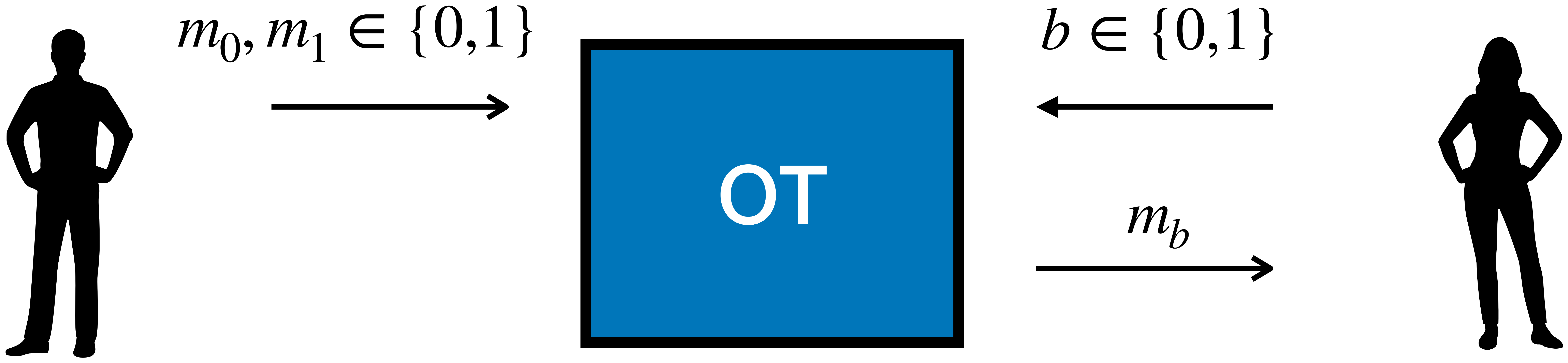
A Framework for Statistically Sender Private OT with Optimal Rate

Pedro Branco *Max-Planck Institute for Security and Privacy*

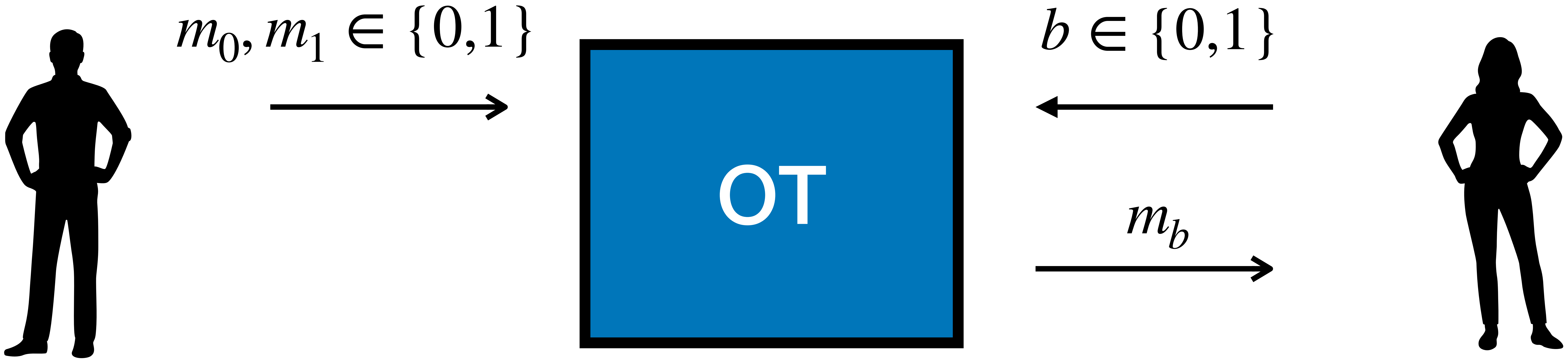
Nico Döttling *Helmholtz Center for Information Security (CISPA)*

Akshayaram Srinivasan *Tata Institute of Fundamental Research*

Oblivious Transfer



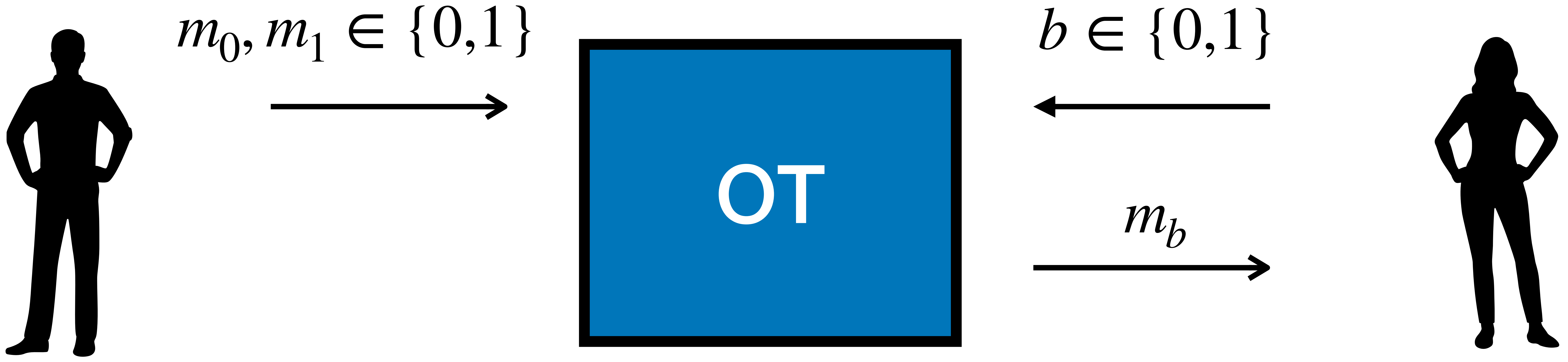
Oblivious Transfer



Receiver security: b is hidden from the sender

Sender security: m_{1-b} hidden from the receiver

Oblivious Transfer

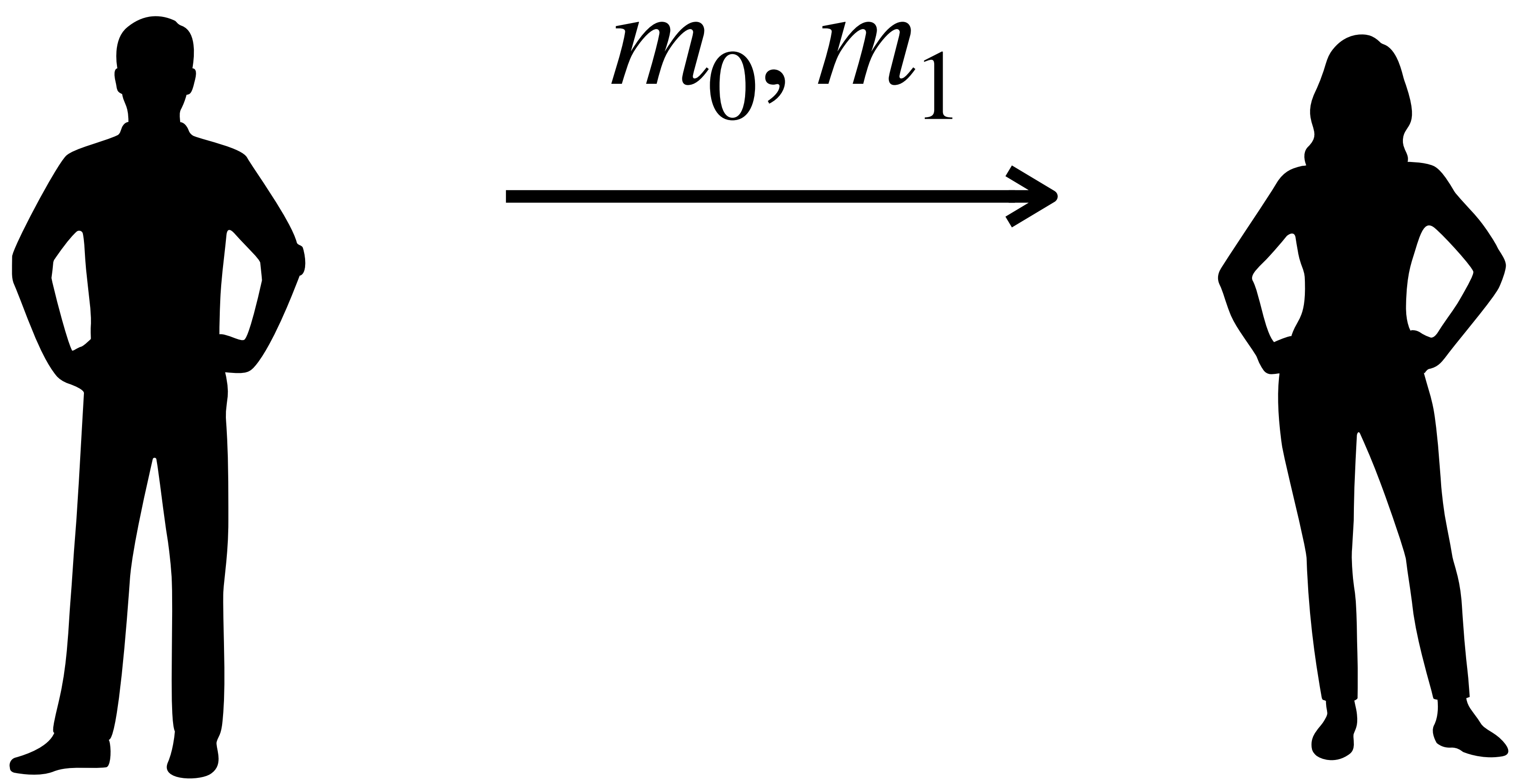


Receiver security: b is hidden from the sender

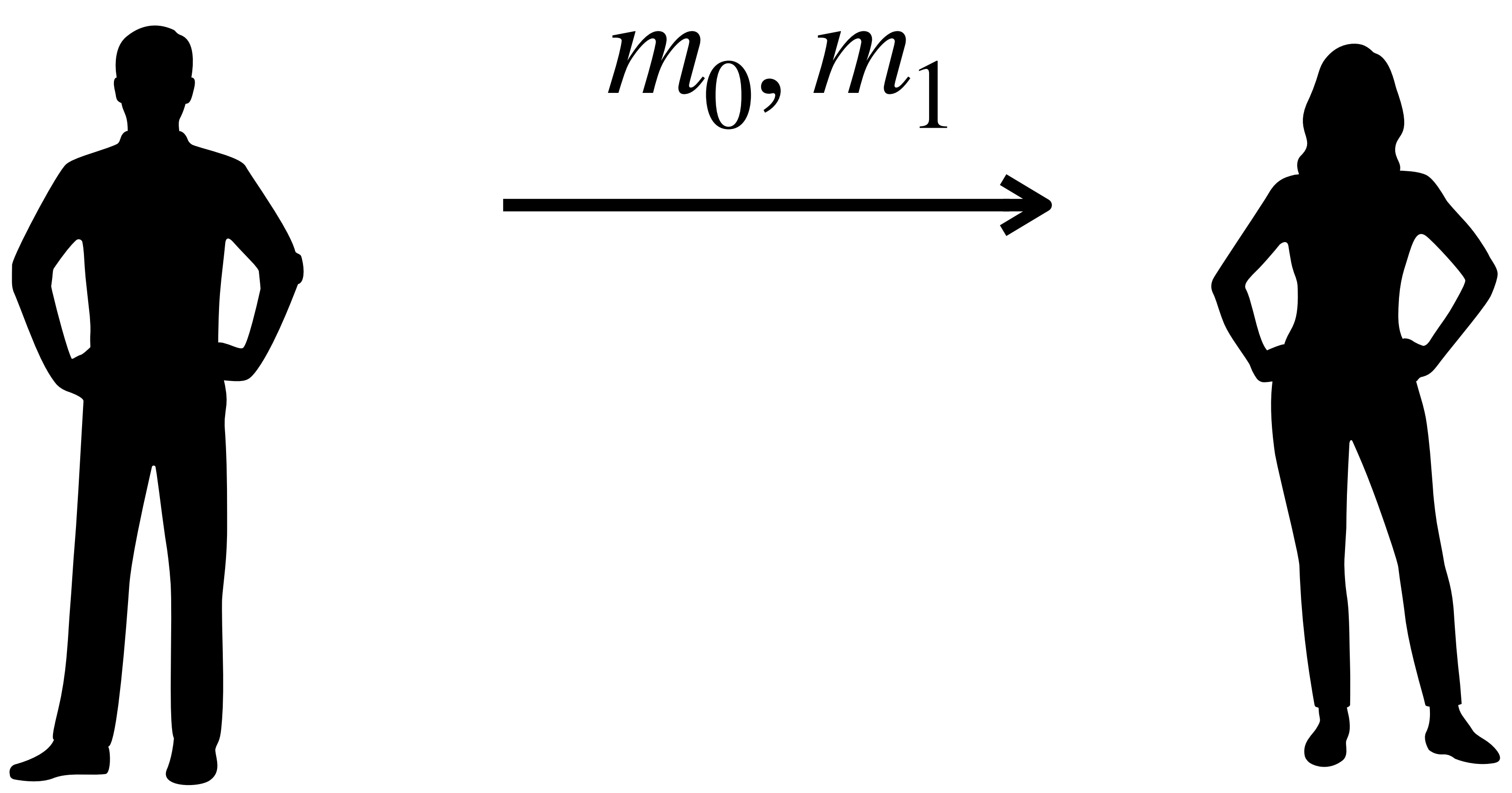
Sender security: m_{1-b} hidden from the receiver

