Sublinear Secure Computation from New Assumptions

Elette Boyle[1,2] Geoffroy Couteau[3] Pierre Meyer[1,3]

[1]Reichman University
[2]NTT Research
[3]Université Paris Cité, IRIF, CNRS

TCC 2022

Sublinear Secure Computation from New Assumptions

Elette Boyle[1,2] Geoffroy Couteau[3] Pierre Meyer[1,3]

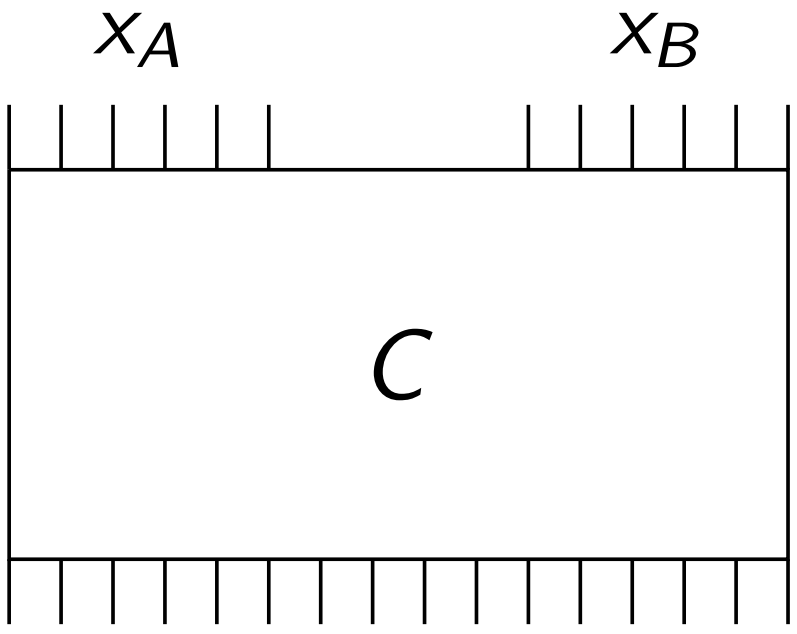
[1]Reichman University
[2]NTT Research
[3]Université Paris Cité, IRIF, CNRS

Standard, Well Founded

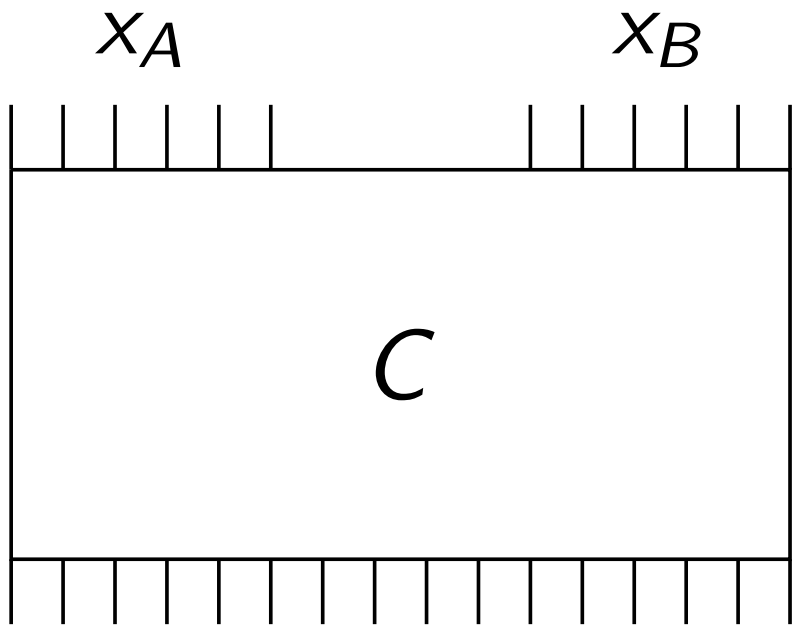
TCC 2022

NEW = Not Previously Known to Imply Sublinear Secure Computation

Sublinear Secure General Computation



Sublinear Secure General Computation

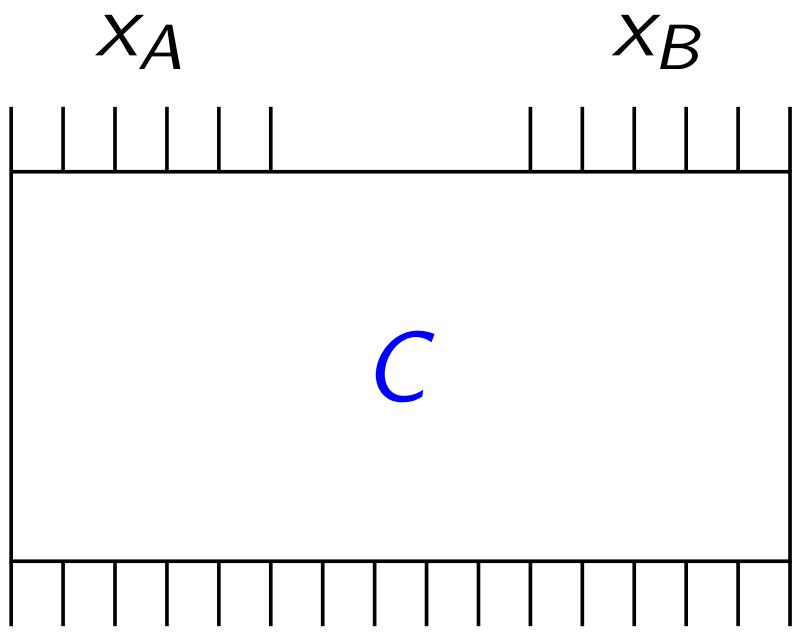


Communication

$$\mathcal{O}(|x_A| + |x_B| + |y|) + o(|C|) + \mathsf{poly}(\lambda)$$

Sublinear in the Circuit-Size

Sublinear Secure General Computation



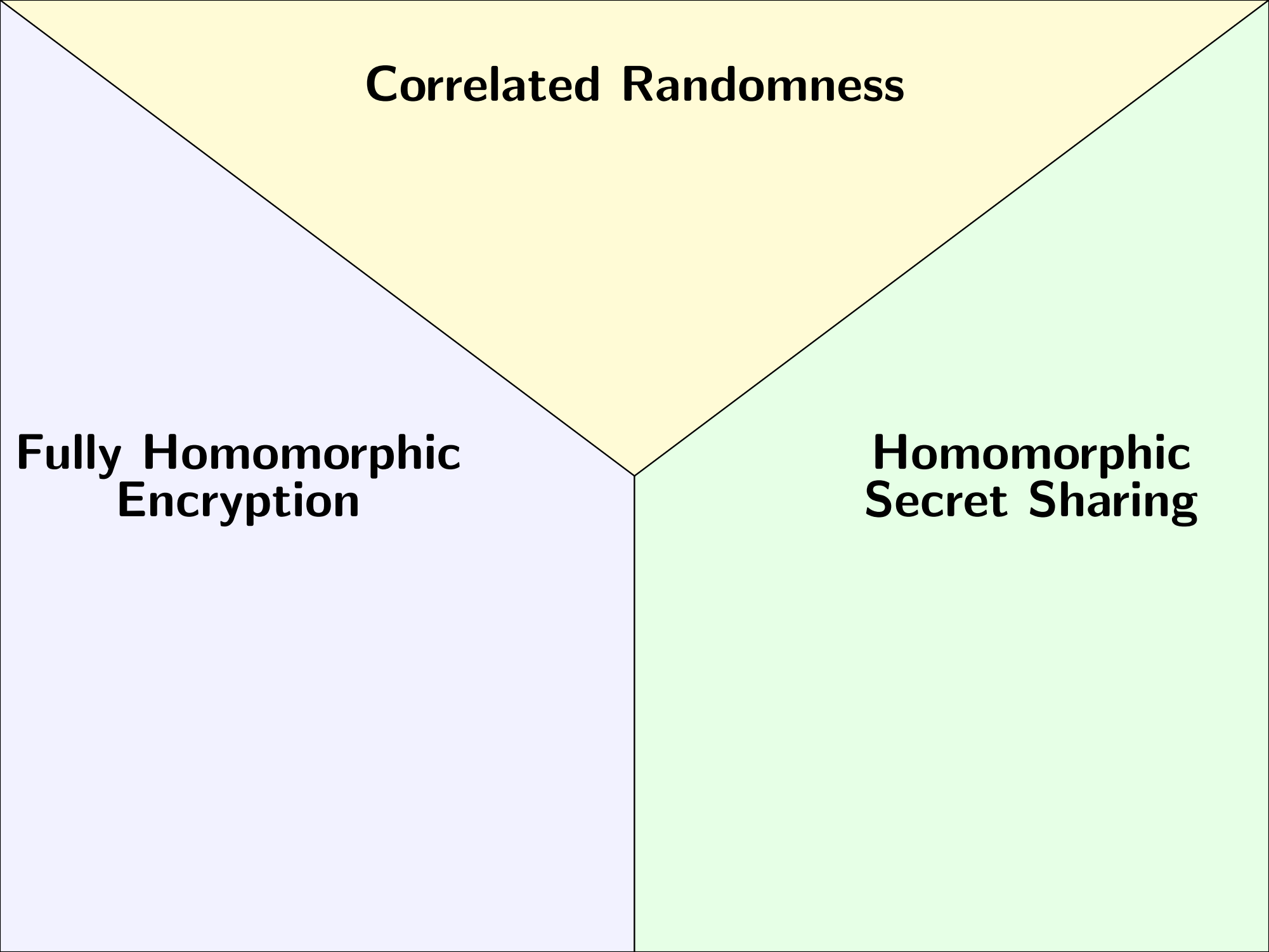
Supported Class?

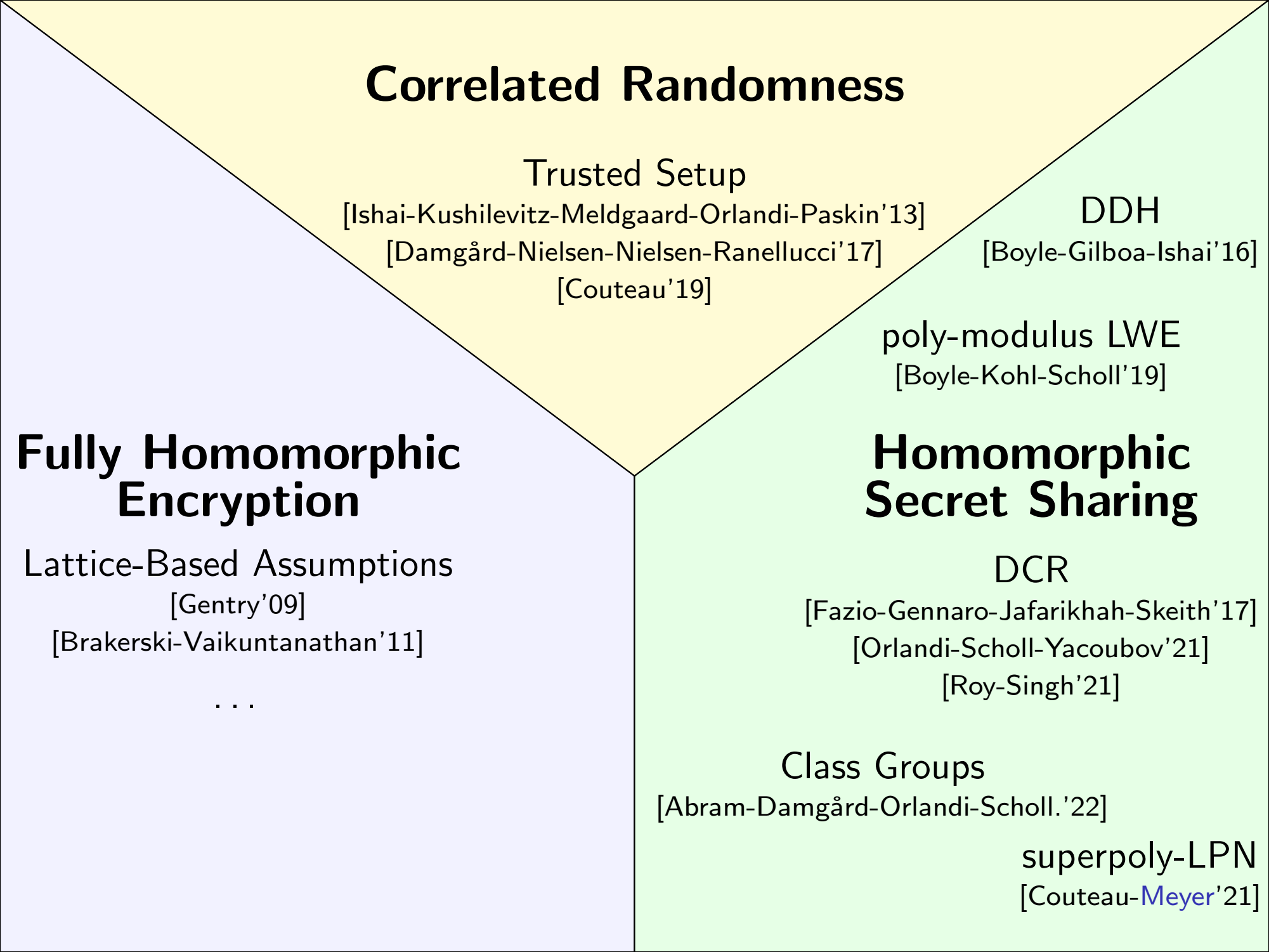
P/Poly
log-depth (NC^1)
log log-depth
Layered Circuits
...

