Structure-Aware PSI

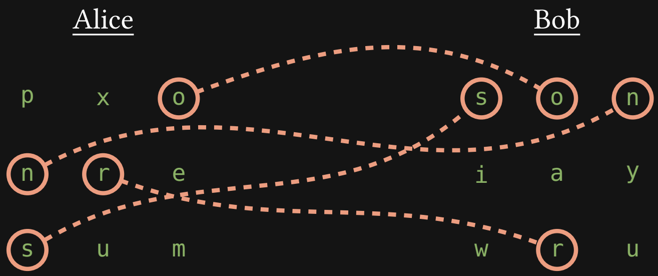
Gayathri Garimella Mike Rosulek Jaspal Singh

Oregon State University

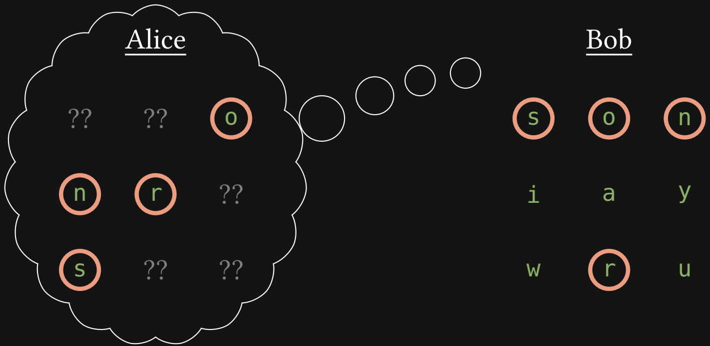
what is private set intersection (PSI)?

<u>Alice</u>			<u>Bob</u>		
p	x	o	s	o	n
n	r	e	i	a	y
s	u	m	w	r	u

what is private set intersection (PSI)?

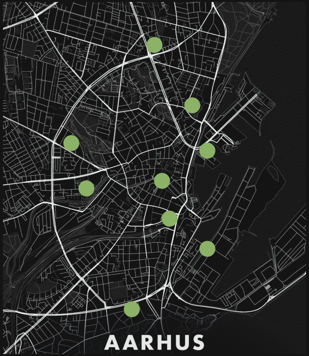


what is private set intersection (PSI)?

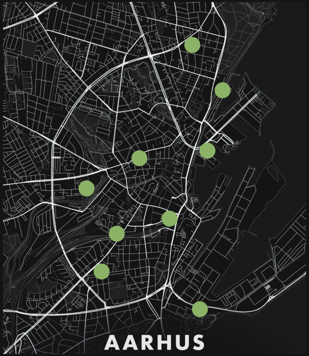


what if sets are geospatial points?

Alice



Bob

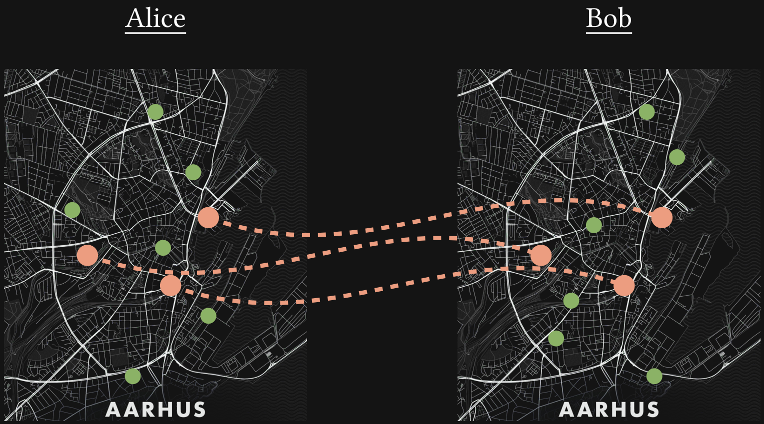


what if sets are geospatial points?

Alice

Bob

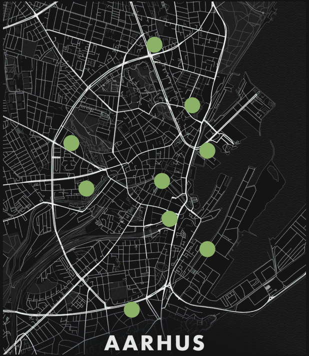
what if sets are geospatial points?



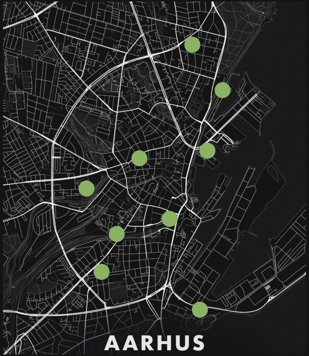
Unlikely that Alice & Bob have identical GPS coordinates

fuzzy PSI: find all $(a, b) \in A \times B : d(a, b) \leq \delta$

Alice

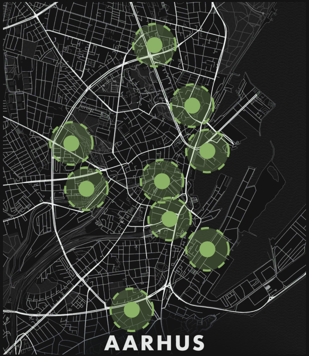


Bob

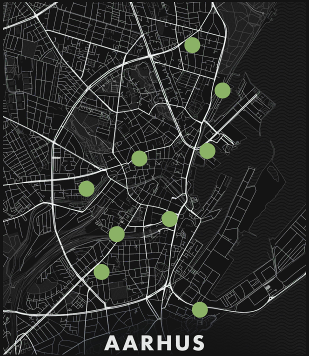


fuzzy PSI: find all $(a, b) \in A \times B : d(a, b) \leq \delta$

Alice



Bob



Naive fuzzy PSI: Alice enumerates all nearby points $\longrightarrow$ plain PSI

fuzzy PSI: find all $(a, b) \in A \times B : d(a, b) \le \delta$

Alice

Bob

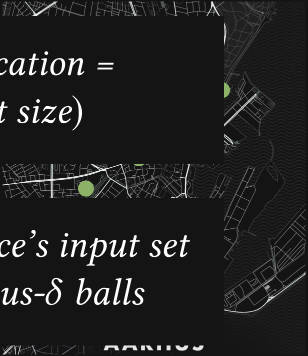
Alice's communication =
$O($expanded set size$)$

