Structure-Aware PSI

Gayathri Garimella Mike Rosulek Jaspal Singh

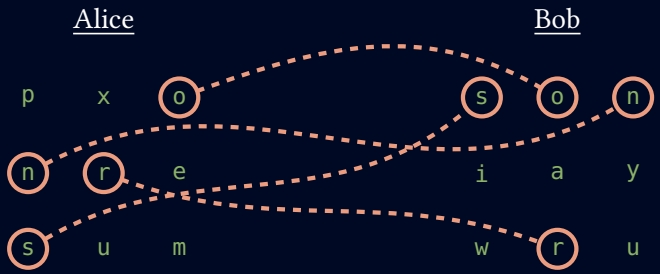
Oregon State University

CRYPTO 2022

what is private set intersection (PSI)?

Alice			Bob		
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

SANTA BARBARA

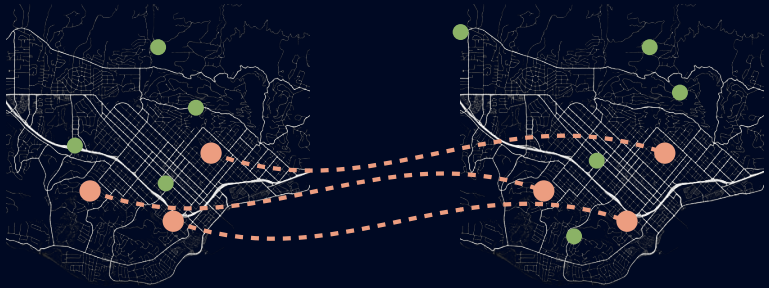
Bob

SANTA BARBARA

what if sets are geospatial points?

Alice

Bob



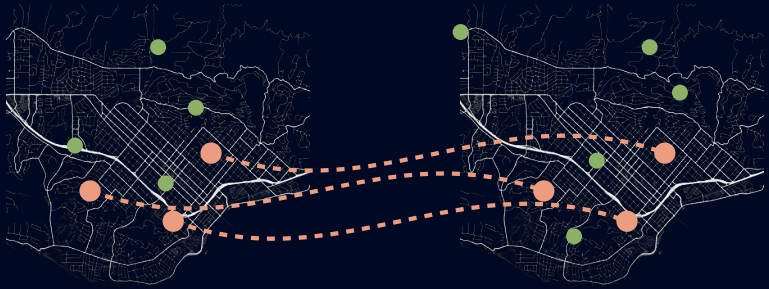
SANTA BARBARA

SANTA BARBARA

what if sets are geospatial points?

Alice

Bob



SANTA BARBARA

SANTA BARBARA

Unlikely that Alice & Bob have identical GPS coordinates

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

Alice

SANTA BARBARA

Bob

SANTA BARBARA

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

Alice

SANTA BARBARA

Bob

SANTA BARBARA

Naive fuzzy PSI: Alice enumerates all nearby points → plain PSI

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

Alice

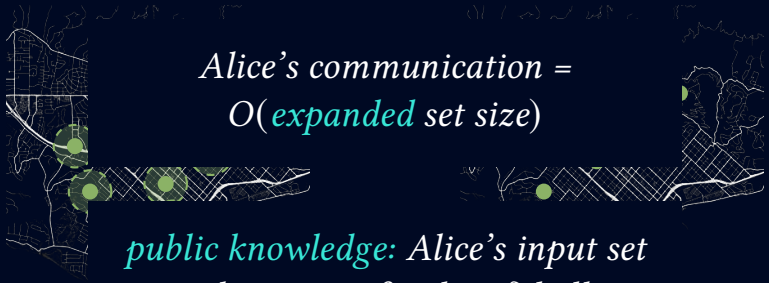
Bob

Naive fuzzy PSI: Alice enumerates all nearby points → plain PSI

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 → plain PSI

structure-aware PSI:

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

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

and more

structure-aware PSI:

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

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

and more

weak FSS:

reduce PSI to (new variant of) function secret sharing

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

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

structure-aware PSI:

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

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

and more

weak FSS:

reduce PSI to (new variant of) function secret sharing

Alice's PSI communication = $O(\lambda \cdot$ 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:

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

Bob:

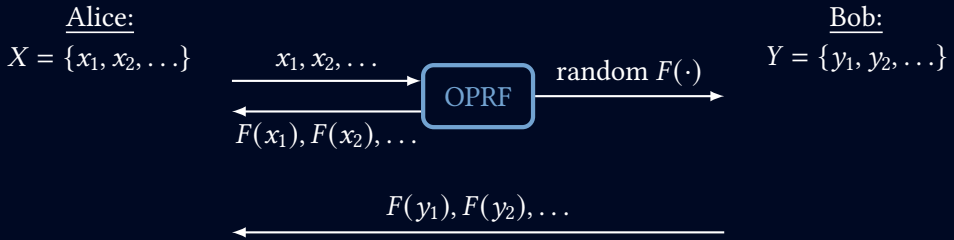
$Y = \{y_1, y_2, \ldots\}$

oblivious PRF (OPRF) paradigm for PSI

[FreedmanIshaiPinkasReingold05]

