Lower-Bounds on Public-Key Operations in PIR

Jesko Dujmovic, Mohammad Hajiabadi

CISPA Helmoltz Center for Information Security

University of Waterloo

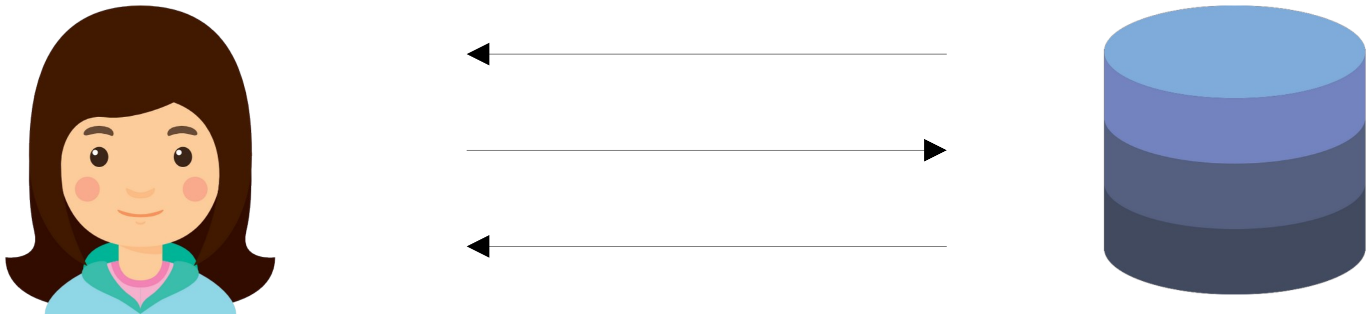
Funded by
the European Union

European Research Council
Established by the European Commission

(Non-Preprocessing, Single-Server, Non-Trivial) Private Information Retrieval

$i \in [n]$

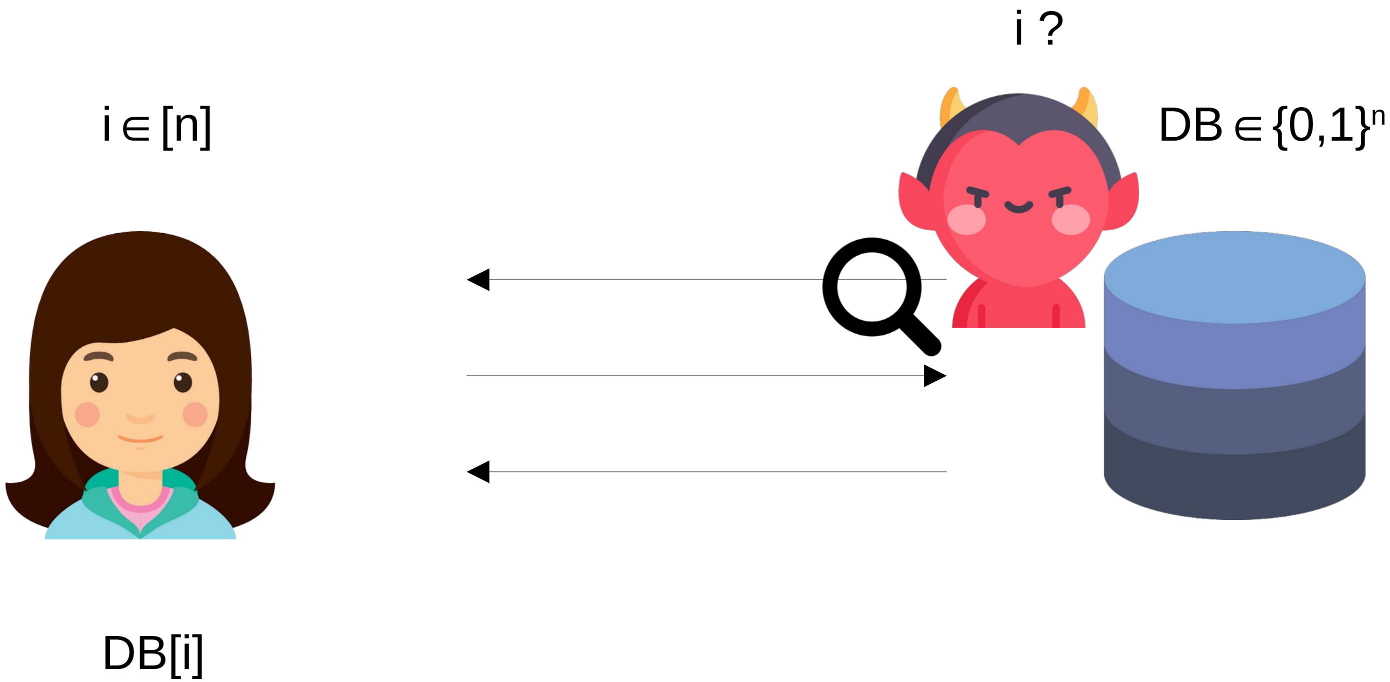
$DB \in \{0,1\}^n$



$DB[i]$

[CGKS95,KO97,DMO00]

(Non-Preprocessing, Single-Server, Non-Trivial) Private Information Retrieval



i ?

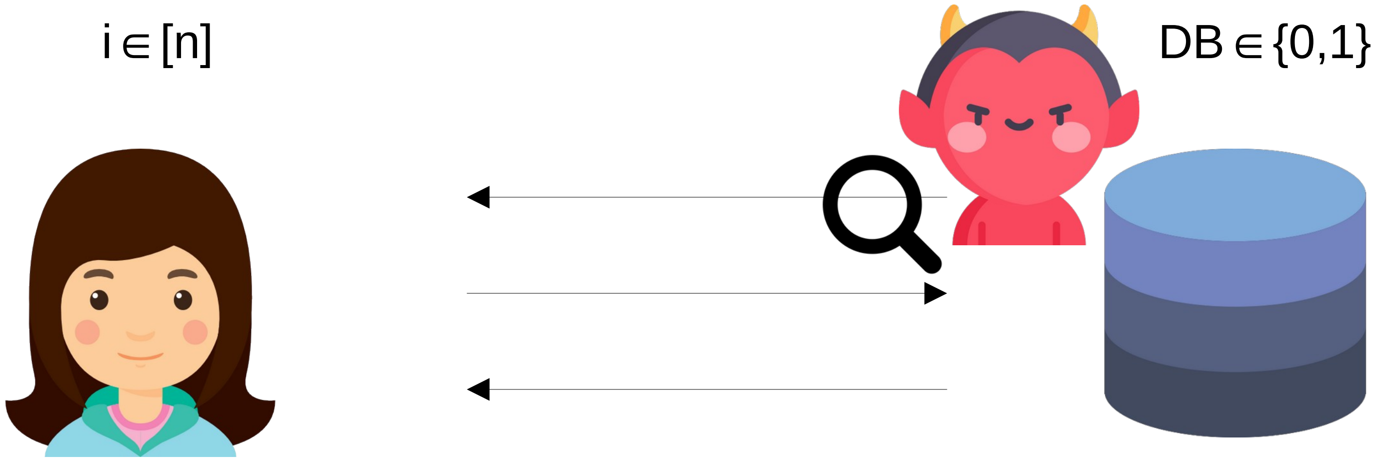
$i \in [n]$

$DB \in \{0,1\}^n$

DB[i]

[CGKS95,KO97,DMO00]

(Non-Preprocessing, Single-Server, Non-Trivial) Private Information Retrieval



i ?

