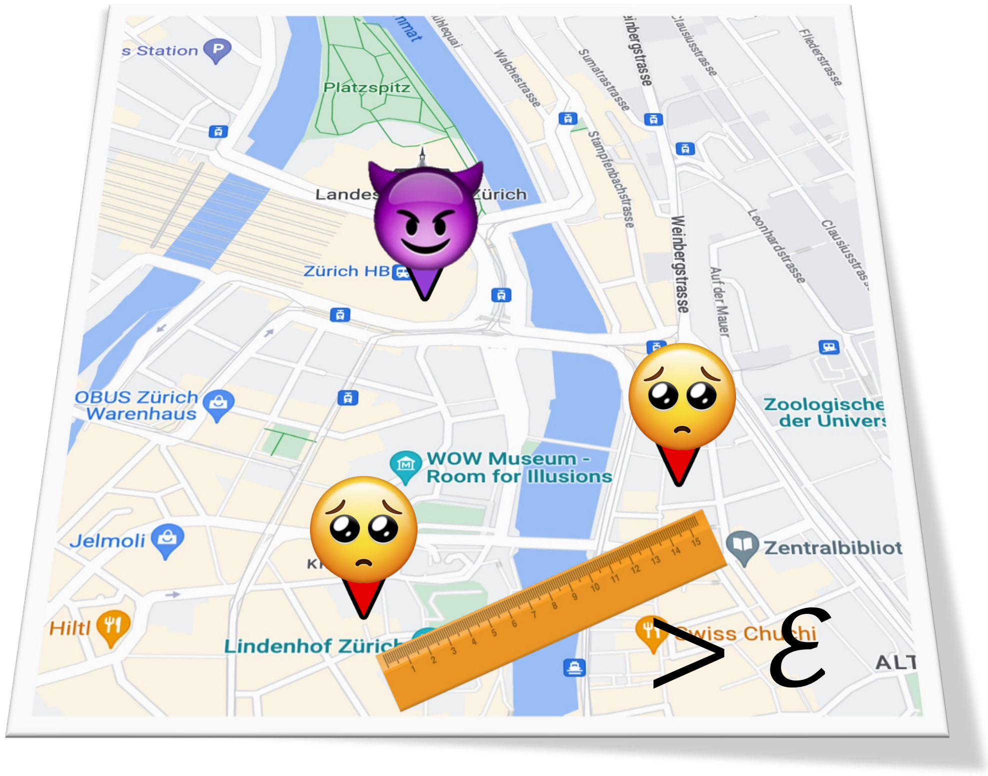
How many corruptions can be tolerated?





In $\mathbb{R}^2$, t $\geq n/3$ is too much.

How many corruptions can be tolerated?



In $\mathbb{R}^2$, t $\geq n/3$ is too much.

How many corruptions can be tolerated?

- $t < n/(D+1)$: necessary.

[PODC:VaiGar13]

How many corruptions can be tolerated?

- $t < n/(D+1)$: necessary and sufficient **in the synchronous model.**

(where parties' clocks are synchronized; messages get delivered within Δ time)

[PODC:VaiGar13]

How many corruptions can be tolerated?

- $t < n/(D+1)$: necessary and sufficient **in the synchronous model.**
  (where parties' clocks are synchronized; messages get delivered within Δ time)
  [PODC:VaiGar13]

- $t < n/(D+2)$: necessary and sufficient **in the asynchronous model.**
  [STOC:MenHer13, PODC:VaiGar13]

Main question

The parties do not know whether the network is synchronous or not:

- synchronous $\Rightarrow t_s < n/(D+1)$ corruptions.
- asynchronous $\Rightarrow t_a < n/(D+2)$ corruptions ($t_a \leq t_s$).

Can we achieve D-AA in this model?

Main question

The parties do not know whether the network is synchronous or not:

- synchronous $\Rightarrow t_s < n/(D+1)$ corruptions.
- asynchronous $\Rightarrow t_a < n/(D+2)$ corruptions ($t_a \leq t_s$).

Can we achieve D-AA in this model?