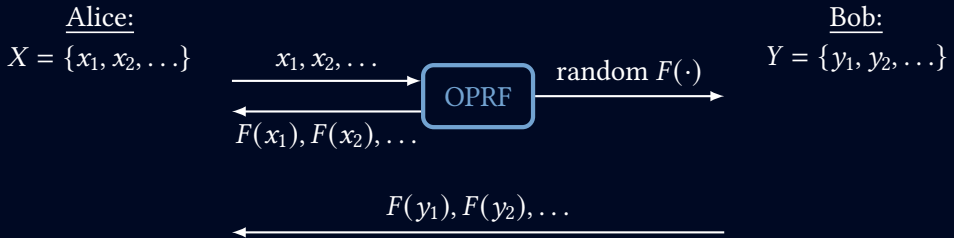
oblivious PRF (OPRF) paradigm for PSI

[FreedmanIshaiPinkasReingold05]



oblivious PRF (OPRF) paradigm for PSI

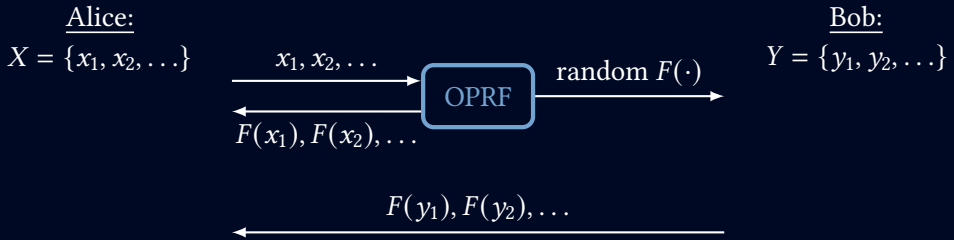
[FreedmanIshaiPinkasReingold05]



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

oblivious PRF (OPRF) paradigm for PSI

[FreedmanIshaiPinkasReingold05]



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

structure-aware OPRF: Alice's communication = $O(\lambda \cdot$ 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)

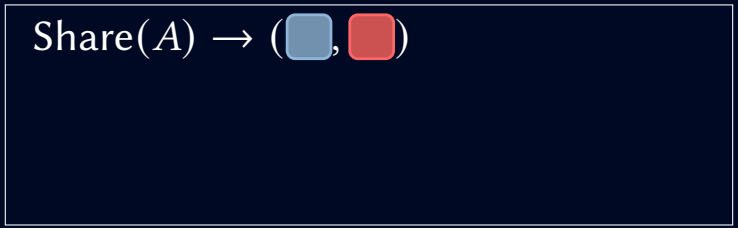
and hence a structure-aware PSI with Alice communication $O(\lambda \cdot \sigma)$

boolean function secret sharing (bFSS)

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

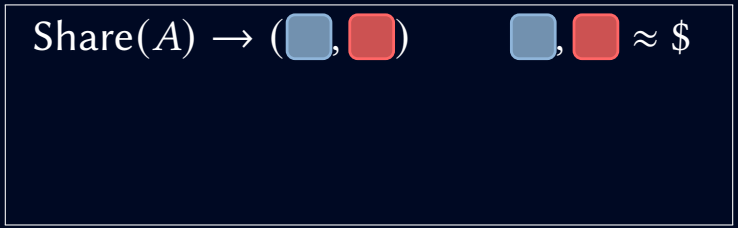
boolean function secret sharing (bFSS)

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



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

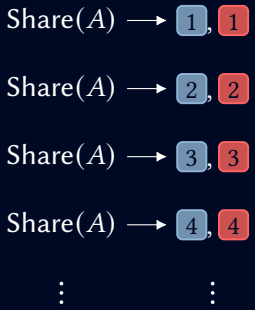
$\mathsf{Share}(A) \to (\blacksquare, \blacksquare)$ $\qquad$ $\blacksquare, \blacksquare \approx \$$

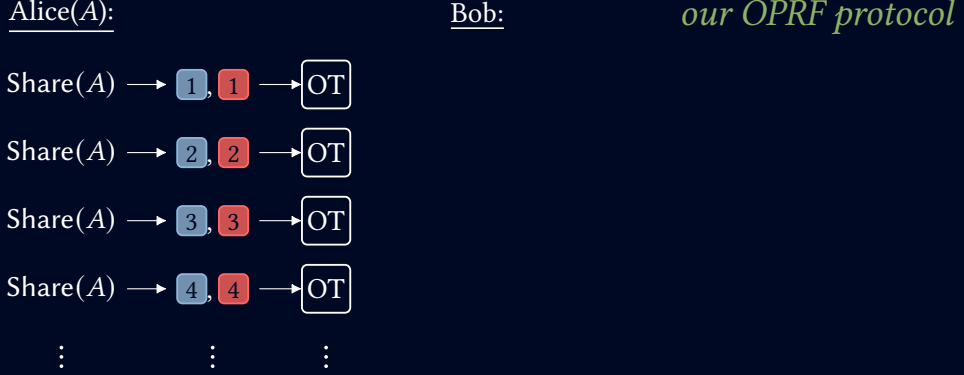
$x \in A \implies \mathsf{Ev}(\blacksquare, x) \oplus \mathsf{Ev}(\blacksquare, x) = 0$

