Threshold Private Set Intersection with Better Communication Complexity

Satrajit Ghosh & Mark Simkin

Private Set Intersection

1	3	4	8	9

1	2	3	4	5

Private Set Intersection

1	3	4	8	9

1	2	3	4	5

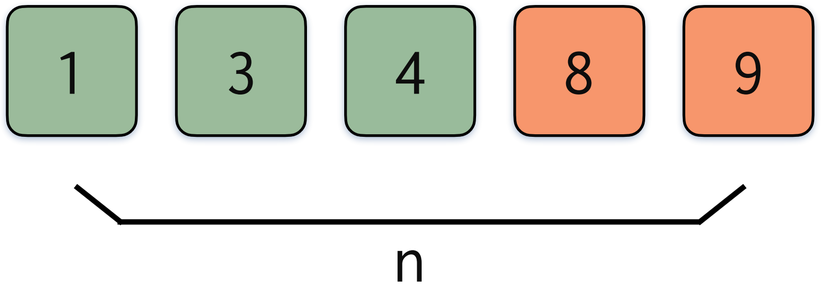
Threshold PSI

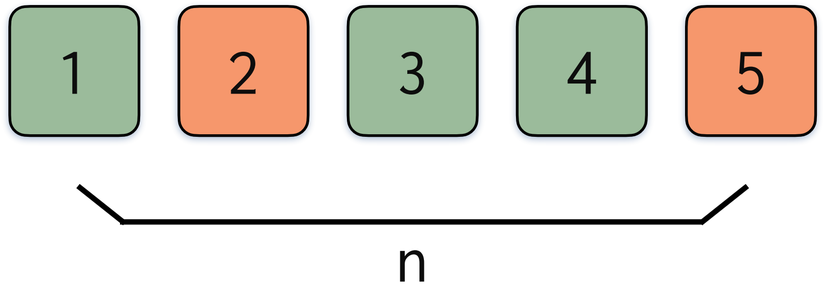
1	3	4	8	9

1	2	3	4	5

Only compute intersection when large enough

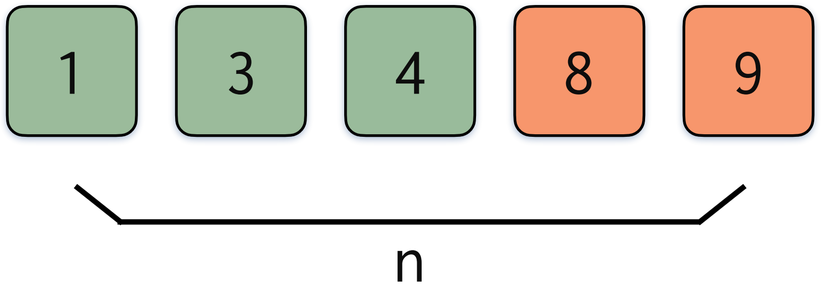
Threshold PSI

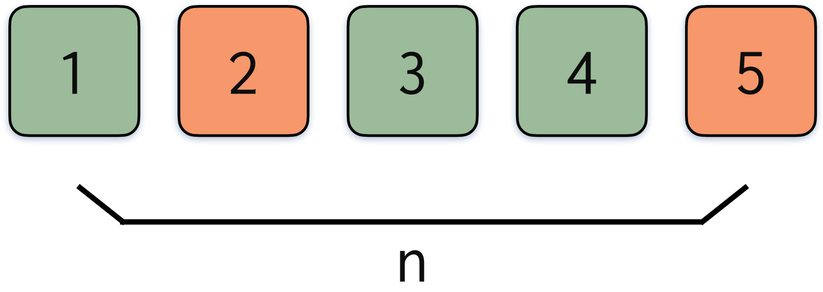




Only compute intersection when large enough

Threshold PSI





Only compute intersection when ~~large enough~~
larger than n-t

Threshold PSI

1	3	4	8	9

n

1	2	3	4	5

n

Communication can just depend on t [GS19]

Threshold PSI

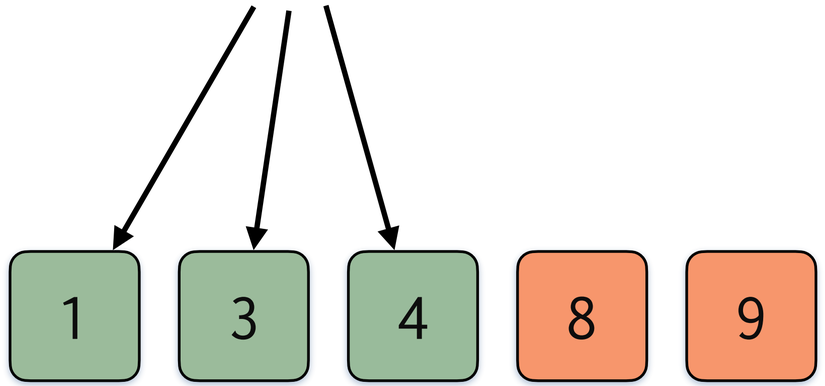
High-Level Idea

Communication can just depend on t [GS19]

Threshold PSI

High-Level Idea

To determine intersection

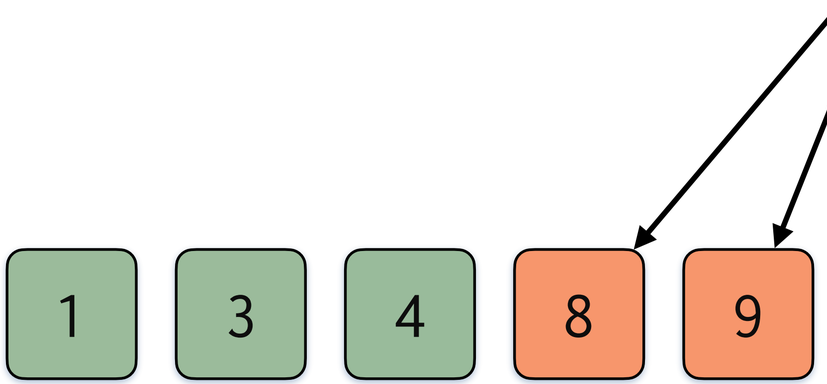


Communication can just depend on t [GS19]