Communication

$$\mathcal{O}(|x_A| + |x_B| + |y|) + o(|C|) + \text{poly}(\lambda)$$

Sublinear in the Circuit-Size

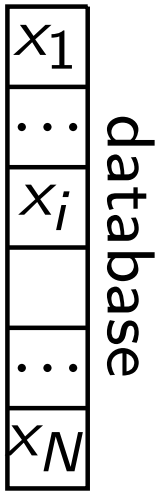

Correlated Randomness
Fully Homomorphic Encryption
Homomorphic Secret Sharing


Correlated Randomness
Trusted Setup
[Ishai-Kushilevitz-Meldgaard-Orlandi-Paskin'13]
[Damgård-Nielsen-Nielsen-Ranellucci'17]
[Couteau'19]
DDH
[Boyle-Gilboa-Ishai'16]
poly-modulus LWE
[Boyle-Kohl-Scholl'19]
Fully Homomorphic Encryption
Lattice-Based Assumptions
[Gentry'09]
[Brakerski-Vaikuntanathan'11]
...
Homomorphic Secret Sharing
DCR
[Fazio-Gennaro-Jafarikhah-Skeith'17]
[Orlandi-Scholl-Yacoubov'21]
[Roy-Singh'21]
Class Groups
[Abram-Damgård-Orlandi-Scholl.'22]
superpoly-LPN
[Couteau-Meyer'21]

(Single-Server) Private Information Retrieval

[Chor-Goldreich-Kushilevitz-Sudan'95] and [Kushilevitz-Ostrovsky'97]

index: i



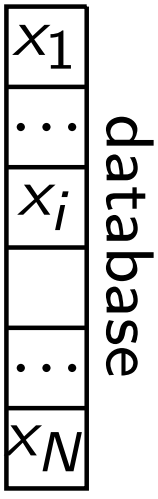
Client

Server

(Single-Server) Private Information Retrieval

[Chor-Goldreich-Kushilevitz-Sudan'95] and [Kushilevitz-Ostrovsky'97]

index: i



Client

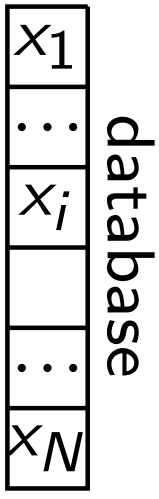
Server

- **Specialised Computation (Information Retrieval):**
  The client gets x_i (without revealing i).

(Single-Server) Private Information Retrieval

[Chor-Goldreich-Kushilevitz-Sudan'95] and [Kushilevitz-Ostrovsky'97]

index: i



Client

Server

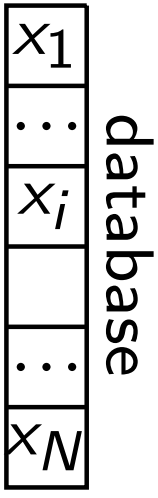
- **Specialised Computation (Information Retrieval):** The client gets x_i (without revealing i).
- **Symmetric PIR (SPIR):** The client *only* gets x_i, *i.e.*

$$C(i, (x_1, \ldots, x_N)) := (x_i, \perp)$$

(Single-Server) Private Information Retrieval

[Chor-Goldreich-Kushilevitz-Sudan'95] and [Kushilevitz-Ostrovsky'97]

index: i



Client

Server

- **Specialised Computation (Information Retrieval):** The client gets x_i (without revealing i).
- **Symmetric PIR (SPIR):** The client *only* gets x_i, *i.e.*

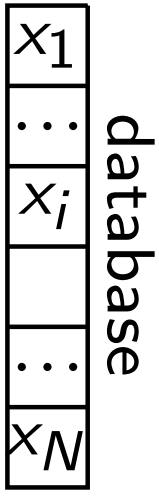
$$C(i, (x_1, \ldots, x_N)) := (x_i, \perp)$$

- **Communication:** $o(N)$; ideally polylog(N)

(Single-Server) Private Information Retrieval

[Chor-Goldreich-Kushilevitz-Sudan'95] and [Kushilevitz-Ostrovsky'97]

index: i



Client

Server

- **Specialised Computation (Information Retrieval):** The client gets x_i (without revealing i).
- **Symmetric PIR (SPIR):** The client *only* gets x_i, *i.e.*
$$C(i, (x_1, \ldots, x_N)) := (x_i, \perp)$$
- **Communication:** $o(N)$; ideally polylog(N)

$$\text{DCR} \vee \text{LWE} \vee \Phi\text{-Hiding} \vee \text{DDH} \vee \text{QR} \implies \text{(Two-Round) Polylog PIR}$$

[Cachin-Micali-Stadler'99], [Lipmaa'05], [Chang'04]
[Ostrovsky-Skeith'07], [Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky'19]

Our Results

1. Sublinear 2PC for Layered Circuits

- Assumption: Quadratic Residuosity assumption (QR) + Learning Parity with Noise (LPN).

2. Polylogarithmic PIR from CDH

- Assumption: Computational Diffie-Hellman.

Our Results

1. **Sublinear 2PC for Layered Circuits**

- Assumption: Quadratic Residuosity assumption (QR) + Learning Parity with Noise (LPN).

2. **Polylogarithmic PIR from CDH**

- Assumption: Computational Diffie-Hellman.
- Key Feature: Uses **polylog communication** and **log rounds**.

Previously: $\Omega(N)$ from CDH
Now: $\mathrm{polylog}(N)$

Our Results

1. **Sublinear 2PC for Layered Circuits**

- Assumption: Quadratic Residuosity assumption (QR) + Learning Parity with Noise (LPN).

2. **Polylogarithmic PIR from CDH**

- Assumption: Computational Diffie-Hellman.
- Key Feature: Uses **polylog communication** and **log rounds**.

Previously: $\Omega(N)$ from CDH
Now: polylog(N)

From DDH, LWE...: 2-round

Our Results

1. Sublinear 2PC for Layered Circuits

- Assumption: Quadratic Residuosity assumption (QR) + Learning Parity with Noise (LPN).
- Key Feature: New approach to break the circuit-size barrier.
- Circuit Class: Layered Circuits $\mathcal{O}(|\text{in}| + |\text{out}| + \frac{|C|}{\log\log|C|})$ or LogLog-Depth Circuits $\mathcal{O}(|\text{in}| + |\text{out}| + \sqrt{|C|})$.

2. Polylogarithmic PIR from CDH

- Assumption: Computational Diffie-Hellman.
- Key Feature: Uses polylog communication and log rounds.