- $D = 1$: yes, iff $2 \cdot t_s + t_a < n$ (with PKI). [PODC:GhLiWa22]
- $D > 1$: yes, if $(D+1) \cdot t_s + t_a < n$ (without setup). [this work]

Algorithm outline

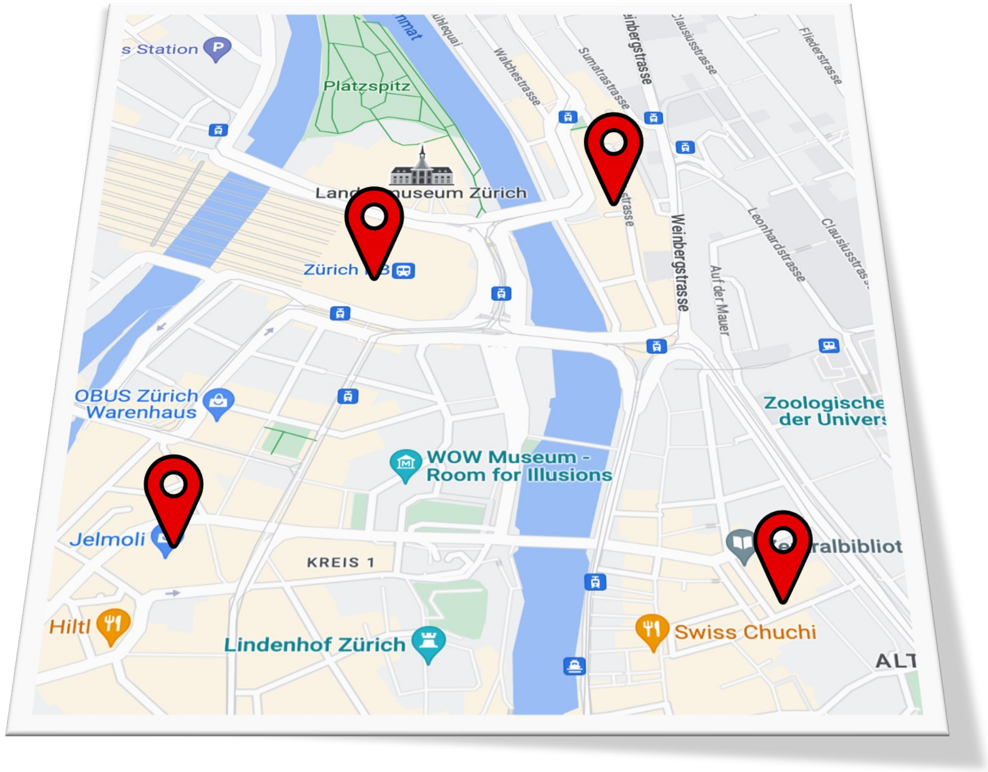
- Iterations:

    1. Parties distribute their current values via Overlap All-to-All Broadcast (OBC).

    2. Based on the values received, compute a *safe area.*

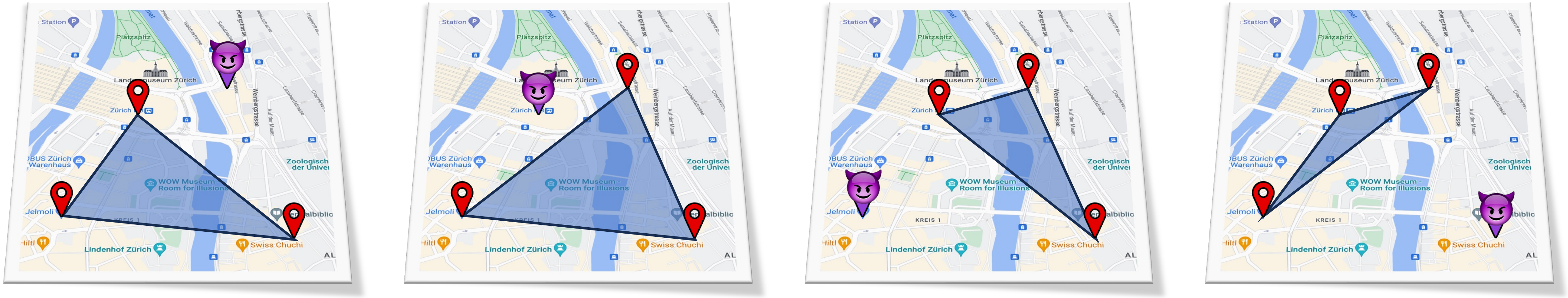
    3. Choose a new value from the safe area for the next iteration.