Threshold PSI

High-Level Idea

To determine intersection, determine difference



Communication can just depend on t [GS19]

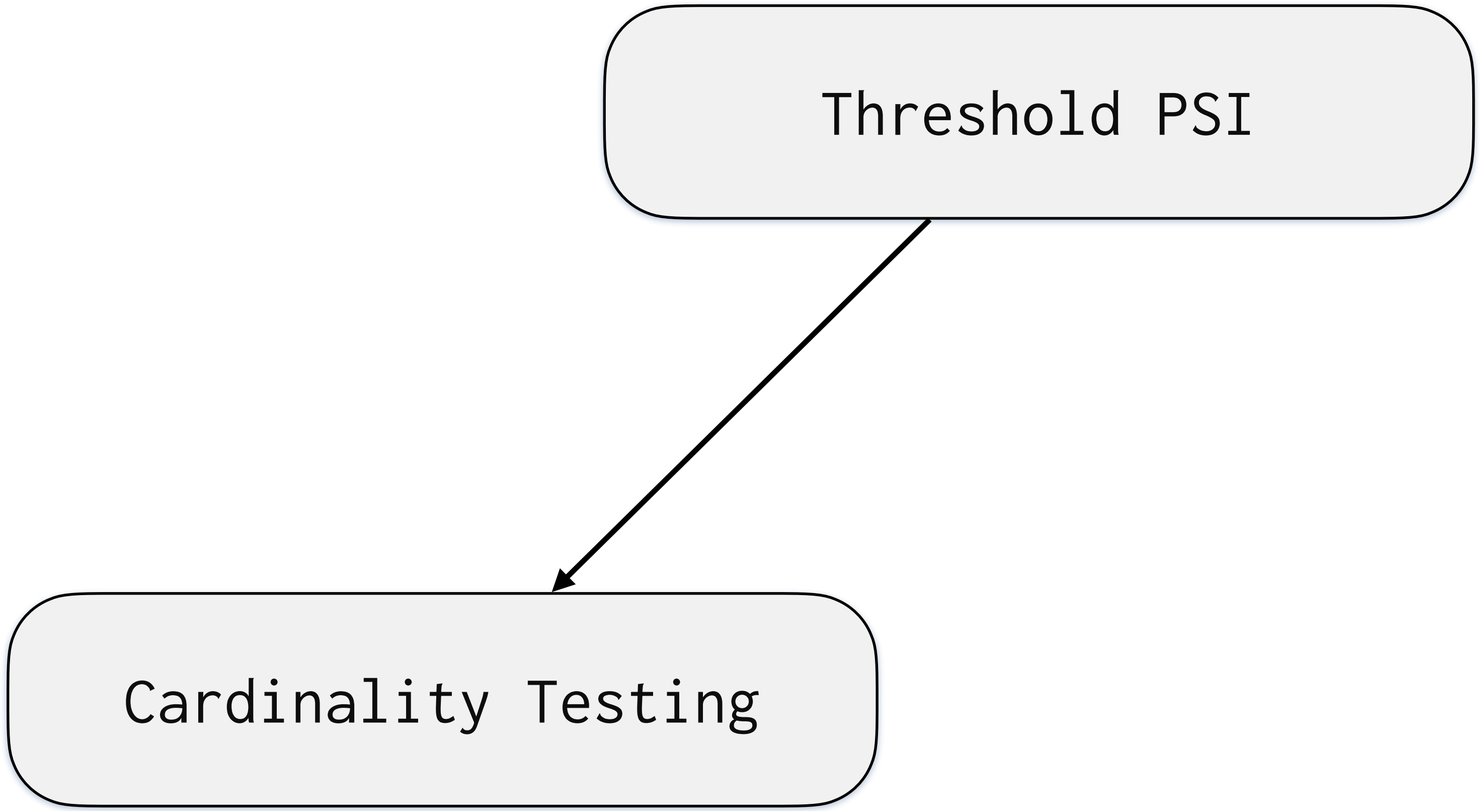
Construction Blueprint

[Ghosh & Simkin 2019]