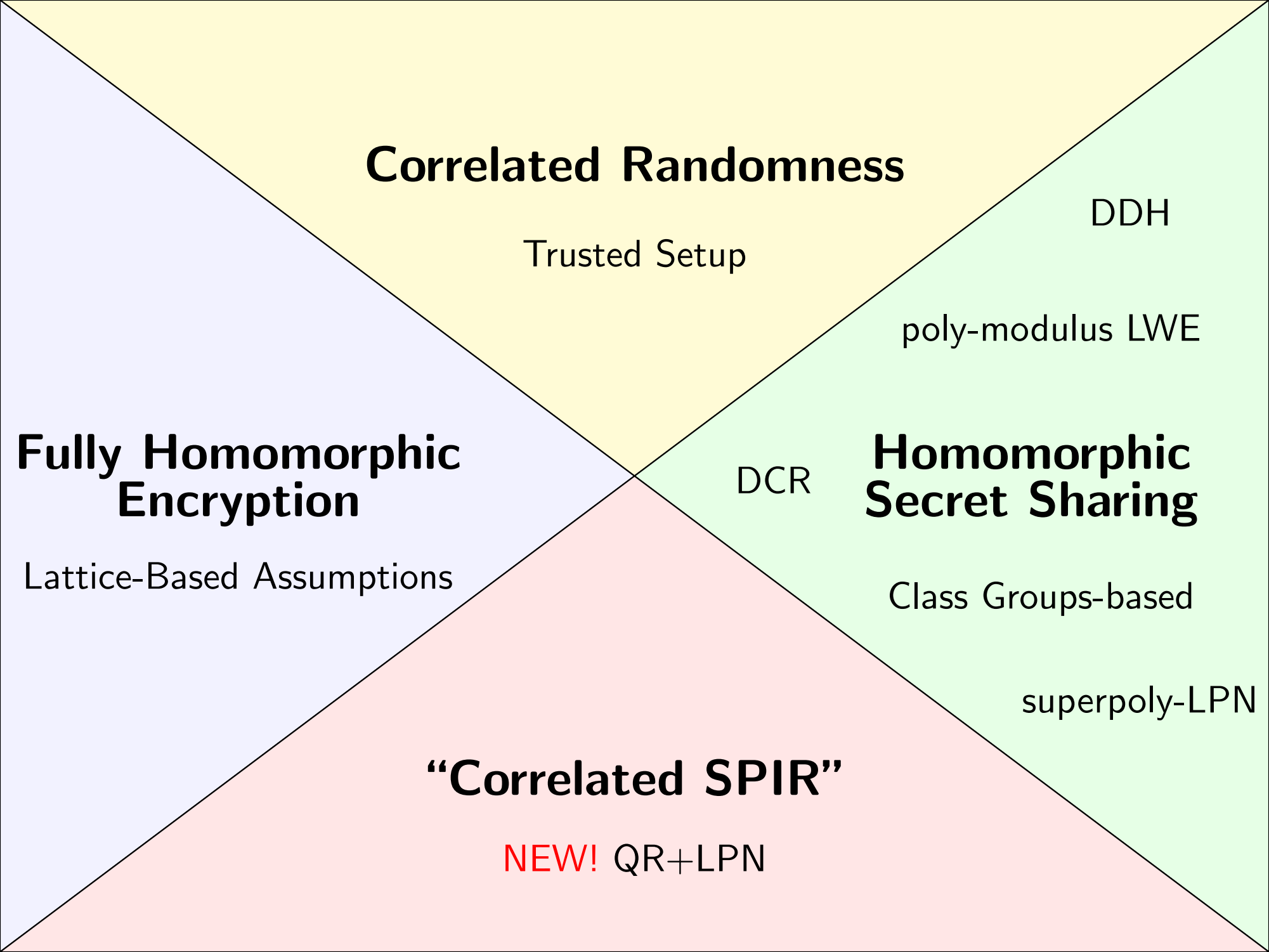
Our Results

1. Sublinear 2PC for Layered Circuits

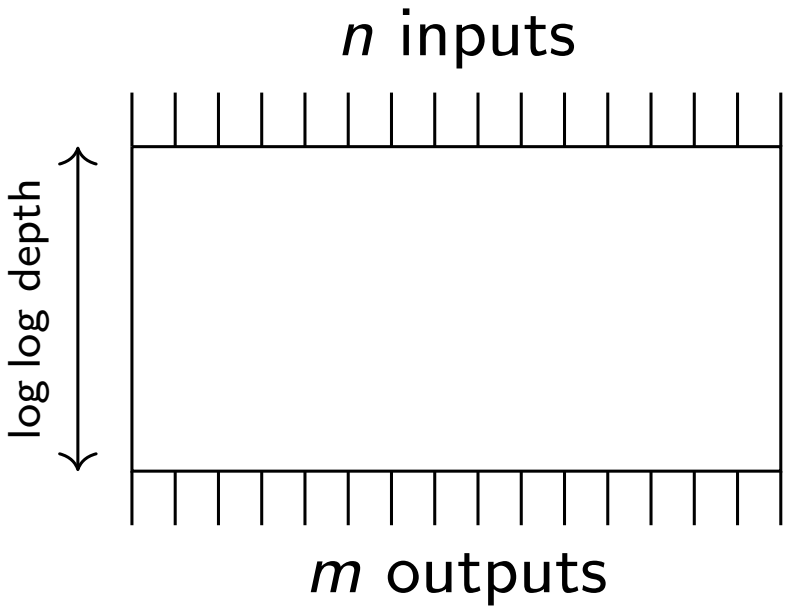
- Assumption: Quadratic Residuosity assumption (QR) + Learning Parity with Noise (LPN).
- Key Feature: New approach to break the circuit-size barrier.
- Circuit Class: Layered Circuits $\mathcal{O}(|\text{in}| + |\text{out}| + \frac{|C|}{\log\log|C|})$ or LogLog-Depth Circuits $\mathcal{O}(|\text{in}| + |\text{out}| + \sqrt{|C|})$.

2. Polylogarithmic PIR from CDH

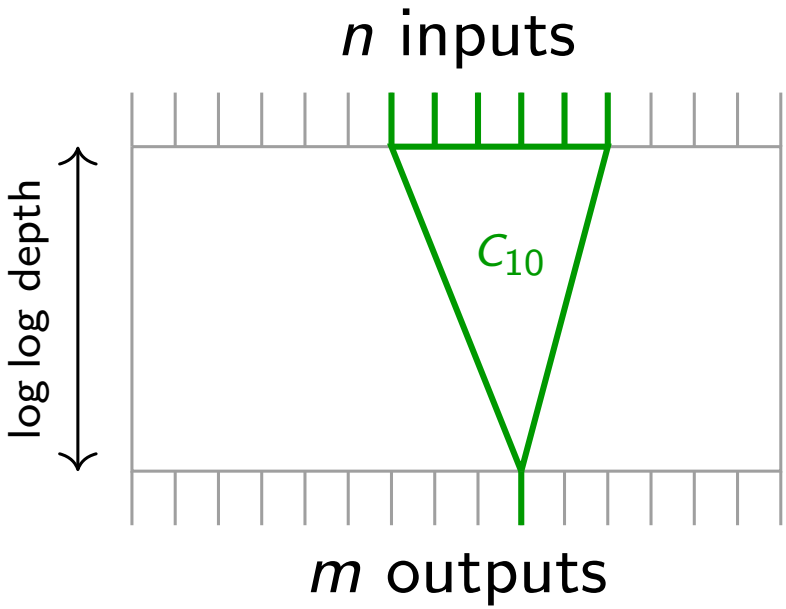
- Assumption: Computational Diffie-Hellman.
- Key Feature: Uses polylog communication and log rounds.


Correlated Randomness
Trusted Setup
DDH
poly-modulus LWE
Fully Homomorphic Encryption
Lattice-Based Assumptions
DCR
Homomorphic Secret Sharing
Class Groups-based
superpoly-LPN
"Correlated SPIR"
NEW! QR+LPN

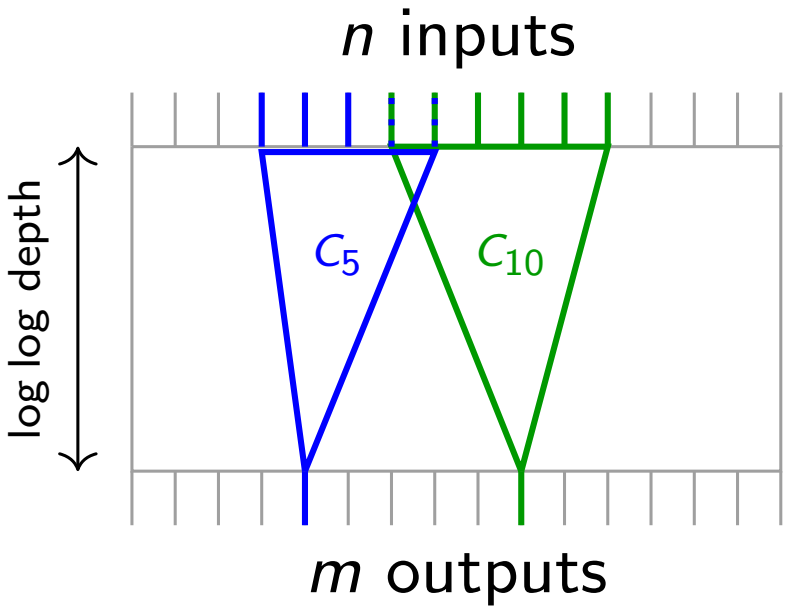
Reduction to a form of PIR: Exploiting Log-Locality



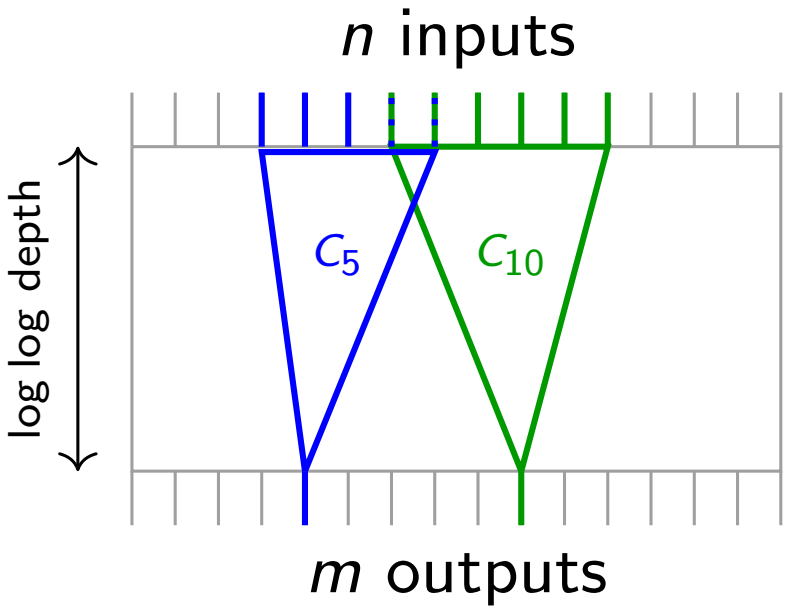
Reduction to a form of PIR: Exploiting Log-Locality

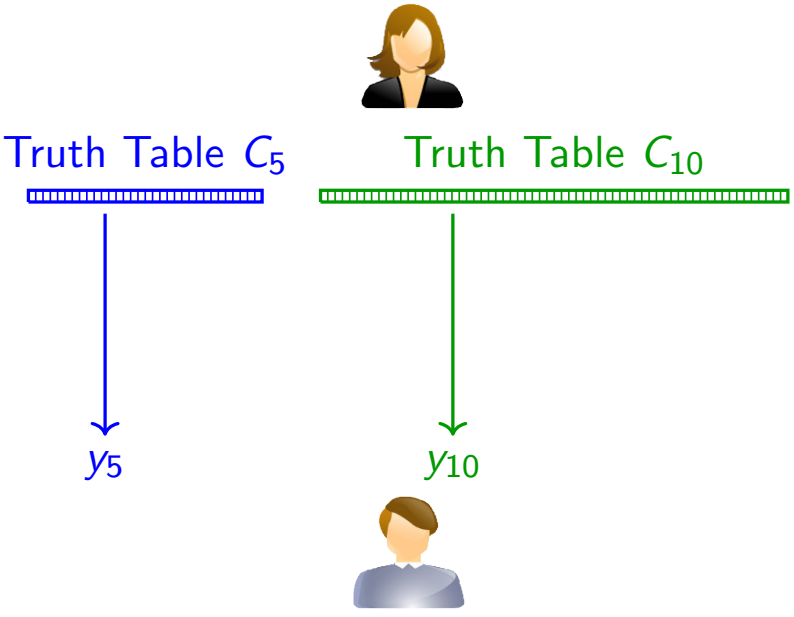


Reduction to a form of PIR: Exploiting Log-Locality

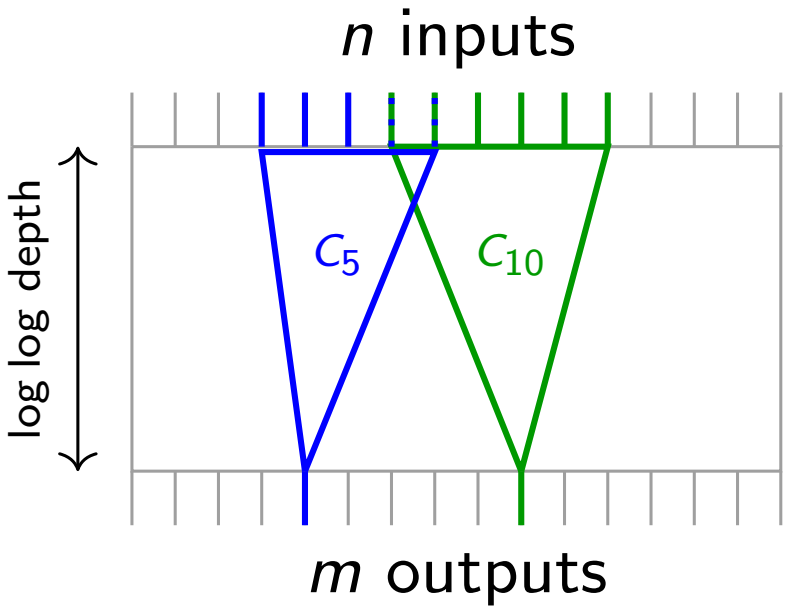


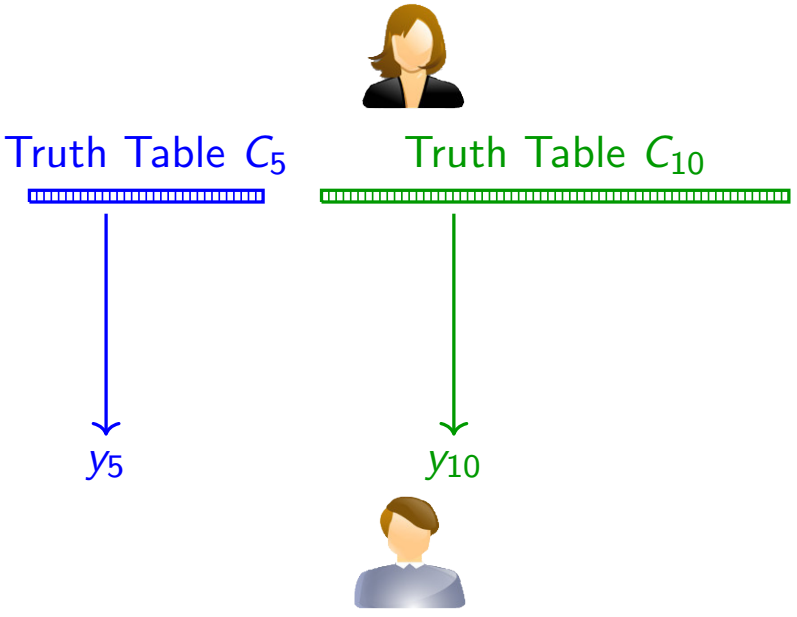
Reduction to a form of PIR: Exploiting Log-Locality