Safe areas



[STOC:MenHer13, PODC:VaiGar13]

Safe areas



[STOC:MenHer13, PODC:VaiGar13]

Safe areas

[STOC:MenHer13, PODC:VaiGar13]

Safe areas

- $\mathcal{M}$: multiset containing the $n - t_s + k$ values received via OBC.

Safe areas

- $\mathcal{M}$: multiset containing the $n - t_s + k$ values received via OBC.
- The network is synchronous?

  $\Rightarrow$ at most k of these values are corrupted.

Safe areas

- $\mathcal{M}$: multiset containing the $n - t_s + k$ values received via OBC.
- The network is synchronous?

  $\Rightarrow$ at most k of these values are corrupted.
- The network is asynchronous?

  $\Rightarrow$ at most t_a of these values are corrupted.

Safe areas

- $\mathcal{M}$: multiset containing the $n - t_s + k$ values received via OBC.
- The network is synchronous?

  $\Rightarrow$ at most k of these values are corrupted.
- The network is asynchronous?

  $\Rightarrow$ at most t_a of these values are corrupted.

$\Rightarrow$ Intersect the convex hulls of all subsets of $\mathcal{M}$ of size $|\mathcal{M}| - \max(k, t_a)$.

Safe areas

- $\mathcal{M}$: multiset containing the $n - t_s + k$ values received via OBC.
- The network is synchronous?

  $\Rightarrow$ at most k of these values are corrupted.
- The network is asynchronous?

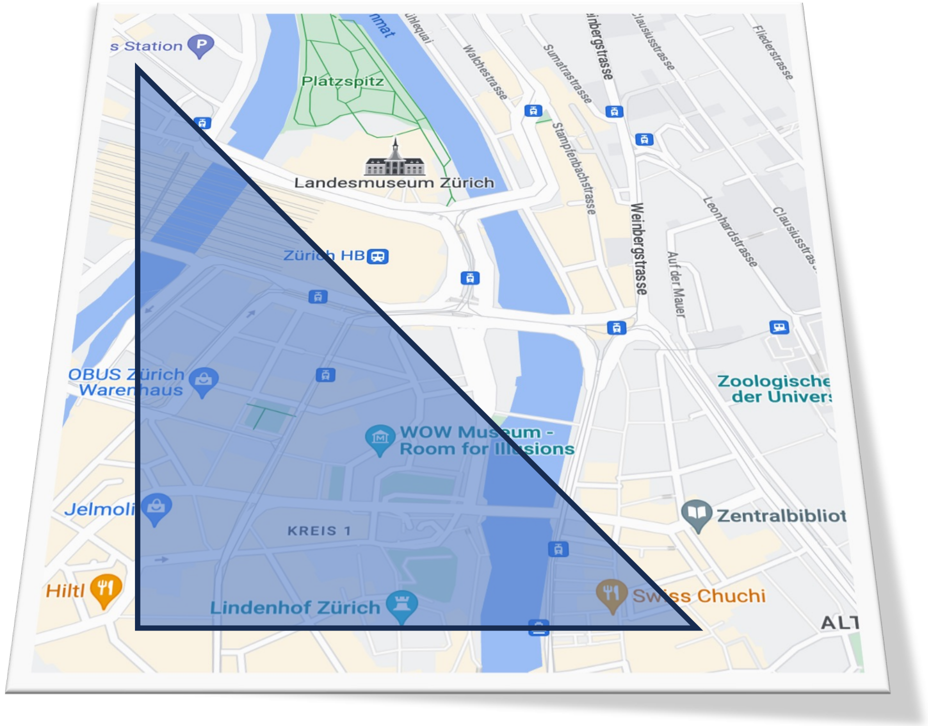
  $\Rightarrow$ at most t_a of these values are corrupted.