$i \in [n]$

$DB \in \{0,1\}^n$

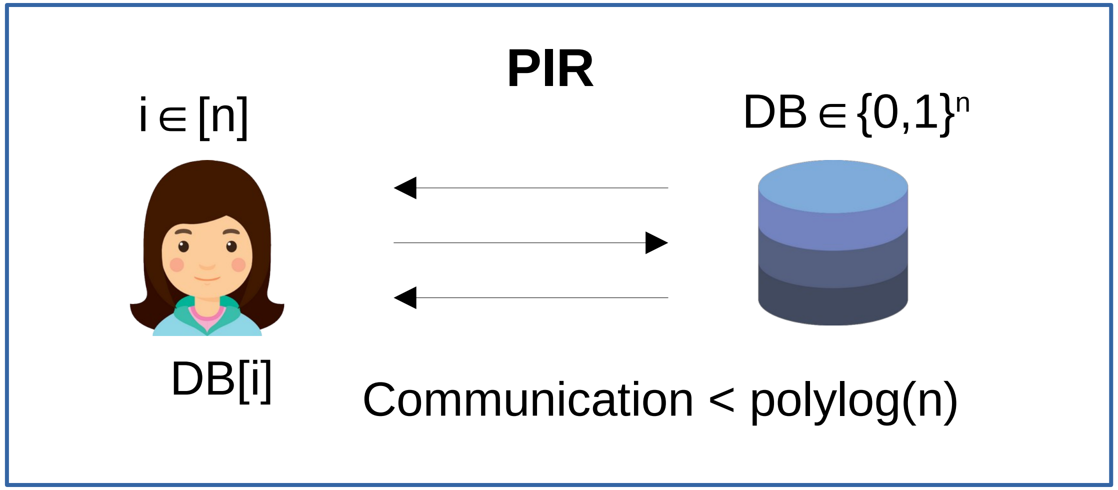
DB[i]

Communication < (1-ε)n

[CGKS95,KO97,DMO00]

Why Private Information Retrieval?

Why Private Information Retrieval?



PIR

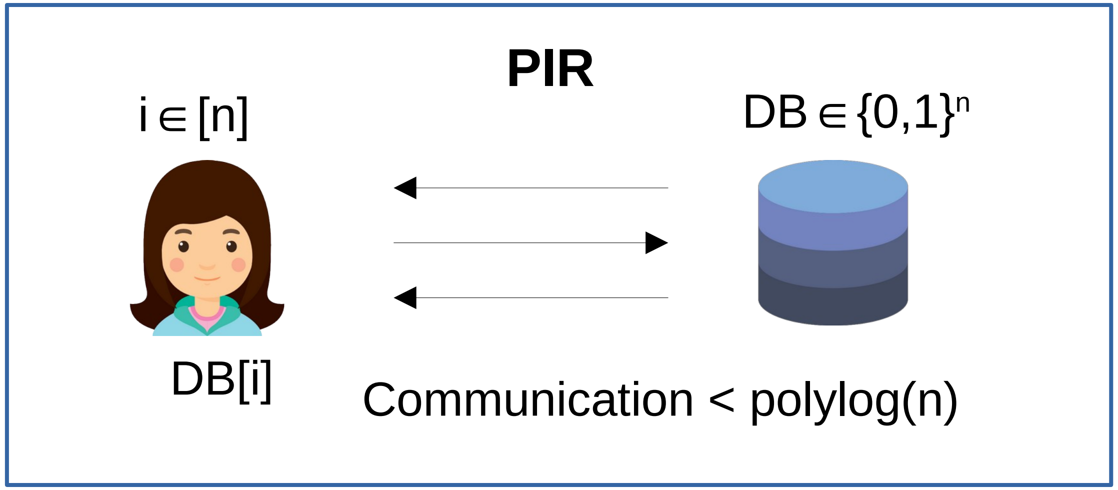
$i \in [n]$

$DB \in \{0,1\}^n$

DB[i]

Communication < polylog(n)

Why Private Information Retrieval?



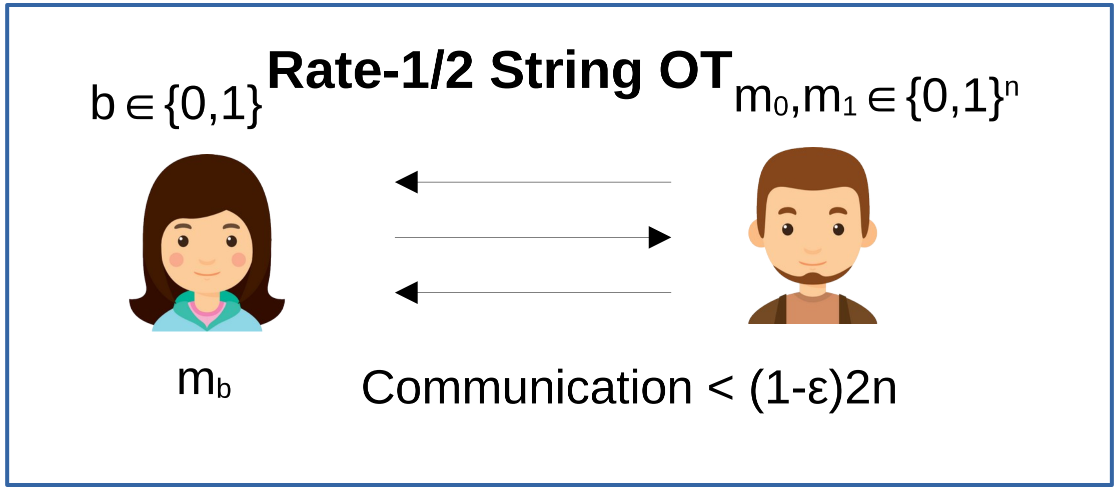
PIR

$i \in [n]$

$DB \in \{0,1\}^n$

$DB[i]$

Communication < polylog(n)