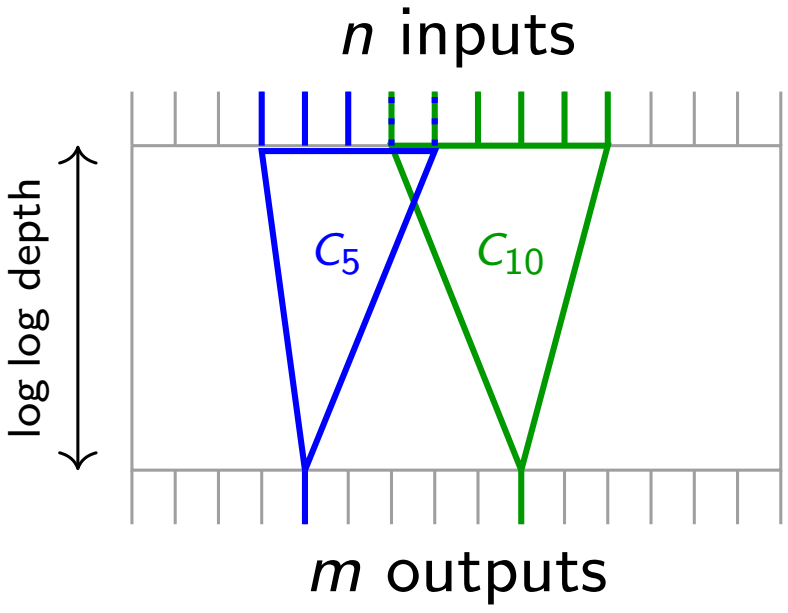
Reduction to a form of PIR: Exploiting Log-Locality

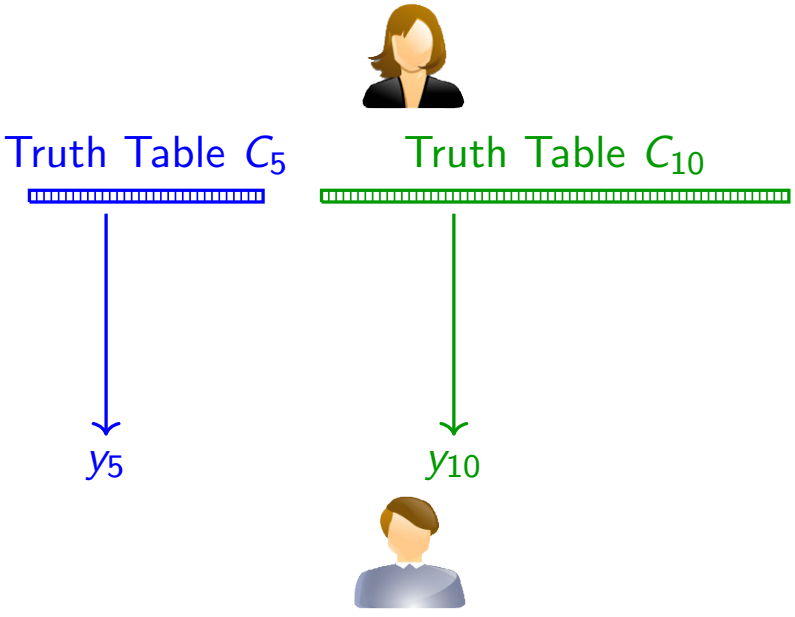




Parallel instances of specialised computation

Reduction to a form of PIR: Exploiting Log-Locality

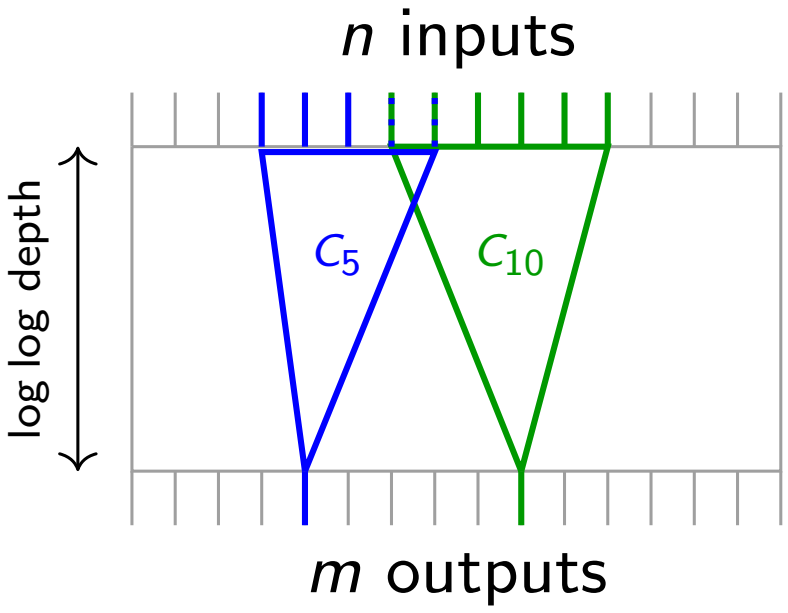


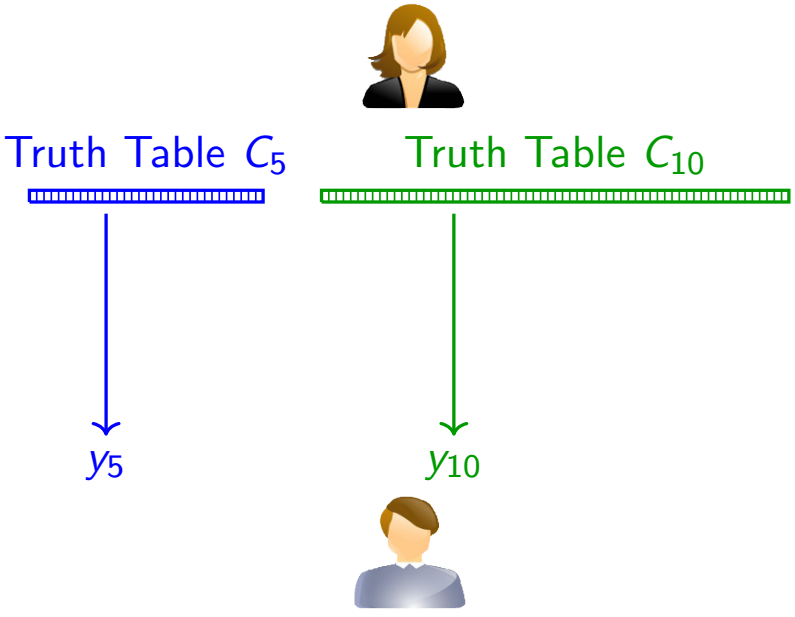


Parallel instances of specialised computation

- Independent instances?

Reduction to a form of PIR: Exploiting Log-Locality

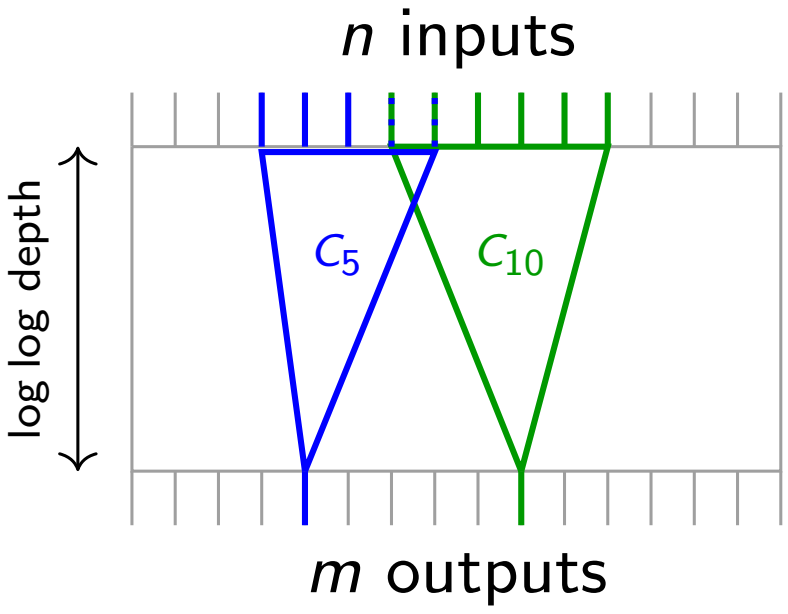


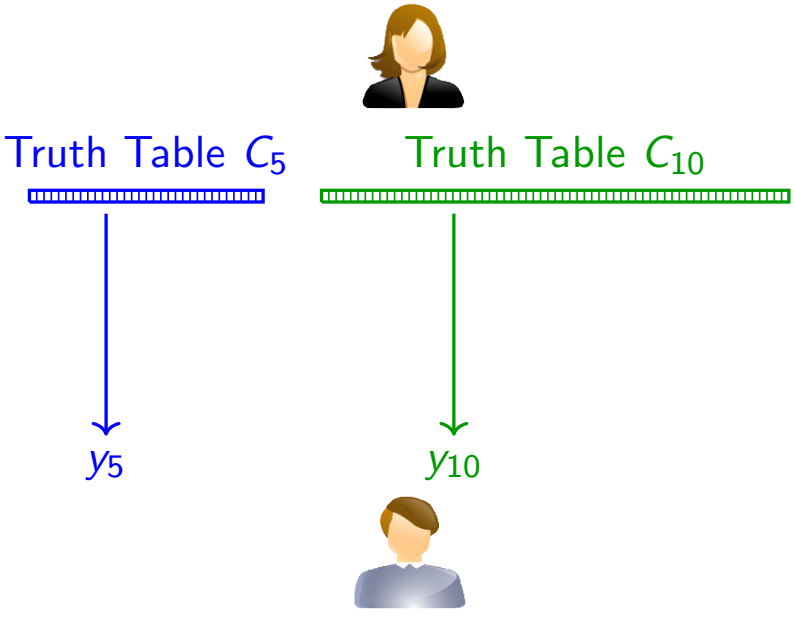


Parallel instances of specialised computation

- Independent instances? Too much communication!