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

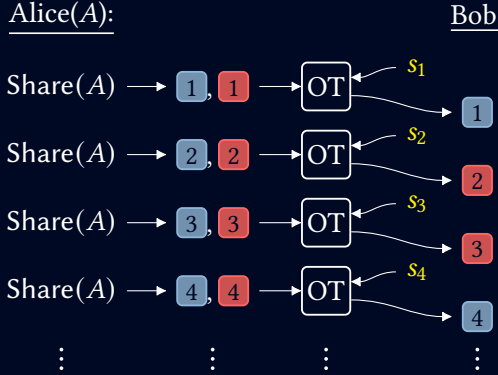
Alice(A): Bob: *our OPRF protocol*

Alice(A): Bob: *our OPRF protocol*

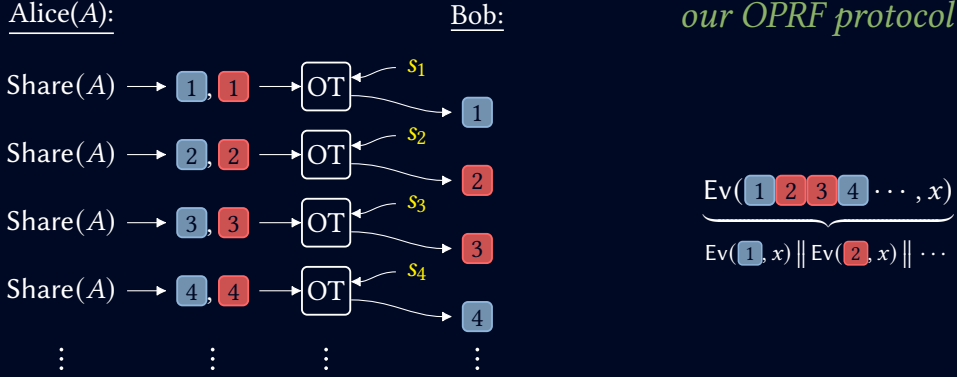


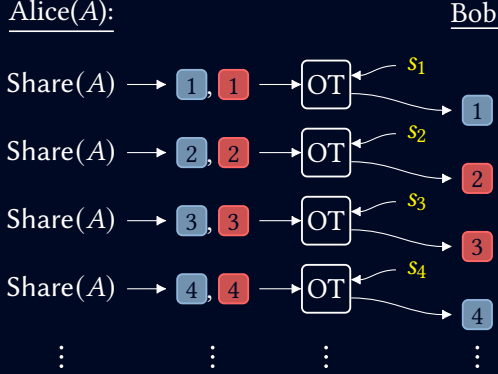

Alice(A):
Bob:
our OPRF protocol
Share(A)
1
1
OT
Share(A)
2
2
OT
Share(A)
3
3
OT
Share(A)
4
4
OT

our OPRF protocol



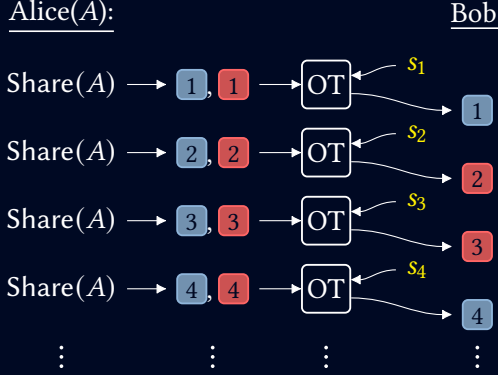
our OPRF protocol





our OPRF protocol

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

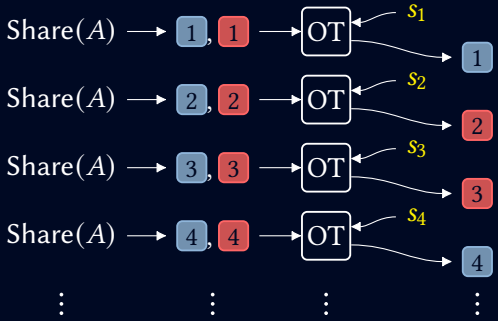


our OPRF protocol

$$F(x) \stackrel{\text{def}}{=} H\Big(\underbrace{\mathsf{Ev}(\square_1\ \square_2\ \square_3\ \square_4\ \cdots, x)}_{\mathsf{Ev}(\square_1, x) \,\|\, \mathsf{Ev}(\square_2, x) \,\|\, \cdots}\Big)$$

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

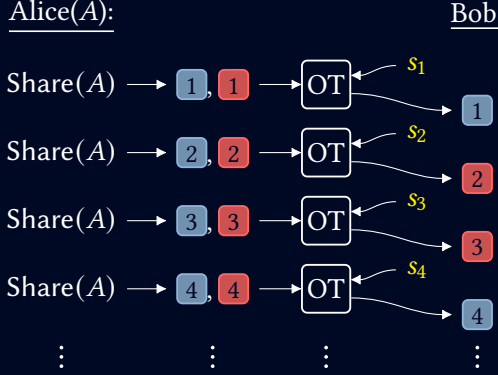
our OPRF protocol



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

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

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

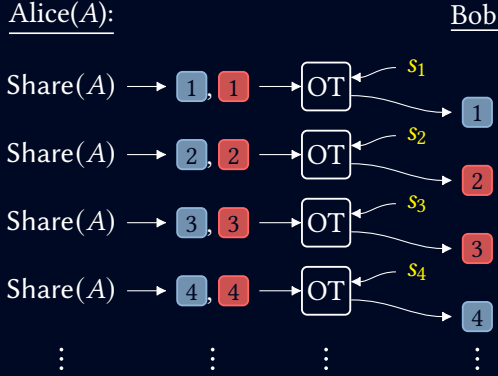


our OPRF protocol

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

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

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



our OPRF protocol

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

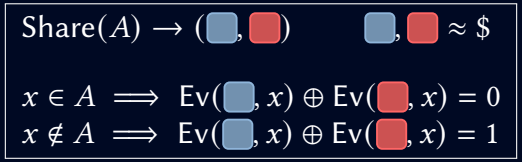
$$\boxed{x \in A} \implies \mathsf{Ev}(\square, x) = \mathsf{Ev}(\square, x)$$