Threshold PSI

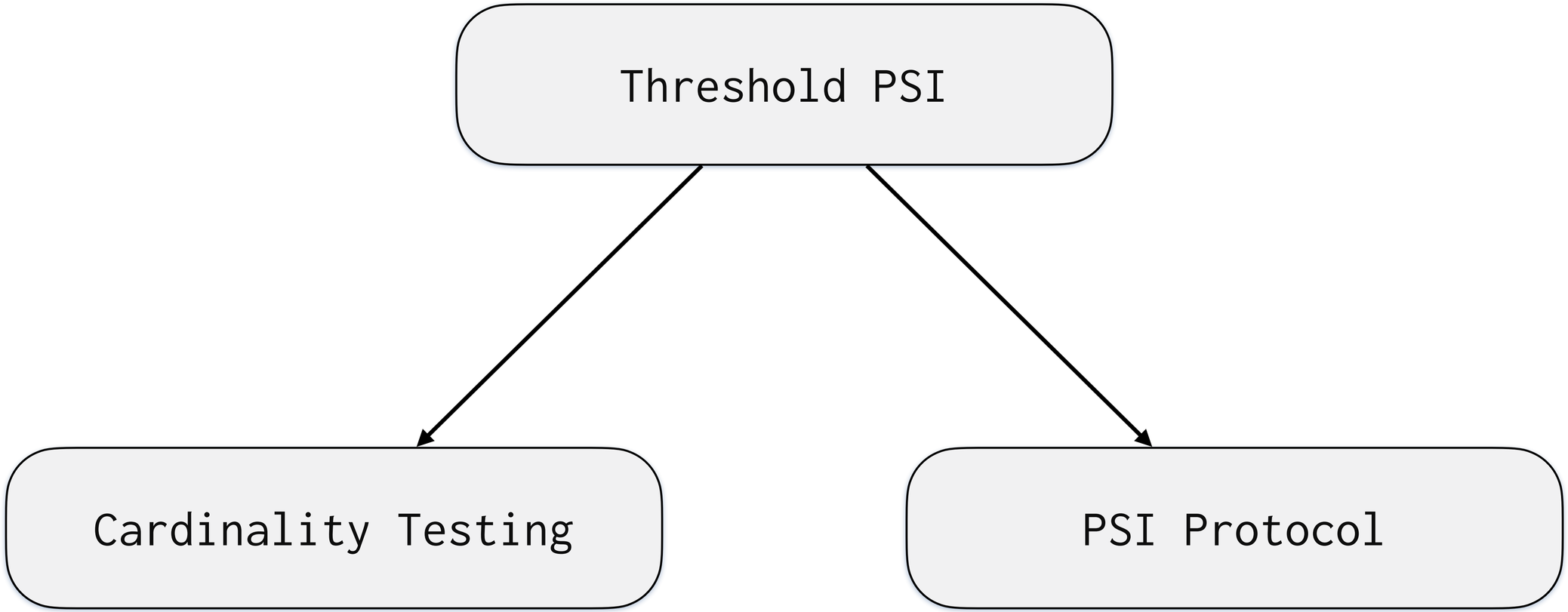
Construction Blueprint

[Ghosh & Simkin 2019]



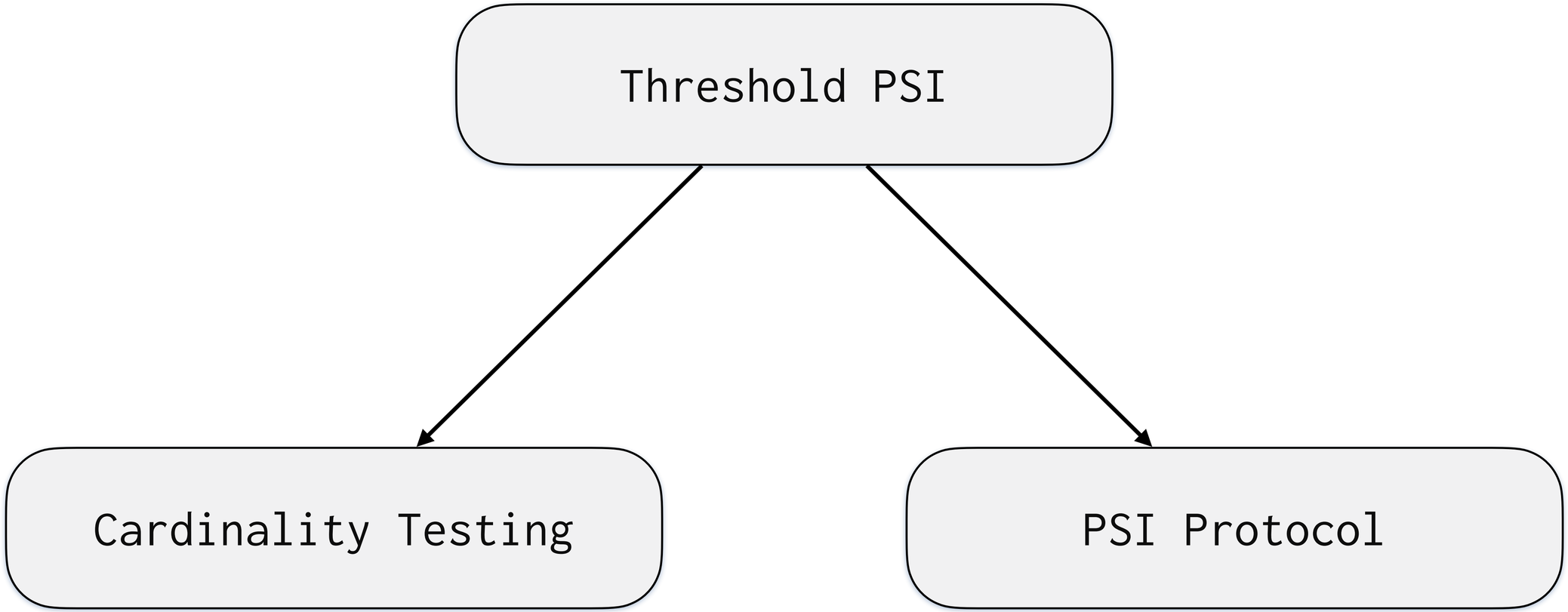
Construction Blueprint

[Ghosh & Simkin 2019]



Construction Blueprint

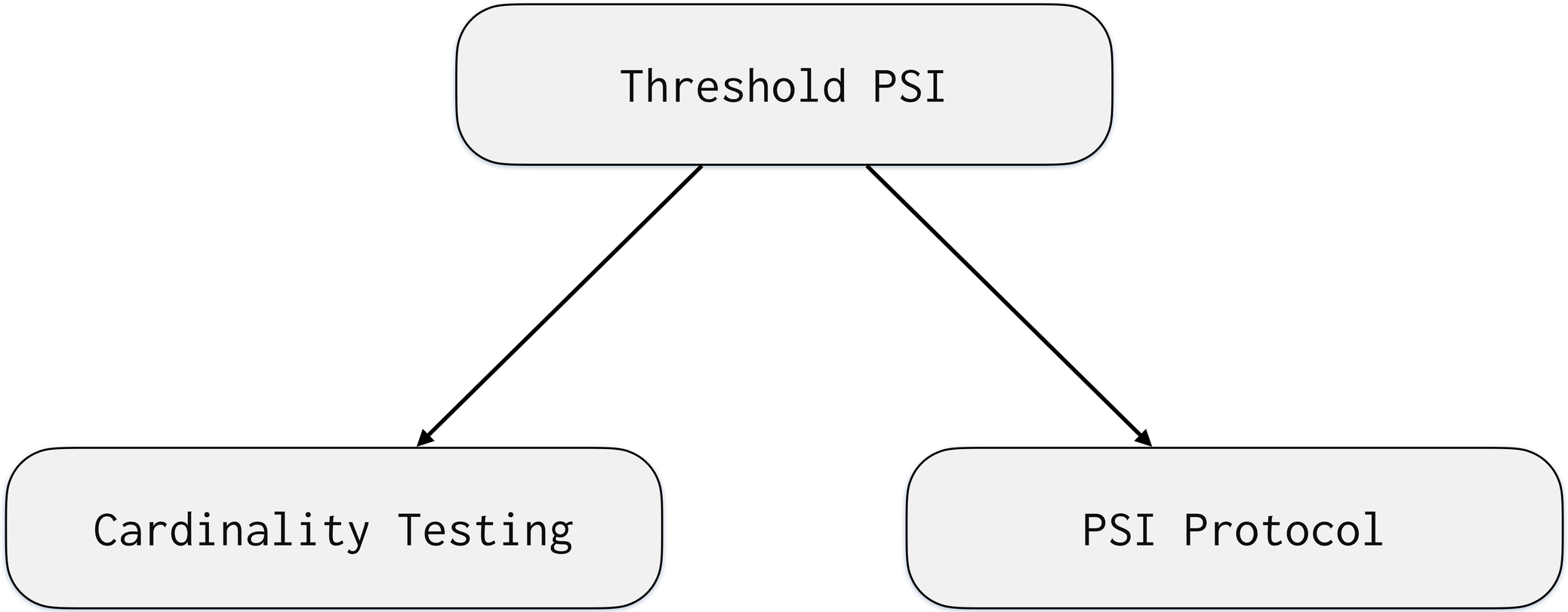
[Ghosh & Simkin 2019]