Reduction to a form of PIR: Exploiting Log-Locality

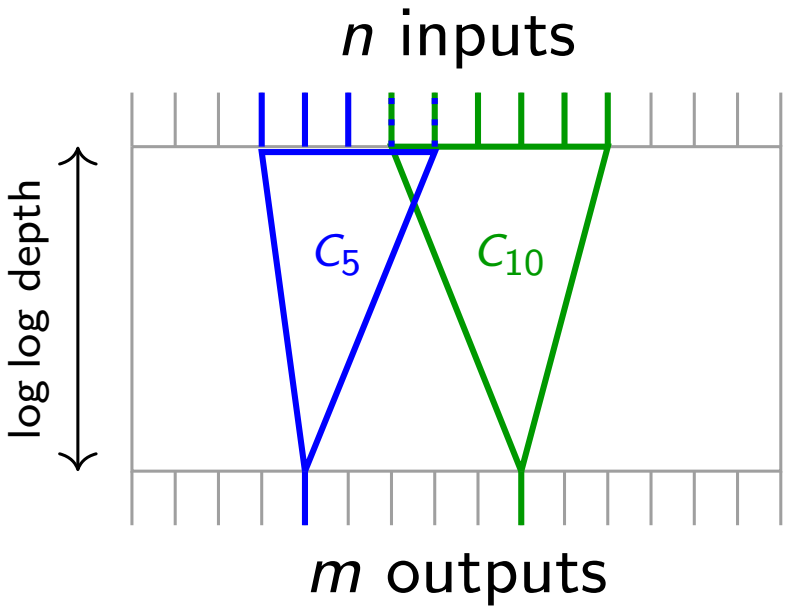


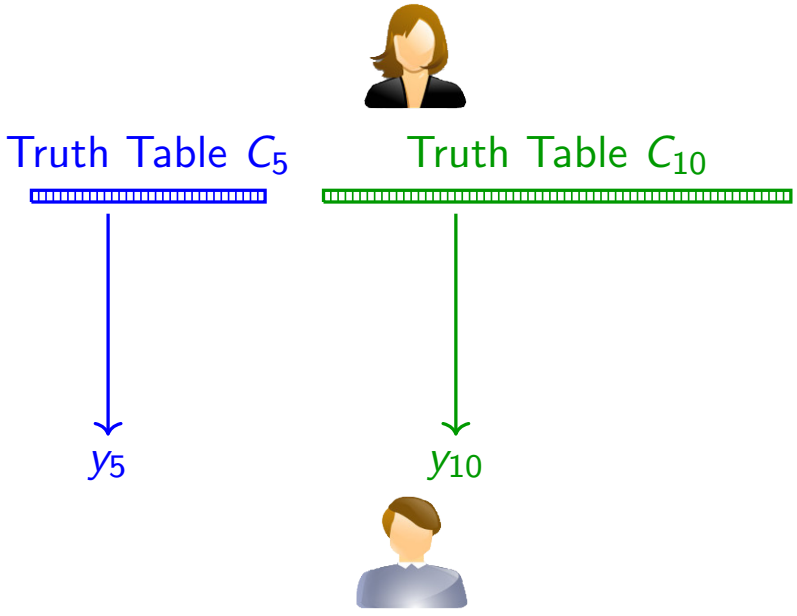


Parallel instances of specialised computation

- Independent instances? Too much communication!
- Exploiting redundancies ("Total Entropy": x_A and x_B)

Reduction to a form of PIR: Exploiting Log-Locality





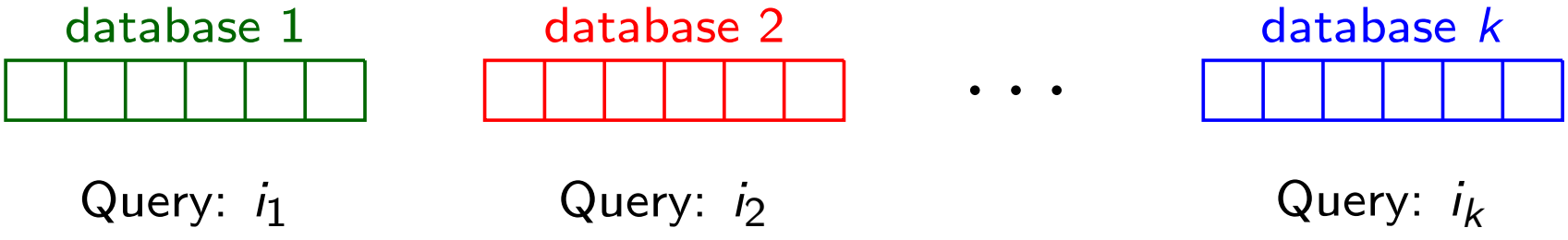
Parallel instances of specialised computation

- Independent instances? Too much communication!
- Exploiting redundancies ("Total Entropy": x_A and x_B)
  - **With a "Correlated Randomness" approach.** [Couteau'19],[Couteau-Meyer'21].
  - **NEW! Correlated SPIR.** [Boyle-Couteau-Meyer'22]: Up next!

What is Correlated SPIR?

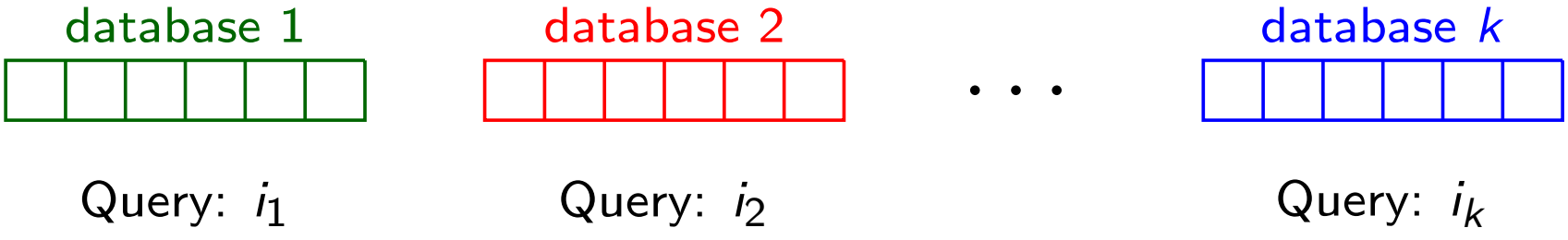
What is Correlated SPIR?

Uncorrelated SPIR

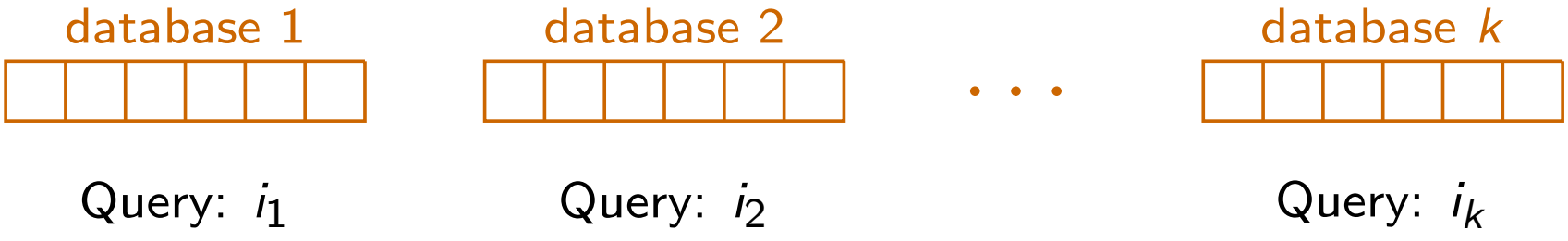


What is Correlated SPIR?

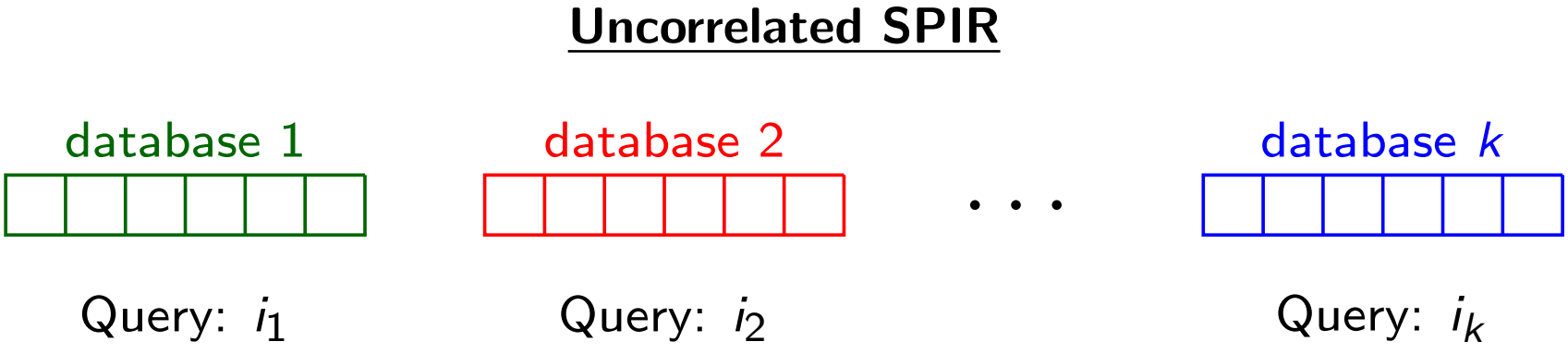
Uncorrelated SPIR



Batch SPIR

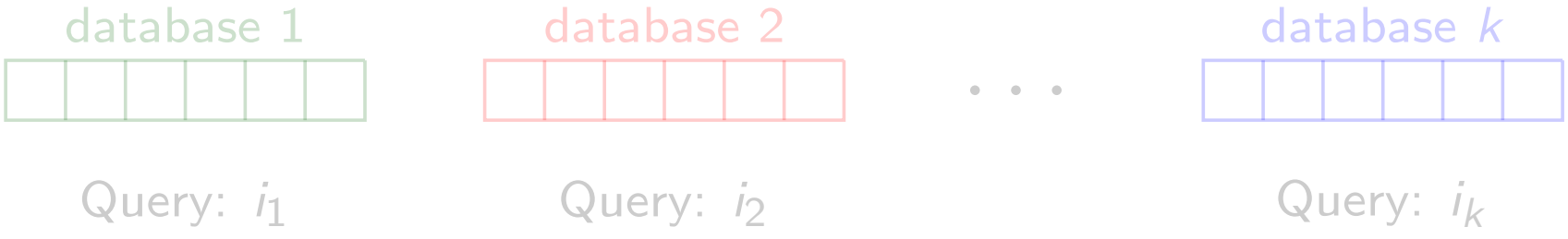


What is Correlated SPIR?



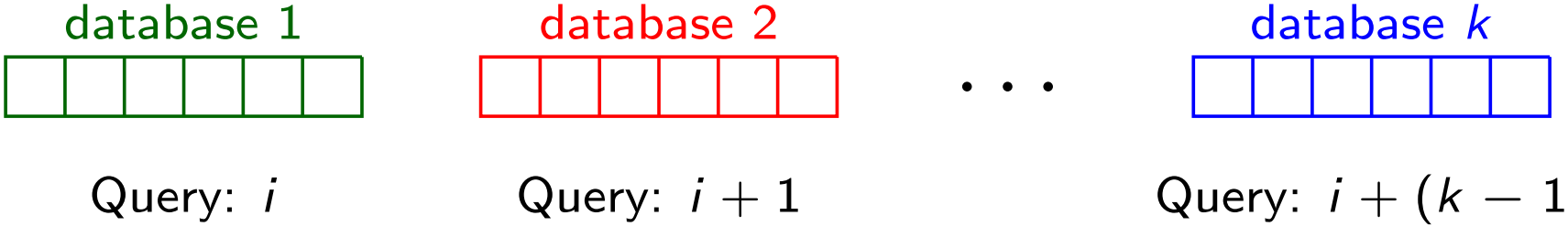
What is Correlated SPIR?