Rate-1/2 String OT

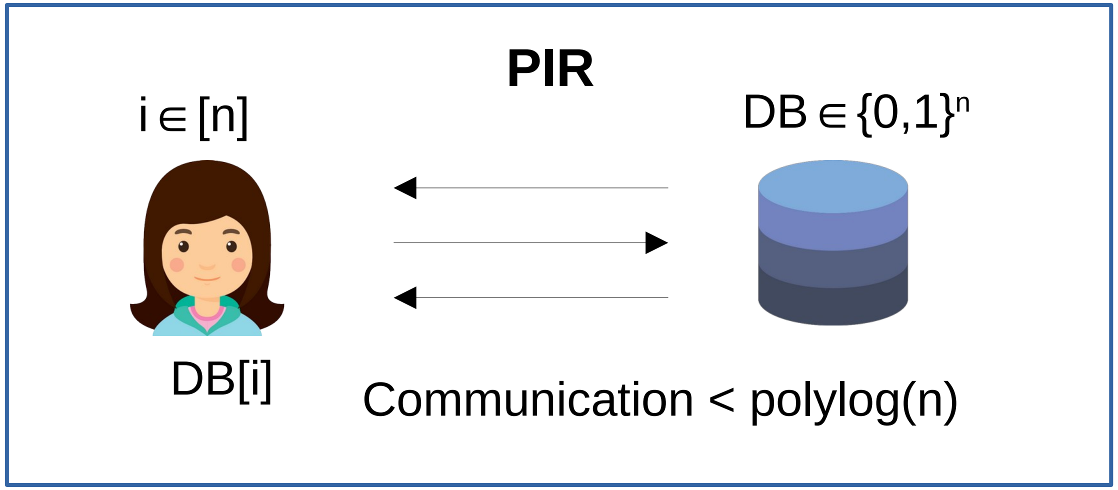
$b \in \{0,1\}$

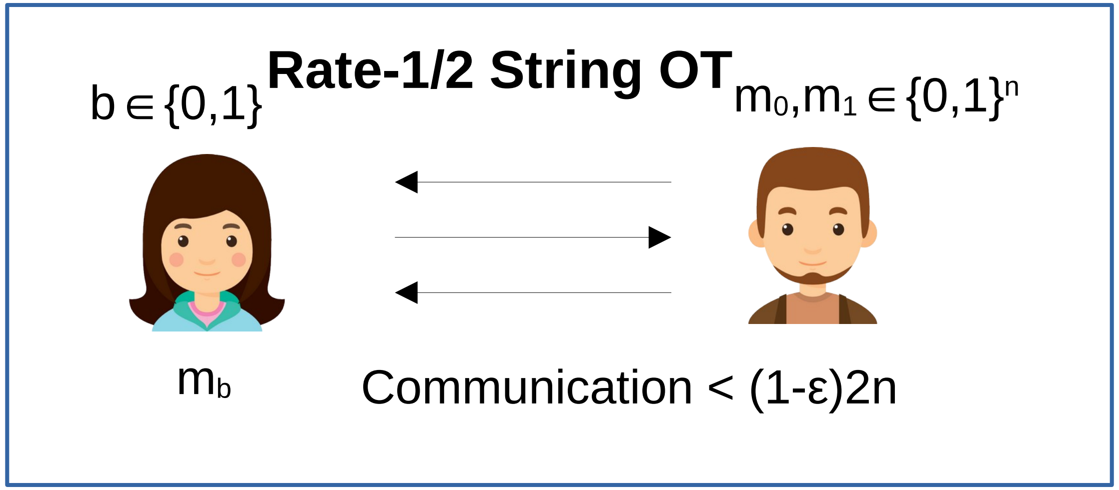
$m_0, m_1 \in \{0,1\}^n$

m_b

Communication < (1-ε)2n

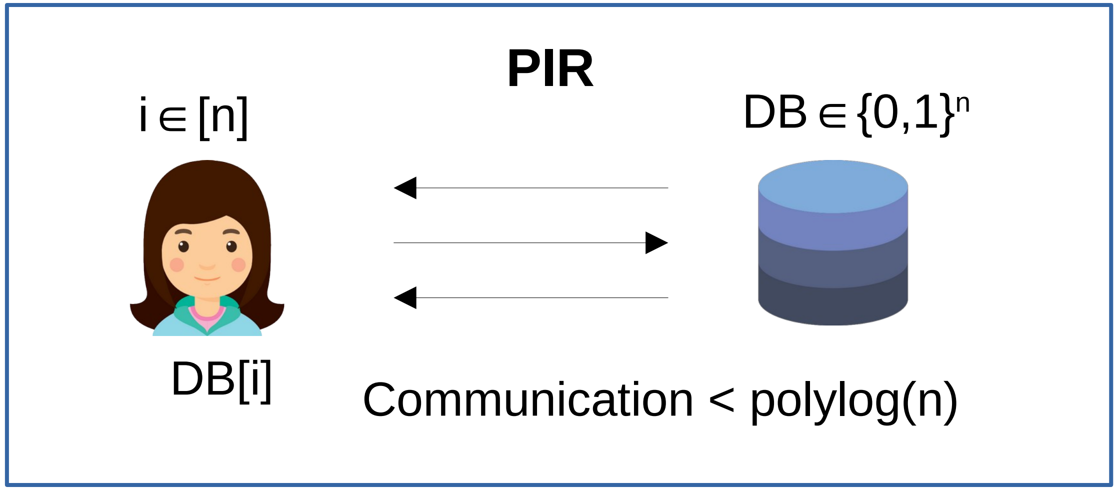
Why Private Information Retrieval?





- Non-trivial PIR ⇒ Oblivious Transfer [DMO00]

Why Private Information Retrieval?



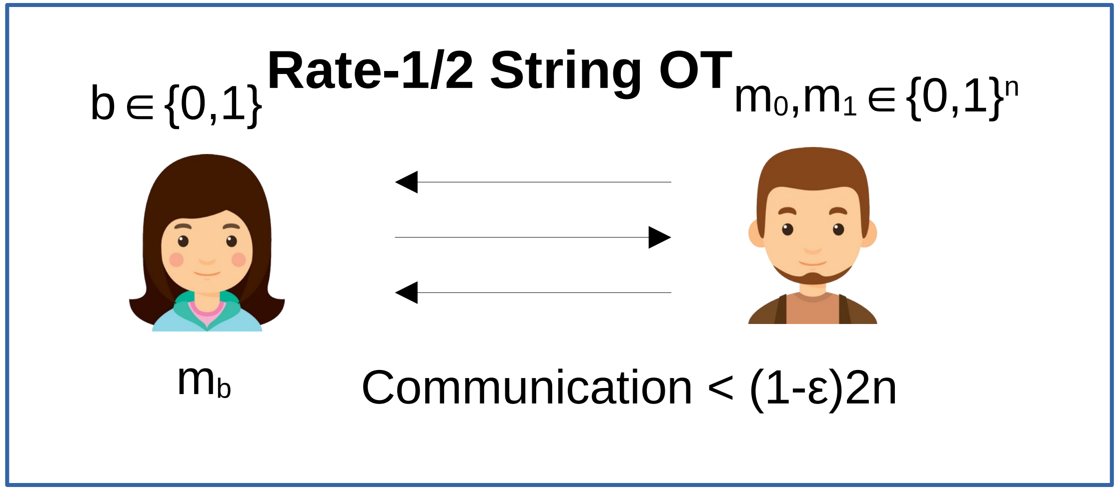
PIR

$i \in [n]$

$DB \in \{0,1\}^n$

$DB[i]$

Communication < polylog(n)



Rate-1/2 String OT

$b \in \{0,1\}$

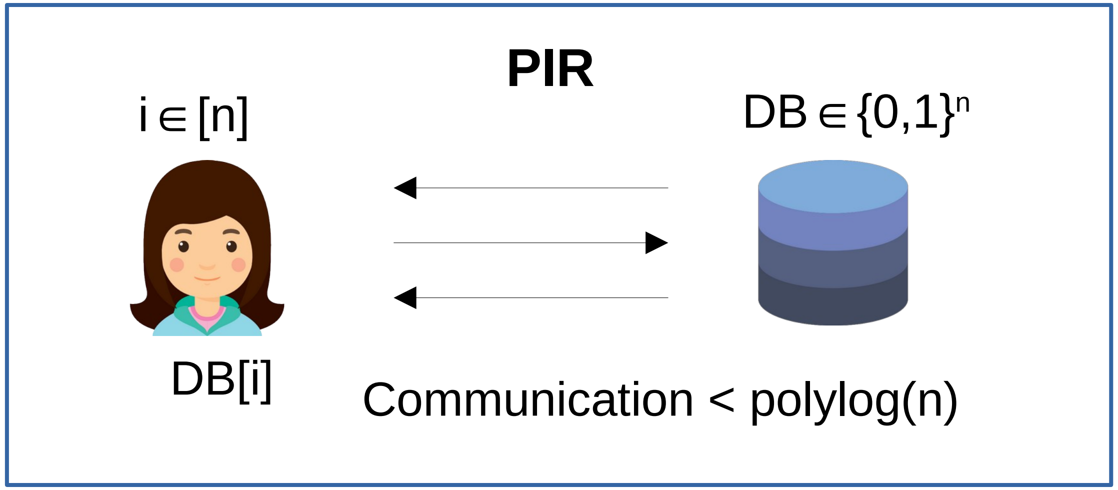
$m_0, m_1 \in \{0,1\}^n$

m_b

Communication < (1-ε)2n

- Non-trivial PIR ⇒ Oblivious Transfer [DMO00]
- Requires public-key operations [IR89,GKM+06]

Why Private Information Retrieval?