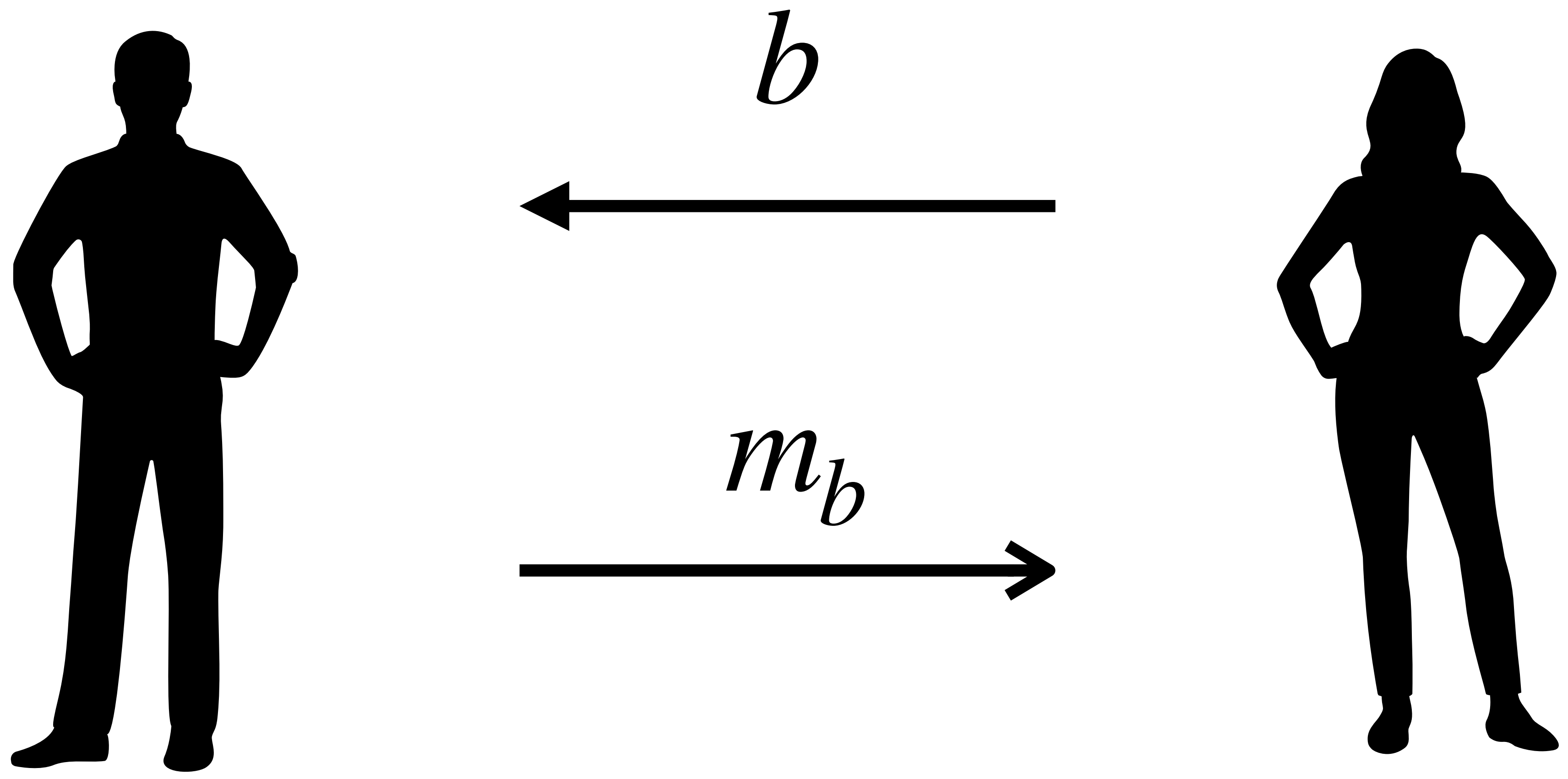
Main Application: OT is complete for 2PC/MPC

What is the communication complexity of OT?

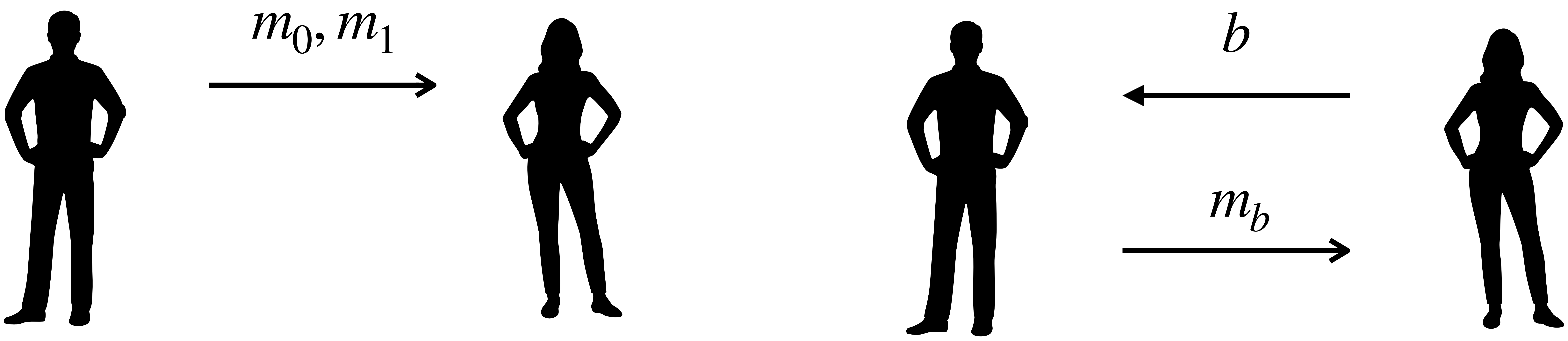


What is the communication complexity of OT?





What is the communication complexity of OT?



Lower bound: k OTs need at least 2k bits of communication

OT schemes with Optimal Rate

OT with optimal rate?*

*Excluding trivial FHE-based solutions

OT schemes with Optimal Rate

OT with optimal rate?*

- **Optimal-rate OT:** [BBDP22] from DDH+LPN.

*Excluding trivial FHE-based solutions

OT schemes with Optimal Rate

OT with optimal rate?*

- **Optimal-rate OT:** [BBDP22] from DDH+LPN.

  Security: Semi-honest and computationally bounded.

*Excluding trivial FHE-based solutions

OT schemes with Optimal Rate

OT with optimal rate?*

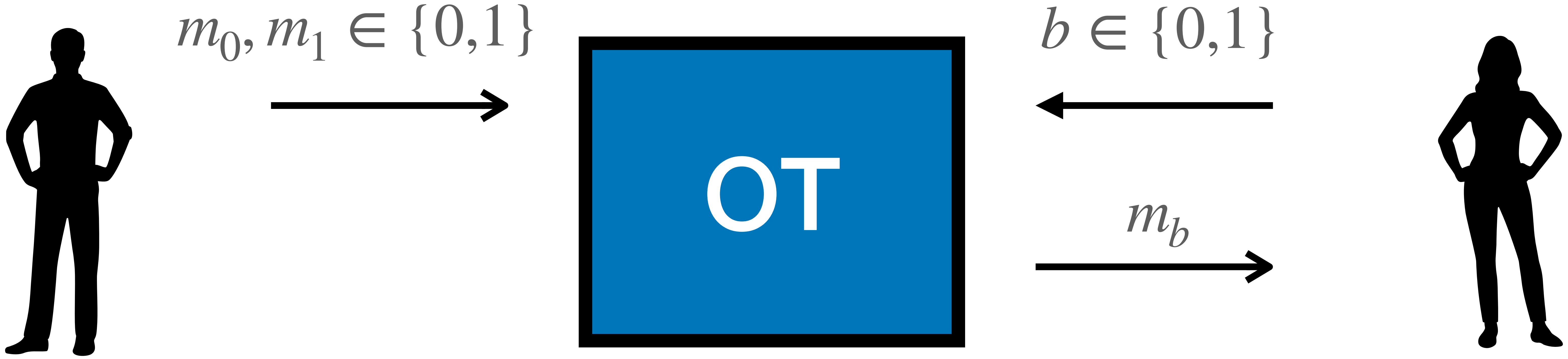
- **Optimal-rate OT:** [BBDP22] from DDH+LPN.

  Security: Semi-honest and computationally bounded.

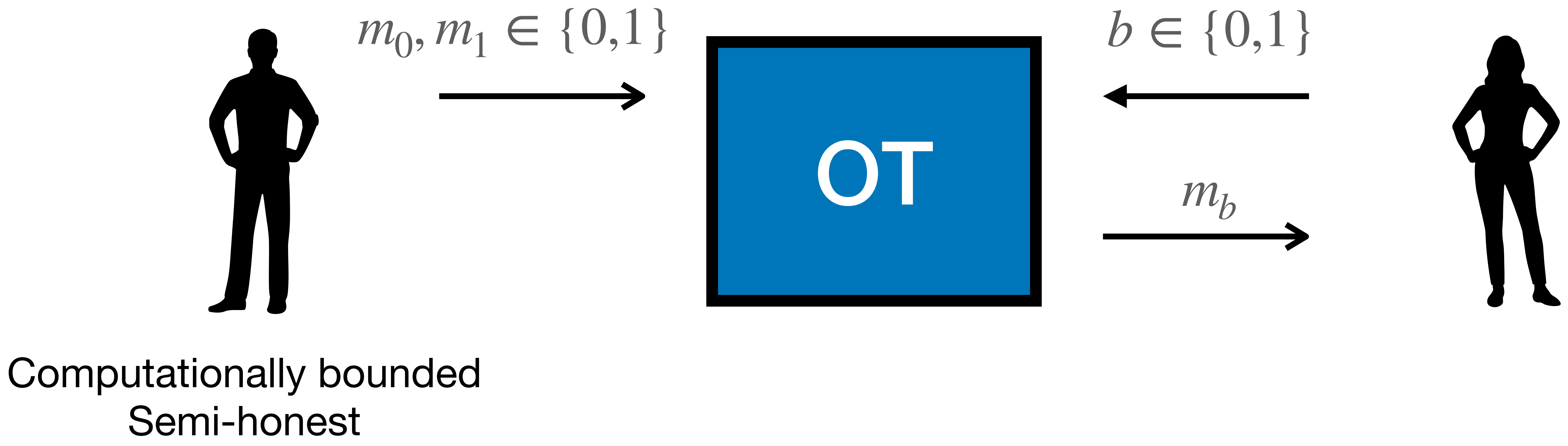
Strongest security possible for OT with optimal rate?*

*Excluding trivial FHE-based solutions

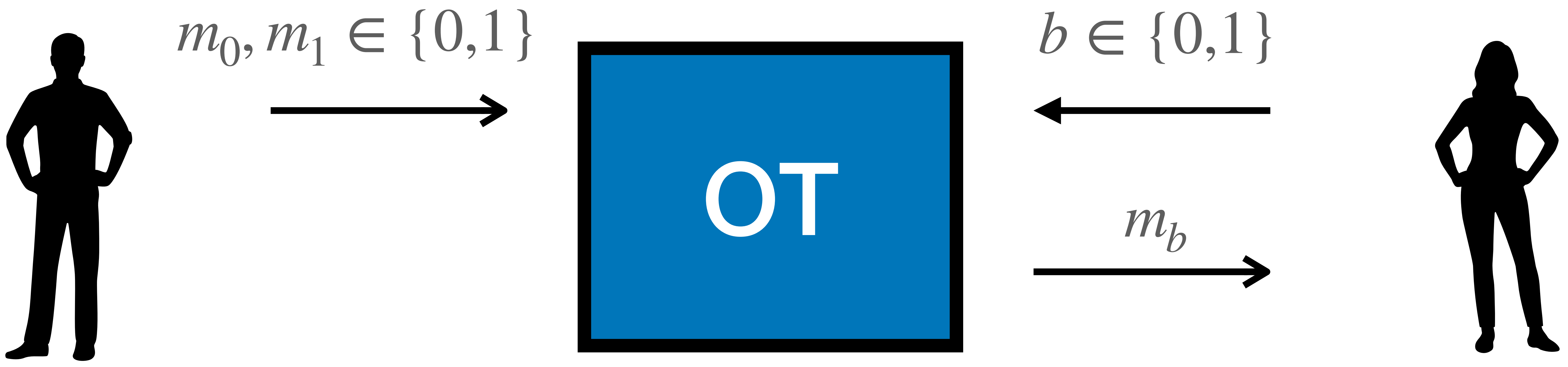
What is Statistical Sender Privacy?



What is Statistical Sender Privacy?



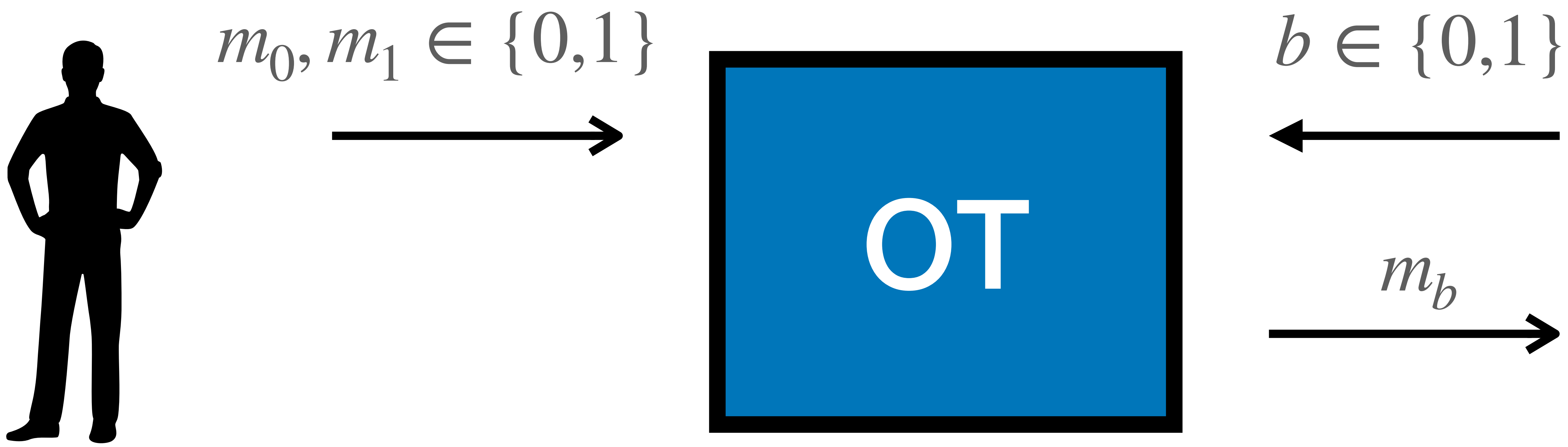
What is Statistical Sender Privacy?