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

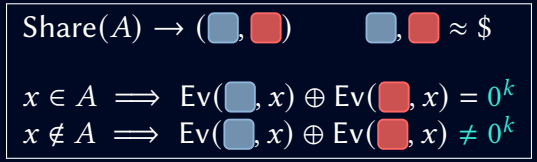
$$F(x) = H\Big(\mathsf{Ev}(1\,2\,3\,4\cdots, x)\Big)$$
$$= H\Big(\mathsf{Ev}(1\,2\,3\,4\cdots, x)\Big)$$

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

(new) (p, k)−weak bFSS



(new) (p, k)−weak bFSS



1. Ev can output multiple bits

(new) (p, k)−weak bFSS

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

(new) (p, k)–weak bFSS

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

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

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

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

basic bFSS

with 128 (,) pairs:

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

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

weak bFSS ($p = 1/2$)

with 440 (,) pairs:

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

basic bFSS

with 128 (,) pairs:

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

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

weak bFSS ($p = 1/2$)

with 440 (,) pairs:

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

at least 128 pairs satisfy:
$\mathsf{Ev}(, x) = \mathsf{Ev}(, x) \oplus 1$

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

basic bFSS

with 128 (,) pairs:

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

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

weak bFSS ($p = 1/2$)

with 440 (,) pairs:

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

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

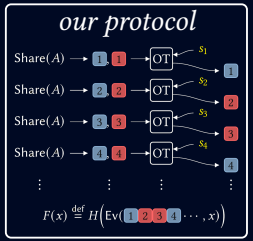
128 bits of entropy!

PSI from bFSS for unstructured sets

PSI from bFSS for unstructured sets

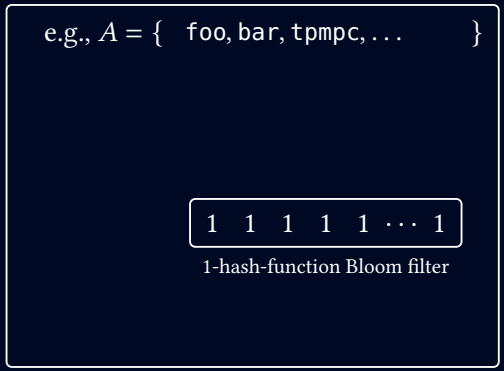
weak/strong bFSS for unstructured sets

+

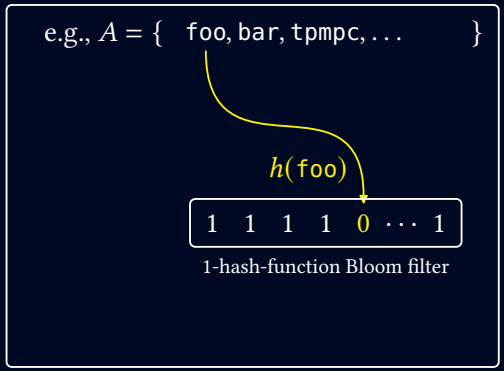


= PSI

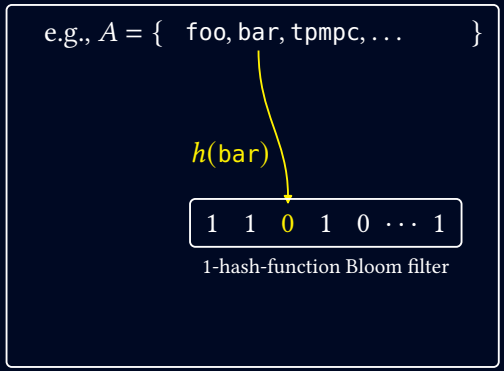
*weak bFSS for **arbitrary sets**, from Bloom filters*



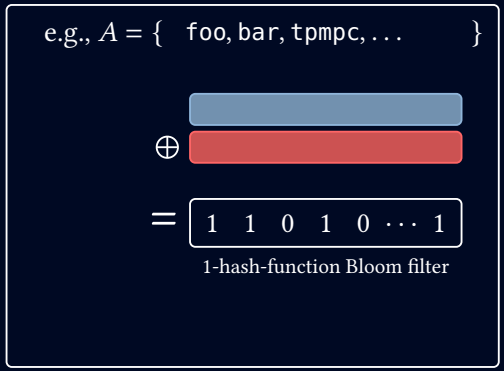
*weak bFSS for **arbitrary sets**, from Bloom filters*



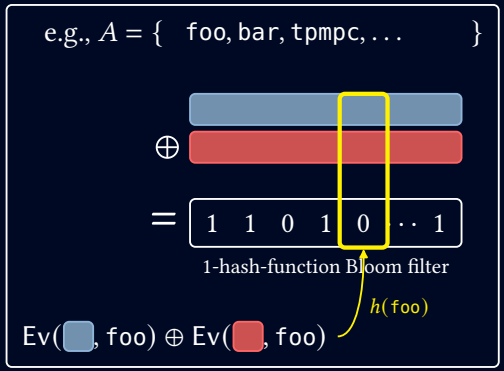
*weak bFSS for **arbitrary sets**, from Bloom filters*



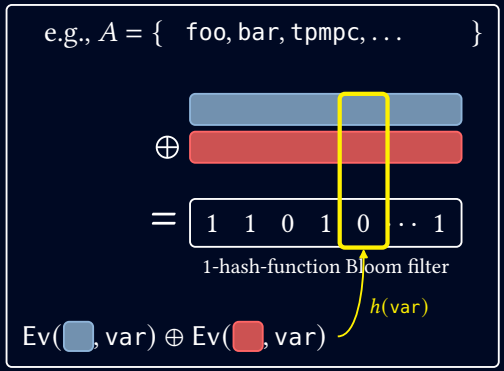
*weak bFSS for **arbitrary sets**, from Bloom filters*