Secure if intersection large

Construction Blueprint

[Ghosh & Simkin 2019]

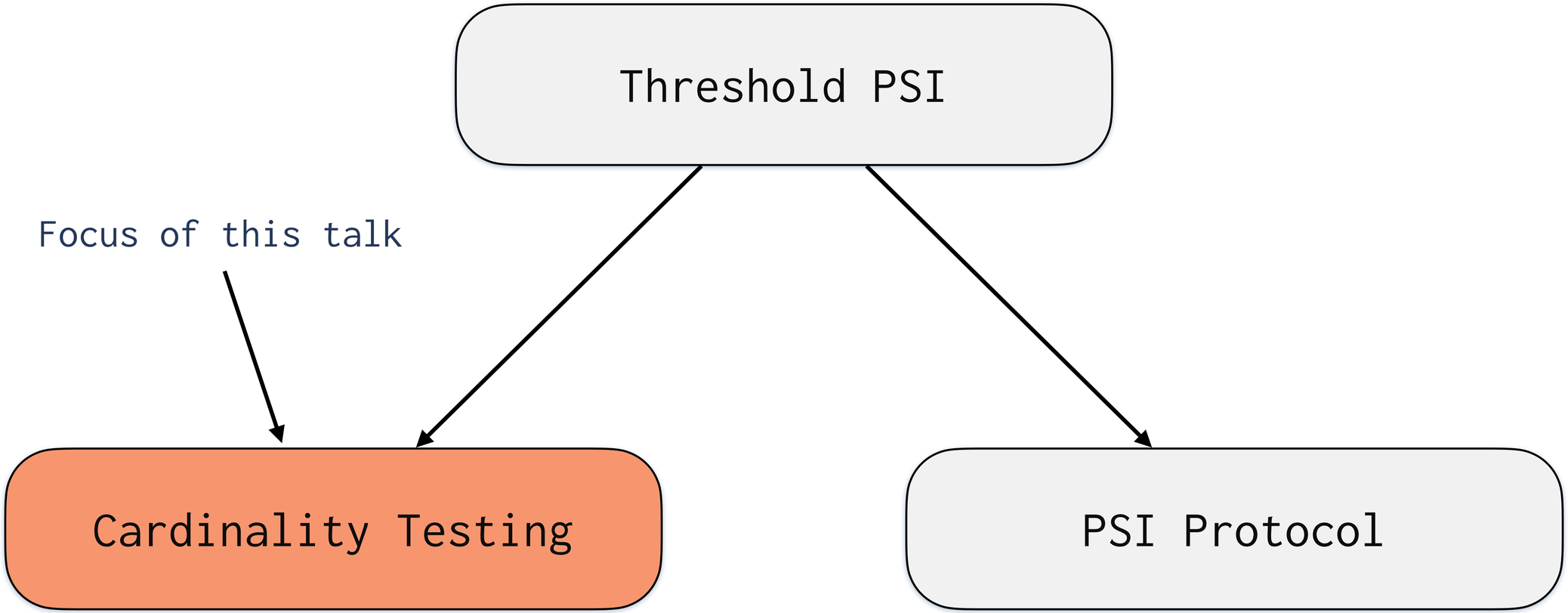


Secure if intersection large

“Solved” in [GS19]

Construction Blueprint

[Ghosh & Simkin 2019]



Secure if intersection large

“Solved” in [GS19]

What We Know

What We Know

Lower Bounds [GS19, BDP21]

Need linear in t communication

What We Know

Ignoring Polylogs

Lower Bounds [GS19, BDP21]

Need linear in t communication

Two Parties

$O(t)$ from FHE [GS19]

$O(t^2)$ from AHE [GS19]

$O(t)$ from AHE [BMRR21]

What We Know

Ignoring Polylogs

Lower Bounds [GS19, BDP21]

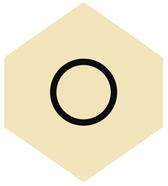
Need linear in t communication

Two Parties

$O(t)$ from FHE [GS19]

$O(t^2)$ from AHE [GS19]

$O(t)$ from AHE [BMRR21]



Many Parties

$O(t^2)$ from AHE [BMRR21]*

$O(t^2)$ from AHE [BDP21]

What We Know

Ignoring Polylogs

Lower Bounds [GS19, BDP21]

Need linear in t communication

Two Parties

O(t) from FHE [GS19]

$O(t^2)$ from AHE [GS19]

O(t) from AHE [BMRR21]

Many Parties

$O(t^2)$ from AHE [BMRR21]*

$O(t^2)$ from AHE [BDP21]