Computationally bounded
Semi-honest

Computationally unbounded
Malicious

What is Statistical Sender Privacy?



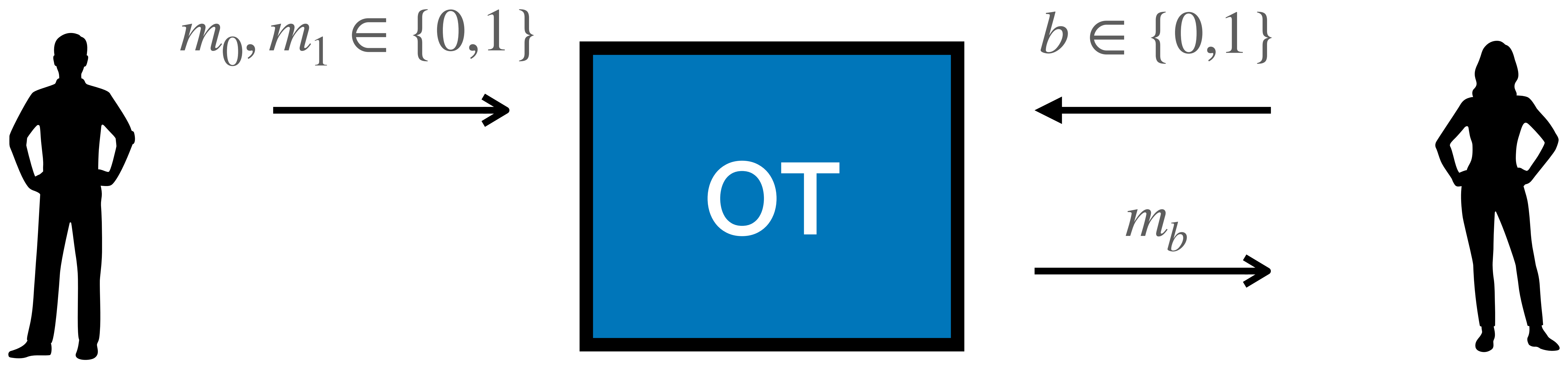
Computationally bounded
Semi-honest

Computationally unbounded
Malicious

↓

Existence of extractor that extracts
b

What is Statistical Sender Privacy?



Computationally bounded
Semi-honest

Computationally unbounded
Malicious

↓

Existence of extractor that extracts
b

↓

$\text{Send}(m_0, m_1) \approx_s \text{Send}(m_b, m_b)$

Why SSP?

Theory:

Best security in two rounds in plain model

Why SSP?

Theory:

Best security in two rounds in plain model

Applications:

- Statistical zaps
- Circuit-private FHE
- Non-malleable commitments

⋮

Our Results

Our Result: A two-round SSP OT with optimal rate in the plain model assuming DDH+LPN.

Our Results

Our Result: A two-round SSP OT with optimal rate in the plain model assuming DDH+LPN.

- **Sender security:** Statistical against malicious receivers
- **Receiver security:** DDH and LPN assumptions against semi-honest senders

Our Results

Our Result: A two-round SSP OT with optimal rate in the plain model assuming DDH+LPN.

- **Sender security:** Statistical against malicious receivers
- **Receiver security:** DDH and LPN assumptions against semi-honest senders
- **Communication Complexity:** $2k(1 + o(1))$ for k independent OT executions

Blueprint [BBDP22]

[BBDP22] building blocks:

- LPN
- Rate-1 LHE w/ circuit privacy
- PIR
- Co-PIR

Blueprint [BBDP22]

[BBDP22] building blocks:

- LPN
- Rate-1 LHE w/ circuit privacy
- PIR
- Co-PIR

↓

OT with optimal rate

semi-honest

Blueprint [BBDP22]

[BBDP22] building blocks:

- LPN
- Rate-1 LHE w/ circuit privacy → DDH
- PIR → DDH
- Co-PIR → DDH

↓

OT with optimal rate

semi-honest

Blueprint [BBDP22]

[BBDP22] building blocks:

- LPN
- Rate-1 LHE w/ circuit privacy → DDH
- PIR → DDH
- Co-PIR → DDH

↓ ↓

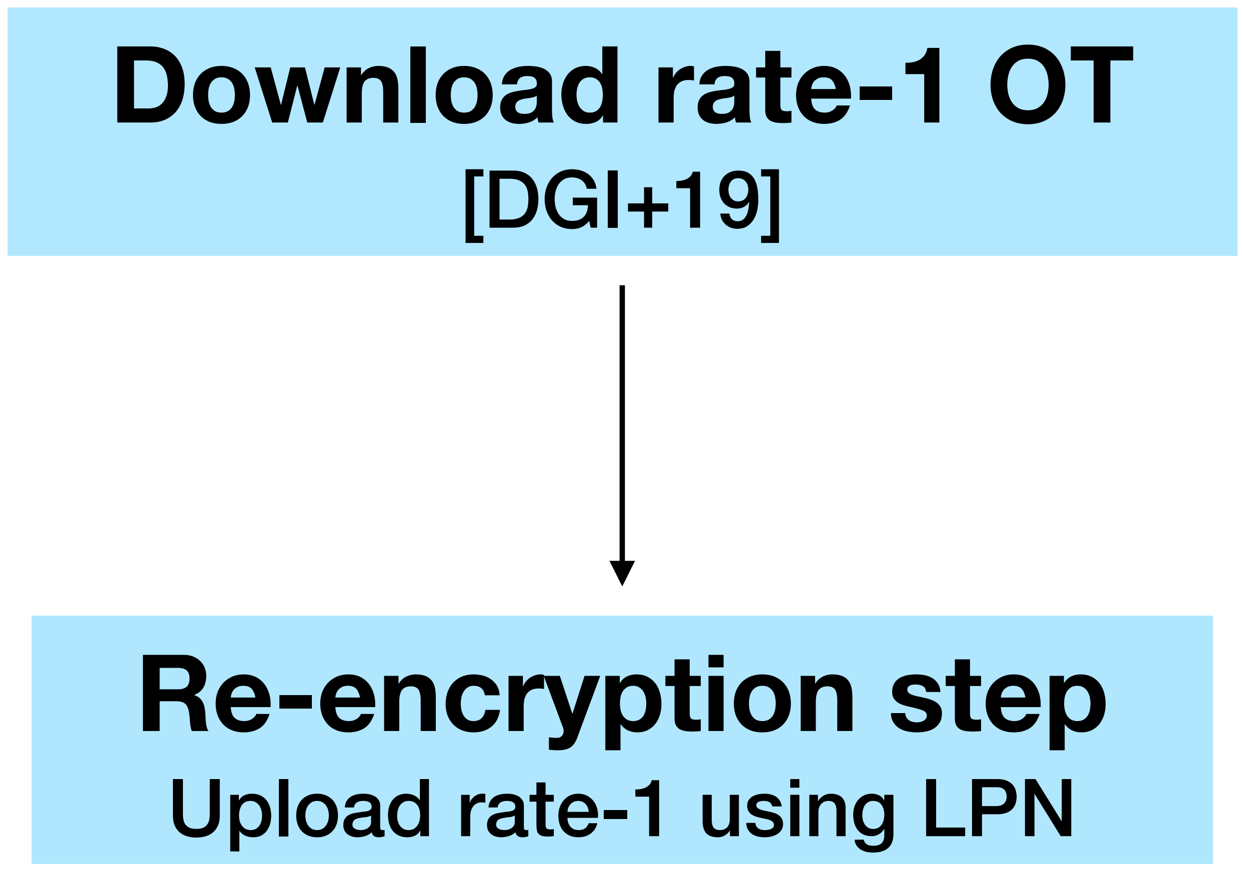
OT with optimal rate → DDH + LPN

semi-honest

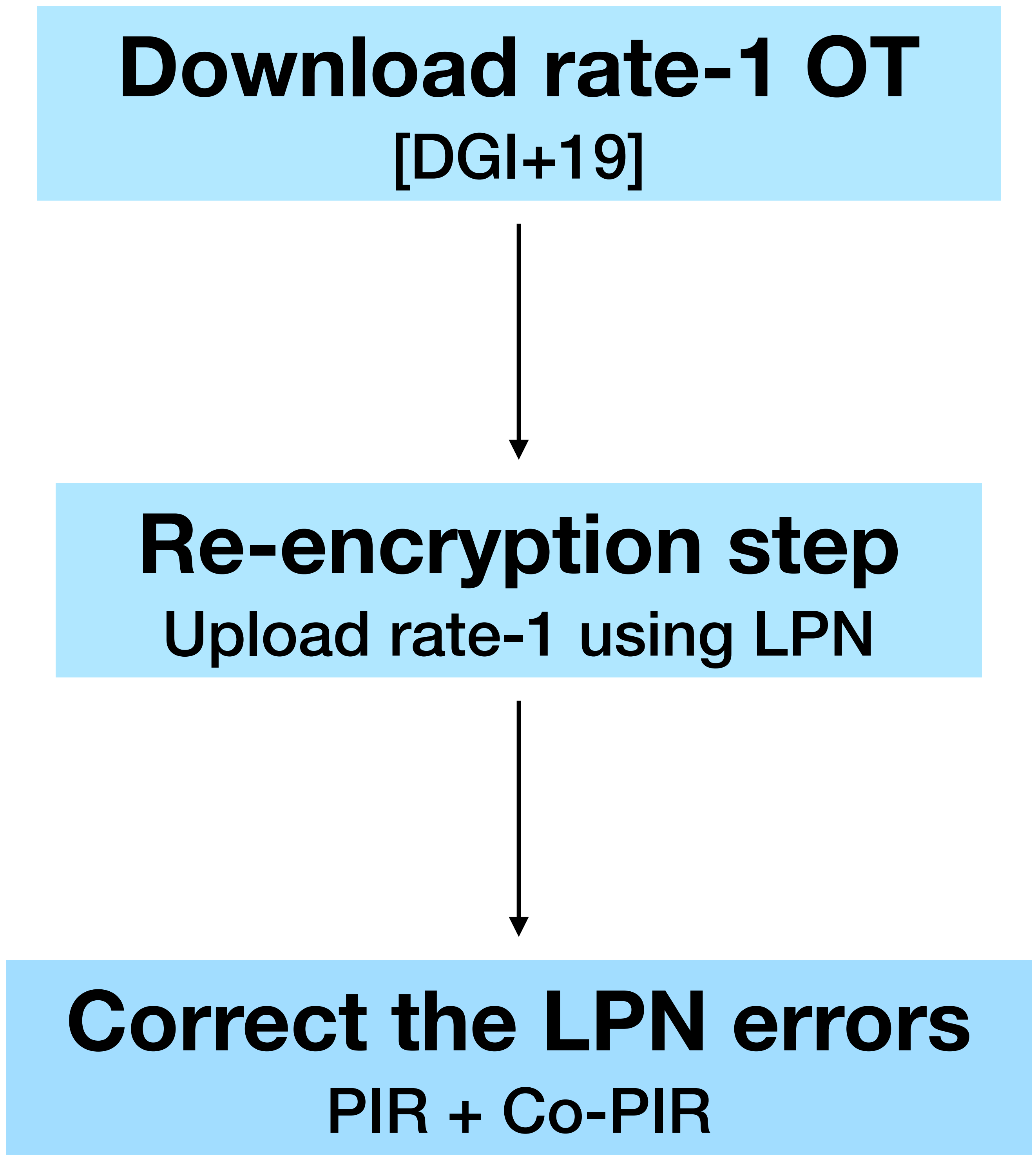
Blueprint [BBDP22]

Download rate-1 OT
[DGI+19]

Blueprint [BBDP22]



Blueprint [BBDP22]



Our construction: Blueprint

[BBDP22] building blocks:

- LPN
- Rate-1 LHE w/ circuit privacy
- PIR
- Co-PIR

↓

OT with optimal rate

Our Construction:

- LPN

Our construction: Blueprint

[BBDP22] building blocks:

- LPN
- Rate-1 LHE w/ circuit privacy
- PIR
- Co-PIR

↓

OT with optimal rate

Our Construction:

- LPN
- Malicious Rate-1 LHE w/ circuit privacy
- SSP PIR
- SSP Co-PIR

Our construction: Blueprint

[BBDP22] building blocks:

- LPN
- Rate-1 LHE w/ circuit privacy
- PIR
- Co-PIR

↓

OT with optimal rate

Our Construction:

- LPN
- Malicious Rate-1 LHE w/ circuit privacy
- SSP PIR
- SSP Co-PIR

↓

SSP OT with optimal rate

Our Construction: Blueprint

Our Construction: Assumptions

- LPN
- Malicious Rate-1 LHE w/ circuit privacy
- SSP PIR
- SSP Co-PIR

Our Construction: Blueprint

Our Construction: Assumptions

- LPN
- Malicious Rate-1 LHE w/ circuit privacy ⟶ DDH [BBDP22] + [ADD+22]
- SSP PIR
- SSP Co-PIR

Our Construction: Blueprint

Our Construction: Assumptions

- LPN
- Malicious Rate-1 LHE w/ circuit privacy ⟶ DDH [BBDP22] + [ADD+22]
- SSP PIR ⟶ DDH [ADD+22]
- SSP Co-PIR

Our Construction: Blueprint

Our Construction: Assumptions

- LPN
- Malicious Rate-1 LHE w/ circuit privacy ⟶ DDH [BBDP22] + [ADD+22]
- SSP PIR ⟶ DDH [ADD+22]
- SSP Co-PIR ⟶ ?