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



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



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

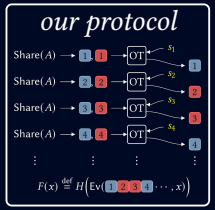
e.g., $A = \{$ `foo`, `bar`, `tpmpc`, $\ldots$ $\}$

$\oplus$

$=$ 1 1 0 1 0 $\cdots$ 1

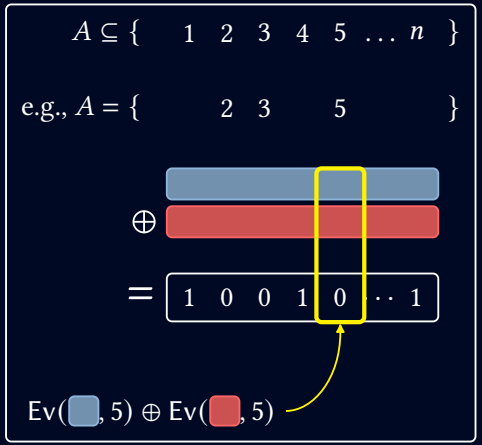
1-hash-function Bloom filter

$+$

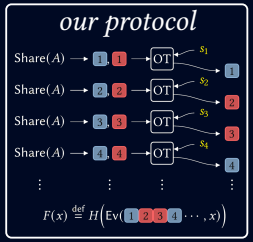


$=$ [ChaseMiao20]

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



$+$



$=$ IKNP

[IshaiKilianNissimPetrank03]

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

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

■ = a PRF seed

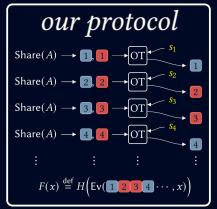
P = coeffs. of a polynomial s.t.

$F(■, a) =$ P(a) for $a \in A$

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

+

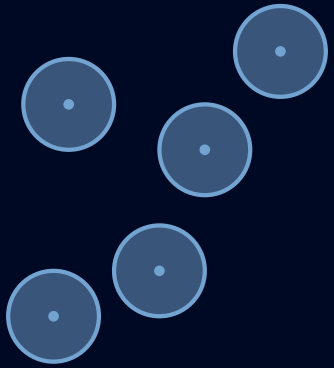
our protocol



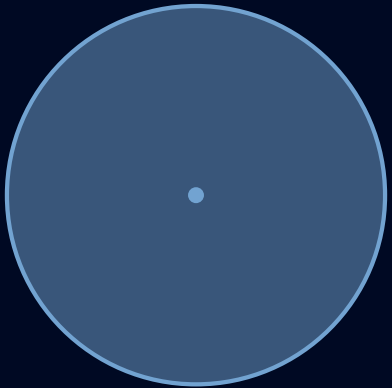
= `spot-light`

[PinkasRosulekTrieuYanai19]

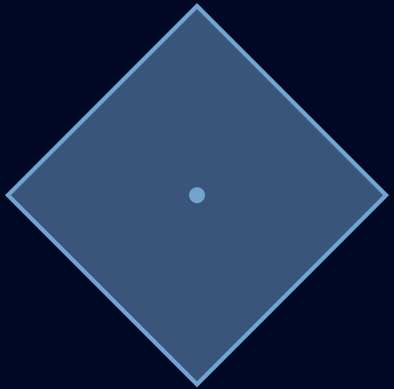
bFSS for structured sets



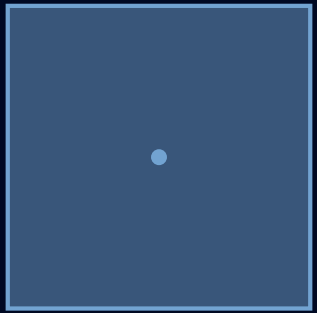
Alice’s set (in fuzzy PSI) = union of balls



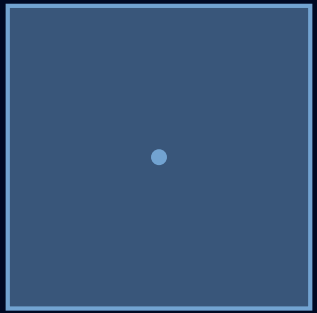
an ℓ_2 ball



an ℓ_1 ball



an ℓ_∞ ball



an ℓ_∞ ball

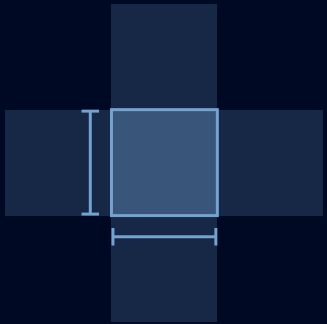
ℓ_∞ intersection of d intervals
ℓ_1 intersection of 2^{d-1} intervals

strong bFSS (n balls; dimension d; b bit numbers)

[BoyleGilboaIshai18]

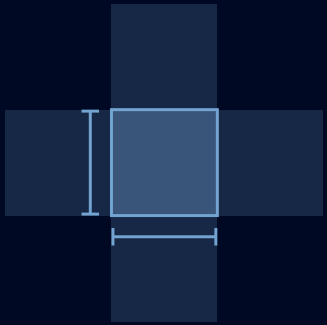
strong bFSS (n balls; dimension d; b bit numbers)

[BoyleGilboaIshai18]



strong bFSS (n balls; dimension d; b bit numbers)

[BoyleGilboaIshai18]