Naive fuzzy PSI: Alice enumerates all nearby points $\longrightarrow$ plain PSI

fuzzy PSI: find all $(a, b) \in A \times B : d(a, b) \leq \delta$

Alice

Bob



Alice's communication =
$O($expanded set size$)$

public knowledge: Alice's input set is the union of radius-δ balls

Naive fuzzy PSI: Alice enumerates all nearby points $\longrightarrow$ plain PSI

structure-aware PSI:

new, viable approach for (semi-honest) fuzzy PSI

and more

practical PSI protocol where Alice's set has **any** publicly known structure

structure-aware PSI:

new, viable approach for (semi-honest) fuzzy PSI

and more

practical PSI protocol where Alice's set has **any** publicly known structure

weak FSS:

reduce PSI to (new variant of) function secret sharing

Alice's PSI communication = $O(\lambda \cdot \text{FSS share size})$

*i.e., **description size**—not cardinality—of set*

structure-aware PSI:

new, viable approach for (semi-honest) fuzzy PSI

and more

practical PSI protocol where Alice's set has **any** publicly known structure

weak FSS:

reduce PSI to (new variant of) function secret sharing

Alice's PSI communication = $O(\lambda \cdot \text{FSS share size})$

i.e., ***description size****—not cardinality—of set*

new FSS techniques:

focus on FSS for unions of geometric balls

oblivious PRF (OPRF) paradigm for PSI

[FreedmanIshaiPinkasReingold05]

Alice:
$X = \{x_1, x_2, \ldots\}$

Bob:
$Y = \{y_1, y_2, \ldots\}$

oblivious PRF (OPRF) paradigm for PSI

[FreedmanIshaiPinkasReingold05]

Alice:

$X = \{x_1, x_2, \ldots\}$

$x_1, x_2, \ldots$

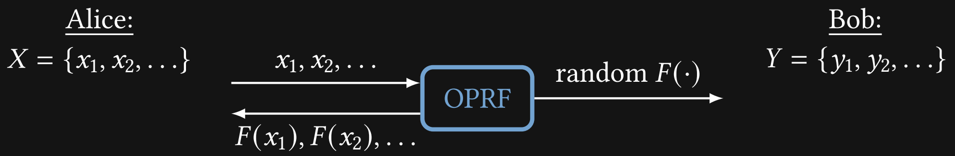
OPRF

Bob:

$Y = \{y_1, y_2, \ldots\}$

oblivious PRF (OPRF) paradigm for PSI

[FreedmanIshaiPinkasReingold05]



oblivious PRF (OPRF) paradigm for PSI

[FreedmanIshaiPinkasReingold05]

Alice:

$X = \{x_1, x_2, \ldots\}$

Bob:

$Y = \{y_1, y_2, \ldots\}$

$x_1, x_2, \ldots$

OPRF

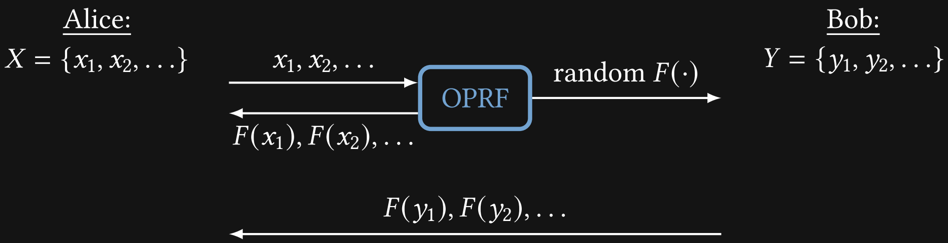
random $F(\cdot)$

$F(x_1), F(x_2), \ldots$

$F(y_1), F(y_2), \ldots$

oblivious PRF (OPRF) paradigm for PSI

[FreedmanIshaiPinkasReingold05]



typical OPRF: Alice's communication = $O(\lambda \cdot \text{cardinality of } X)$

oblivious PRF (OPRF) paradigm for PSI

[FreedmanIshaiPinkasReingold05]

Alice:

$X = \{x_1, x_2, ...\}$

Bob:

$Y = \{y_1, y_2, ...\}$

$x_1, x_2, \ldots$

OPRF

random $F(\cdot)$

$F(x_1), F(x_2), \ldots$

$F(y_1), F(y_2), \ldots$

typical OPRF: Alice's communication = $O(\lambda \cdot \text{cardinality of } X)$

structure-aware OPRF: Alice's communication = $O(\lambda \cdot \text{description size of } X)$

our main protocol construction

if Alice's set can be represented by weak function secret sharing with share size σ

(defined on next slide)

our main protocol construction

if Alice's set can be represented by weak function secret sharing with share size σ

(defined on next slide)

then there is a structure-aware OPRF with communication $O(\lambda \cdot \sigma)$

(semi-honest)

our main protocol construction

if Alice's set can be represented by weak function secret sharing with share size σ

(defined on next slide)

then there is a structure-aware OPRF with communication $O(\lambda \cdot \sigma)$

(semi-honest)

and hence a structure-aware PSI with Alice communication $O(\lambda \cdot \sigma)$

our main protocol construction

if Alice's set can be represented by weak function secret sharing with share size σ

(defined on next slide)

then there is a structure-aware OPRF with communication $O(\lambda \cdot \sigma)$

(semi-honest)

and hence a structure-aware PSI with Alice communication $O(\lambda \cdot \sigma)$

boolean function secret sharing (bFSS)

[BoyleGilboaIshai15]-style FSS for the "membership in A" function

boolean function secret sharing (bFSS)

[BoyleGilboaIshai15]-style FSS for the "membership in A" function

$$\mathrm{Share}(A) \to (\square, \square)$$

boolean function secret sharing (bFSS)

[BoyleGilboaIshai15]-style FSS for the "membership in A" function

$\mathsf{Share}(A) \rightarrow (\; , \;)$ $\quad\quad$ $\; , \; \approx \$$

boolean function secret sharing (bFSS)

[BoyleGilboaIshai15]-style FSS for the "membership in A" function

$$\mathsf{Share}(A) \to (\textcolor{blue}{\blacksquare}, \textcolor{red}{\blacksquare}) \qquad \textcolor{blue}{\blacksquare}, \textcolor{red}{\blacksquare} \approx \$$$

$$x \in A \implies \mathsf{Ev}(\textcolor{blue}{\blacksquare}, x) \oplus \mathsf{Ev}(\textcolor{red}{\blacksquare}, x) = 0$$

$$x \notin A \implies \mathsf{Ev}(\textcolor{blue}{\blacksquare}, x) \oplus \mathsf{Ev}(\textcolor{red}{\blacksquare}, x) = 1$$

Alice(A):

Bob:

our OPRF protocol

Alice(A):

Bob:

our OPRF protocol

$\text{Share}(A) \longrightarrow \boxed{1}, \boxed{1}$

$\text{Share}(A) \longrightarrow \boxed{2}, \boxed{2}$

$\text{Share}(A) \longrightarrow \boxed{3}, \boxed{3}$

$\text{Share}(A) \longrightarrow \boxed{4}, \boxed{4}$

$\vdots \qquad \vdots$

our OPRF protocol

Alice(A):

Bob:

Share(A) $\longrightarrow$ 1, 1 $\longrightarrow$ $\boxed{\text{OT}}$

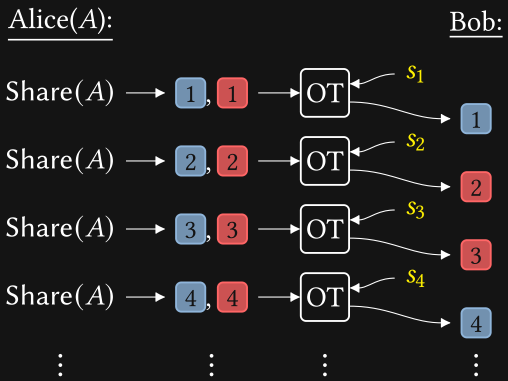
Share(A) $\longrightarrow$ 2, 2 $\longrightarrow$ $\boxed{\text{OT}}$

Share(A) $\longrightarrow$ 3, 3 $\longrightarrow$ $\boxed{\text{OT}}$

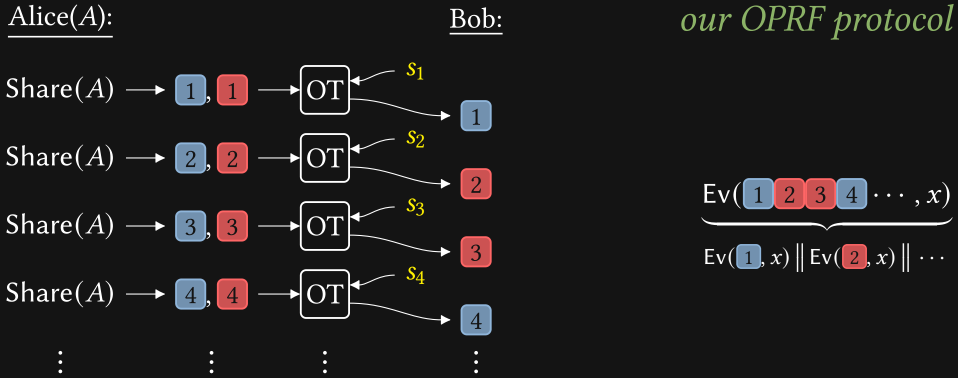
Share(A) $\longrightarrow$ 4, 4 $\longrightarrow$ $\boxed{\text{OT}}$

$\vdots$ $\vdots$ $\vdots$

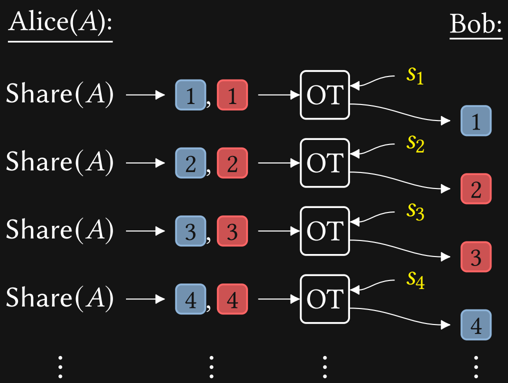
our OPRF protocol



our OPRF protocol

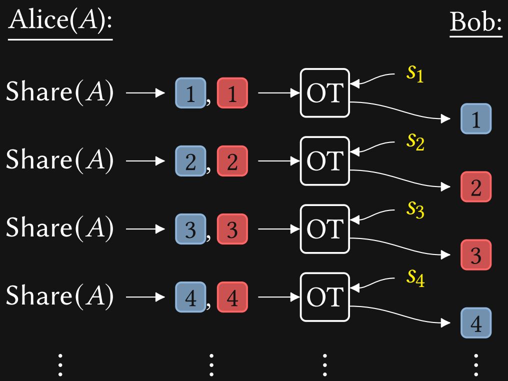


our OPRF protocol



$$F(x) \stackrel{\text{def}}{=} H\Big(\underbrace{\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)}_{\mathsf{Ev}(\boxed{1}, x)\,\|\,\mathsf{Ev}(\boxed{2}, x)\,\|\,\cdots}\Big)$$

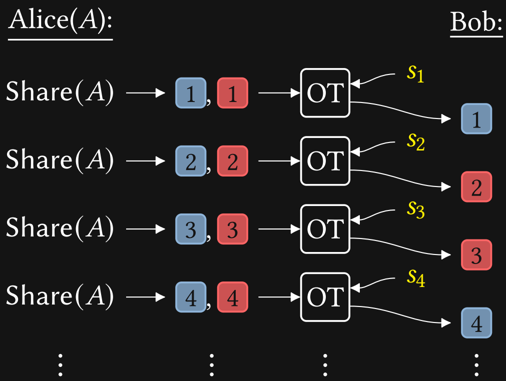
our OPRF protocol



$$F(x) \overset{\text{def}}{=} H\Big(\underbrace{\mathrm{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)}_{\mathrm{Ev}(\boxed{1},\, x) \,\|\, \mathrm{Ev}(\boxed{2},\, x) \,\|\, \cdots}\Big)$$

$$\boxed{x \in A} \implies \mathrm{Ev}(\boxed{}, x) = \mathrm{Ev}(\boxed{}, x)$$

our OPRF protocol

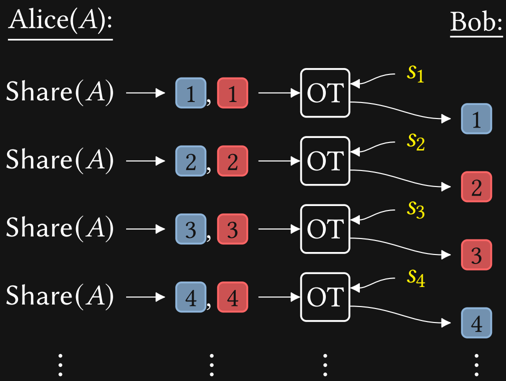


$$F(x) \stackrel{\text{def}}{=} H\left(\underbrace{\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)}_{\mathsf{Ev}(\boxed{1}, x) \,\|\, \mathsf{Ev}(\boxed{2}, x) \,\|\, \cdots}\right)$$

$$\boxed{x \in A} \implies \mathsf{Ev}(\boxed{}, x) = \mathsf{Ev}(\boxed{}, x)$$

$$\begin{aligned} F(x) &= H\left(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)\right) \\ &= H\left(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)\right) \end{aligned}$$

our OPRF protocol



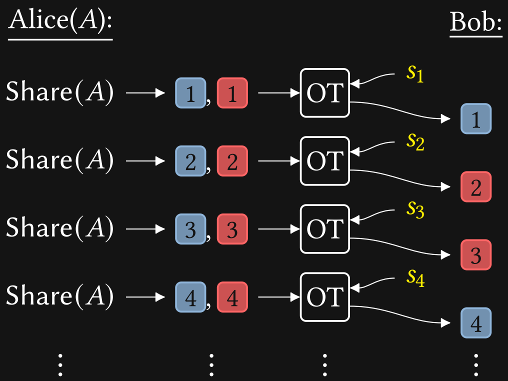
$$F(x) \stackrel{\text{def}}{=} H\Big(\underbrace{\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)}_{\mathsf{Ev}(\boxed{1}, x) \,\|\, \mathsf{Ev}(\boxed{2}, x) \,\|\, \cdots}\Big)$$