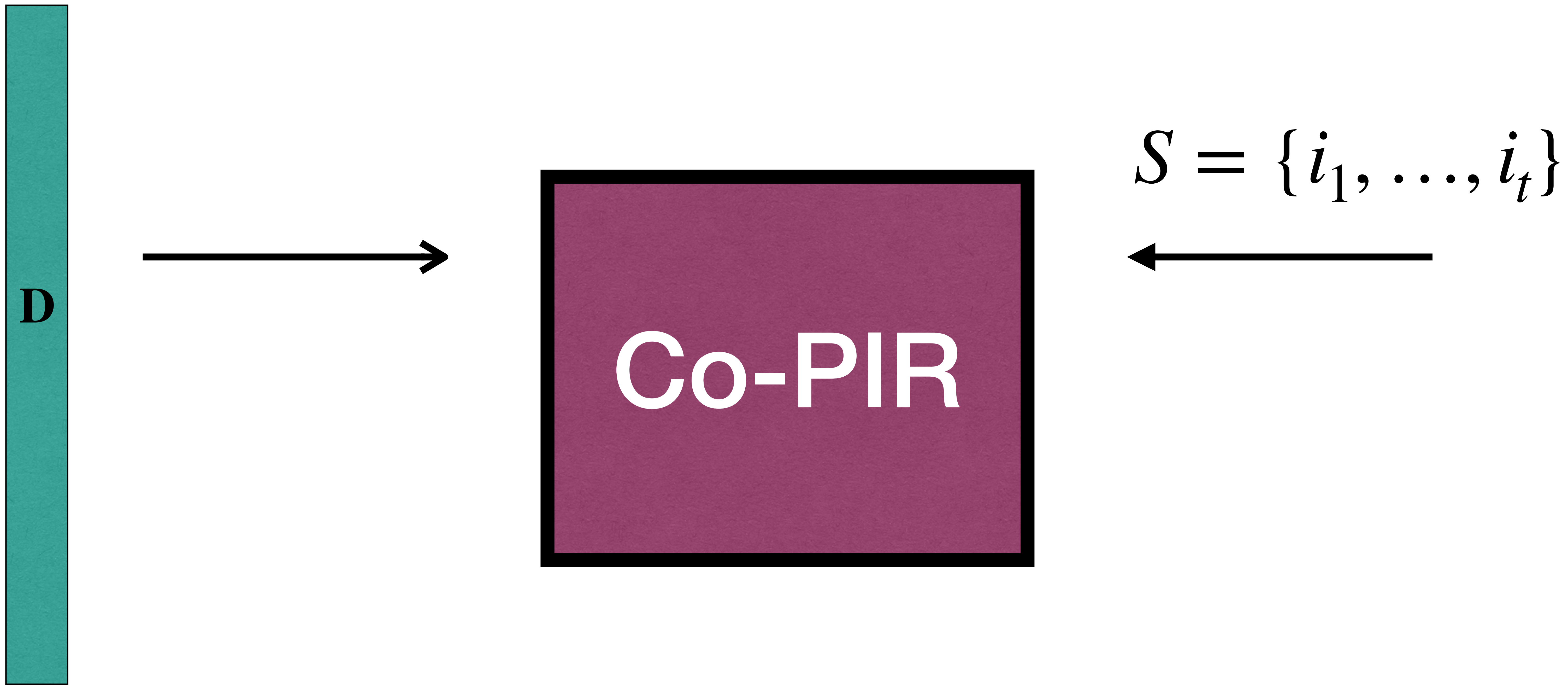
Our Construction: Blueprint

Our Construction: Assumptions

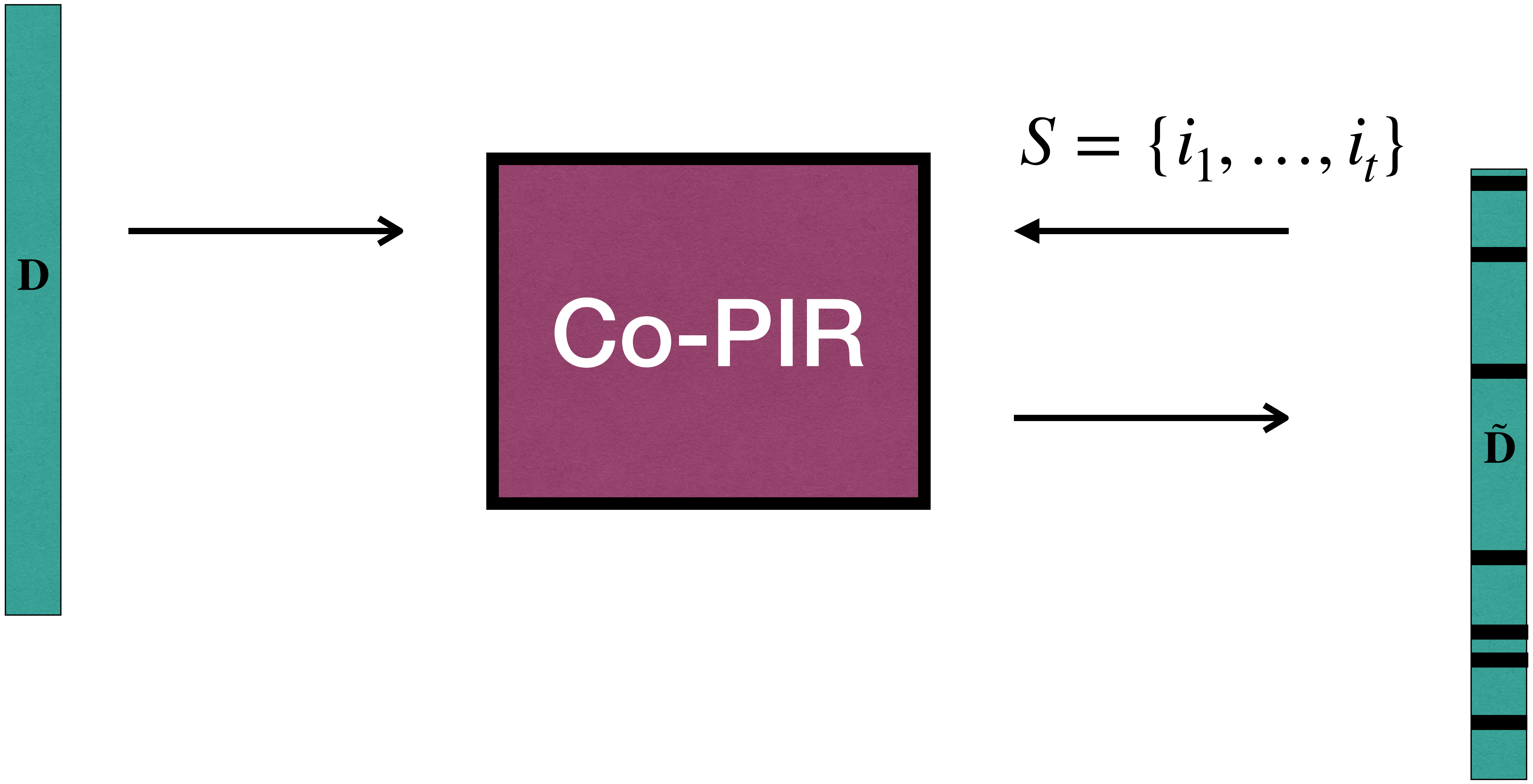
- LPN
- Malicious Rate-1 LHE w/ circuit privacy ⟶ DDH [BBDP22] + [ADD+22]
- SSP PIR ⟶ DDH [ADD+22]
- SSP Co-PIR ⟶ ?

SSP Co-PIR from DDH

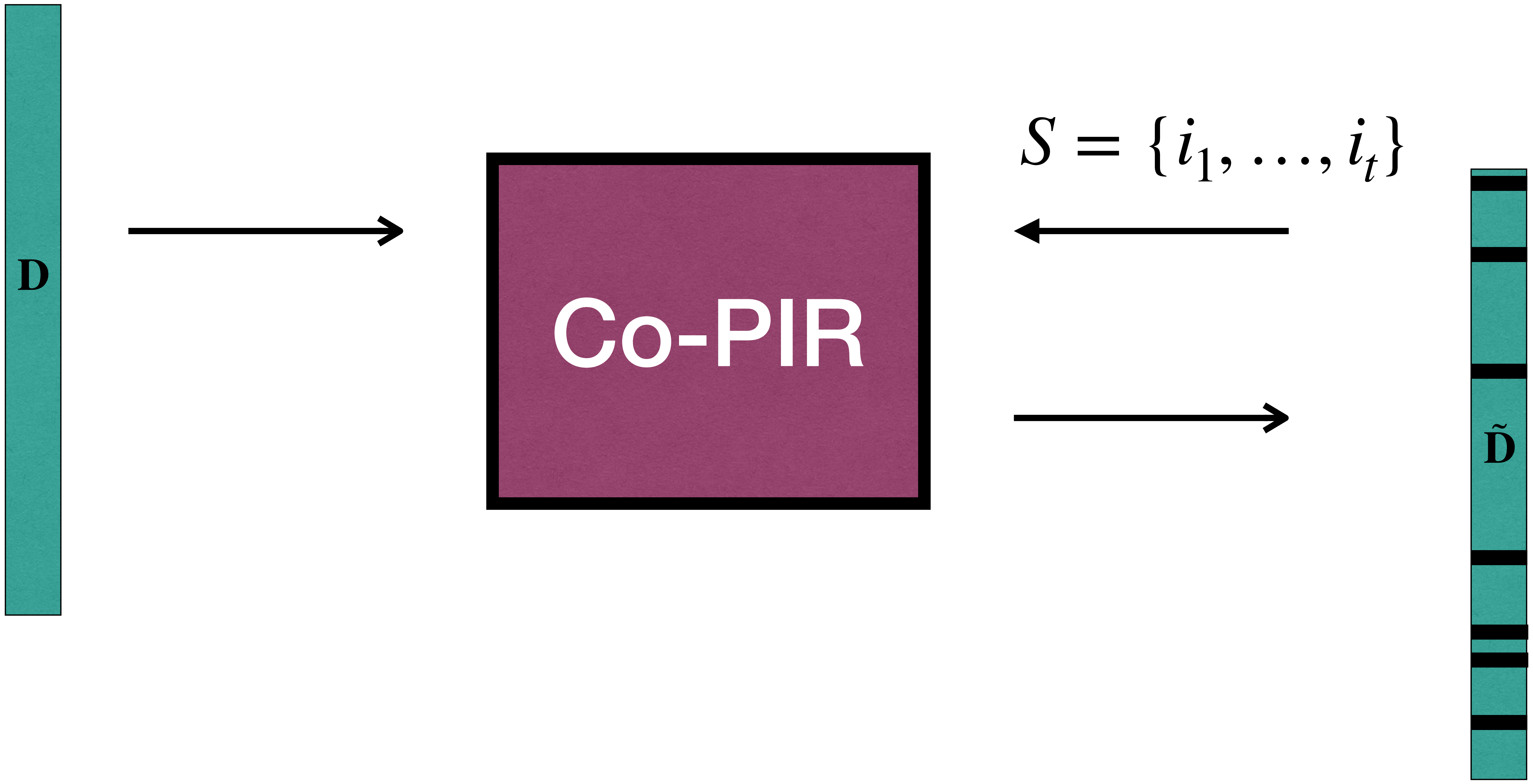
Co-Private Information Retrieval



Co-Private Information Retrieval



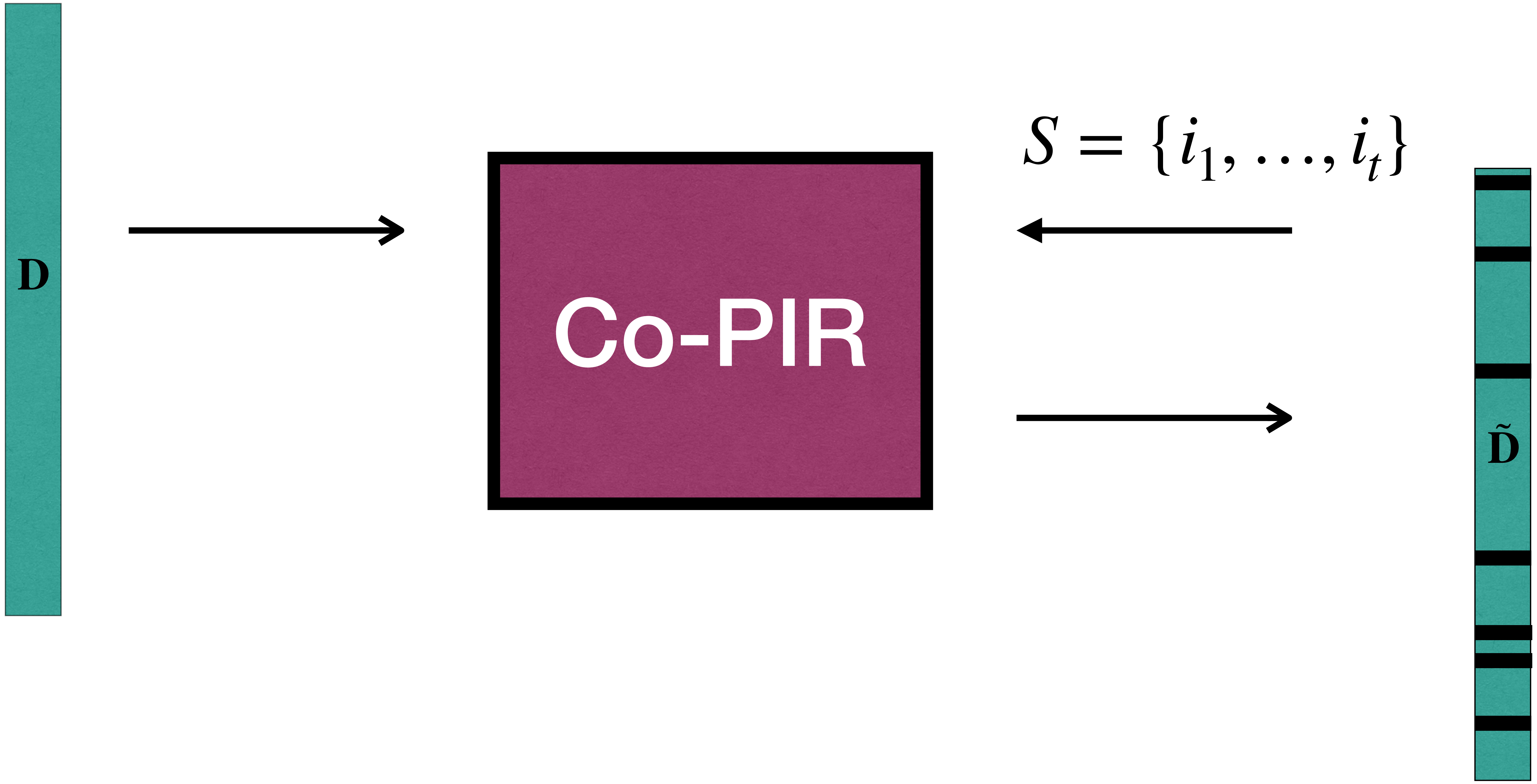
Co-Private Information Retrieval



Receiver's message of size $|S| \cdot \text{poly}(\lambda)$

Sender's message of size $\approx |\mathbf{D}|$

Co-Private Information Retrieval



Receiver's message of size $|S| \cdot \text{poly}(\lambda)$

Sender's message of size $\approx |\mathbf{D}|$

$\mathbf{D}_j$ for $j \in S$ is hidden from the receiver

S is hidden from the sender

Statistical Co-PIR

Problems:

- Previous constructions from PPRF
- PPRF only have computational security.