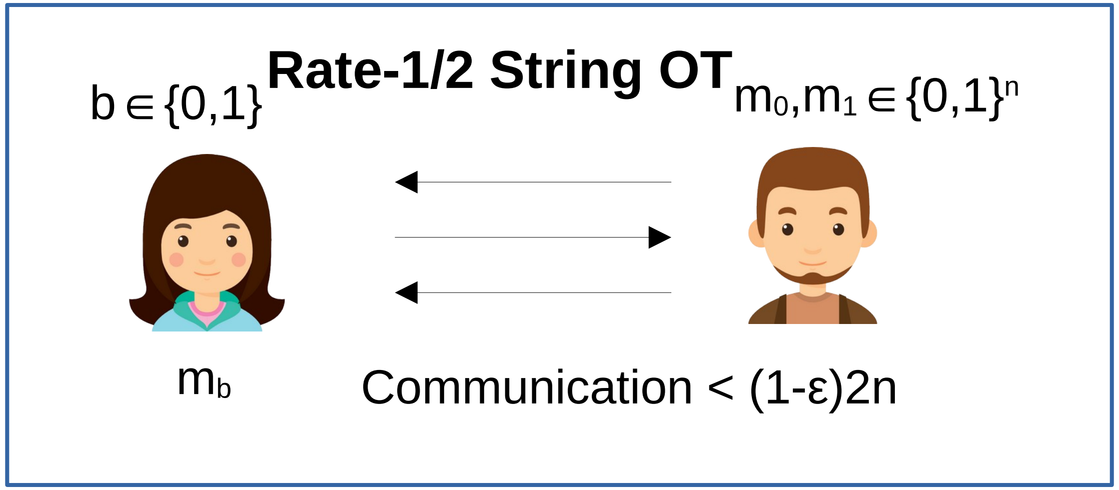
PIR

$i \in [n]$

$DB \in \{0,1\}^n$

DB[i]

Communication < polylog(n)



Rate-1/2 String OT

$b \in \{0,1\}$

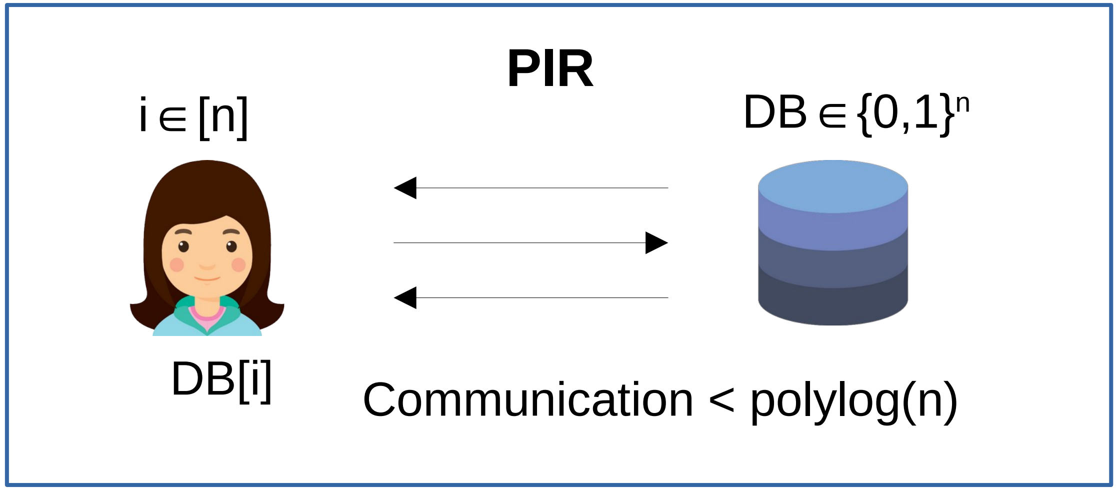
$m_0, m_1 \in \{0,1\}^n$

m_b

Communication < (1-ε)2n

- Non-trivial PIR ⇒ Oblivious Transfer [DMO00]
- Requires public-key operations [IR89,GKM+06]
- Requires $\Omega(n)$ server computation [BIM00]

Why Private Information Retrieval?



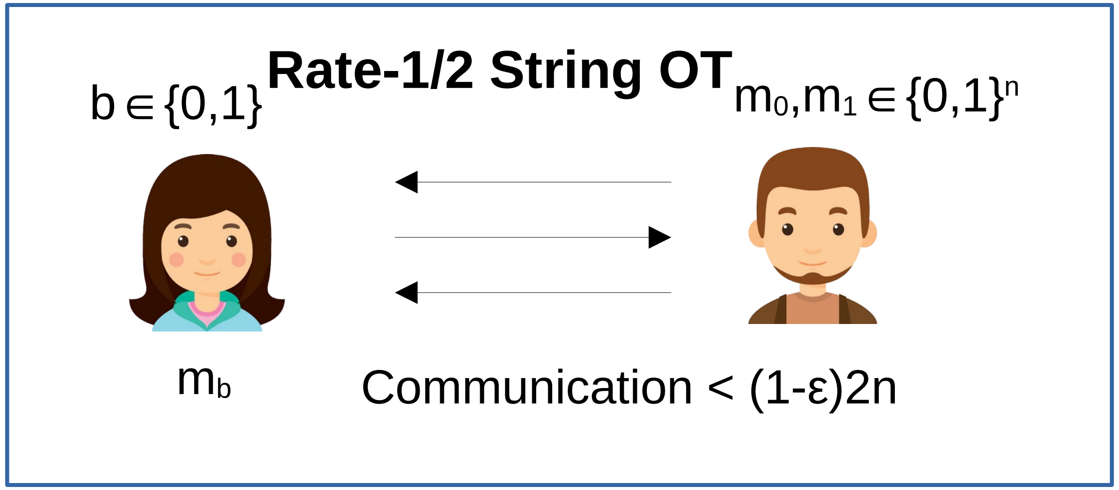
PIR

$i \in [n]$

$DB \in \{0,1\}^n$

$DB[i]$

Communication < polylog(n)



Rate-1/2 String OT

$b \in \{0,1\}$

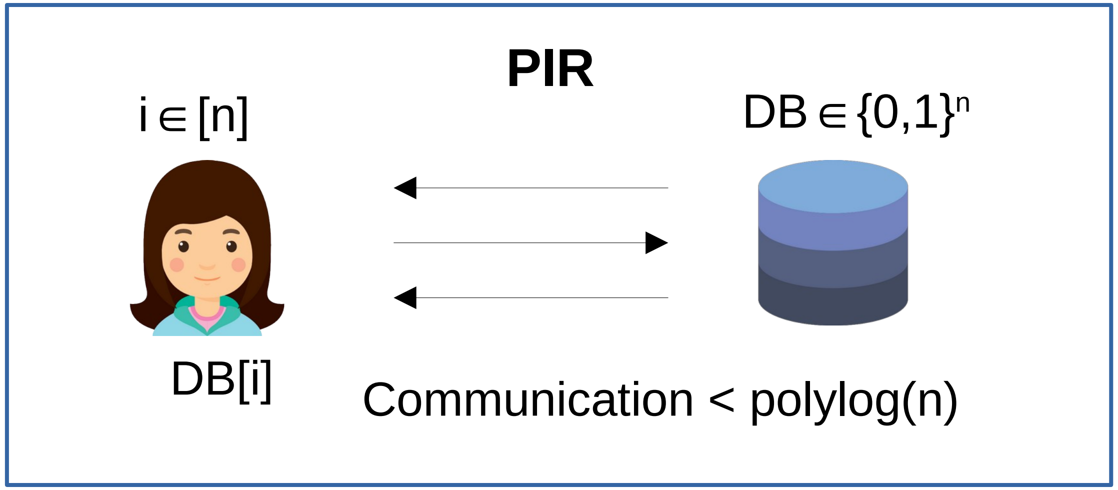
$m_0, m_1 \in \{0,1\}^n$

m_b

Communication < (1-ε)2n

- Non-trivial PIR ⇒ Oblivious Transfer [DMO00]
- Requires public-key operations [IR89,GKM+06]
- Requires Ω(n) server computation [BIM00]
- All known constructions Ω(n) public-key operations

Why Private Information Retrieval?