Uncorrelated SPIR

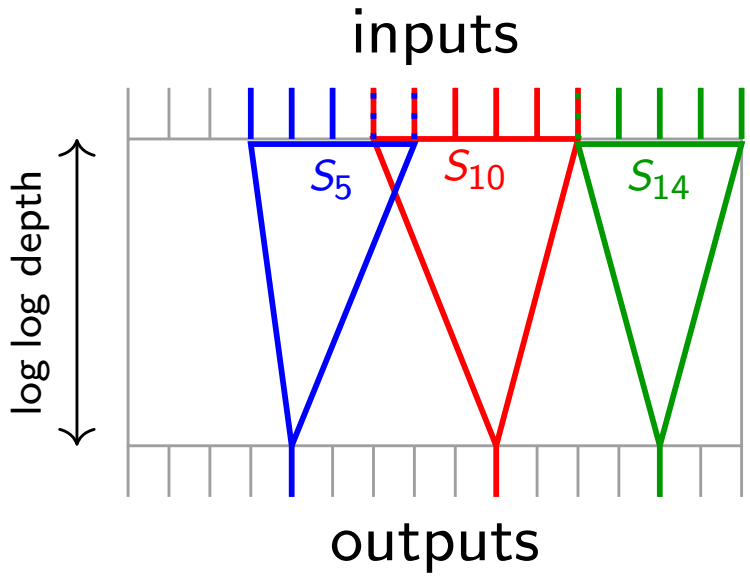


Batch SPIR

Correlated SPIR with Sequential Queries

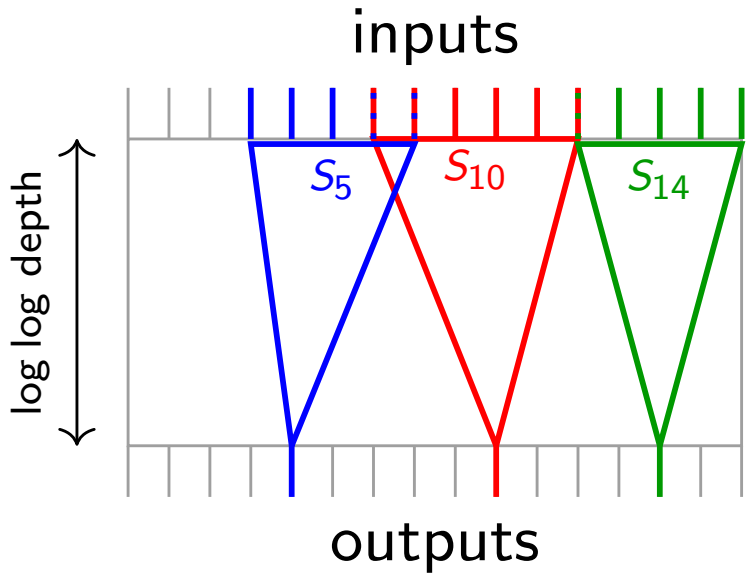


Correlated SPIR with "Mix and Match" Queries



The j^{th} output depends on subset S_j of Bob's input vector x_B.

Correlated SPIR with "Mix and Match" Queries



The j^{th} output depends on subset S_j of Bob's input vector x_B.

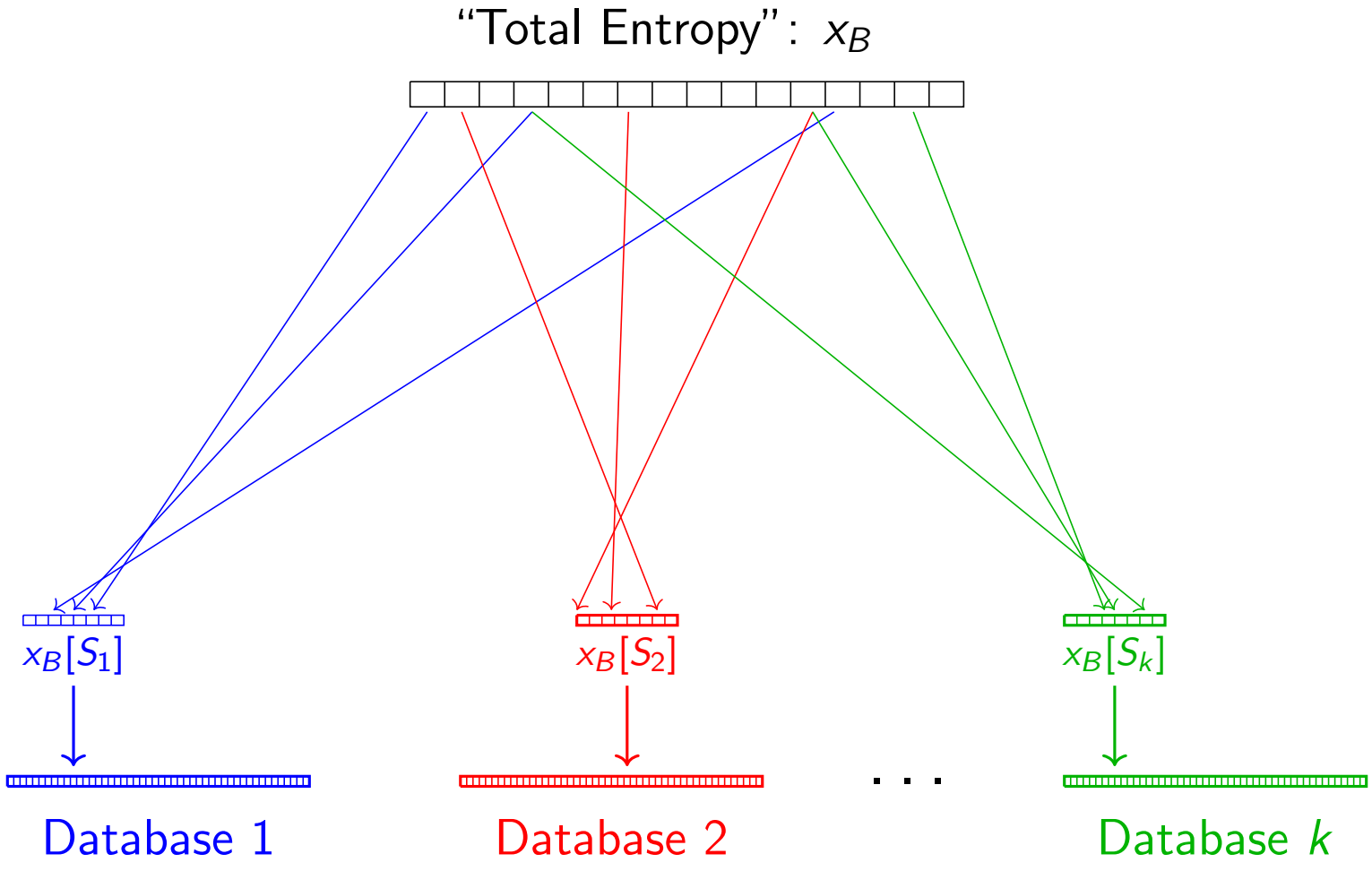
---

database 1 | database 10 | ... | database 14

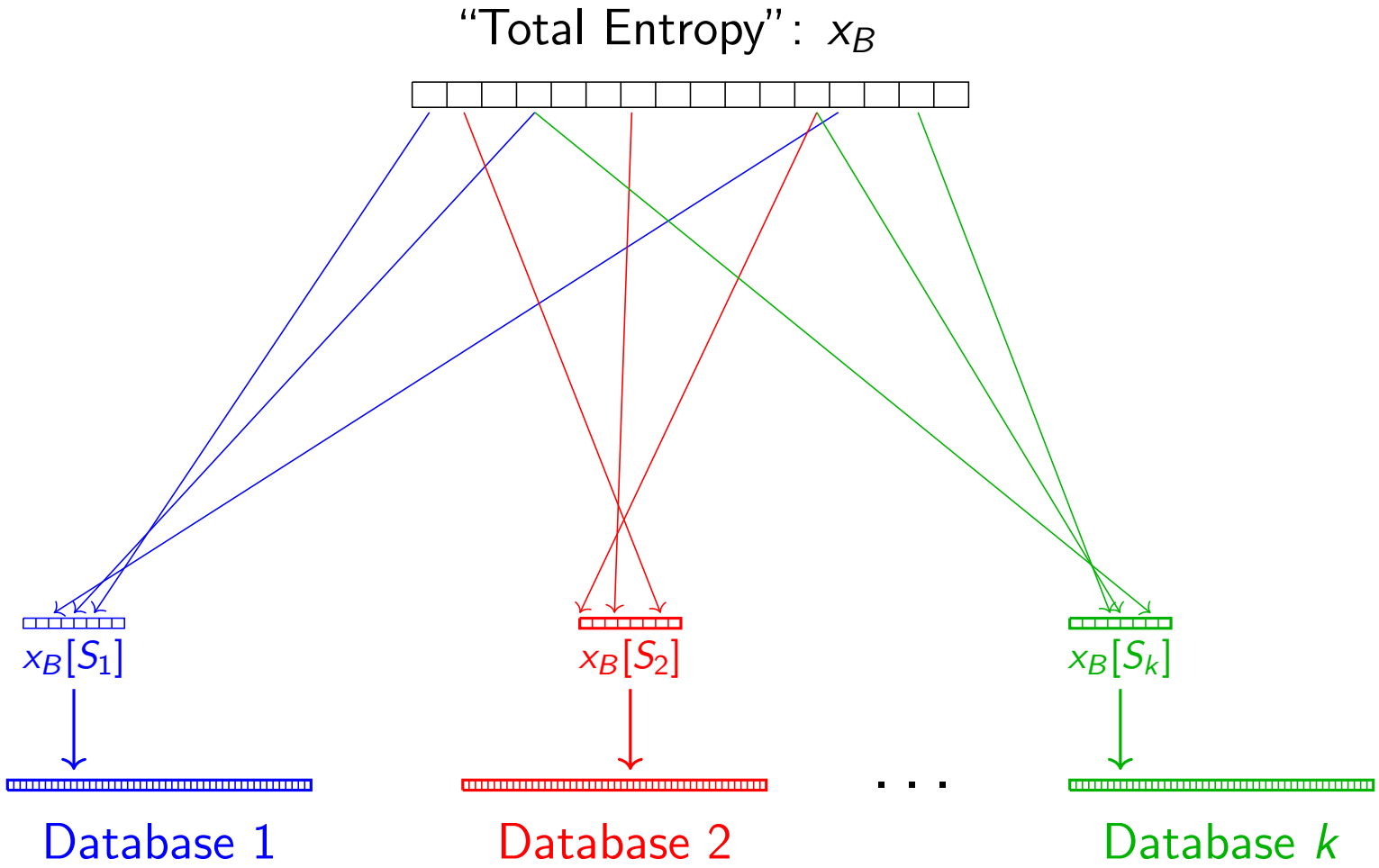
Query: $x_B[S_5]$ | Query: $x_B[S_{10}]$ | Query: $x_B[S_{14}]$

"Total Entropy": x_B, of n_B bits

Why "Mixing and Matching"?



Why "Mixing and Matching"?