Statistical Co-PIR

Problems:

- Previous constructions from PPRF
- PPRF only have computational security.

New co-PIR constructions providing SSP from DDH:

- From rate-1 SSP PIR with computational complexity of $|\mathbf{D}|^2$.
- From All-but-One Lossy Functions with computational complexity of $|\mathbf{D}|^{1+\varepsilon}$

Statistical Co-PIR

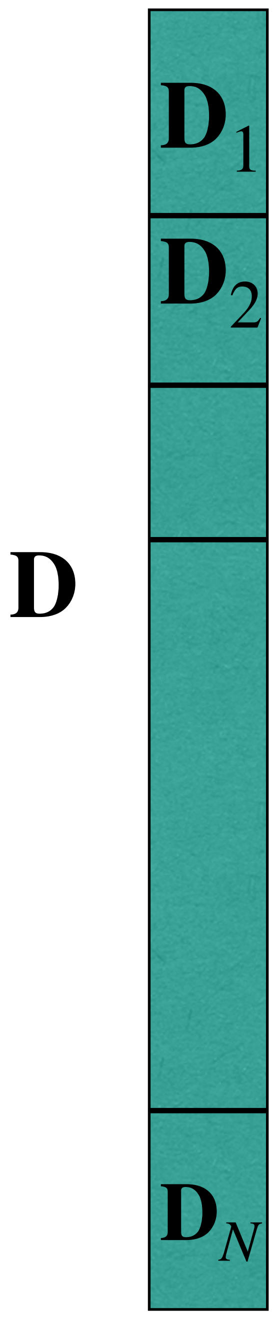
Problems:

- Previous constructions from PPRF
- PPRF only have computational security.

New co-PIR constructions providing SSP from DDH:

- From rate-1 SSP PIR with computational complexity of $|\mathbf{D}|^2$.
- From All-but-One Lossy Functions with computational complexity of $|\mathbf{D}|^{1+\varepsilon}$