$\Rightarrow$ Intersect the convex hulls of all subsets of $\mathcal{M}$ of size $|\mathcal{M}| - \max(k, t_a)$.

- Safe areas are:
  - non-empty.
  - included in the honest values' convex hulls.

New values from the safe areas

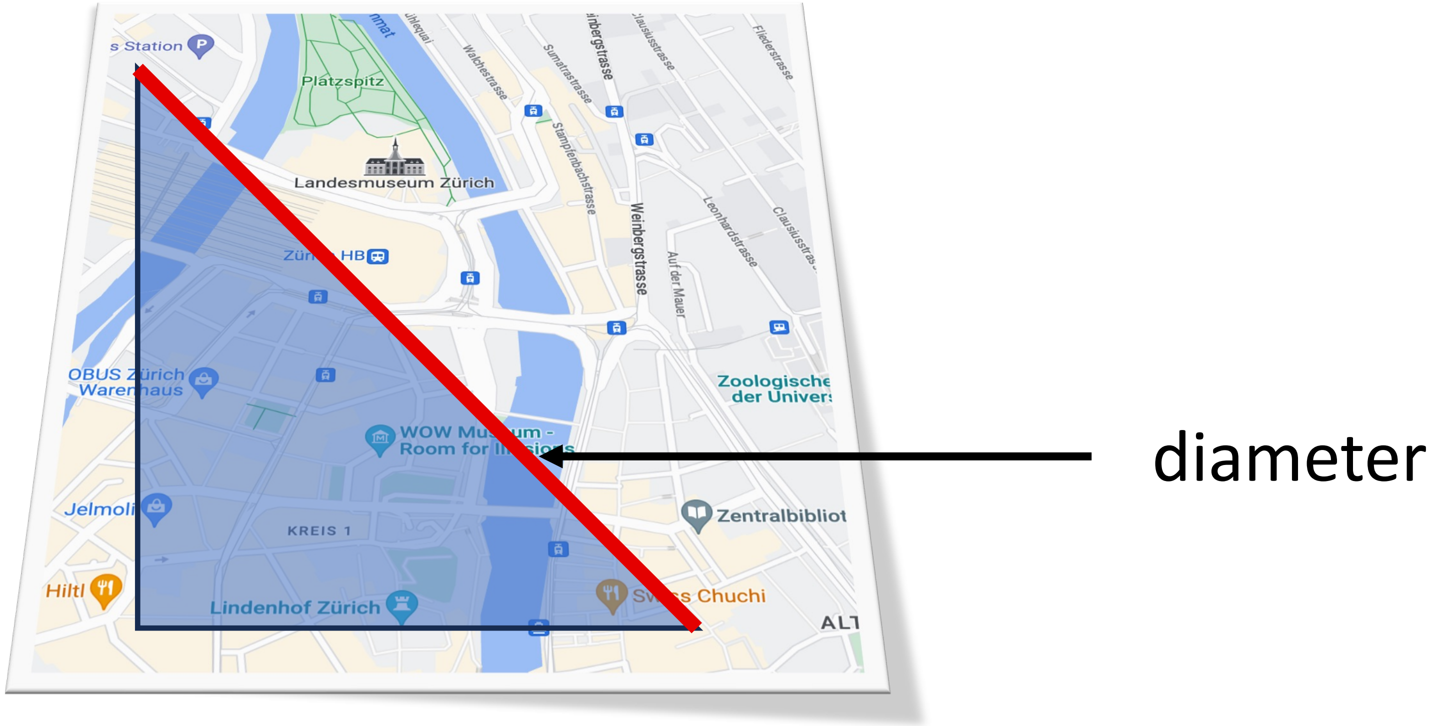
- New value: the midpoint of a segment realizing the safe area's diameter.