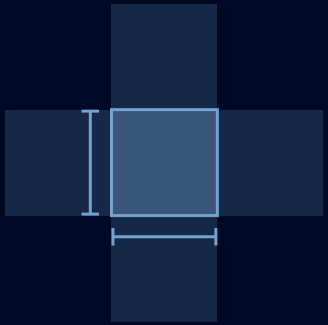


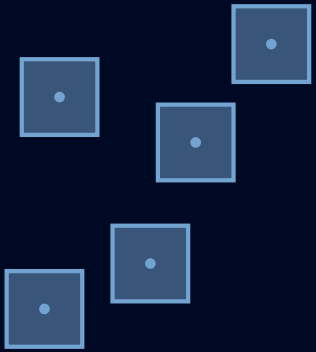
ball = **intersection** of intervals

FSS key size = $O(\lambda b^d)$

strong bFSS (n balls; dimension d; b bit numbers)

[BoyleGilboaIshai18]



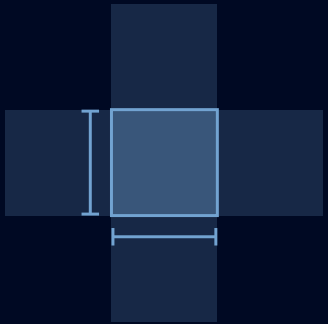


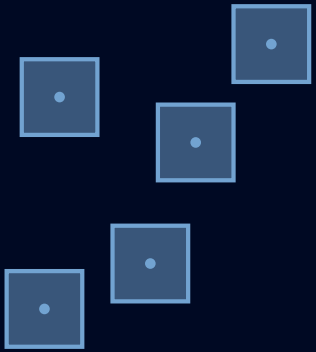
ball = **intersection** of intervals

FSS key size = $O(\lambda b^d)$

strong bFSS (n balls; dimension d; b bit numbers)

[BoyleGilboaIshai18]





ball = **intersection** of intervals

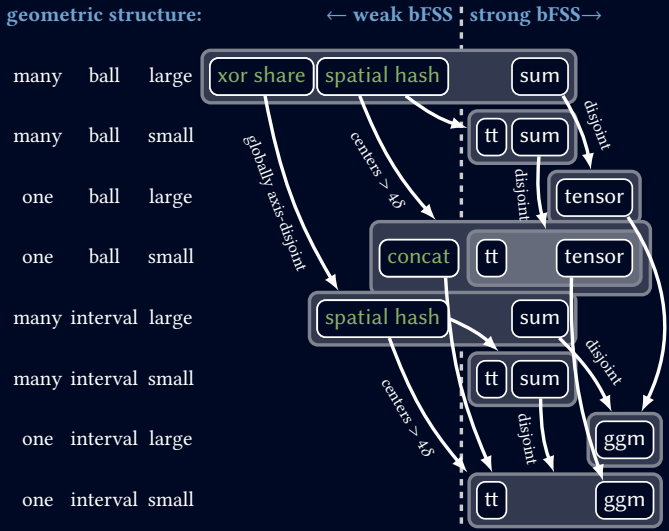
FSS key size = $O(\lambda b^d)$

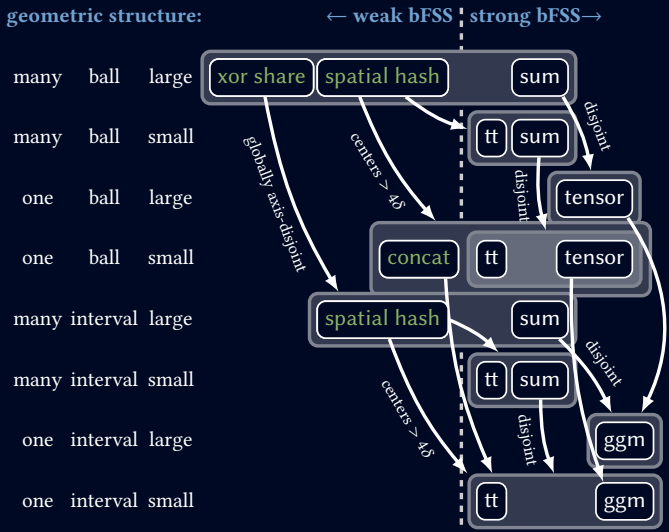
Alice's set = **union** of balls

FSS key size = $O(n\lambda b^d)$

evalcost = $n \times$ evalcost(1 ball)

new weak bFSS for union of balls


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
globally axis-disjoint
centers > 4δ
disjoint
tt
sum
tensor
concat
tt
tensor
spatial hash
sum
disjoint
centers > 4δ
tt
sum
disjoint
ggm
tt
ggm



our bFSS contributions:

simple constructions

scratched the surface

weak bFSS $\Longrightarrow$
more efficient bFSS

(multi-bit output; false positives)

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

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

$$\text{Share}(A) \longrightarrow (\in A?, \in A?)$$
$$\text{Share}(B) \longrightarrow (\in B?, \in B?)$$

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

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

(Ev can output multiple bits!)

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

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

(Ev can output multiple bits!)

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

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

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

(Ev can output multiple bits!)

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

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

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

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

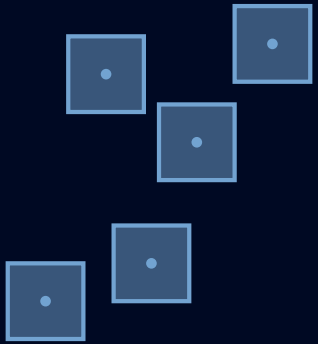
(Ev can output multiple bits!)