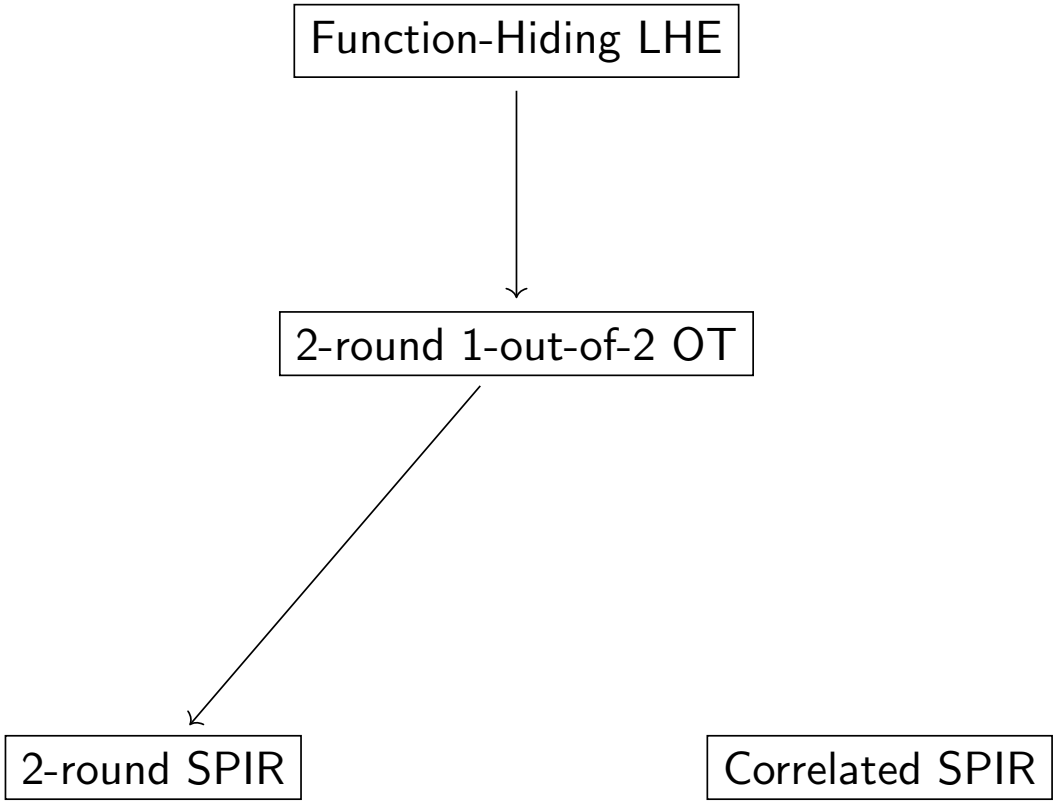


For Sublinear 2PC: Upload $\mathcal{O}(|x_B|)$ and Download $|\text{out}| \cdot (1 + o(1))$

no hidden factor poly(λ)!

How to build Correlated SPIR? — From Rate-1 Batch-LHE

Fact: Function-Hiding Linearly-Homomorphic Encryption implies SPIR



How to build Correlated SPIR? — From Rate-1 Batch-LHE

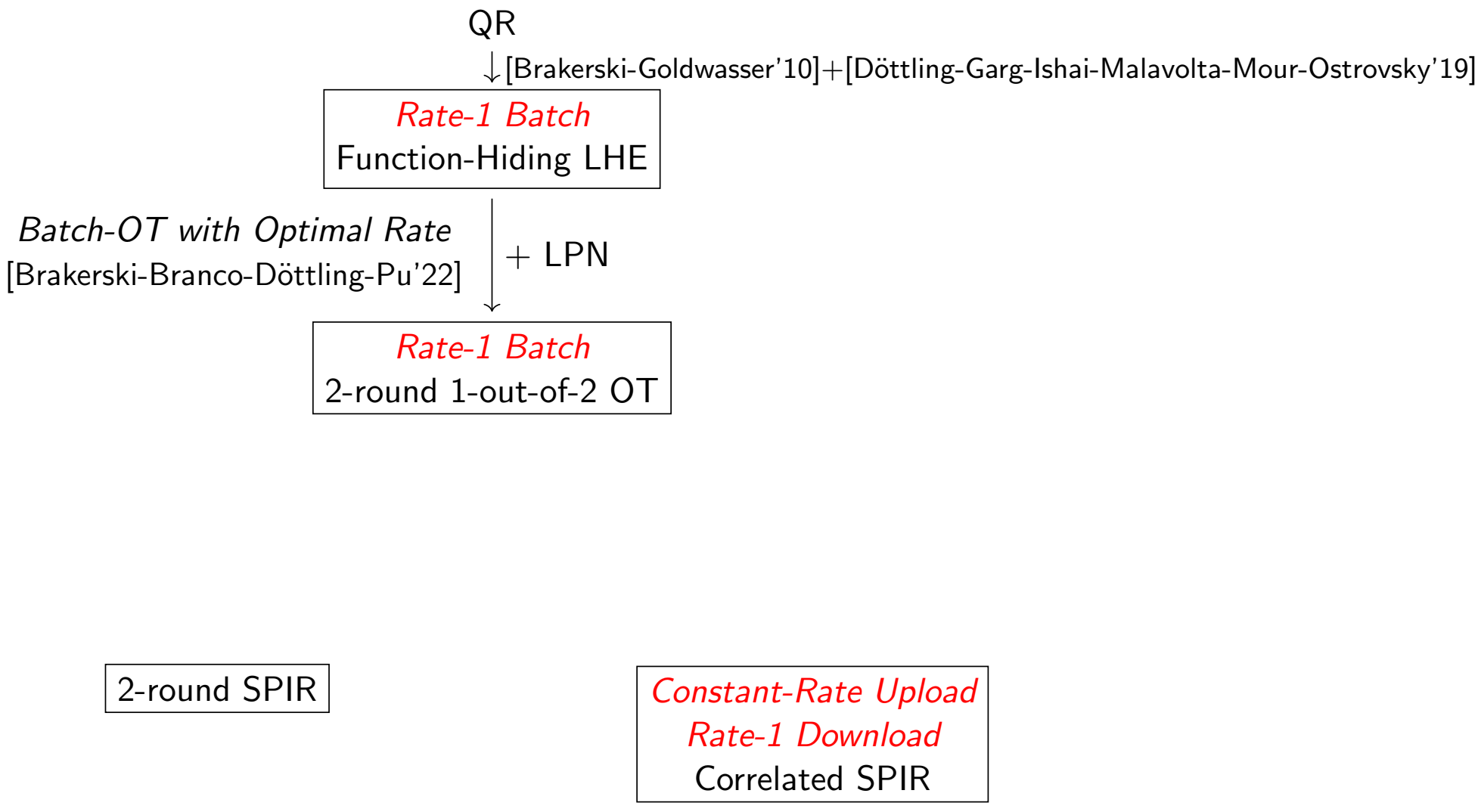
Rate-1 Batch
Function-Hiding LHE

Rate-1 Batch
2-round 1-out-of-2 OT

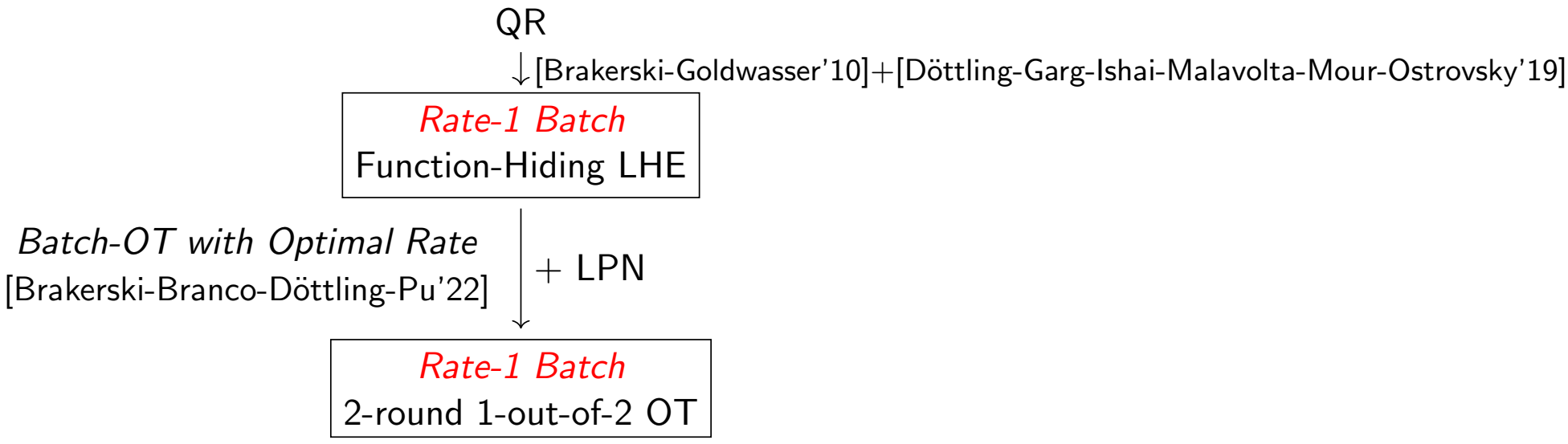
2-round SPIR

Constant-Rate Upload
Rate-1 Download
Correlated SPIR

How to build Correlated SPIR? — From Rate-1 Batch-LHE



How to build Correlated SPIR? — From Rate-1 Batch-LHE



Downside of Batching:

Cannot "Mix and Match"
the atomic 1-out-of-2 OTs

Constant-Rate Upload
Rate-1 Download
Correlated SPIR

How to build Correlated SPIR? — From Rate-1 Batch-LHE

QR

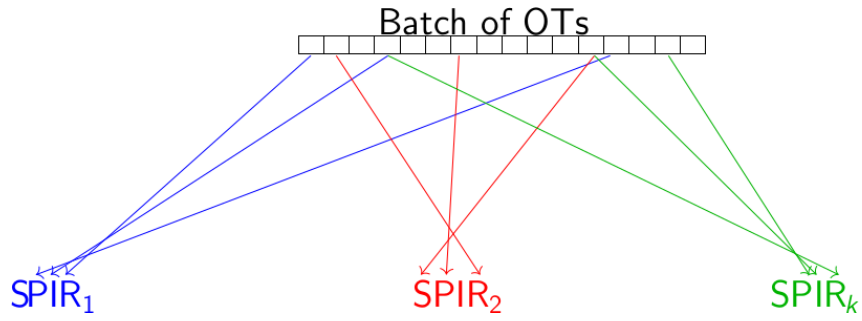
↓

Rate-1 Batch
Function-Hiding LHE

Batch-OT with Optimal Rate
[Brakerski-Branco-Döttling-Pu'22]

↓ + LPN

Rate-1 Batch
2-round 1-out-of-2 OT



Correlated SPIR

Downside of Batching:

Cannot "Mix and Match"
the atomic 1-out-of-2 OTs

Constant-Rate Upload
Rate-1 Download
Correlated SPIR

How to build Correlated SPIR? — From Rate-1 Batch-LHE

QR

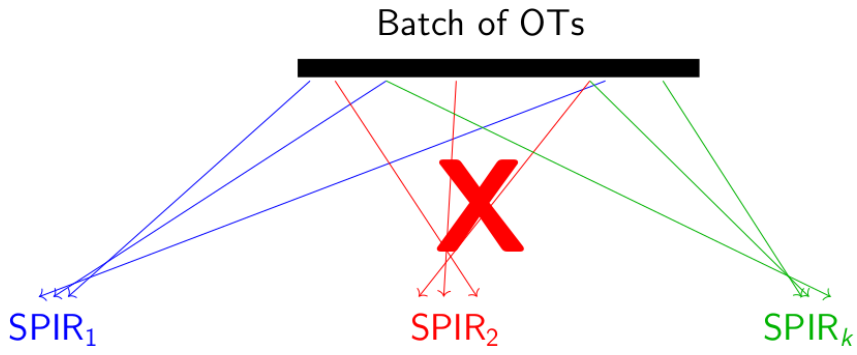
↓

Rate-1 Batch
Function-Hiding LHE

Batch-OT with Optimal Rate
[Brakerski-Branco-Döttling-Pu'22]

↓ + LPN

Rate-1 Batch
2-round 1-out-of-2 OT



Correlated SPIR

Downside of Batching:

Cannot "Mix and Match"
the atomic 1-out-of-2 OTs

Constant-Rate Upload
Rate-1 Download
Correlated SPIR

How to build Correlated SPIR? — From Rate-1 Batch-LHE

QR

↓

Rate-1 Batch
Function-Hiding LHE

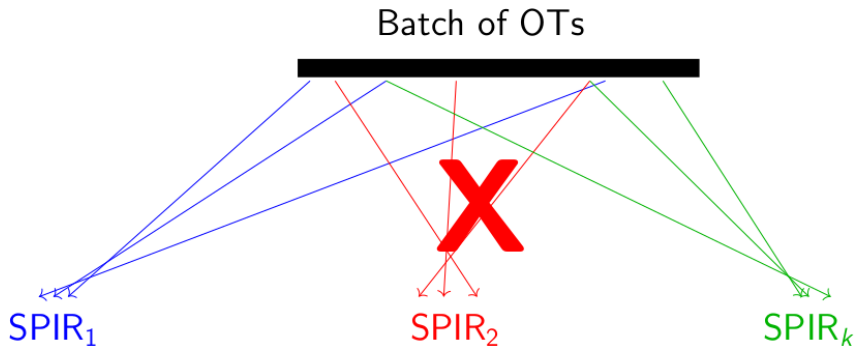
Batch-OT with Optimal Rate
[Brakerski-Branco-Döttling-Pu'22]