[DISC:FügNow18]

New values from the safe areas

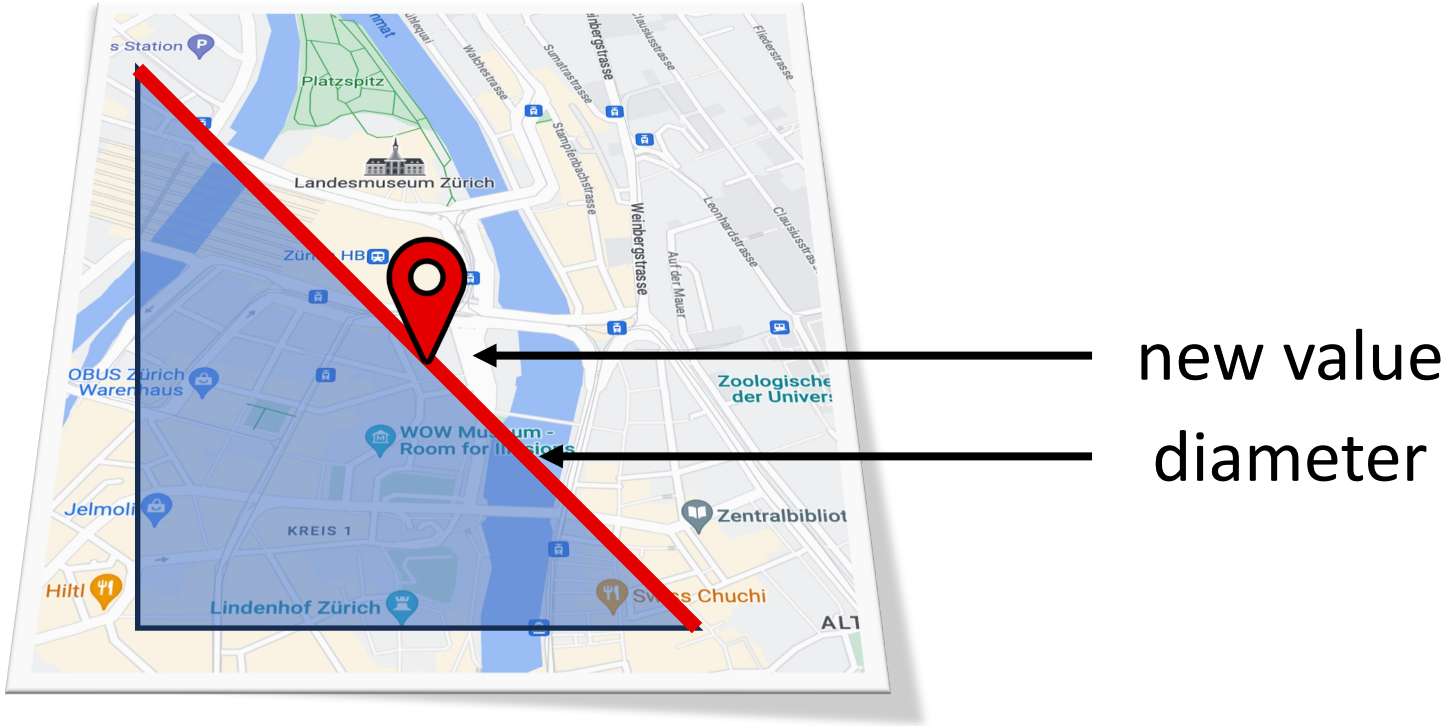
- New value: the midpoint of a segment realizing the safe area's diameter.