$\boxed{x \in A} \implies \mathsf{Ev}(\boxed{}, x) = \mathsf{Ev}(\boxed{}, x)$

$\boxed{x \notin A} \implies \mathsf{Ev}(\boxed{}, x) = \mathsf{Ev}(\boxed{}, x) \oplus 1$

$$\begin{aligned} F(x) &= H\Big(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)\Big) \\ &= H\Big(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)\Big) \end{aligned}$$

our OPRF protocol



$$F(x) \stackrel{\text{def}}{=} H\Big(\underbrace{\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)}_{\mathsf{Ev}(\boxed{1}, x)\,\|\,\mathsf{Ev}(\boxed{2}, x)\,\|\,\cdots}\Big)$$

$\boxed{x \in A} \implies \mathsf{Ev}(\boxed{}, x) = \mathsf{Ev}(\boxed{}, x)$

$\boxed{x \notin A} \implies \mathsf{Ev}(\boxed{}, x) = \mathsf{Ev}(\boxed{}, x) \oplus 1$

$$F(x) = H\Big(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)\Big) = H\Big(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)\Big)$$

$$F(x) = H\Big(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)\Big) = H\Big(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x) \oplus s\Big) \approx \$$$

(trivial) bFSS for subsets of $[n]$

$A \subseteq \{ \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \;\ldots\; n \quad \}$

(trivial) bFSS for subsets of $[n]$

$$A \subseteq \{ \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad \dots \quad n \quad \}$$

$$\text{e.g., } A = \{ \quad \quad 2 \quad 3 \quad \quad 5 \quad \quad \quad \}$$

$$1 \quad 0 \quad 0 \quad 1 \quad 0 \cdots 1$$

(trivial) bFSS for subsets of $[n]$

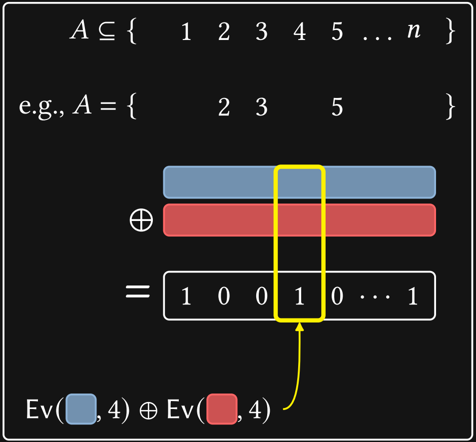
$$A \subseteq \{\ 1\ \ 2\ \ 3\ \ 4\ \ 5\ \ \ldots\ n\ \}$$

$$\text{e.g., } A = \{\ \ \ 2\ \ 3\ \ \ \ 5\ \ \ \ \}$$

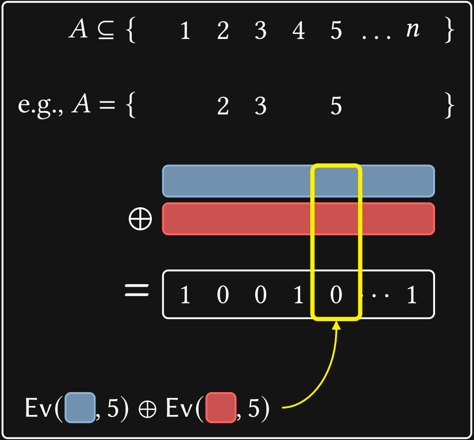
$$\oplus$$

$$= \boxed{1\ \ 0\ \ 0\ \ 1\ \ 0\ \cdots\ 1}$$

(trivial) bFSS for subsets of [n]



(trivial) bFSS for subsets of $[n]$



(trivial) bFSS for subsets of $[n]$

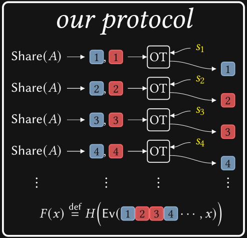
$A \subseteq \{ \; 1 \;\; 2 \;\; 3 \;\; 4 \;\; 5 \; \ldots \; n \; \}$

e.g., $A = \{ \; 2 \;\; 3 \;\; 5 \; \}$

$\oplus$

$= \boxed{1 \;\; 0 \;\; 0 \;\; 1 \;\; 0 \cdots 1}$

$+$



$=$ IKNP

[IshaiKilianNissimPetrank03]

(new) *weak* bFSS

$$\mathsf{Share}(A) \rightarrow (\textcolor{blue}{\blacksquare}, \textcolor{red}{\blacksquare}) \qquad \textcolor{blue}{\blacksquare}, \textcolor{red}{\blacksquare} \approx \$$$

$$x \in A \implies \mathsf{Ev}(\textcolor{blue}{\blacksquare}, x) \oplus \mathsf{Ev}(\textcolor{red}{\blacksquare}, x) = 0$$

$$x \notin A \implies \mathsf{Ev}(\textcolor{blue}{\blacksquare}, x) \oplus \mathsf{Ev}(\textcolor{red}{\blacksquare}, x) = 1$$

(new) *weak* bFSS

$$\mathsf{Share}(A) \to (\textcolor{blue}{\blacksquare}, \textcolor{red}{\blacksquare}) \qquad \textcolor{blue}{\blacksquare}, \textcolor{red}{\blacksquare} \approx \$$$

$$x \in A \implies \mathsf{Ev}(\textcolor{blue}{\blacksquare}, x) \oplus \mathsf{Ev}(\textcolor{red}{\blacksquare}, x) = 0^k$$
$$x \notin A \implies \mathsf{Ev}(\textcolor{blue}{\blacksquare}, x) \oplus \mathsf{Ev}(\textcolor{red}{\blacksquare}, x) \neq 0^k$$

1. Ev can output multiple bits

(new) *weak* bFSS

$\mathsf{Share}(A) \to (\square, \square)$ $\square, \square \approx \$$

$x \in A \implies \mathsf{Ev}(\square, x) \oplus \mathsf{Ev}(\square, x) = 0^k$

$x \notin A \implies \cancel{\mathsf{Ev}(\square, x) \oplus \mathsf{Ev}(\square, x) \neq 0^k}$

$$\Pr\left[\mathsf{Ev}(\square, x) \oplus \mathsf{Ev}(\square, x) \neq 0^k\right] > \frac{1}{2}$$