This Work

Compiler

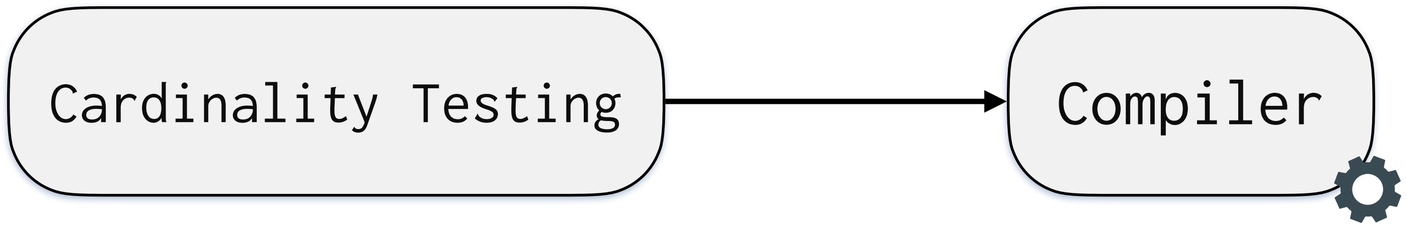
Poly(t) –> O(t·eps)

Our Contribution

Ignoring Polylogs

Our Contribution

Ignoring Polylogs



- Secret shared outputs
- Poly(t) communication

Our Contribution

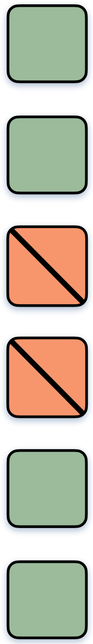
Ignoring Polylogs

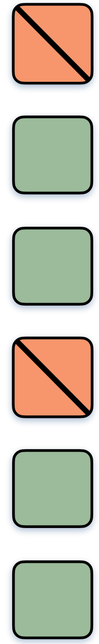
- Secret shared outputs
- Poly(t) communication