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

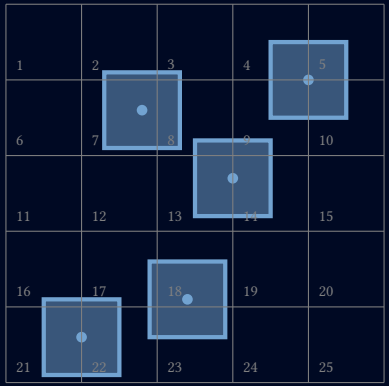
$$\text{sharesize}(A \cap B) = \text{sharesize}(A) + \text{sharesize}(B)$$

$(1, d)$ weak bFSS for l_∞ ball - share size: $O(\lambda d)$

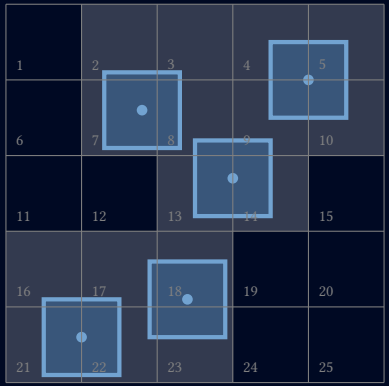
***Spatial hashing**: new **weak** bFSS for union of balls*



***Spatial hashing**: new **weak** bFSS for union of balls*

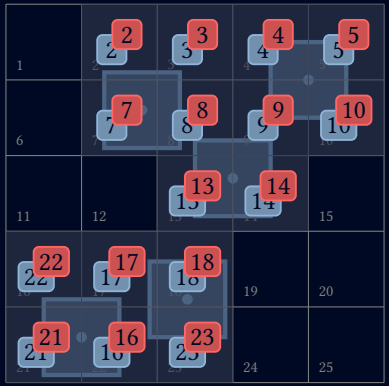


***Spatial hashing**: new **weak** bFSS for union of balls*

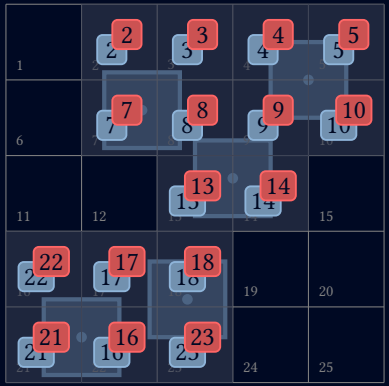


active cells - intersect with an input ball

Spatial hashing: *new* **weak** *bFSS for union of balls*

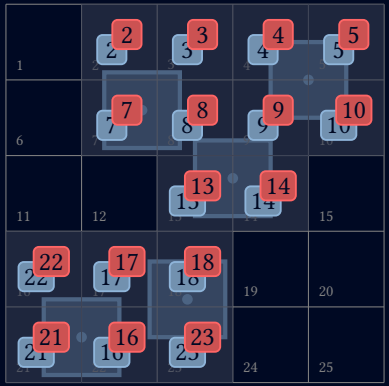


Spatial hashing: new weak bFSS for union of balls



interpolate polynomials $P_0(id) = id$, $P_1(id) = id$

Spatial hashing: new weak bFSS for union of balls



interpolate polynomials $P_0(id) = id$, $P_1(id) = id$

(weak bFSS allows for false positives)

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

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

	geometry	share size	evalcost ×cost(1 ball)
strong FSS	balls disjoint	$O(n\lambda b^d)$	n

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

	geometry	share size	evalcost ×cost(1 ball)
strong FSS	balls disjoint	$O(n\lambda b^d)$	n
weak FSS	balls disjoint	$O(n\lambda(4\log\delta)^d)$	2^d

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

	geometry	share size	evalcost ×cost(1 ball)
strong FSS	balls disjoint	$O(n\lambda b^d)$	n
weak FSS	balls disjoint	$O(n\lambda(4\log\delta)^d)$	2^d
weak FSS	balls $> 4\delta$ apart	$O(n\lambda d 2^d \log\delta)$	1
weak FSS	balls axis-disjoint	$O(n\lambda d \log\delta)$	2

stricter structure, weaker bFSS $\Longrightarrow$ *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

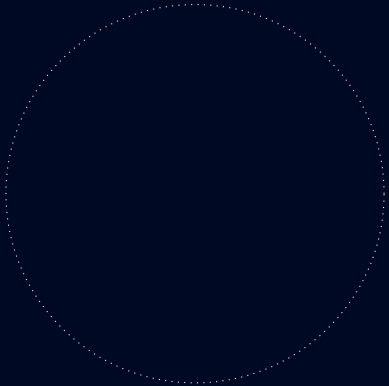
thanks!

eprint: `https://eprint.iacr.org/2022/1011`

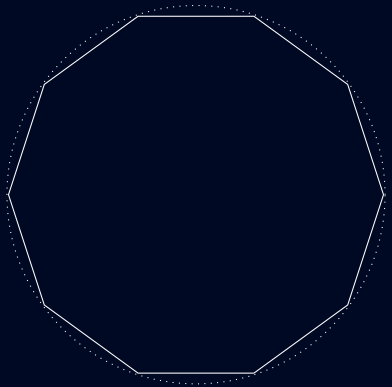
Implementation: `https://github.com/osu-crypto/FuzzyPSI`