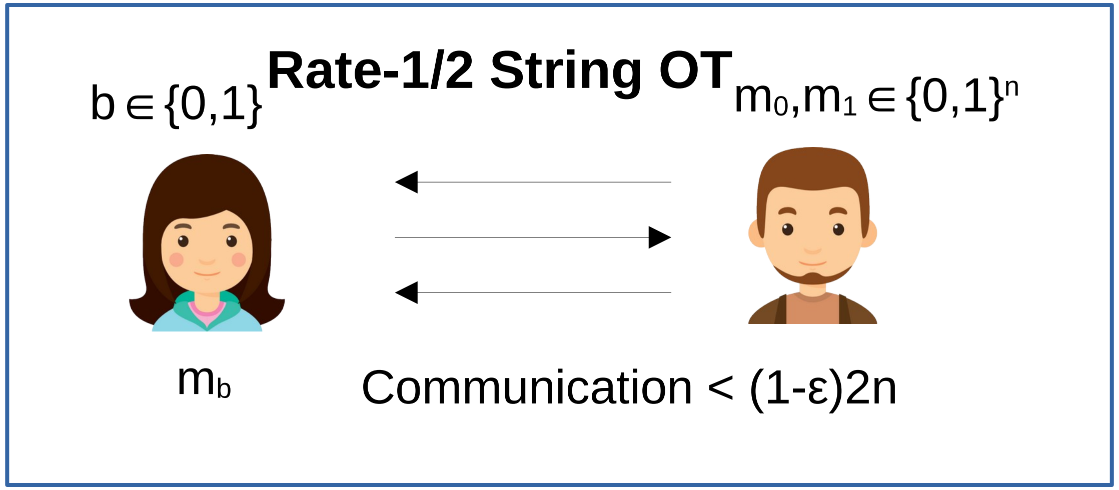
PIR

$i \in [n]$

$DB \in \{0,1\}^n$

DB[i]

Communication < polylog(n)



Rate-1/2 String OT

$b \in \{0,1\}$

$m_0, m_1 \in \{0,1\}^n$

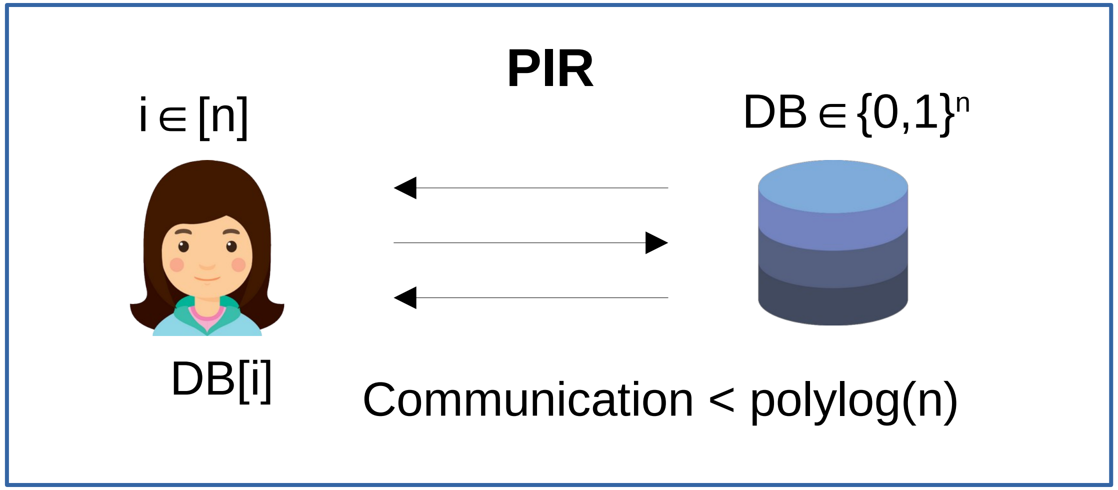
m_b

Communication < $(1-\varepsilon)2n$

- Non-trivial PIR ⇒ Oblivious Transfer [DMO00]
- Requires public-key operations [IR89,GKM+06]
- Requires $\Omega(n)$ server computation [BIM00]
- All known constructions $\Omega(n)$ public-key operations

Are $\Omega(n)$ public-key operations inherent?

Why Private Information Retrieval?



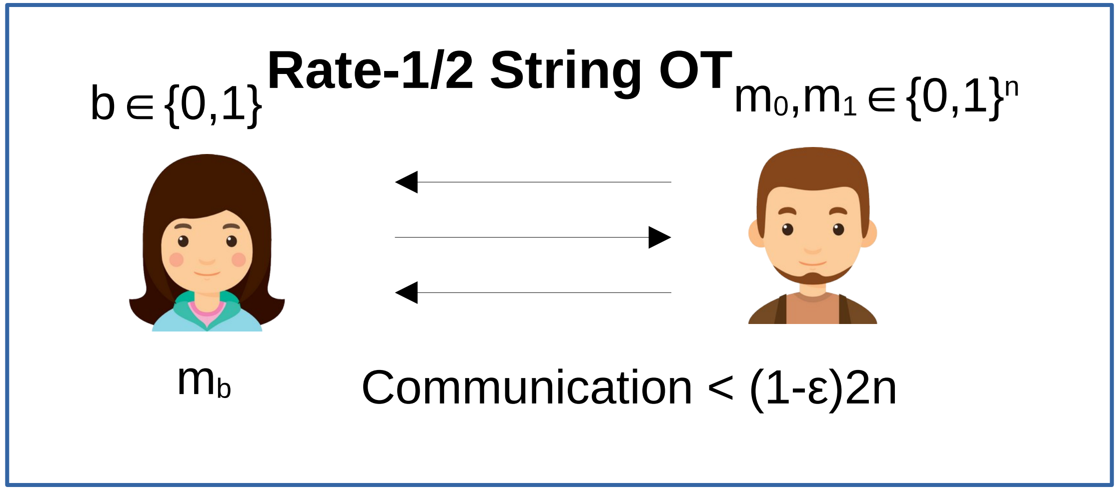
PIR

$i \in [n]$

$DB \in \{0,1\}^n$

DB[i]

Communication < polylog(n)



Rate-1/2 String OT

$b \in \{0,1\}$

$m_0, m_1 \in \{0,1\}^n$

m_b

Communication < $(1-\varepsilon)2n$

- Non-trivial PIR ⇒ Oblivious Transfer [DMO00]
- Requires public-key operations [IR89,GKM+06]
- Requires Ω(n) server computation [BIM00]
- All known constructions Ω(n) public-key operations