- Fails w.p. $O(2^{-eps})$
- $O(t \cdot eps)$ communication

Cardinality Testing

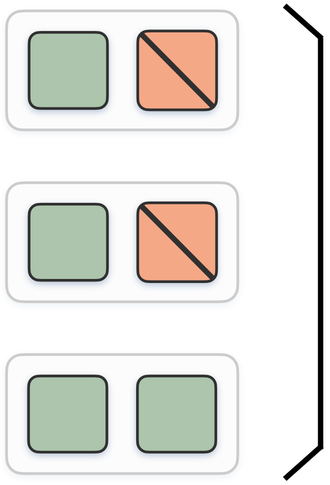
Divide & Conquer



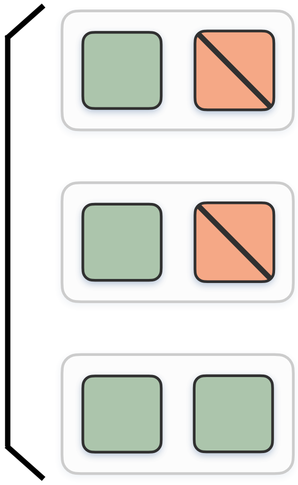


Cardinality Testing

Divide & Conquer



t buckets

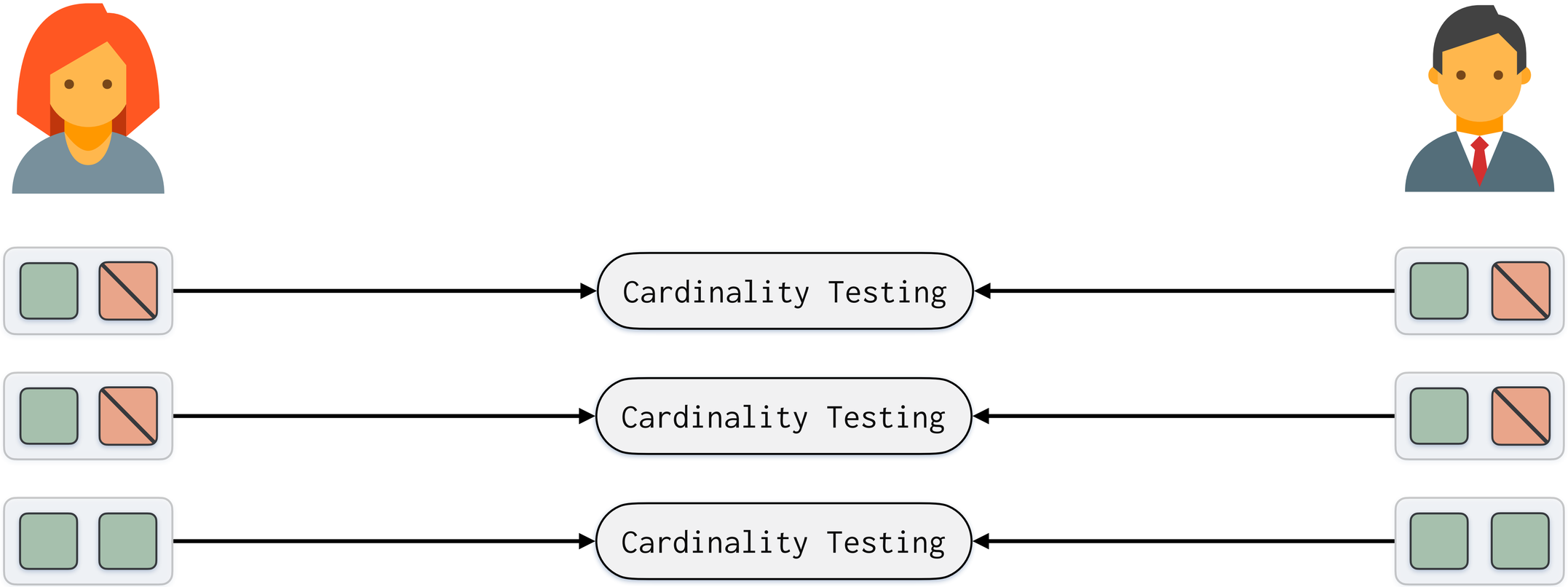


Cardinality Testing

Divide & Conquer

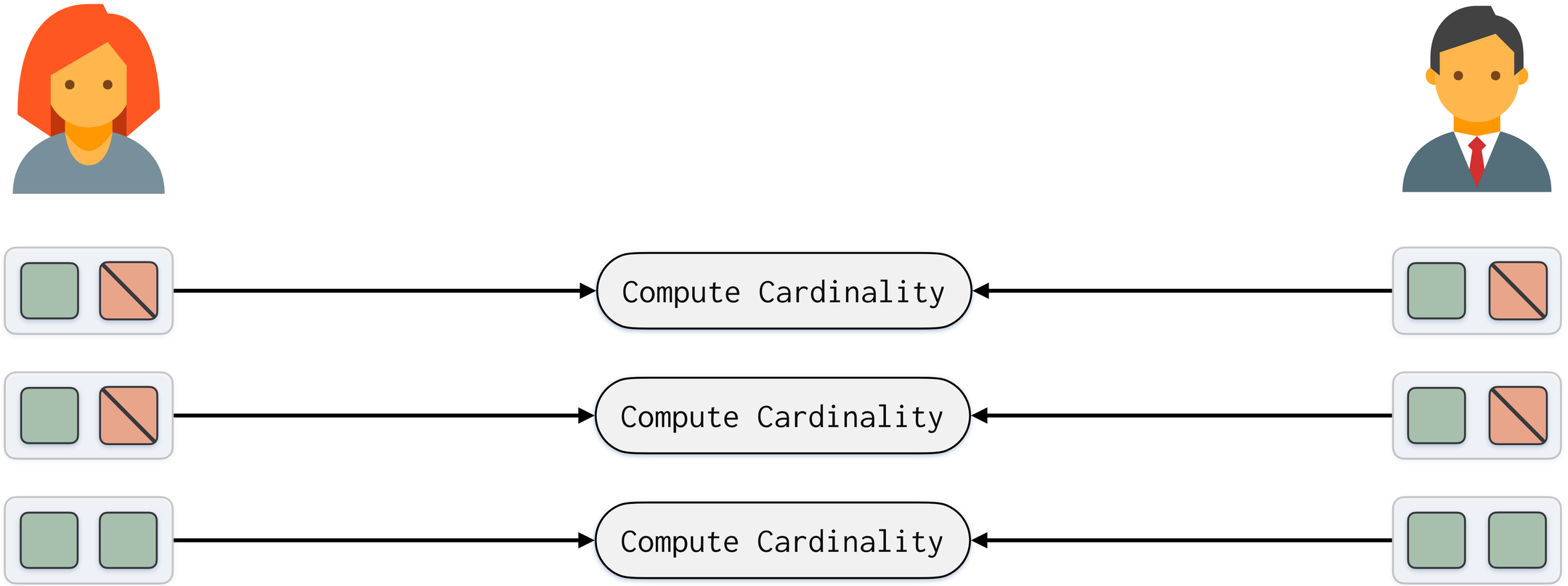
Cardinality Testing

Divide & Conquer



Cardinality Testing

Divide & Conquer



Cardinality Testing

Divide & Conquer

1

1

2

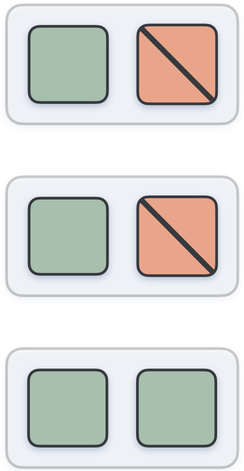
Cardinality Testing

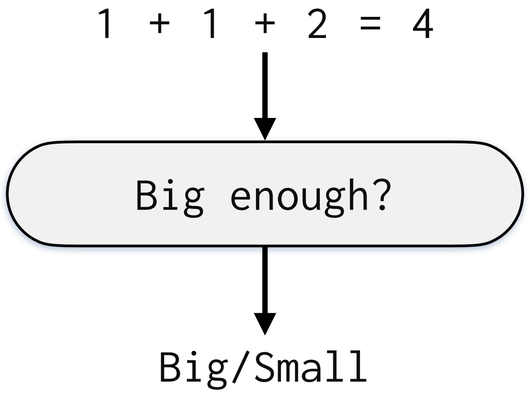
Divide & Conquer

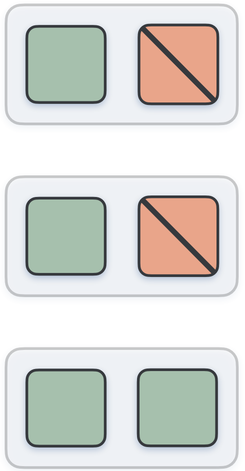
1 + 1 + 2 = 4

Cardinality Testing

Divide & Conquer

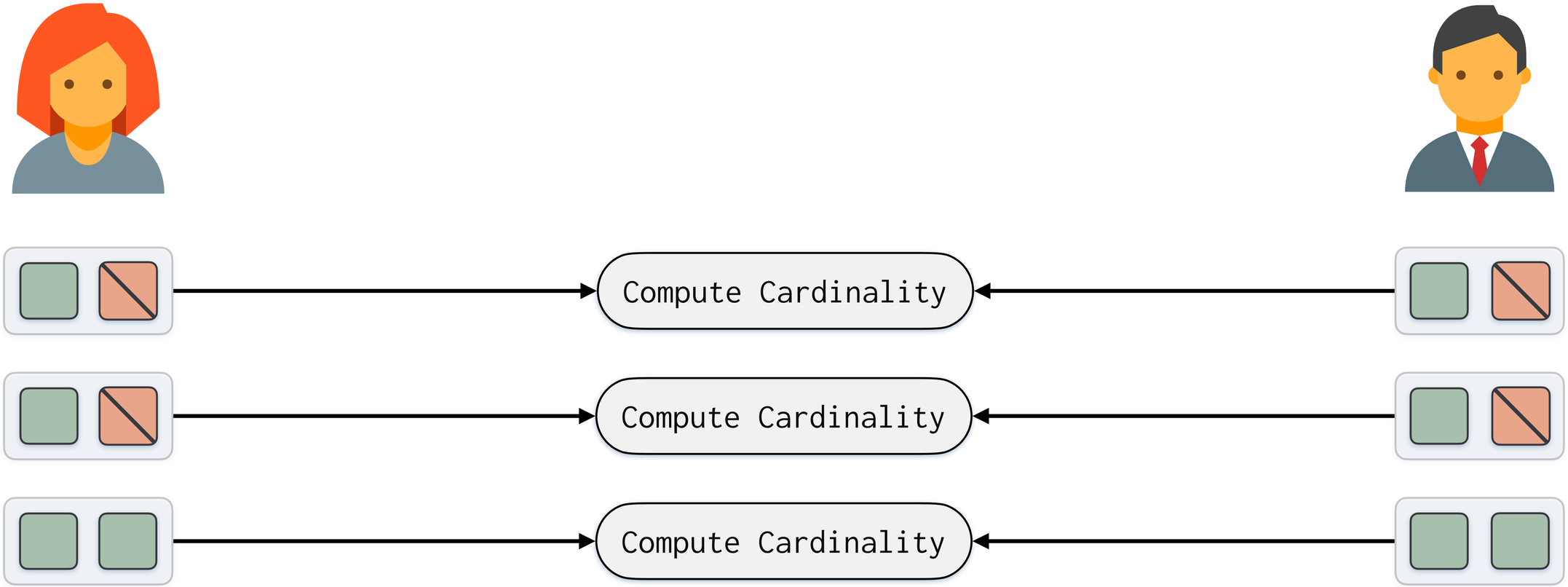