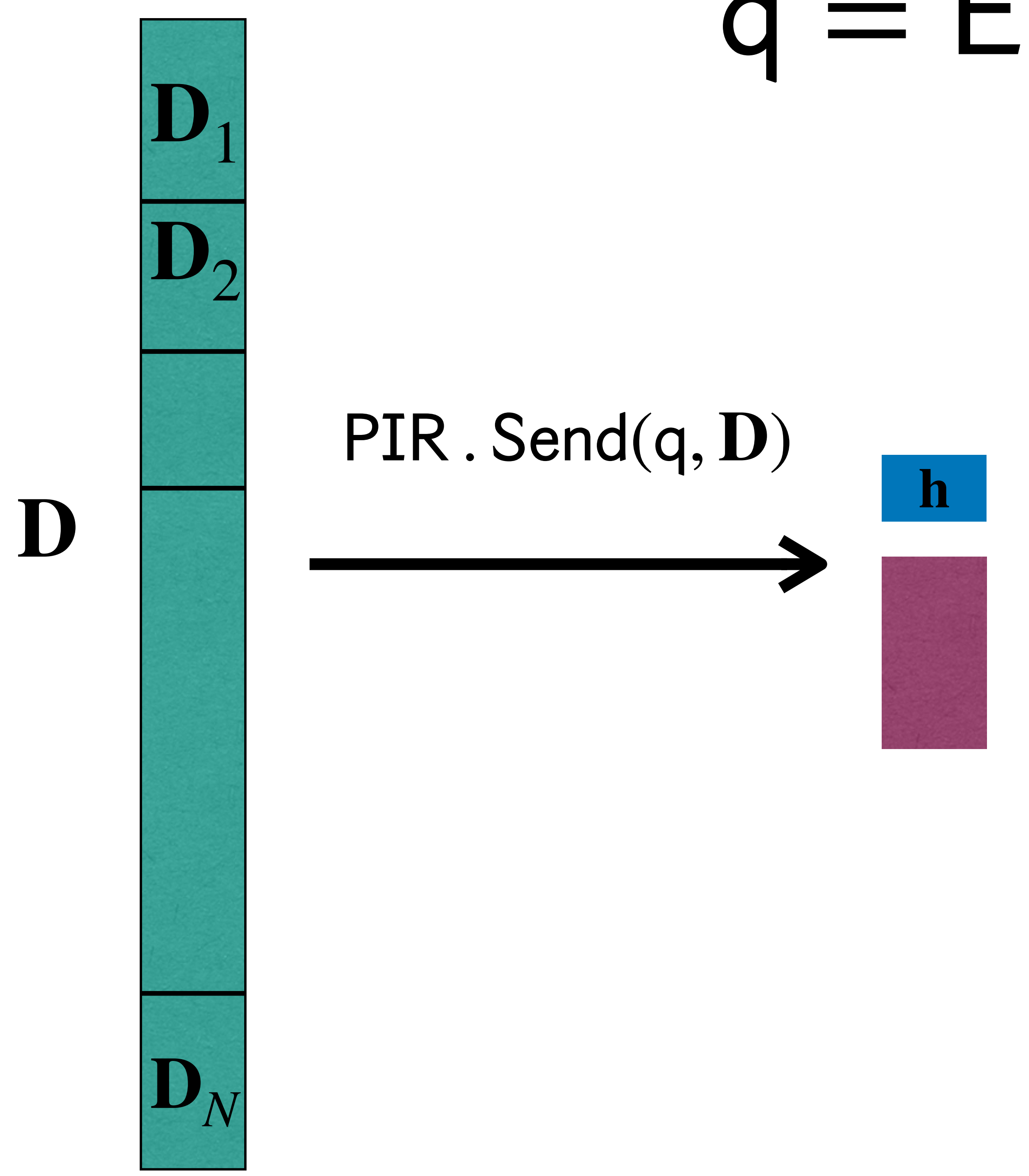
Rate-1 SSP PIR



$$\mathsf{q} = \mathsf{Enc}(i)$$

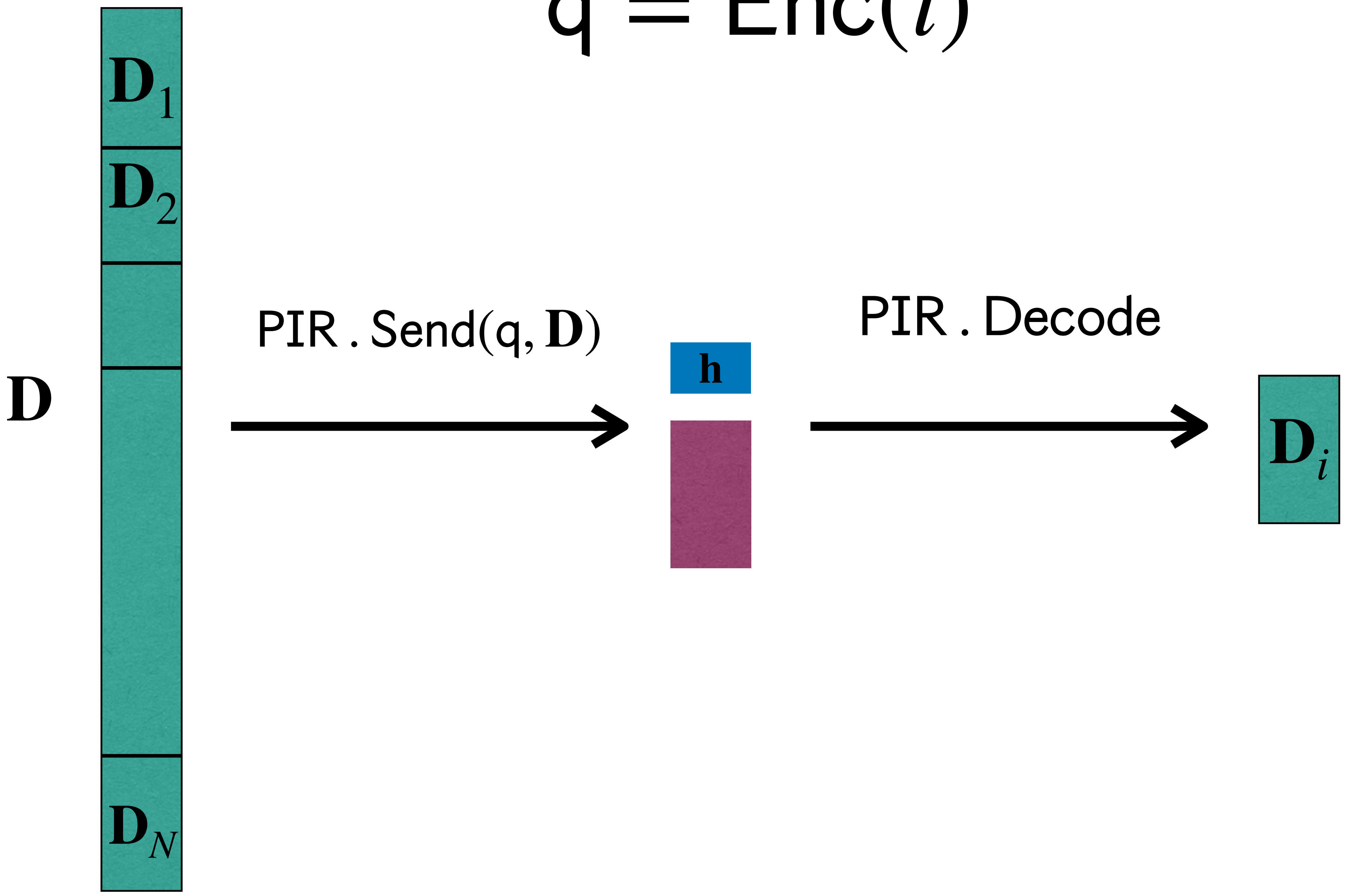
Rate-1 SSP PIR

$$q = \mathsf{Enc}(i)$$

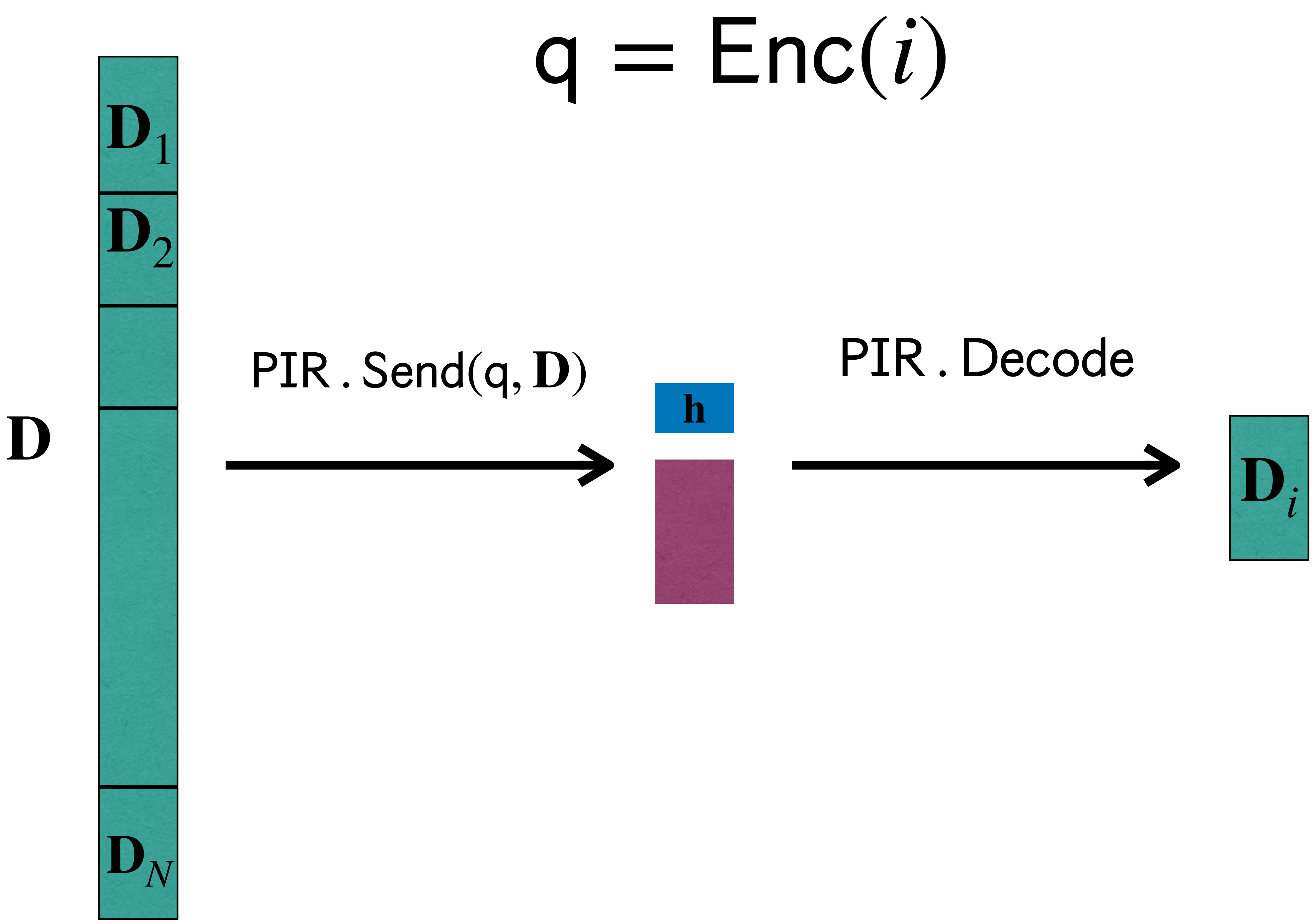


Rate-1 SSP PIR

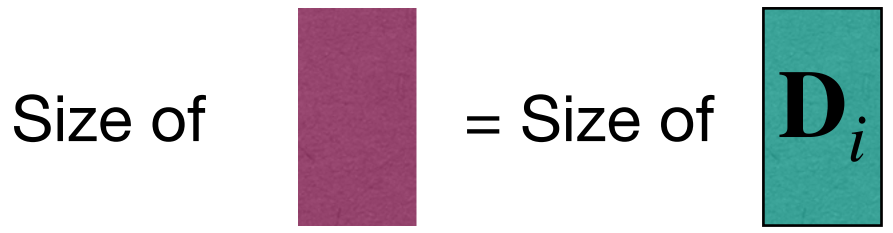
$$q = \mathsf{Enc}(i)$$



Rate-1 SSP PIR

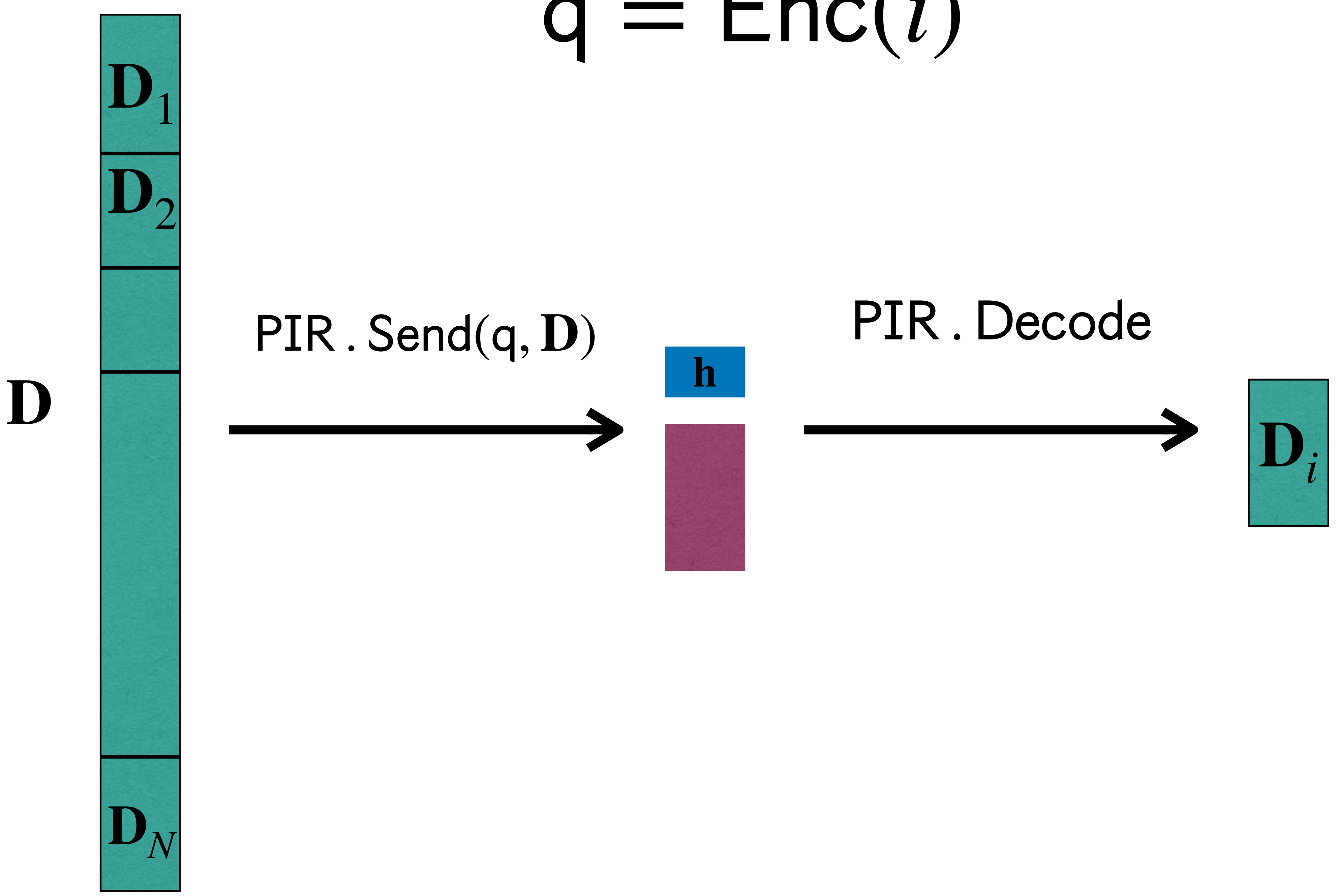


Efficiency:



Rate-1 SSP PIR

$$\mathsf{q} = \mathsf{Enc}(i)$$



Efficiency:

Size of  = Size of 

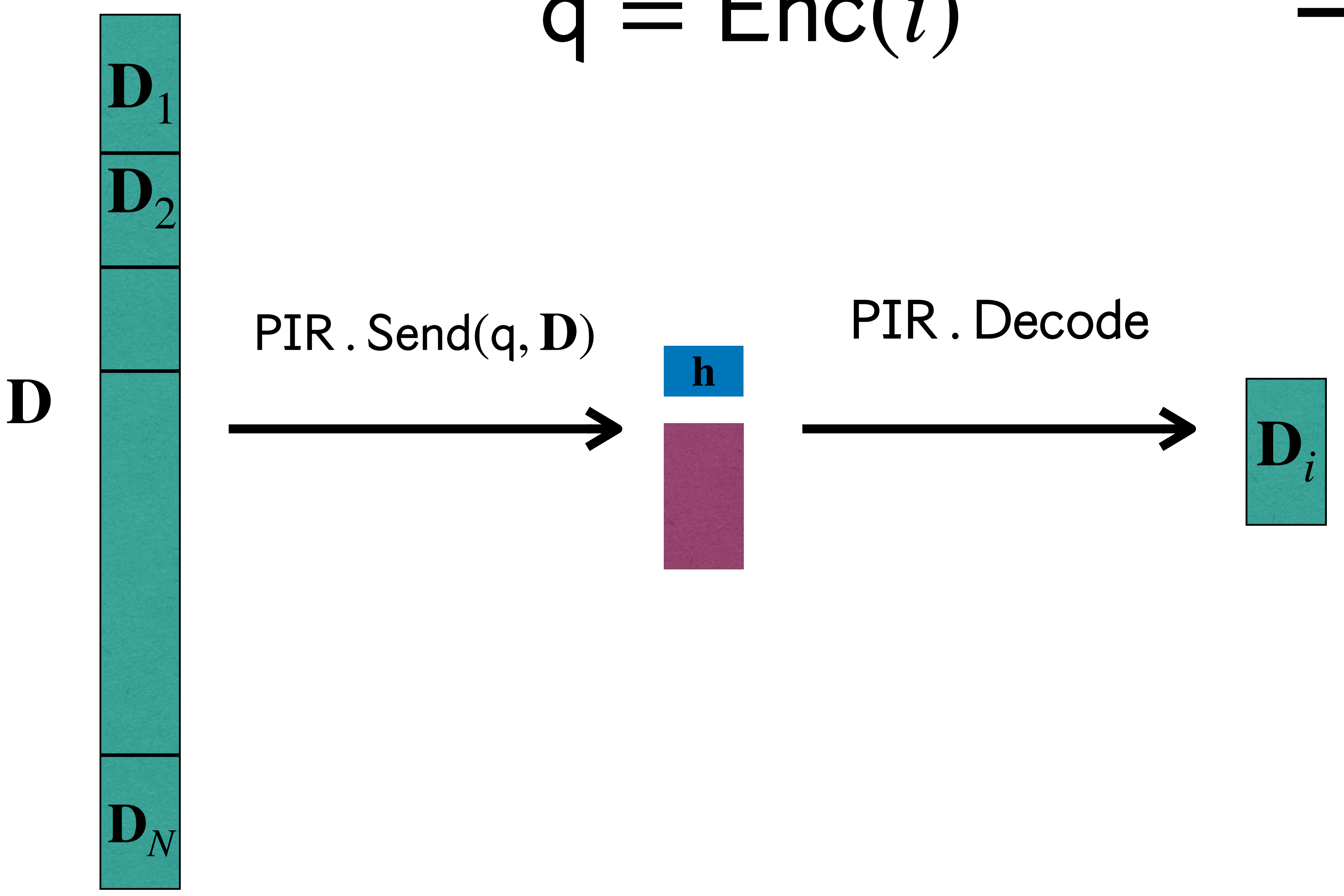
Size of 

$= \mathsf{poly}(\lambda)$

Rate-1 SSP PIR

$q = \mathsf{Enc}(i)$ ⟶

Ext that extracts i
s.t.
$\mathsf{PIR.Send}(q, \mathbf{D}) \approx_s \mathsf{PIR.Send}(q, (\mathbf{D}_i, \ldots, \mathbf{D}_i))$

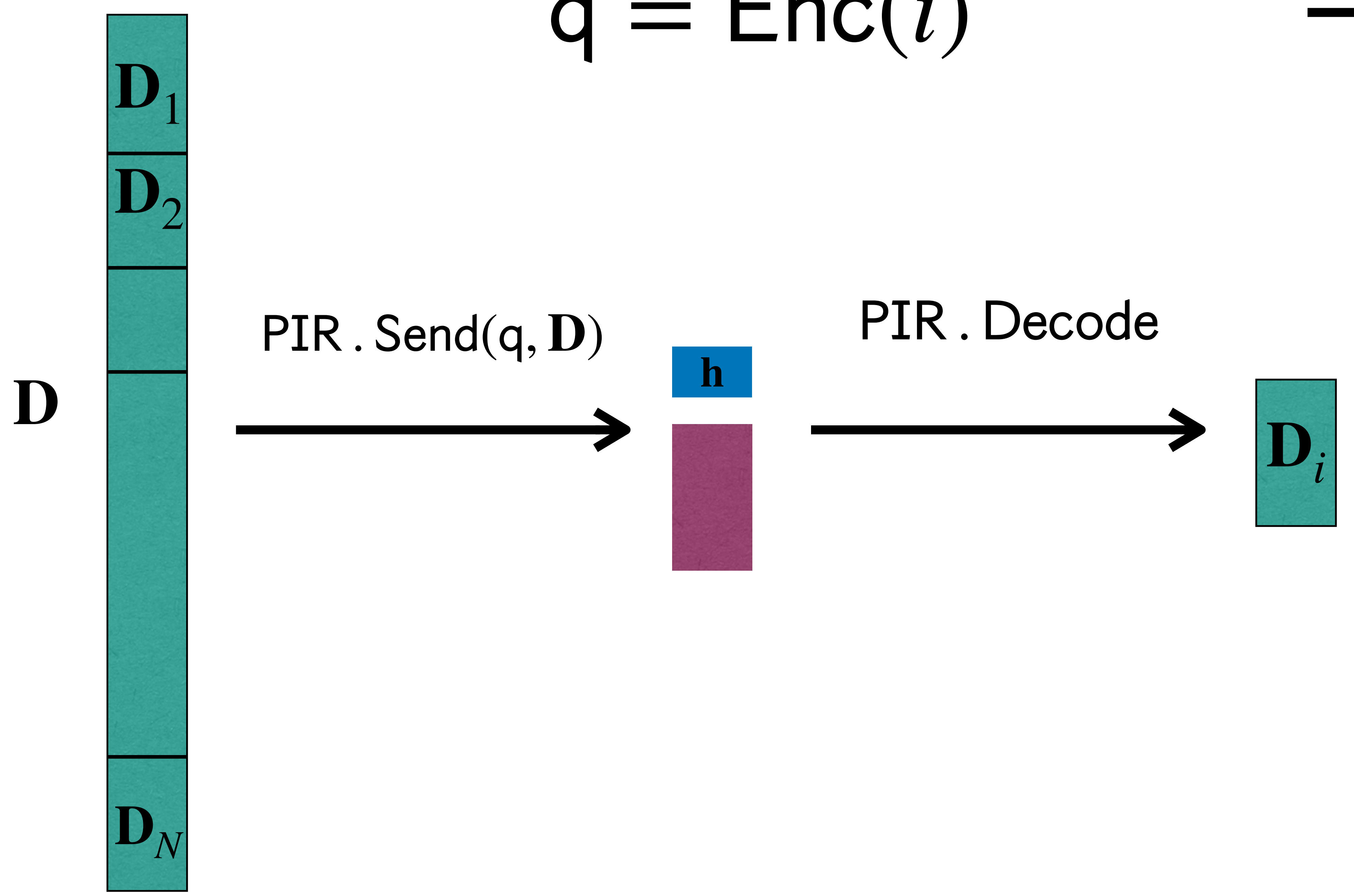


Efficiency: Size of [ ] = Size of $\mathbf{D}_i$

Size of h $= \mathsf{poly}(\lambda)$

Rate-1 SSP PIR

$q = \mathsf{Enc}(i)$ ⟶



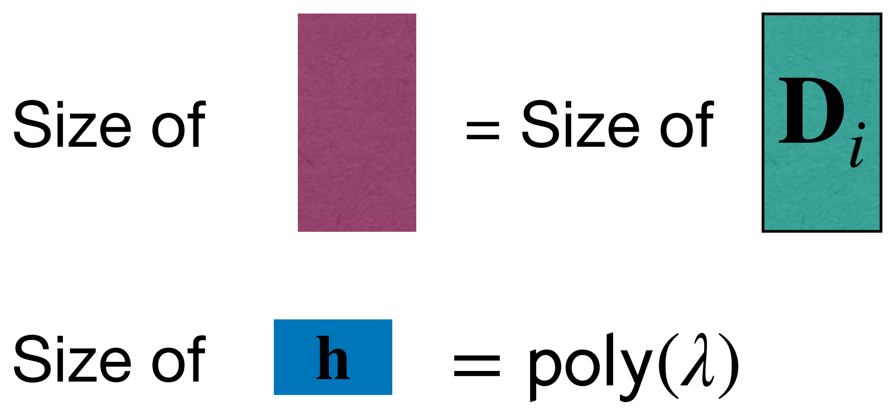
Ext that extracts i

s.t.