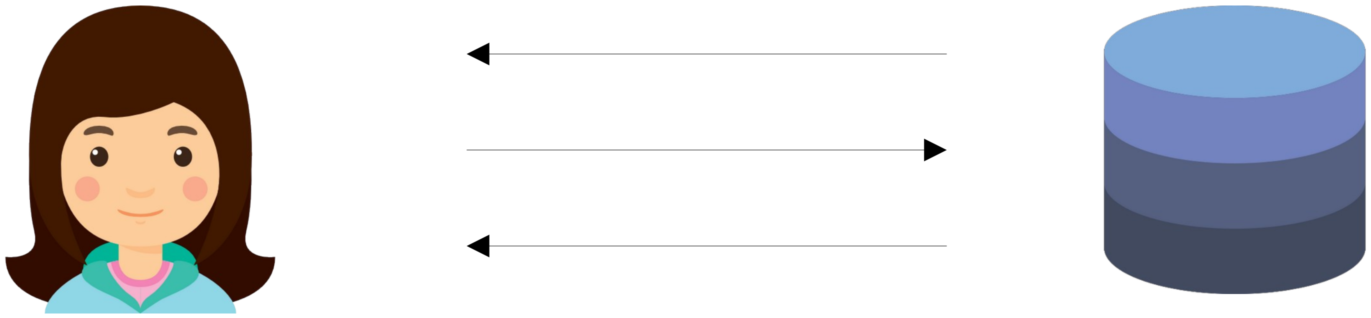
Are Ω(n) public-key operations inherent?

Yes!