↓ + LPN

Rate-1 Batch
2-round 1-out-of-2 OT

Sender-Message Decomposability

Constant-Rate Upload
Rate-1 Download
Correlated SPIR



Downside of Batching:

Cannot "Mix and Match"
the atomic 1-out-of-2 OTs

How to build Correlated SPIR? — From Rate-1 Batch-LHE

QR

↓

Rate-1 Batch
Function-Hiding LHE

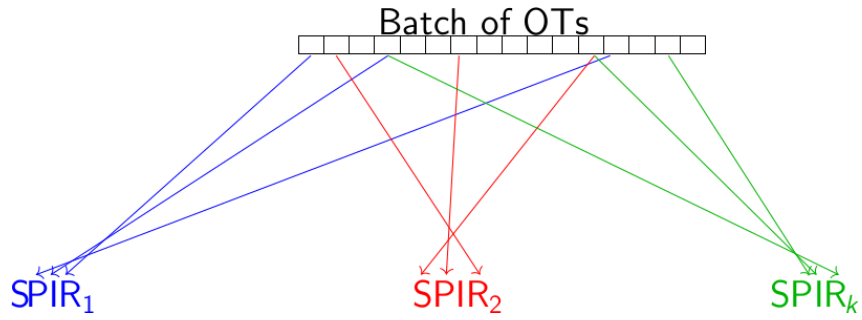
Batch-OT with Optimal Rate
[Brakerski-Branco-Döttling-Pu'22]

↓ + LPN

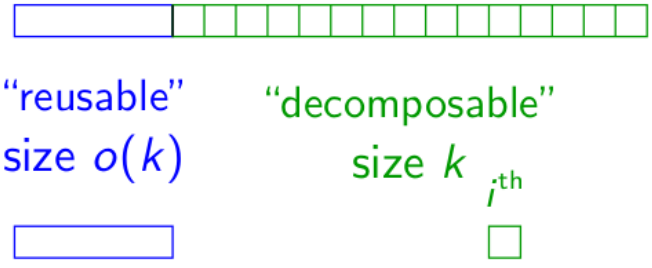
Rate-1 Batch
2-round 1-out-of-2 OT

Sender-Message Decomposability

Constant-Rate Upload
Rate-1 Download
Correlated SPIR



Sender Message for Batch of k OTs



Can be decoded to i^{th} value in batch

Downside of Batching:

Cannot "Mix and Match"
the atomic 1-out-of-2 OTs

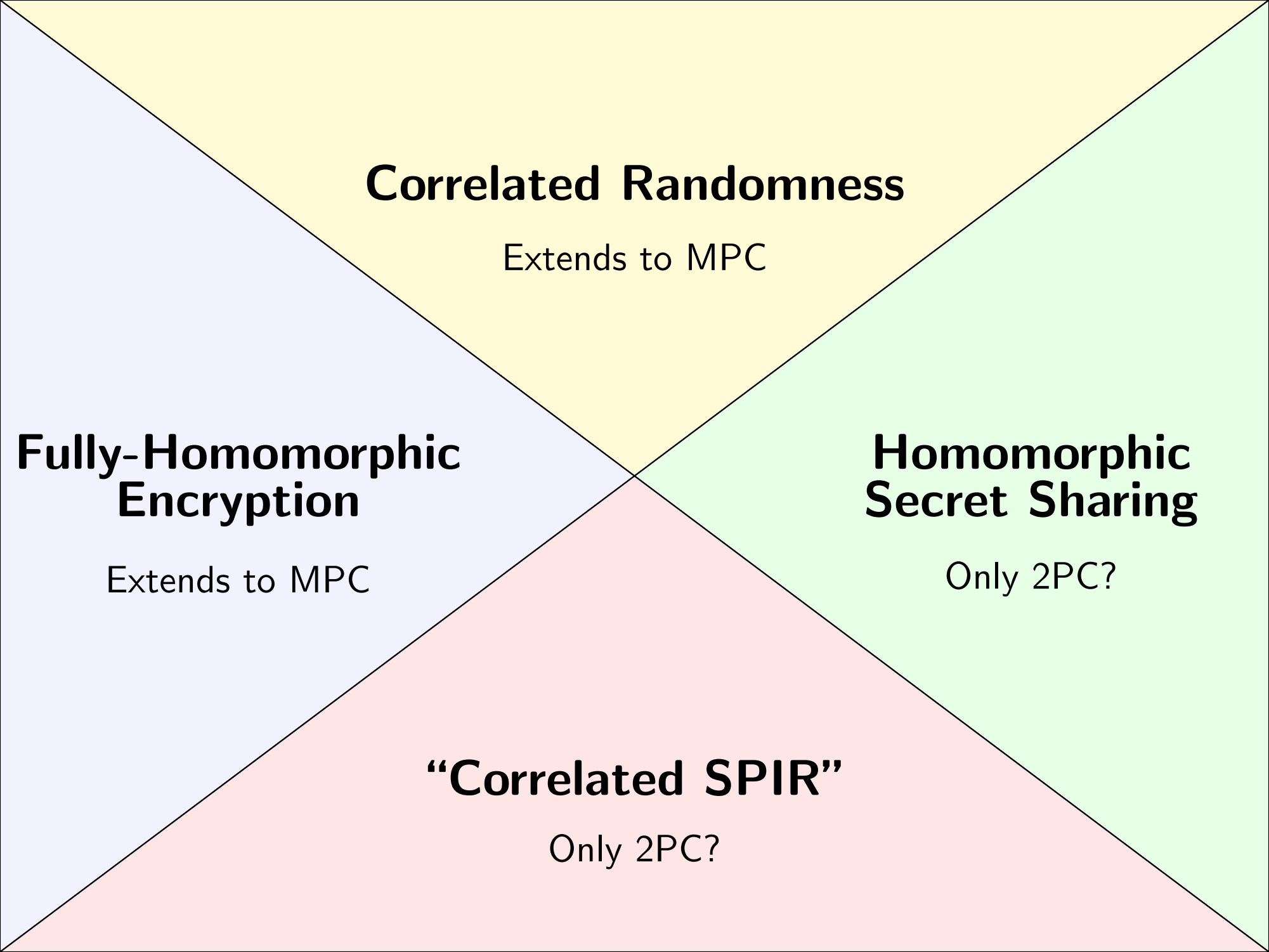
Our Results

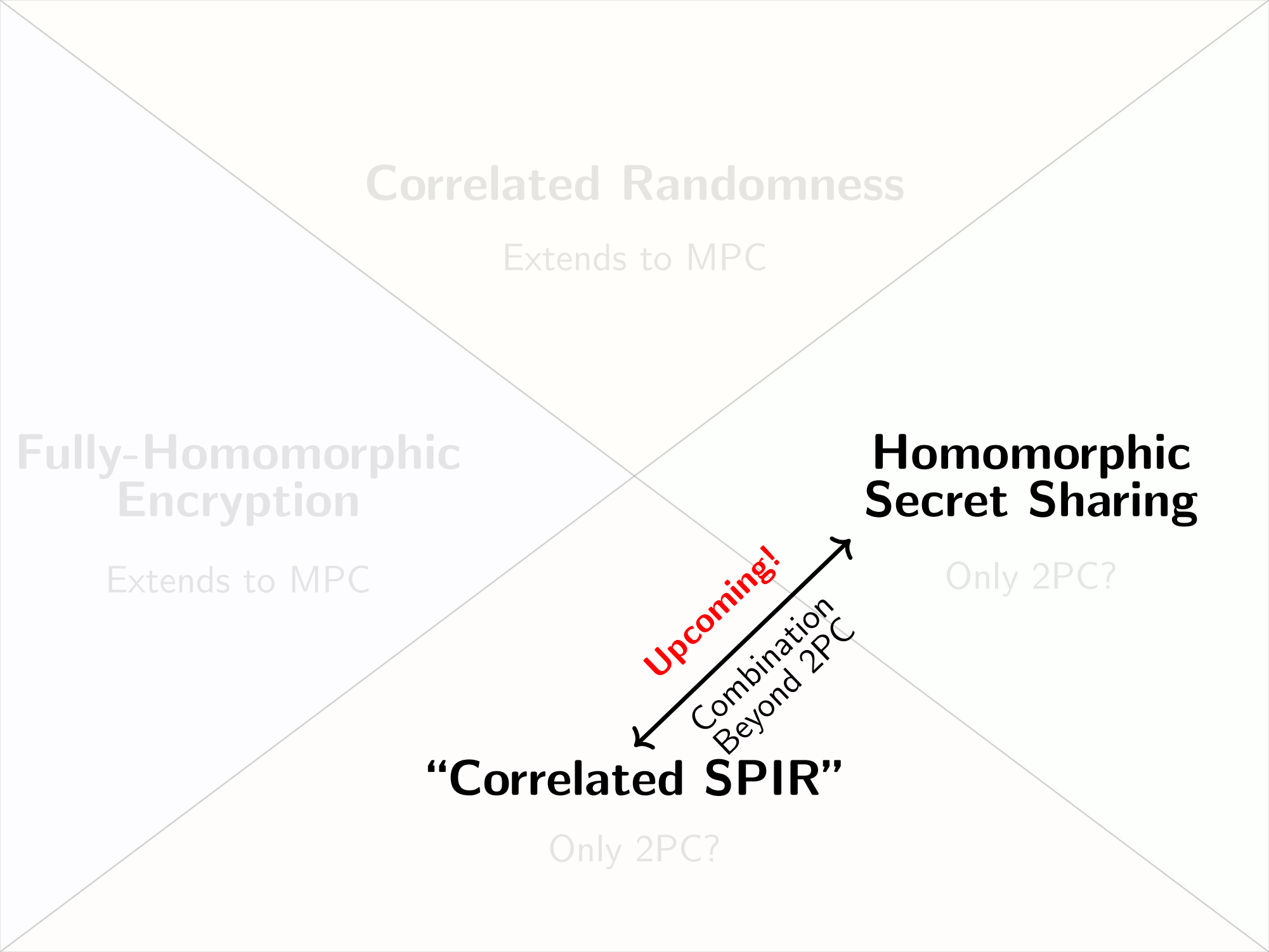
1. Sublinear 2PC for Layered Circuits

- Assumption: QR + LPN.
- Key Feature: New approach to break the circuit-size barrier.
- Circuit Class: Layered Circuits $\mathcal{O}(n + m + \frac{|C|}{\log\log|C|})$ or LogLog-Depth Circuits $\mathcal{O}(n + m + \sqrt{|C|})$.

2. Polylogarithmic PIR from CDH

- Assumption: Computational Diffie-Hellman.
- Key Feature: Uses polylog communication and log rounds.


Correlated Randomness
Extends to MPC
Fully-Homomorphic Encryption
Extends to MPC
Homomorphic Secret Sharing
Only 2PC?
“Correlated SPIR”
Only 2PC?


Correlated Randomness
Extends to MPC
Fully-Homomorphic Encryption
Extends to MPC
Homomorphic Secret Sharing
Only 2PC?
Upcoming!
Combination Beyond 2PC
"Correlated SPIR"
Only 2PC?

Thank you!

Bonus Time!

Polylogarithmic PIR from CDH