$\mathsf{PIR.Send}(q, \mathbf{D}) \approx_s \mathsf{PIR.Send}(q, (\mathbf{D}_i, \ldots, \mathbf{D}_i))$

From DDH [ADD+22]

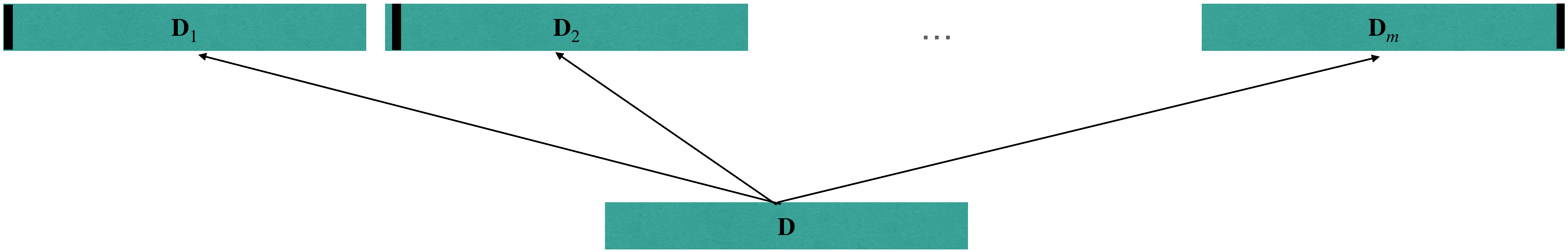
Efficiency:



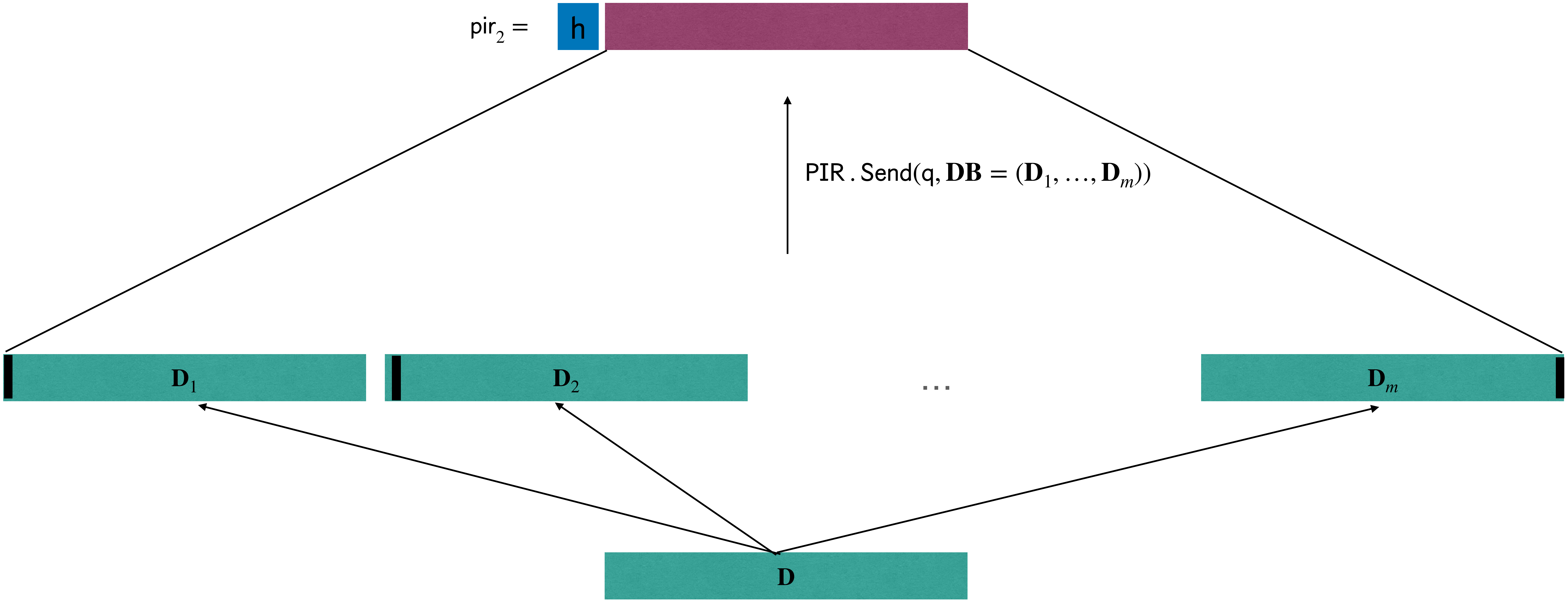
Statistical 1-Query Co-PIR

D

Statistical 1-Query Co-PIR

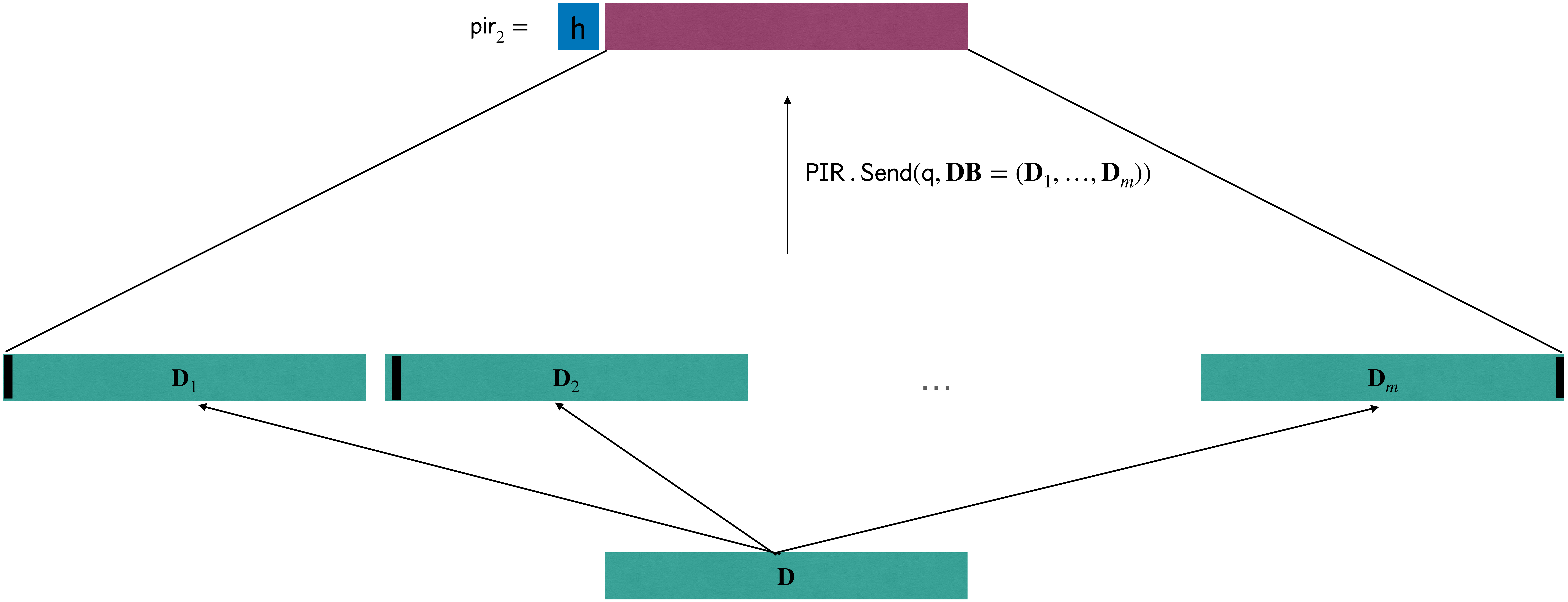


Statistical 1-Query Co-PIR



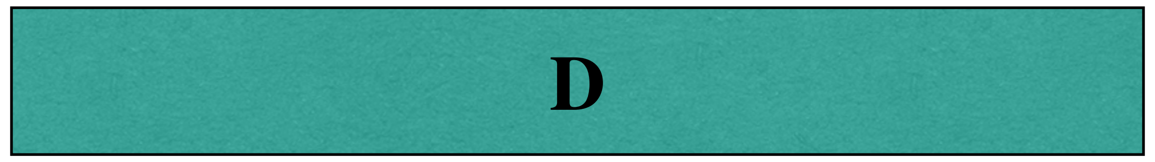
Statistical 1-Query Co-PIR

Rate-1 and SSP



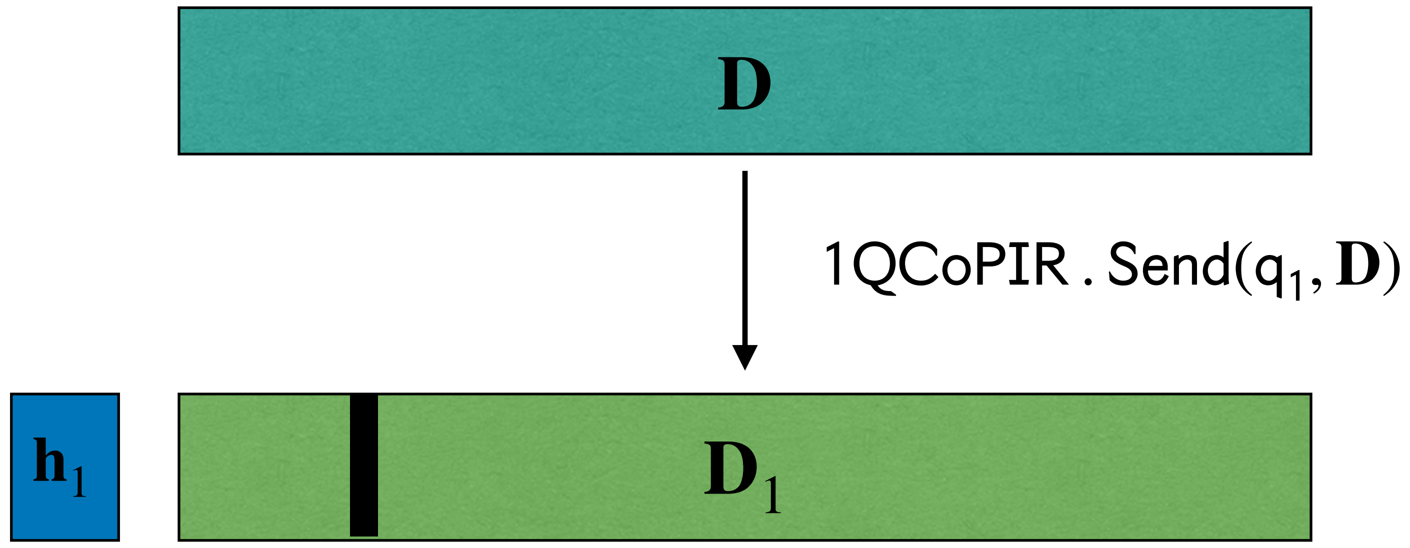
Bootstrapping into Multiple Queries

Given queries $q_1, q_2, \ldots, q_t$ and 1QCoPIR



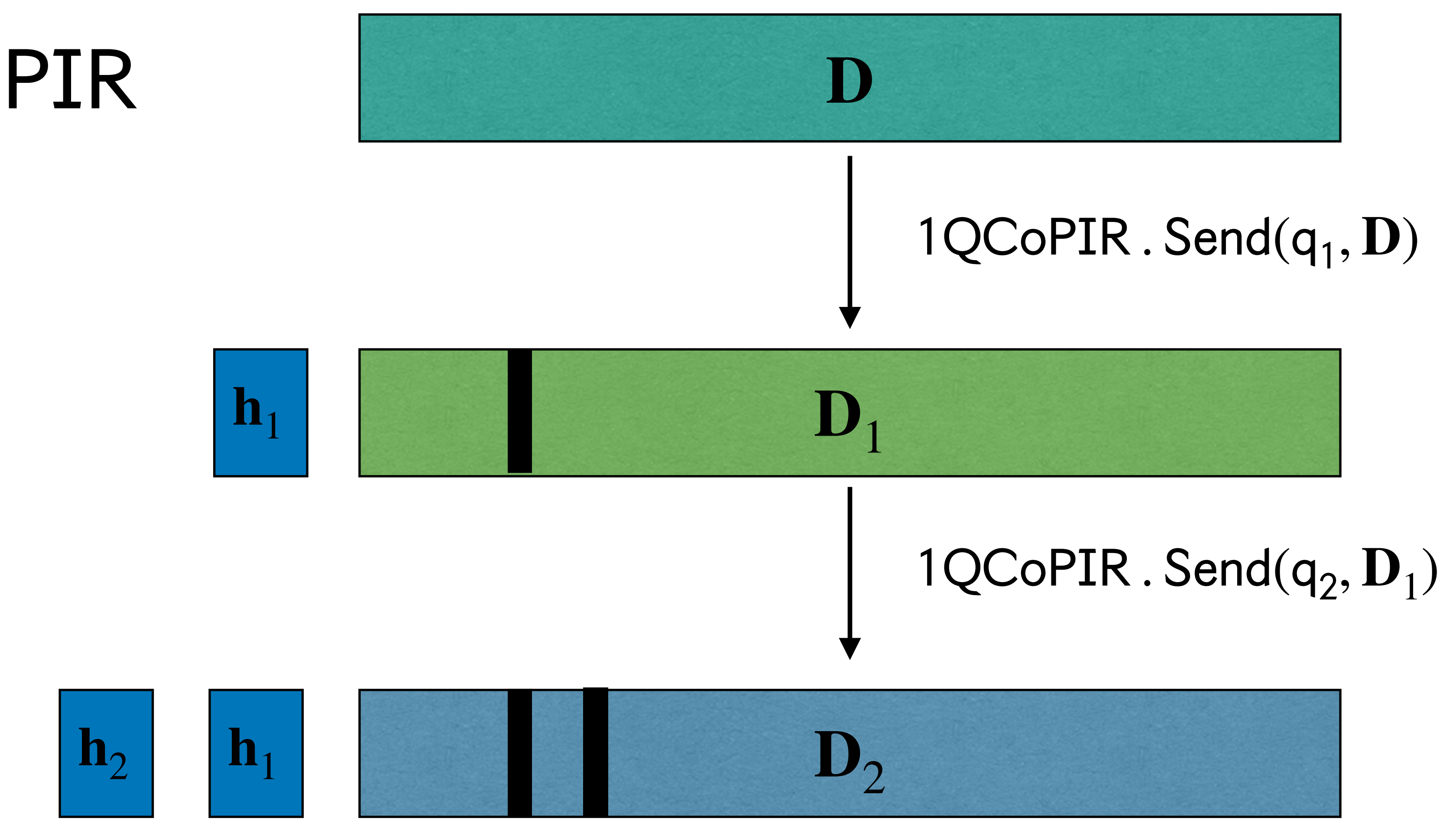
Bootstrapping into Multiple Queries

Given queries $q_1, q_2, \ldots, q_t$ and 1QCoPIR



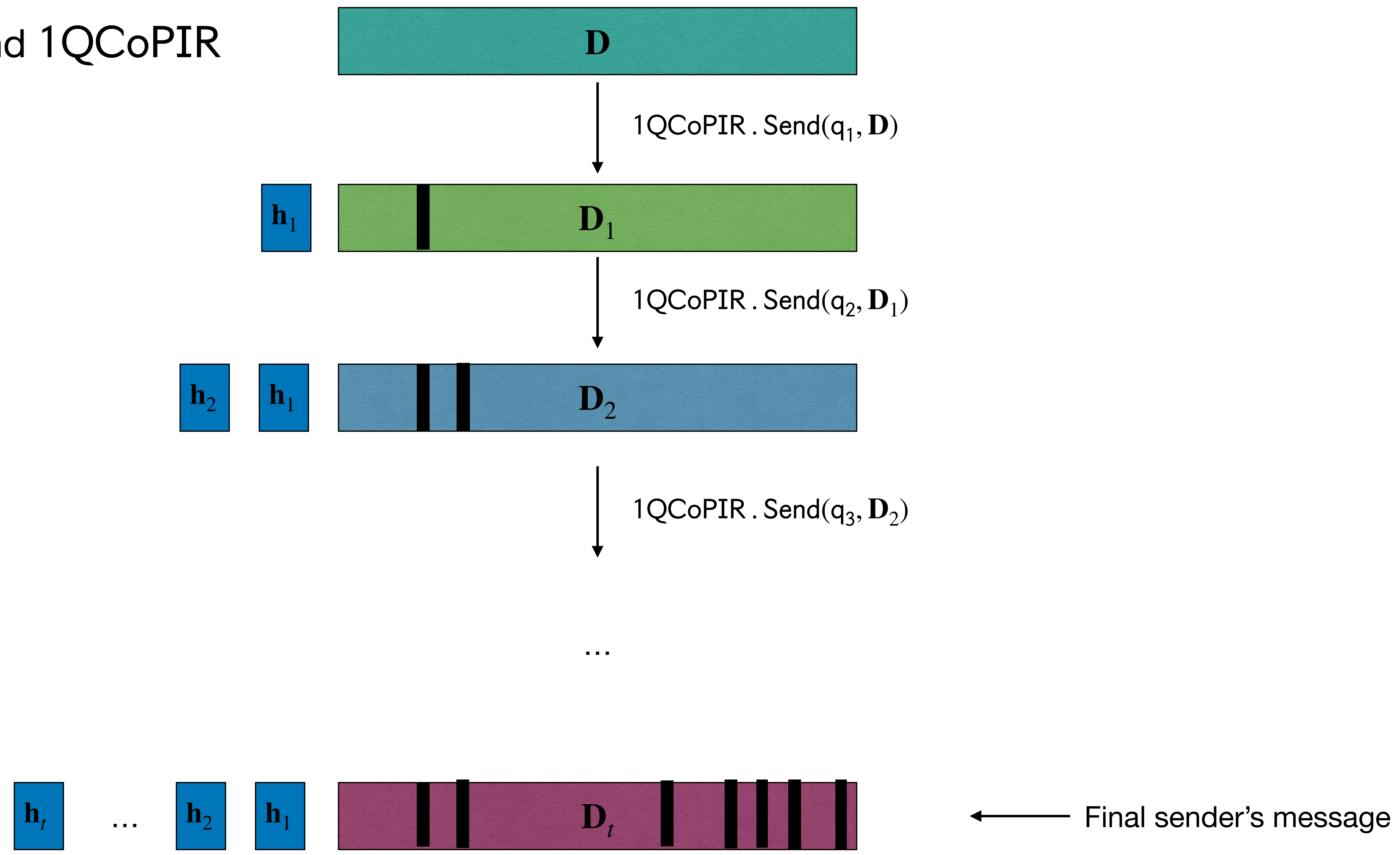
Bootstrapping into Multiple Queries

Given queries $q_1, q_2, \ldots, q_t$ and 1QCoPIR



Bootstrapping into Multiple Queries

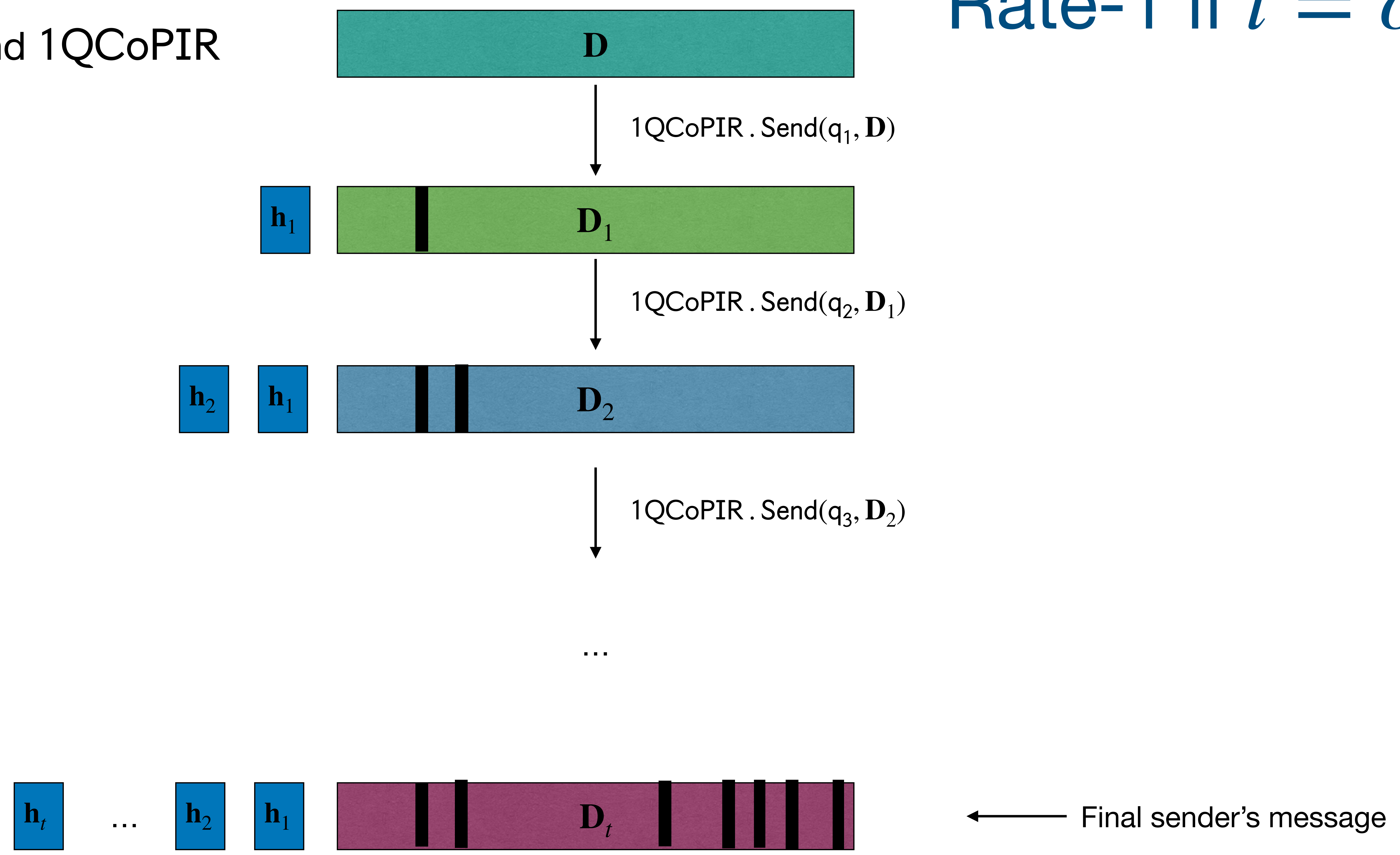
Given queries $q_1, q_2, \ldots, q_t$ and 1QCoPIR



Bootstrapping into Multiple Queries

Given queries $q_1, q_2, \ldots, q_t$ and 1QCoPIR

Rate-1 if $t = o\left(|\mathbf{D}|\right)$

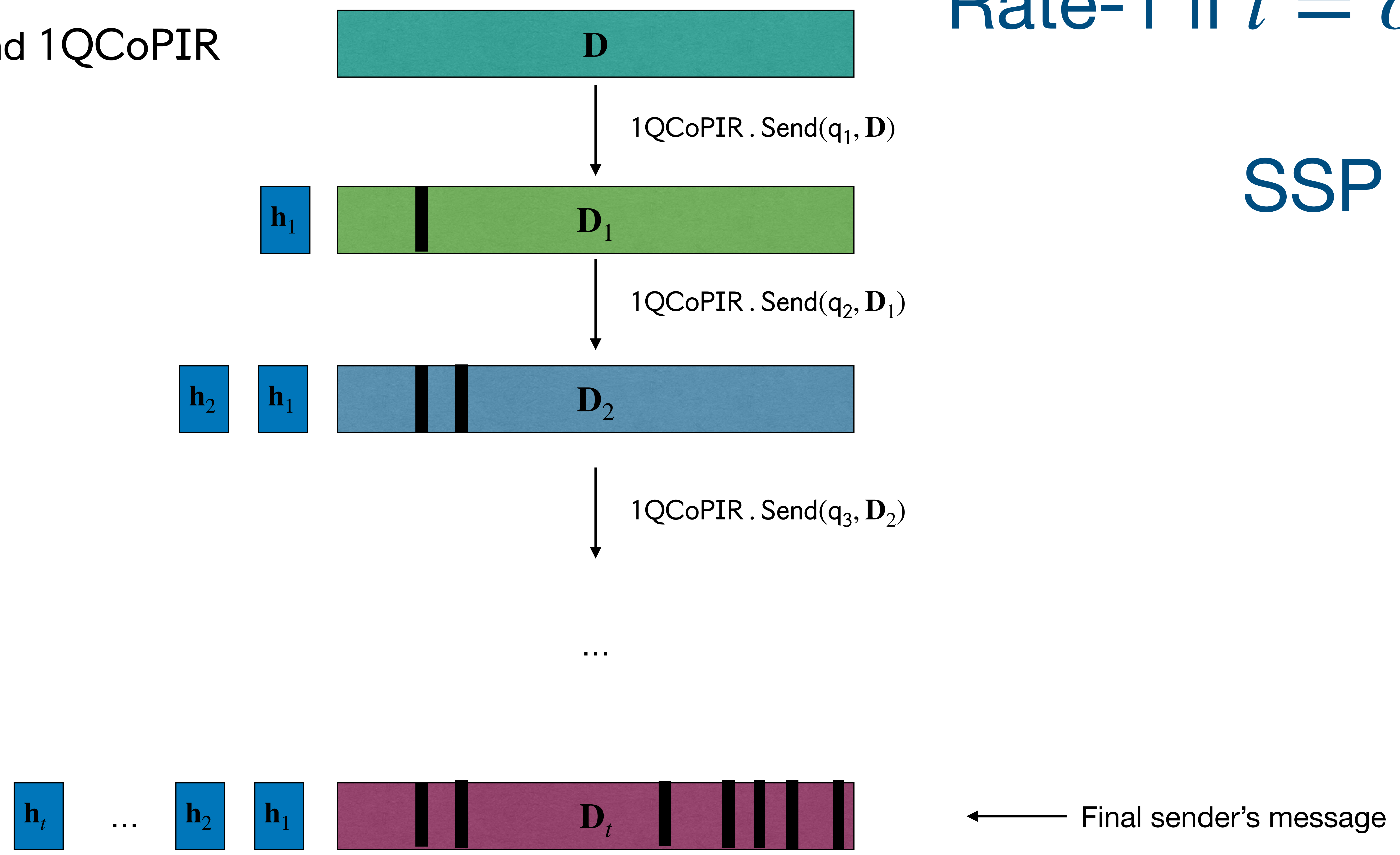


Bootstrapping into Multiple Queries

Given queries $q_1, q_2, \ldots, q_t$ and 1QCoPIR

Rate-1 if $t = o\left(|\mathbf{D}|\right)$

SSP



Recap

- Main Result: two-round SSP OT with optimal rate from DDH + LPN.
- Main building block: SSP Co-PIR from DDH

Recap

- Main Result: two-round SSP OT with optimal rate from DDH + LPN.
- Main building block: SSP Co-PIR from DDH

Thanks!

A Framework for Statistically Sender Private OT with Optimal Rate

Pedro Branco *Max-Planck Institute for Security and Privacy*

Nico Döttling *Helmholtz Center for Information Security (CISPA)*

Akshayaram Srinivasan *Tata Institute of Fundamental Research*