1. Ev can output multiple bits
2. Bounded false positives

(new) weak bFSS

$$\mathsf{Share}(A) \longrightarrow ({\color{steelblue}\blacksquare}, {\color{indianred}\blacksquare}) \qquad {\color{steelblue}\blacksquare}, {\color{indianred}\blacksquare} \approx \$$$

$$x \in A \implies \mathsf{Ev}({\color{steelblue}\blacksquare}, x) \oplus \mathsf{Ev}({\color{indianred}\blacksquare}, x) = 0^k$$

$$x \notin A \implies \xcancel{\mathsf{Ev}({\color{steelblue}\blacksquare}, x) \oplus \mathsf{Ev}({\color{indianred}\blacksquare}, x) \neq 0^k}$$

$$\Pr\left[\mathsf{Ev}({\color{steelblue}\blacksquare}, x) \oplus \mathsf{Ev}({\color{indianred}\blacksquare}, x) \neq 0^k\right] > \frac{1}{2}$$

1. Ev can output multiple bits
2. Bounded false positives

how do false positives affect OPRF protocol?

$$F(x) \stackrel{\text{def}}{=} H\Big(\underbrace{\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)}_{\mathsf{Ev}(\boxed{1}, x) \,\|\, \mathsf{Ev}(\boxed{2}, x) \,\|\, \cdots}\Big)$$

basic bFSS

$$\boxed{x \notin A} \implies \mathsf{Ev}(\boxed{}, x) = \mathsf{Ev}(\boxed{}, x) \oplus 1$$

$$\begin{aligned} F(x) &= H\Big(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)\Big) \\ &= H\Big(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x) \oplus s\Big) \approx \$ \end{aligned}$$

$$F(x) \stackrel{\text{def}}{=} H\Big(\underbrace{\mathrm{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)}_{\mathrm{Ev}(\boxed{1}, x) \,\|\, \mathrm{Ev}(\boxed{2}, x) \,\|\, \cdots}\Big)$$

basic bFSS

with 128 ($\boxed{}$, $\boxed{}$) pairs:

$$\boxed{x \notin A} \implies \mathrm{Ev}(\boxed{}, x) = \mathrm{Ev}(\boxed{}, x) \oplus 1$$

$$\begin{aligned} F(x) &= H\Big(\mathrm{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)\Big) \\ &= H\Big(\mathrm{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x) \oplus s\Big) \approx \$ \end{aligned}$$

weak bFSS

with 440 ($\boxed{}$, $\boxed{}$) pairs:

$$F(x) \overset{\text{def}}{=} H\Big(\underbrace{\mathsf{Ev}(\colorbox{blue}{1}\colorbox{red}{2}\colorbox{red}{3}\colorbox{blue}{4}\cdots, x)}_{\mathsf{Ev}(\colorbox{blue}{1}, x) \,\|\, \mathsf{Ev}(\colorbox{red}{2}, x) \,\|\, \cdots}\Big)$$

basic bFSS

with 128 $(\colorbox{blue}{$$}, \colorbox{red}{$$})$ pairs:

$$\boxed{x \notin A} \implies \mathsf{Ev}(\colorbox{blue}{$$}, x) = \mathsf{Ev}(\colorbox{red}{$$}, x) \oplus 1$$

$$F(x) = H\Big(\mathsf{Ev}(\colorbox{blue}{1}\colorbox{red}{2}\colorbox{red}{3}\colorbox{blue}{4}\cdots, x)\Big)$$

$$= H\Big(\mathsf{Ev}(\colorbox{blue}{1}\colorbox{blue}{2}\colorbox{blue}{3}\colorbox{blue}{4}\cdots, x) \oplus s\Big) \approx \$$$

weak bFSS

with 440 $(\colorbox{blue}{$$}, \colorbox{red}{$$})$ pairs:

$$\boxed{x \notin A} \implies$$ at least 128 pairs satisfy: $$\mathsf{Ev}(\colorbox{blue}{$$}, x) = \mathsf{Ev}(\colorbox{red}{$$}, x) \oplus 1$$

$$F(x) \overset{\text{def}}{=} H\Big(\underbrace{\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)}_{\mathsf{Ev}(\boxed{1}, x) \,\|\, \mathsf{Ev}(\boxed{2}, x) \,\|\, \cdots}\Big)$$

basic bFSS

with 128 ($\boxed{}$, $\boxed{}$) pairs:

$$\boxed{x \notin A} \implies \mathsf{Ev}(\boxed{}, x) = \mathsf{Ev}(\boxed{}, x) \oplus 1$$

$$F(x) = H\Big(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)\Big)$$
$$= H\Big(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x) \oplus s\Big) \approx \$$$

weak bFSS

with 440 ($\boxed{}$, $\boxed{}$) pairs:

$$\boxed{x \notin A} \implies$$

at least 128 pairs satisfy:

$$\mathsf{Ev}(\boxed{}, x) = \mathsf{Ev}(\boxed{}, x) \oplus 1$$

$$F(x) = H\Big(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x)\Big)$$
$$= H\Big(\mathsf{Ev}(\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots, x) \oplus ??\Big) \approx \$$$

128 bits of entropy!

weak bFSS for ***arbitrary sets****, from Bloom filters*

e.g., $A = \{$ `foo`, `bar`, `tpmpc`, $\ldots$ $\}$

$$\boxed{1 \quad 1 \quad 1 \quad 1 \quad 1 \cdots 1}$$

1-hash-function Bloom filter

weak bFSS for ***arbitrary sets****, from Bloom filters*

e.g., $A = \{\ \texttt{foo}, \texttt{bar}, \texttt{tpmpc}, \ldots\ \}$

$h(\texttt{foo})$

$\boxed{1 \quad 1 \quad 1 \quad 1 \quad 0 \cdots 1}$

1-hash-function Bloom filter

weak bFSS for ***arbitrary sets****, from Bloom filters*

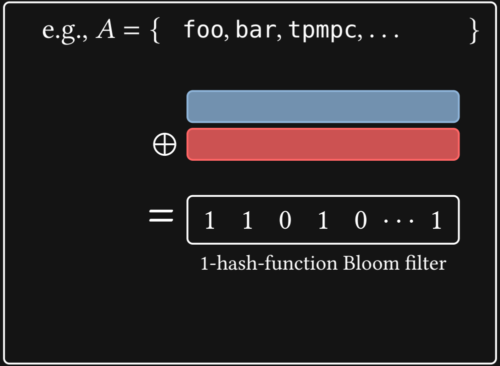
e.g., $A = \{\ \texttt{foo}, \texttt{bar}, \texttt{tpmpc}, \ldots\ \}$