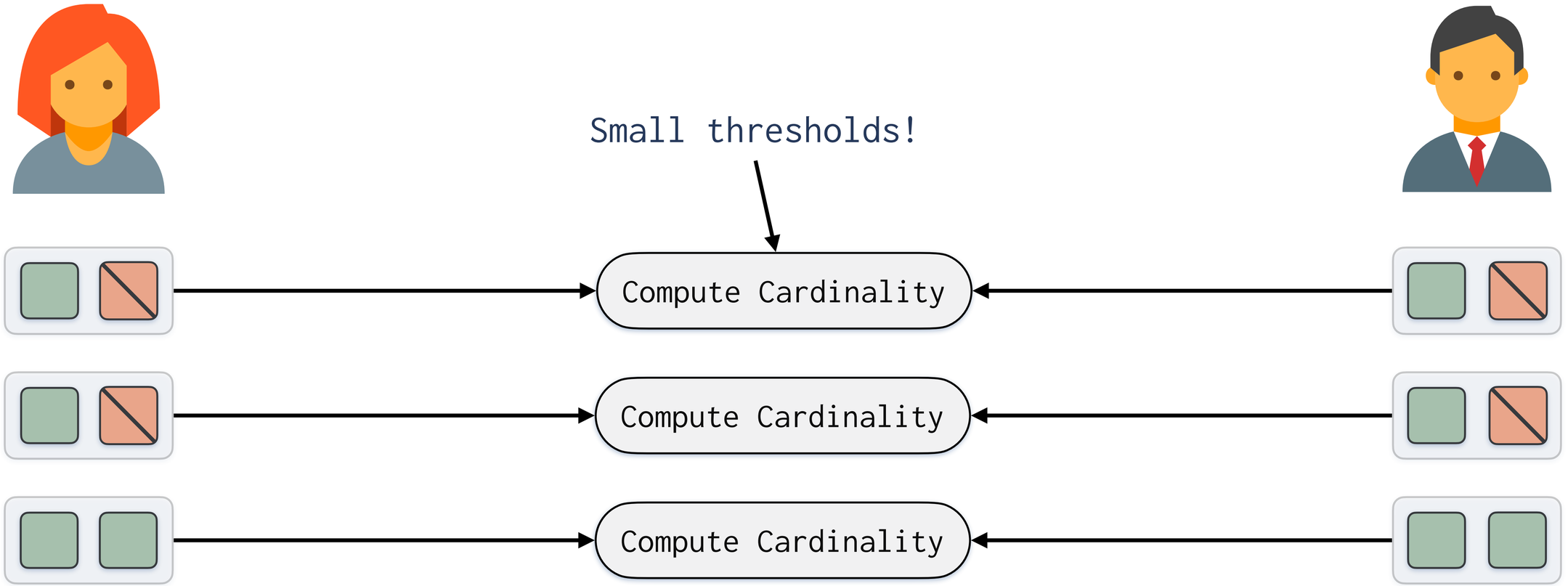
Cardinality Testing

Divide & Conquer



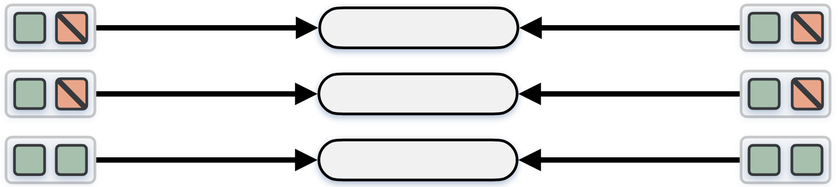
Cardinality Testing

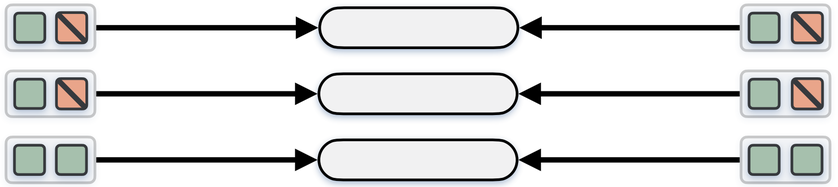
Divide & Conquer

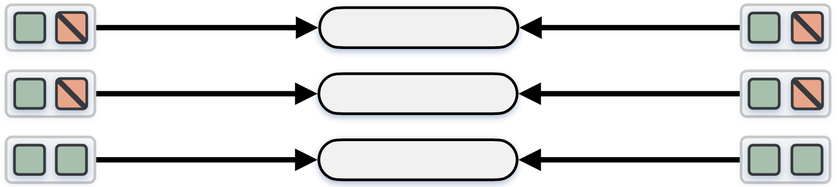


Cardinality Testing

Amplification

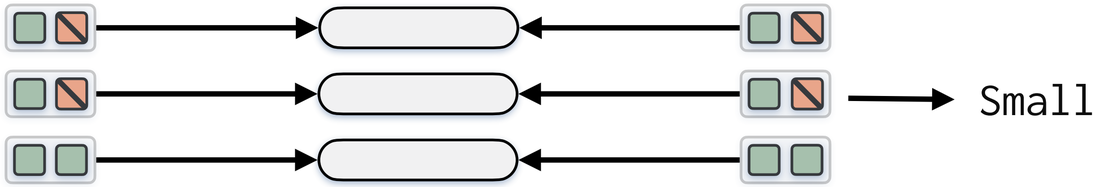


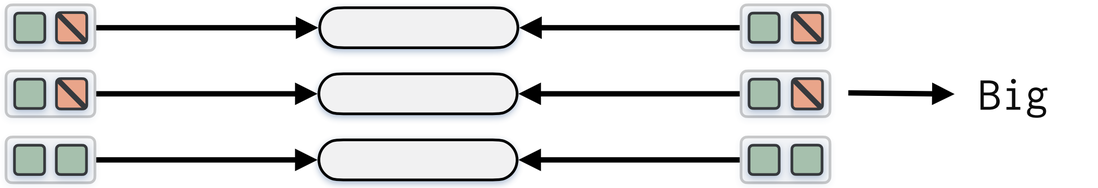


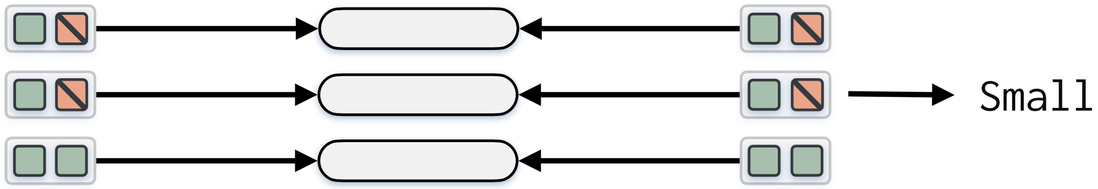


Cardinality Testing

Amplification

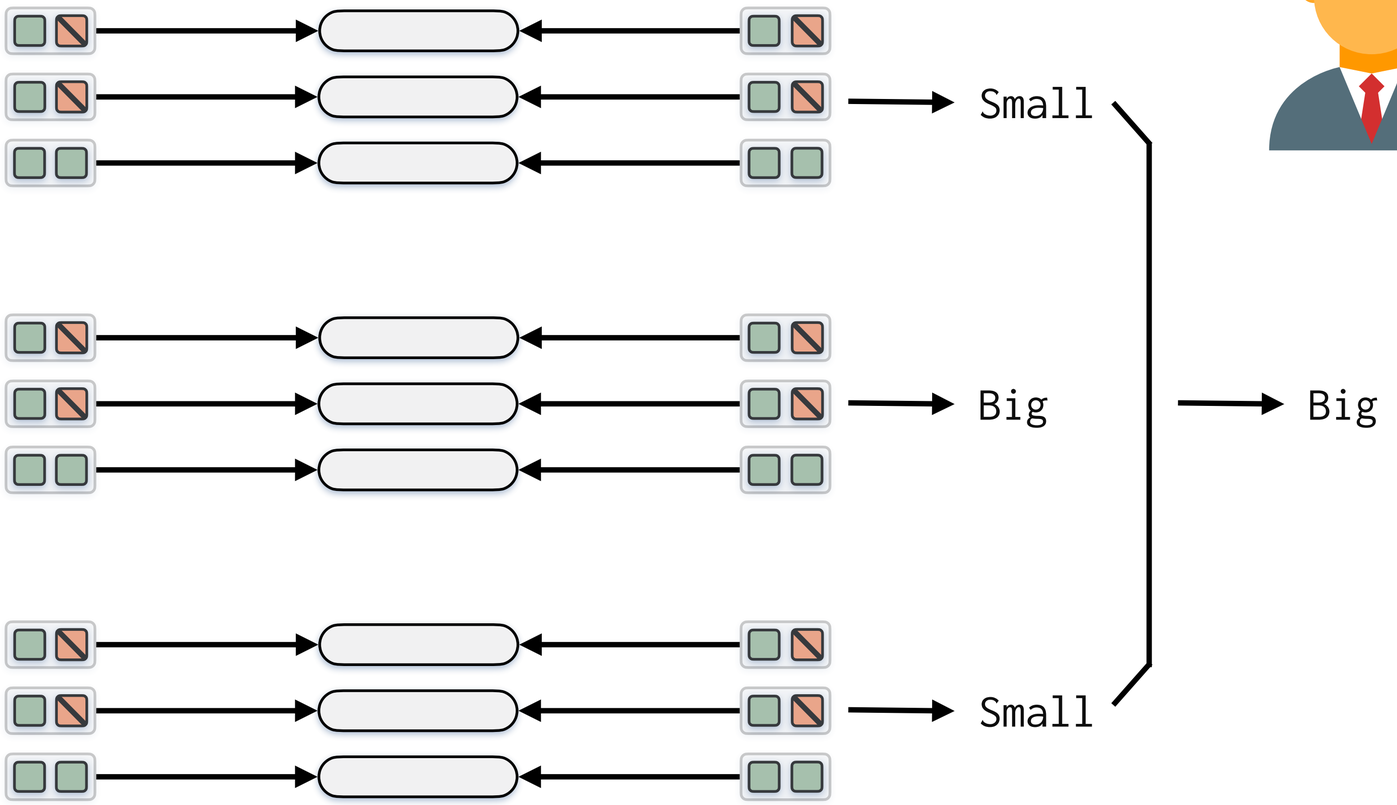






Cardinality Testing

Amplification



Cardinality Testing

The Multiparty Case

Cardinality Testing

The Multiparty Case

Two Parties

Intersection large <=> Symmetric set difference small

Cardinality Testing

The Multiparty Case

Two Parties

Intersection large <=> Symmetric set difference small

Multiple Parties

Cardinality Testing

The Multiparty Case

Two Parties

Intersection large <=> Symmetric set difference small

Multiple Parties

Need to talk about intersection directly

Cardinality Testing

The Multiparty Case

Two Parties

Intersection large <=> Symmetric set difference small

Multiple Parties

Need to talk about intersection directly

Buckets contain different amounts of elements

Cardinality Testing

The Multiparty Case

Two Parties

- Intersection large <=> Symmetric set difference small

Multiple Parties

- Need to talk about intersection directly
- Buckets contain different amounts of elements
- Need padding elements in buckets

Questions?