[DISC:FügNow18]

New values from the safe areas

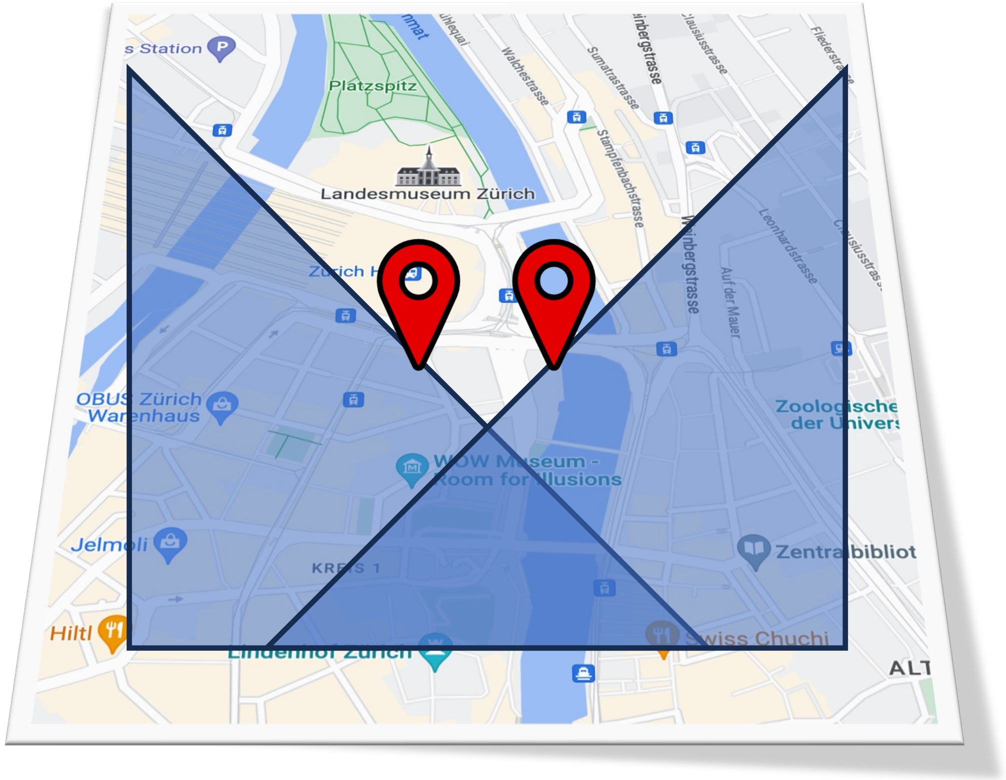
- New value: the midpoint of a segment realizing the safe area’s diameter.



[DISC:FügNow18]

Why do honest parties’ values get closer?

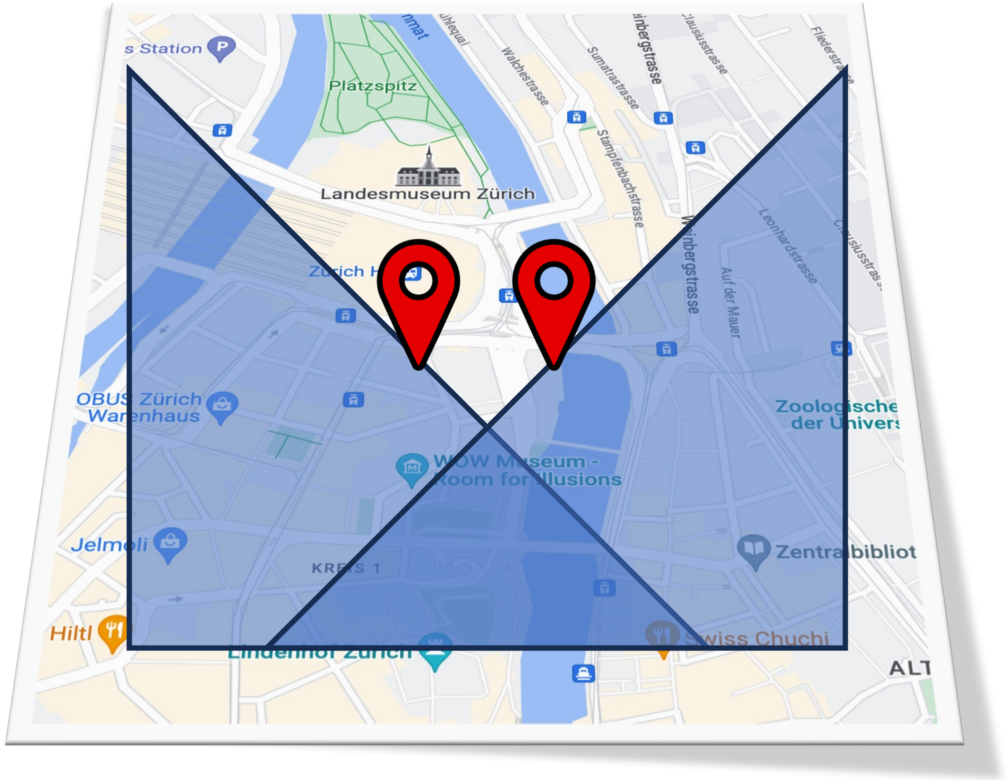
The safe areas obtained by every two honest parties intersect.