$h(\texttt{bar})$

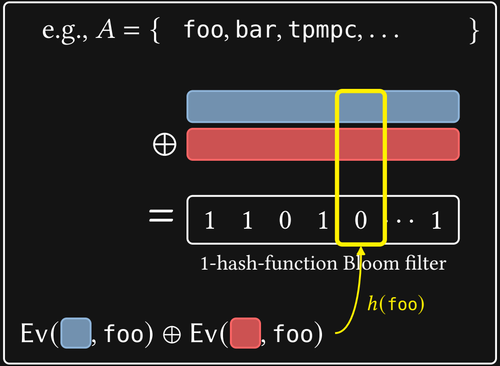
$\boxed{1 \quad 1 \quad 0 \quad 1 \quad 0 \cdots 1}$

1-hash-function Bloom filter

weak bFSS for ***arbitrary sets****, from Bloom filters*



weak bFSS for ***arbitrary sets****, from Bloom filters*



weak bFSS for ***arbitrary sets****, from Bloom filters*

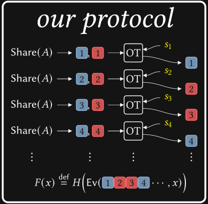
e.g., $A = \{$ `foo`, `bar`, `tpmpc`, $\ldots$ $\}$

$\oplus$

$= \boxed{1 \quad 1 \quad 0 \quad 1 \quad 0 \cdots 1}$

1-hash-function Bloom filter

$+$



= [ChaseMiao20]

*weak bFSS for **arbitrary sets**, from polynomials*

e.g., $A = \{\texttt{foo}, \texttt{bar}, \texttt{tpmpc}, \ldots\}$

$\boxed{}$ = a PRF seed

$\boxed{\text{P}}$ = coeffs. of a polynomial s.t.

$F(\boxed{}, a) = \boxed{\text{P}}(a)$ for $a \in A$

$(\deg(P) = |A|)$

*weak bFSS for **arbitrary sets**, from polynomials*

e.g., $A = \{\texttt{foo}, \texttt{bar}, \texttt{tpmpc}, \ldots\}$

$\boxed{}$ = a PRF seed

$\boxed{\text{P}}$ = coeffs. of a polynomial s.t.

$$F(\boxed{}, a) = \boxed{\text{P}}(a) \text{ for } a \in A$$

$(\deg(P) = |A|)$

weak bFSS for ***arbitrary sets****, from polynomials*

e.g., $A = \{\texttt{foo}, \texttt{bar}, \texttt{tpmpc}, \ldots\}$

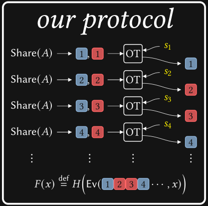
$\square$ = a PRF seed

$\boxed{\text{P}}$ = coeffs. of a polynomial s.t.

$F(\square, a) = \boxed{\text{P}}(a)$ for $a \in A$

$(\deg(P) = |A|)$

+



= `spot-light`

[PinkasRosulekTrieuYanai19]

bFSS schemes $\implies$ *OPRF* $\implies$ *PSI*

bFSS	sets	share size
trivial truth-table	any subset of $[n]$	n
1-hash Bloom filter	any set	$O(\lvert A \rvert)$
polynomial	any set	$\lvert A \rvert$

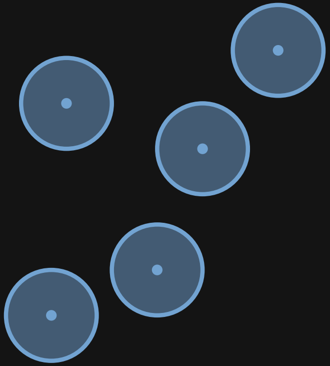
bFSS schemes $\Longrightarrow$ *OPRF* $\Longrightarrow$ *PSI*

	bFSS	sets	share size
plain PSI	trivial truth-table	any subset of $[n]$	n
	1-hash Bloom filter	any set	$O(\lvert A \rvert)$
	polynomial	any set	$\lvert A \rvert$

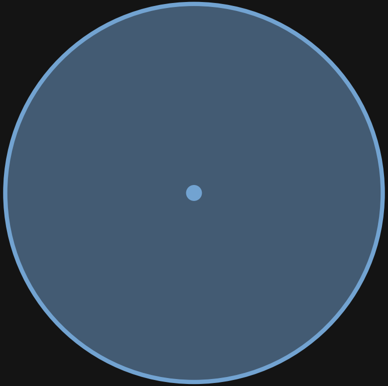
bFSS schemes $\Longrightarrow$ *OPRF* $\Longrightarrow$ *PSI*

	bFSS	sets	share size
plain PSI	trivial truth-table	any subset of $[n]$	n
	1-hash Bloom filter	any set	$O(\lvert A\rvert)$
	polynomial	any set	$\lvert A\rvert$
	???	union of radius-δ balls (for fuzzy PSI)	$\ll \lvert A\rvert$

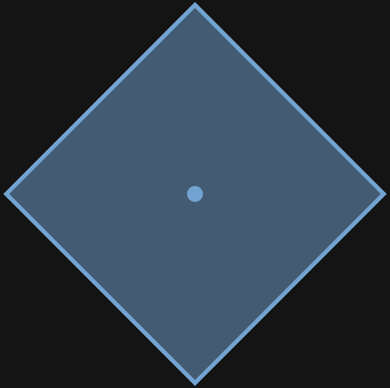
a few tricks for weak bFSS



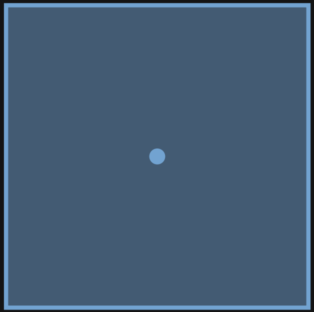
Alice's set (in fuzzy PSI) = union of balls