PIR in the Generic Group Model

$i \in [n]$

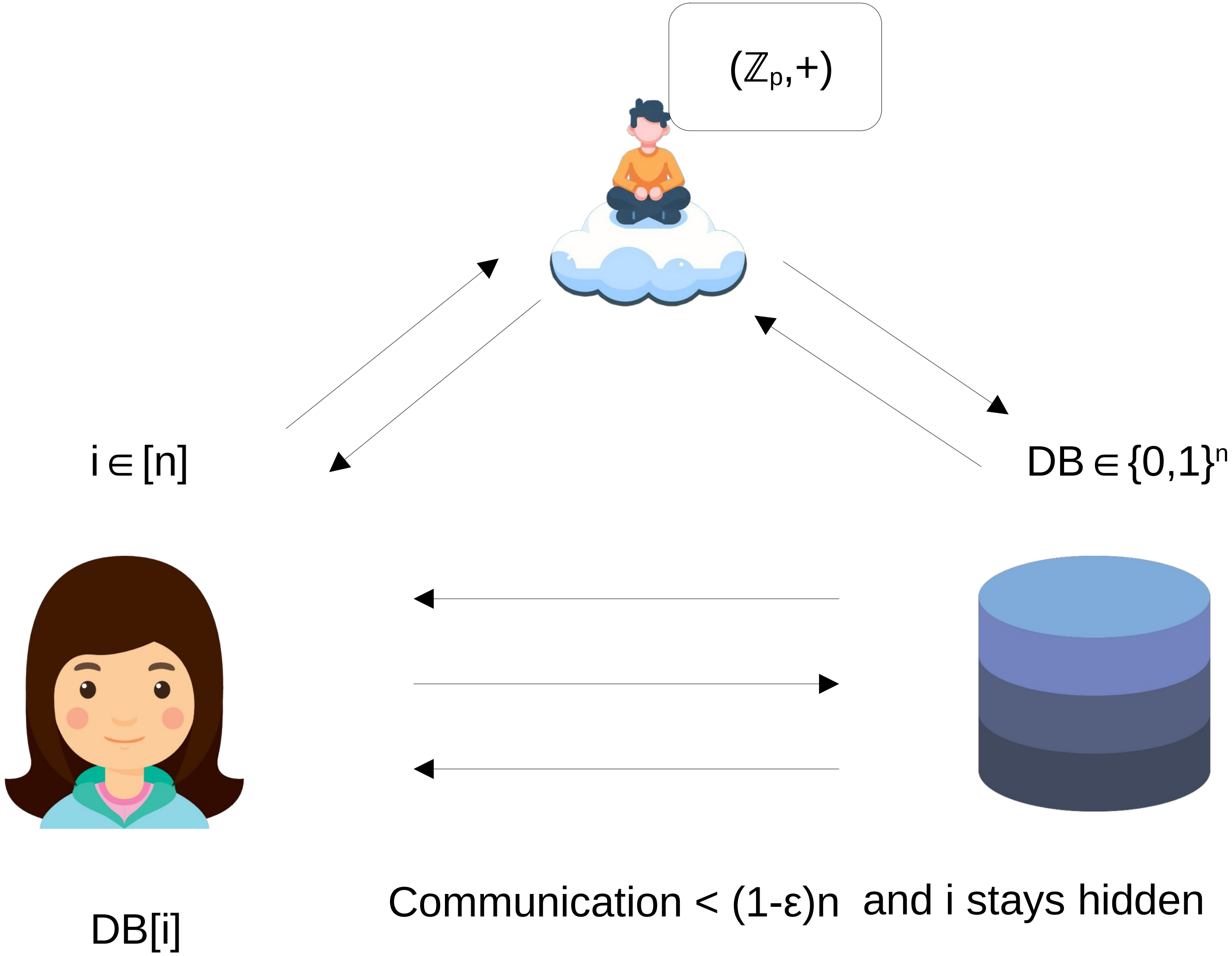
$DB \in \{0,1\}^n$



Communication < $(1-\varepsilon)n$ and i stays hidden

$DB[i]$

PIR in the Generic Group Model



$(\mathbb{Z}_p, +)$

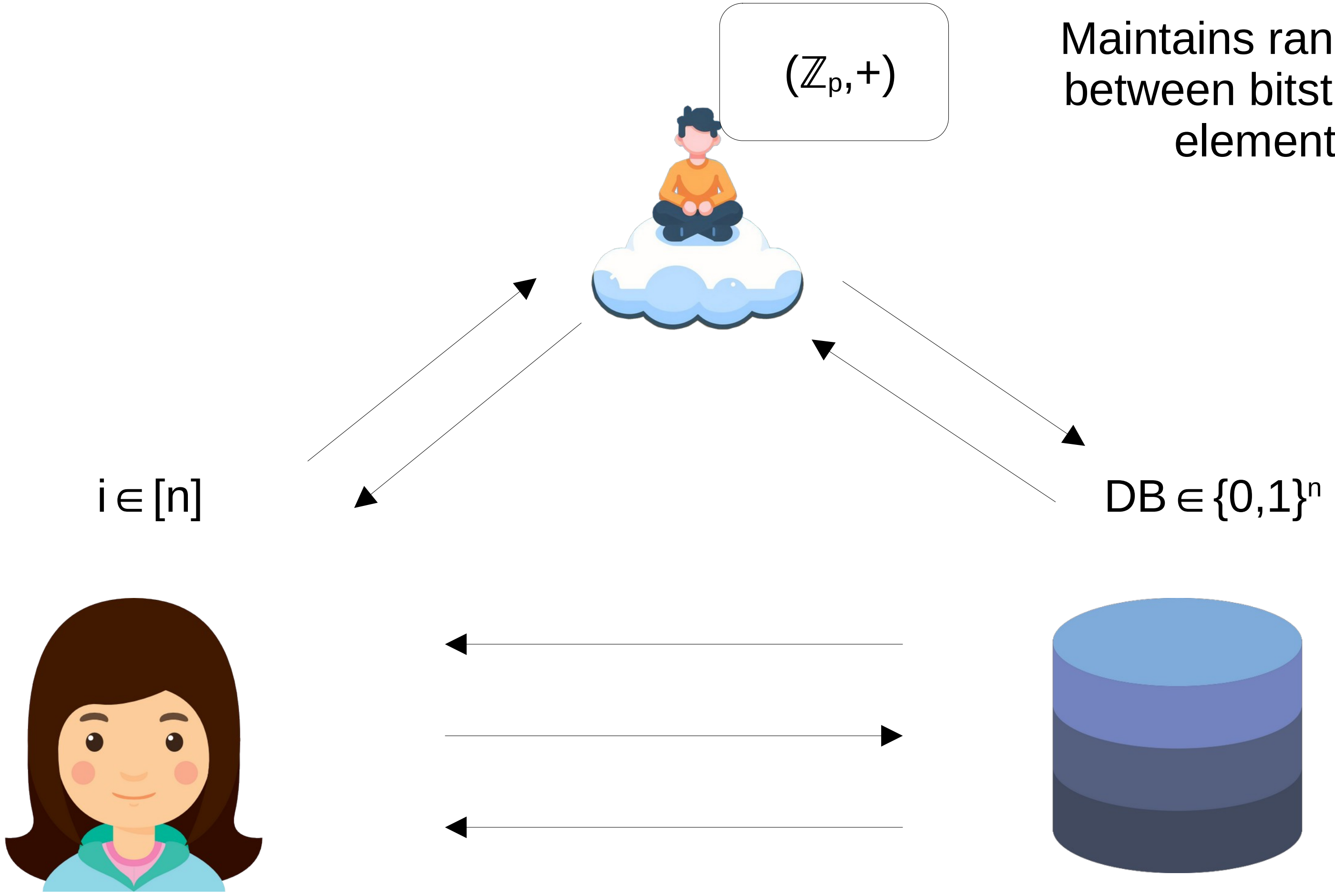
$i \in [n]$

$DB \in \{0,1\}^n$

$DB[i]$

Communication < $(1-\varepsilon)n$ and i stays hidden

PIR in the Generic Group Model



$(\mathbb{Z}_p,+)$

Maintains random map between bitstrings and elements of

$i \in [n]$

$DB \in \{0,1\}^n$

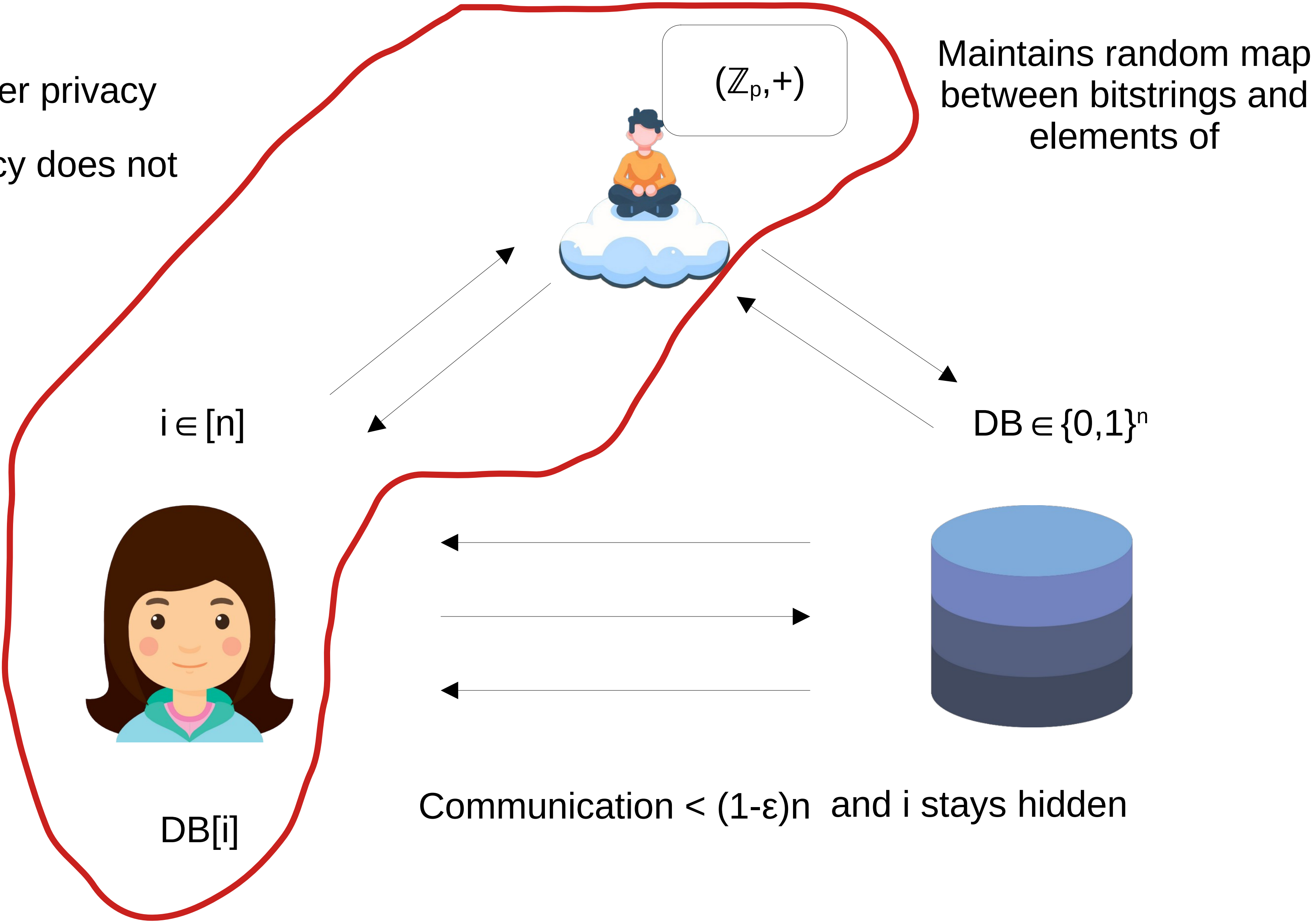
DB[i]