backup slides

ℓ_2 *approximation*

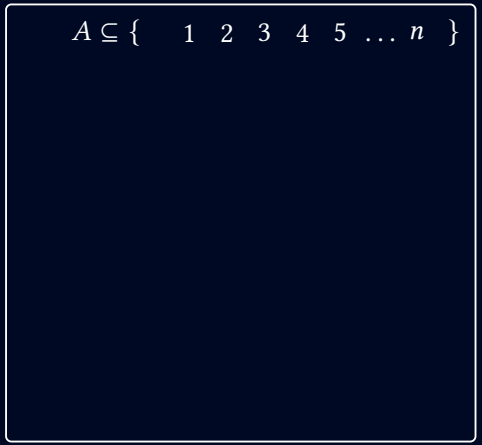


ℓ_2 approximation

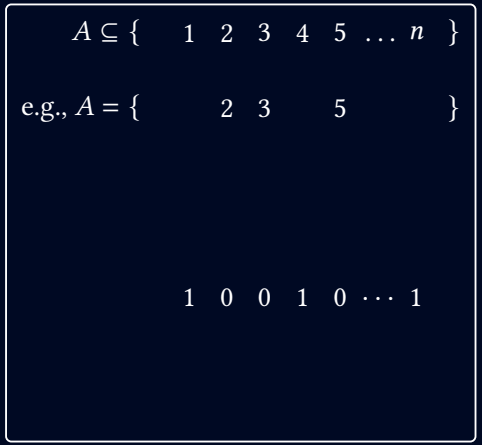


Approximate the l_2 ball by a polyhedron

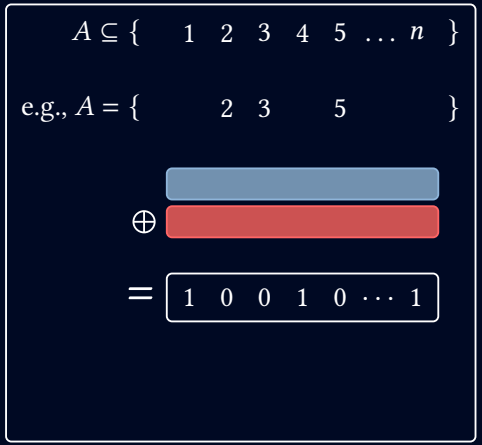
(trivial) bFSS for subsets of $[n]$



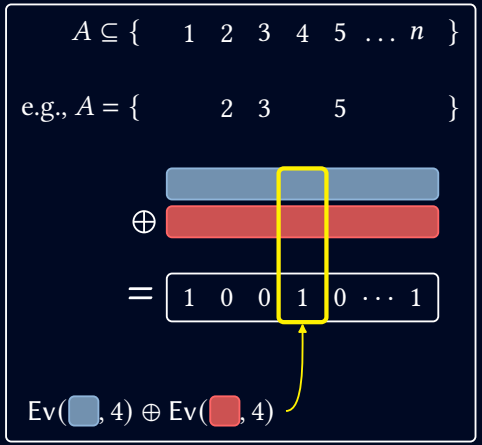
(trivial) bFSS for subsets of $[n]$



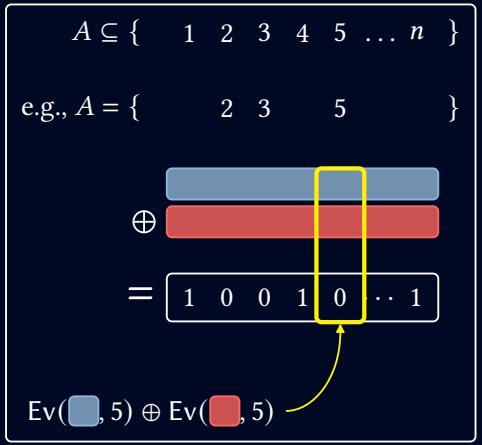
(trivial) bFSS for subsets of $[n]$



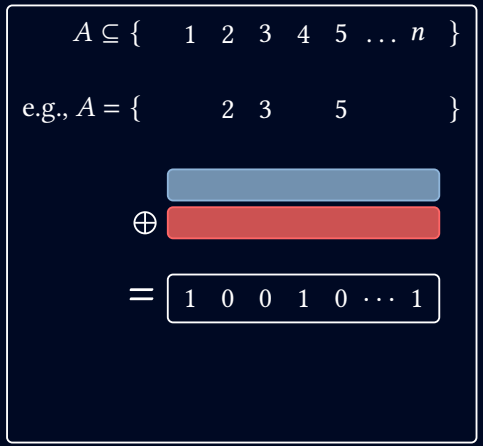
(trivial) bFSS for subsets of $[n]$



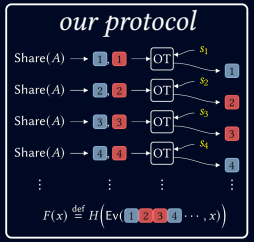
(trivial) bFSS for subsets of $[n]$



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



$+$



$=$ IKNP

[IshaiKilianNissimPetrank03]

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

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

 = a PRF seed

 = coeffs. of a polynomial s.t.

$F($  $, a) =$  (a) for $a \in A$

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

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

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

 = a PRF seed

 = coeffs. of a polynomial s.t.

$F($  $, a) =$  (a) for $a \in A$

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

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

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

■ = a PRF seed

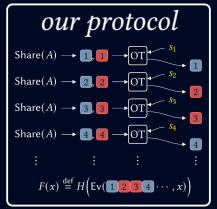
P = coeffs. of a polynomial s.t.

$F(■, a) =$ P(a) for $a \in A$

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

+

our protocol



= spot-light

[PinkasRosulekTrieuYanai19]

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

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

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

plain 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
plain PSI	1-hash Bloom filter	any set	$O(\|A\|)$
plain PSI	polynomial	any set	$\|A\|$
	???	union of radius-δ balls (for fuzzy PSI)	$\ll \|A\|$