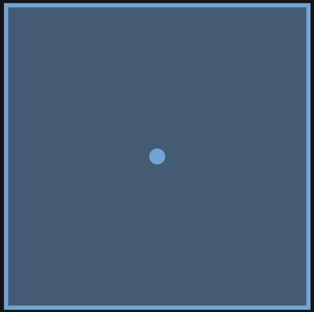
an ℓ_2 ball



an ℓ_1 ball



an ℓ_∞ ball

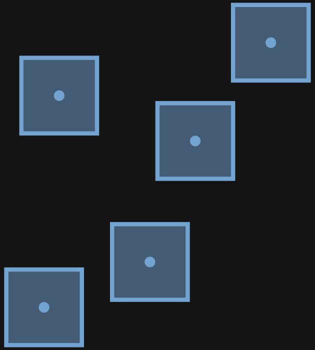


an ℓ_∞ ball

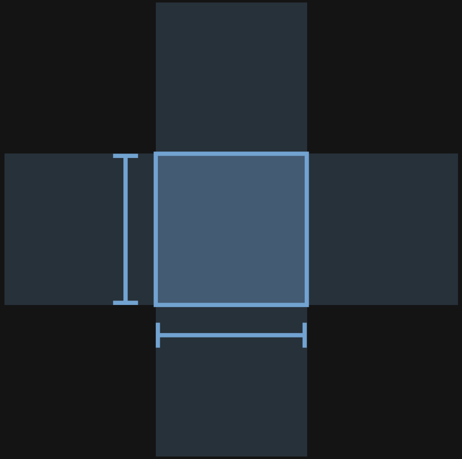
ℓ_∞ intersection of d intervals

ℓ_1 intersection of 2^{d-1} intervals

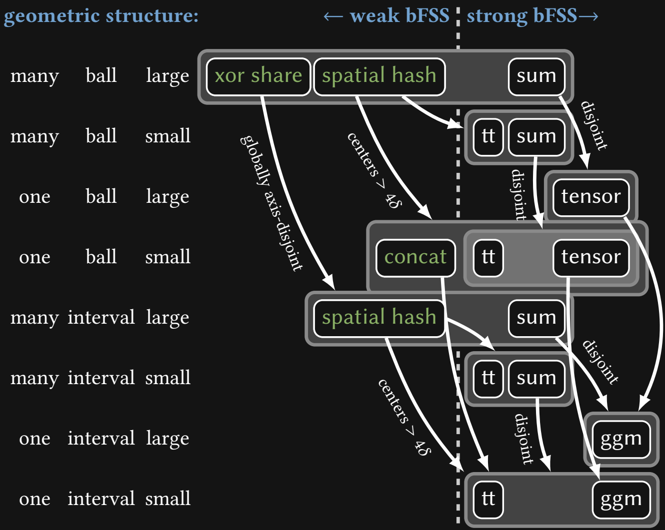
bFSS needed for fuzzy PSI:

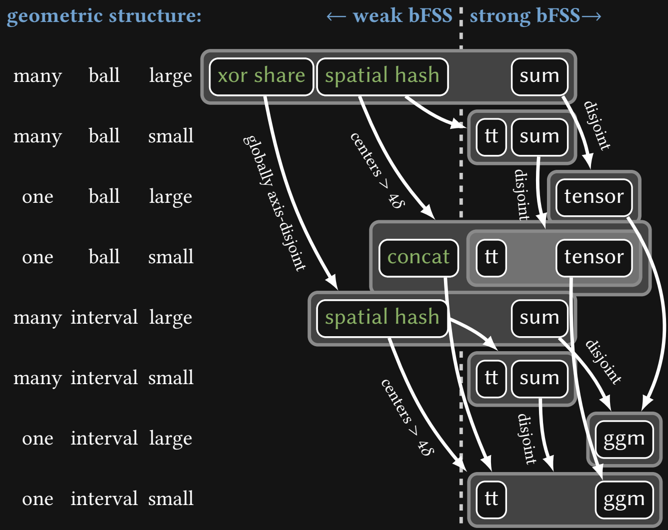


Alice's set = **union** of balls



ball = **intersection** of intervals


geometric structure:
← weak bFSS
strong bFSS→
many ball large
many ball small
one ball large
one ball small
many interval large
many interval small
one interval large
one interval small
xor share
spatial hash
sum
tt
sum
tensor
concat
tt
tensor
spatial hash
sum
tt
sum
ggm
tt
ggm
globally axis-disjoint
centers > 4δ
disjoint
disjoint
disjoint
centers > 4δ
disjoint



our bFSS contributions:

simple constructions

scratched the surface

weak bFSS $\Longrightarrow$
more efficient bFSS

(multi-bit output; false positives)

*intersection of **strong** bFSS:*

state of the art: [BoyleGilboaIshai15]:

$$\begin{aligned}\text{sharesize}(A \cap B) &= \text{sharesize}(A) \\ &\times \text{sharesize}(B)\end{aligned}$$

intersection of ***strong*** *bFSS:*

new intersection of ***weak*** *bFSS:*

state of the art: [BoyleGilboaIshai15]:

$$\mathrm{sharesize}(A \cap B) = \mathrm{sharesize}(A) \times \mathrm{sharesize}(B)$$

$$\mathsf{Share}(A) \longrightarrow \left(\boxed{\in A?}, \boxed{\in A?}\right)$$
$$\mathsf{Share}(B) \longrightarrow \left(\boxed{\in B?}, \boxed{\in B?}\right)$$

intersection of ***strong*** *bFSS:*

state of the art: [BoyleGilboaIshai15]:

$$\mathrm{sharesize}(A \cap B) = \mathrm{sharesize}(A) \times \mathrm{sharesize}(B)$$

new intersection of ***weak*** *bFSS:*

(Ev can output multiple bits!)

$$\mathsf{Share}(A) \longrightarrow \left(\boxed{\in A?}, \boxed{\in A?}\right)$$
$$\mathsf{Share}(B) \longrightarrow \left(\boxed{\in B?}, \boxed{\in B?}\right)$$

intersection of ***strong*** *bFSS:*

state of the art: [BoyleGilboaIshai15]:

$$\mathrm{sharesize}(A \cap B) = \mathrm{sharesize}(A) \times \mathrm{sharesize}(B)$$

new intersection of ***weak*** *bFSS:*

(Ev can output multiple bits!)

$$\mathsf{Share}(A) \longrightarrow \left(\boxed{\in A?}, \boxed{\in A?}\right)$$
$$\mathsf{Share}(B) \longrightarrow \left(\boxed{\in B?}, \boxed{\in B?}\right)$$

$$\underbrace{\begin{matrix} \mathsf{Ev}\left(\boxed{\in A?}, x\right) \,\|\, \mathsf{Ev}\left(\boxed{\in B?}, x\right) \\ \mathsf{Ev}\left(\boxed{\in A?}, x\right) \,\|\, \mathsf{Ev}\left(\boxed{\in B?}, x\right) \end{matrix}}_{\text{secret shares of } 00 \iff x \in A \cap B}$$

intersection of ***strong*** *bFSS:*

state of the art: [BoyleGilboaIshai15]:

$$\mathrm{sharesize}(A \cap B) = \mathrm{sharesize}(A) \times \mathrm{sharesize}(B)$$

new intersection of ***weak*** *bFSS:*

(Ev can output multiple bits!)

$$\mathsf{Share}(A) \longrightarrow \left(\boxed{\in A?}, \boxed{\in A?}\right)$$
$$\mathsf{Share}(B) \longrightarrow \left(\boxed{\in B?}, \boxed{\in B?}\right)$$

$$\underbrace{\begin{matrix} \mathsf{Ev}\left(\boxed{\in A?}, x\right) \| \mathsf{Ev}\left(\boxed{\in B?}, x\right) \\ \mathsf{Ev}\left(\boxed{\in A?}, x\right) \| \mathsf{Ev}\left(\boxed{\in B?}, x\right) \end{matrix}}_{\text{secret shares of } 00 \iff x \in A \cap B}$$