Why do honest parties’ values get closer?

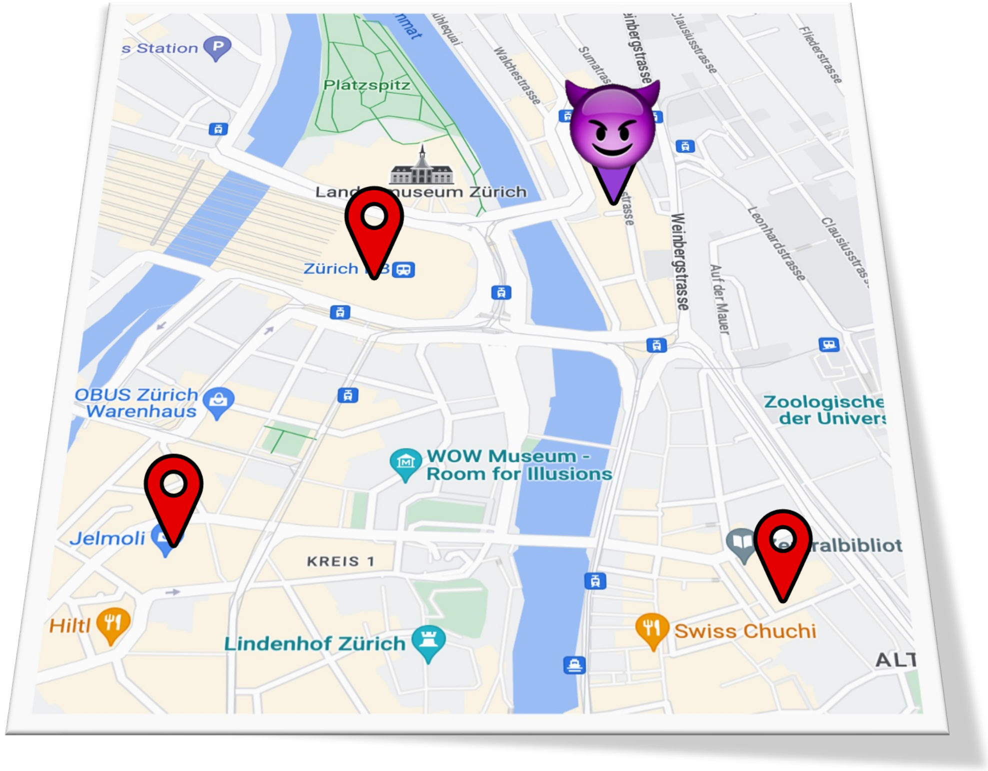
The safe areas obtained by every two honest parties intersect.

=> the diameter of the honest values’ convex hull decreases by a factor of $\sqrt{7/8}$ in each iteration.



How many iterations are needed?

- We estimate the honest inputs’ convex hull.



Summary

We are working in a model where the parties do not know whether the network is synchronous or asynchronous.

- synchronous $\Rightarrow t_s < n/(D+1)$ corruptions.
- asynchronous $\Rightarrow t_a < n/(D+2)$ corruptions ($t_a \leq t_s$).

D-AA can be achieved in this model when:

- $D = 1$: iff $2 \cdot t_s + t_a < n$ (with PKI). [PODC:GhLiWa22]
- $D > 1$: if $(D+1) \cdot t_s + t_a < n$ (without setup). [this work]