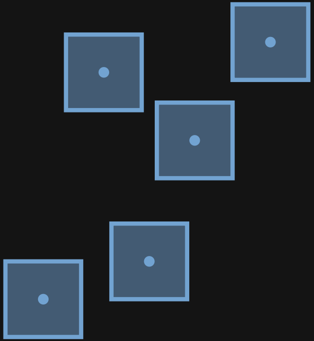
$$\mathrm{sharesize}(A \cap B) = \mathrm{sharesize}(A) + \mathrm{sharesize}(B)$$

union of ***strong*** *bFSS:*

state of the art: [BoyleGilboaIshai15]:

$\text{evalcost}(A_1 \cup \cdots \cup A_n) = n \cdot \text{evalcost}(A_i)$

new union of ***weak*** *bFSS:*

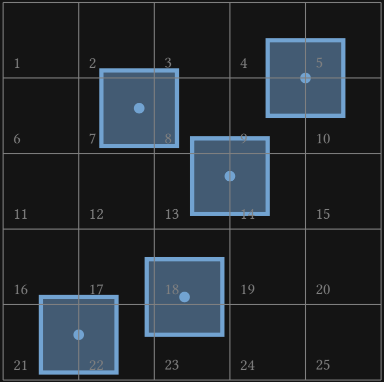


$\text{evalcost}(A_1 \cup \cdots \cup A_n) = O(\text{evalcost}(A_i))$

union of ***strong*** *bFSS:*

state of the art: [BoyleGilboaIshai15]:

new union of ***weak*** *bFSS:*



$$\mathrm{evalcost}(A_1 \cup \cdots \cup A_n) = n \cdot \mathrm{evalcost}(A_i)$$

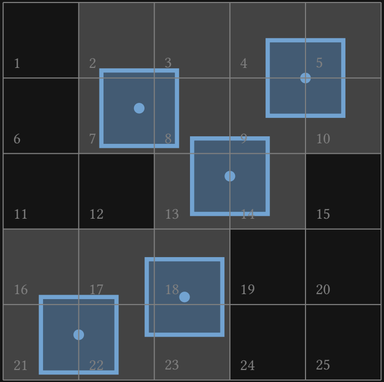
$$\mathrm{evalcost}(A_1 \cup \cdots \cup A_n) = O(\mathrm{evalcost}(A_i))$$

union of ***strong*** *bFSS:*

state of the art: [BoyleGilboaIshai15]:

$$\text{evalcost}(A_1 \cup \cdots \cup A_n) = n \cdot \text{evalcost}(A_i)$$

new union of ***weak*** *bFSS:*



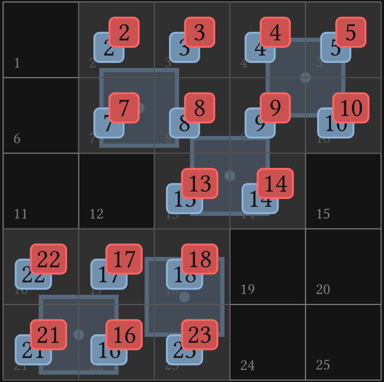
$$\text{evalcost}(A_1 \cup \cdots \cup A_n) = O(\text{evalcost}(A_i))$$

union of ***strong*** *bFSS:*

state of the art: [BoyleGilboaIshai15]:

$$\text{evalcost}(A_1 \cup \cdots \cup A_n) = n \cdot \text{evalcost}(A_i)$$

new union of ***weak*** *bFSS:*

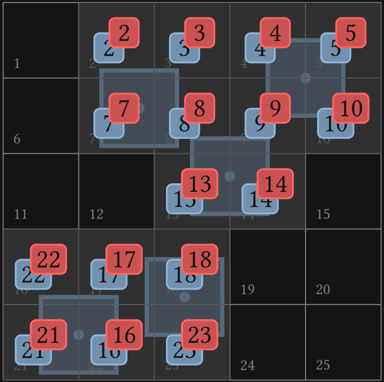


$$\text{evalcost}(A_1 \cup \cdots \cup A_n) = O(\text{evalcost}(A_i))$$

*union of **strong** bFSS:*

state of the art: [BoyleGilboaIshai15]:

*new union of **weak** bFSS:*



interpolate polynomials $P_0(id) = \boxed{id}$
$P_1(id) = \boxed{id}$

$\text{evalcost}(A_1 \cup \cdots \cup A_n) = n \cdot \text{evalcost}(A_i)$

$\text{evalcost}(A_1 \cup \cdots \cup A_n) = O(\text{evalcost}(A_i))$

n balls ; b-bit integers ; radius δ ; dimension d

n balls ; b-bit integers ; radius δ ; dimension d

		share size
strong FSS	balls disjoint	$O(n\lambda b^d)$
weak FSS	balls disjoint	$O(n\lambda(4\log\delta)^d)$
weak FSS	balls $> 4\delta$ apart	$O(n\lambda d2^d\log\delta)$
weak FSS	balls axis-disjoint	$O(n\lambda d\log\delta)$

n balls ; b-bit integers ; radius δ ; dimension d

		share size
strong FSS	balls disjoint	$O(n\lambda b^d)$
weak FSS	balls disjoint	$O(n\lambda(4\log\delta)^d)$
weak FSS	balls $> 4\delta$ apart	$O(n\lambda d2^d \log\delta)$
weak FSS	balls axis-disjoint	$O(n\lambda d\log\delta)$

stricter structure, weaker bFSS $\implies$ *smaller bFSS shares*

summary of our results

if Alice's set has
weak function secret sharing
with share size σ

then there is an OPRF/PSI protocol
with communication $O(\lambda \cdot \sigma)$

+ new weak bFSS tricks
for union of ℓ_∞ balls
(fuzzy PSI)

limitations (open problems)

- Alice's communication is O(FSS share size) but her computation is still O(cardinality)

limitations (open problems)

- Alice's communication is O(FSS share size) but her computation is still O(cardinality)
- only Alice's set has structure

limitations (open problems)

- Alice's communication is O(FSS share size) but her computation is still O(cardinality)
- only Alice's set has structure
- only semi-honest PSI

limitations (open problems)

- Alice's communication is O(FSS share size) but her computation is still O(cardinality)
- only Alice's set has structure
- only semi-honest PSI
- various exponential dependence on dimension (worse for ℓ_1 metric)

limitations (open problems)

- Alice's communication is O(FSS share size) but her computation is still O(cardinality)
- only Alice's set has structure
- only semi-honest PSI
- various exponential dependence on dimension (worse for ℓ_1 metric)
- only explored bFSS for union of balls so far

thanks!