Communication < $(1-\varepsilon)n$ and i stays hidden

PIR in the Generic Group Model

Maintains user privacy

Server privacy does not exist

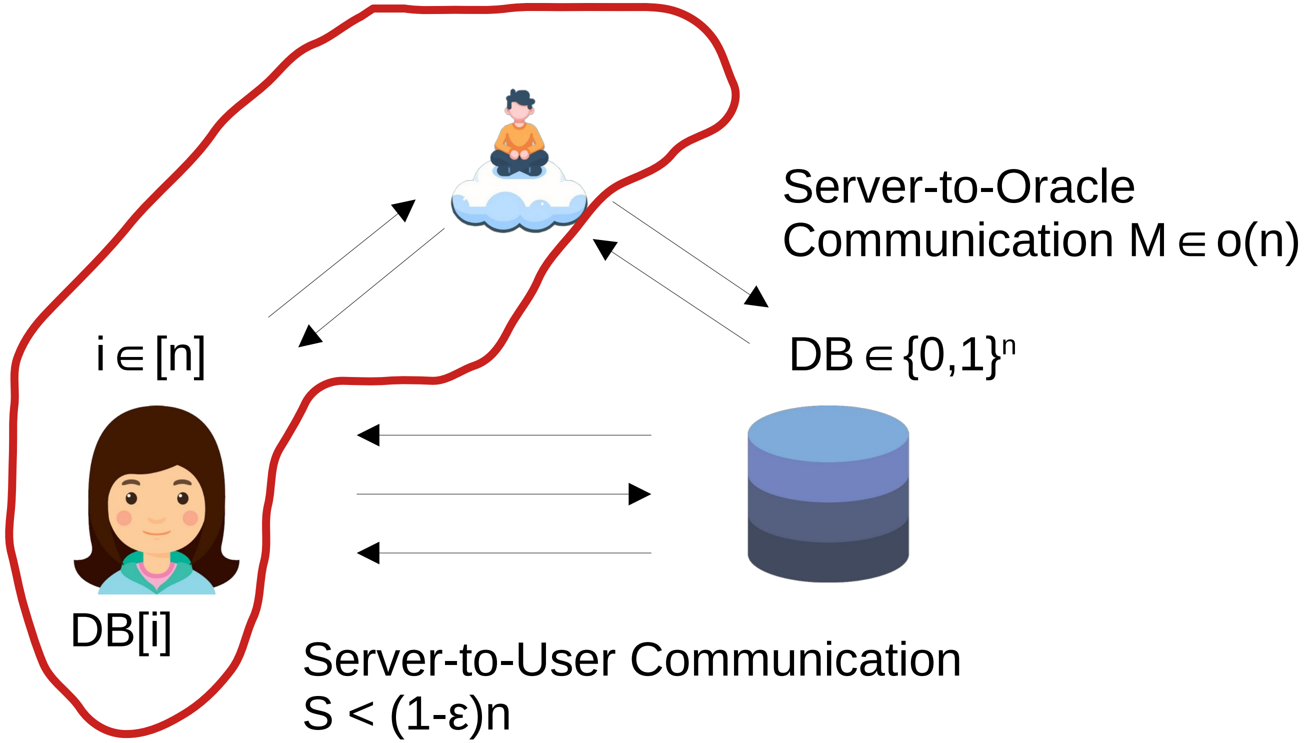


$(\mathbb{Z}_p,+)$

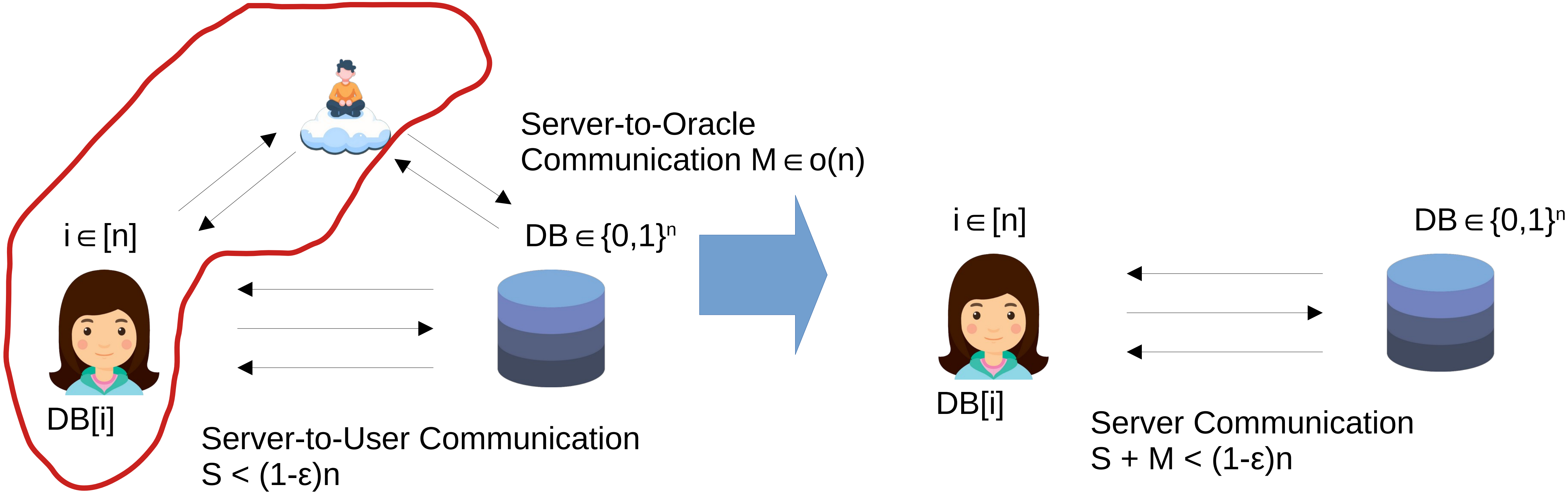
Maintains random map between bitstrings and elements of

Communication < $(1-\varepsilon)n$ and i stays hidden

PIR in the Generic Group Model



PIR in the Generic Group Model



Server-to-Oracle

Communication $M \in o(n)$

$i \in [n]$

$DB \in \{0,1\}^n$

DB[i]

Server-to-User Communication

$S < (1-\varepsilon)n$

$i \in [n]$

$DB \in \{0,1\}^n$

DB[i]

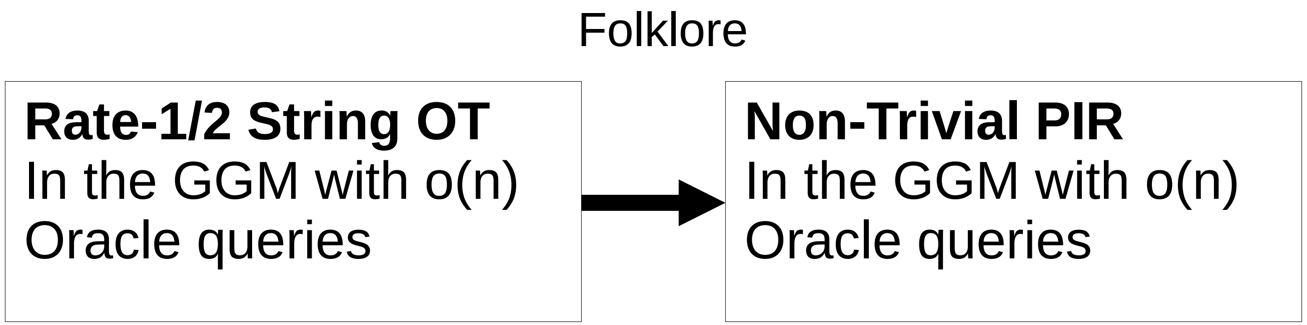
Server Communication

$S + M < (1-\varepsilon)n$

Consequences

Rate-1/2 String OT
In the GGM with o(n)
Oracle queries

Consequences

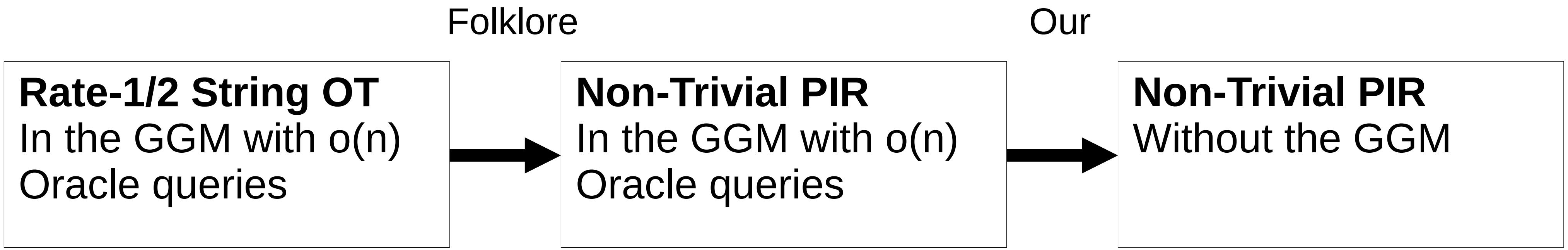


Folklore

Rate-1/2 String OT
In the GGM with o(n)
Oracle queries

Non-Trivial PIR
In the GGM with o(n)
Oracle queries

Consequences



Folklore

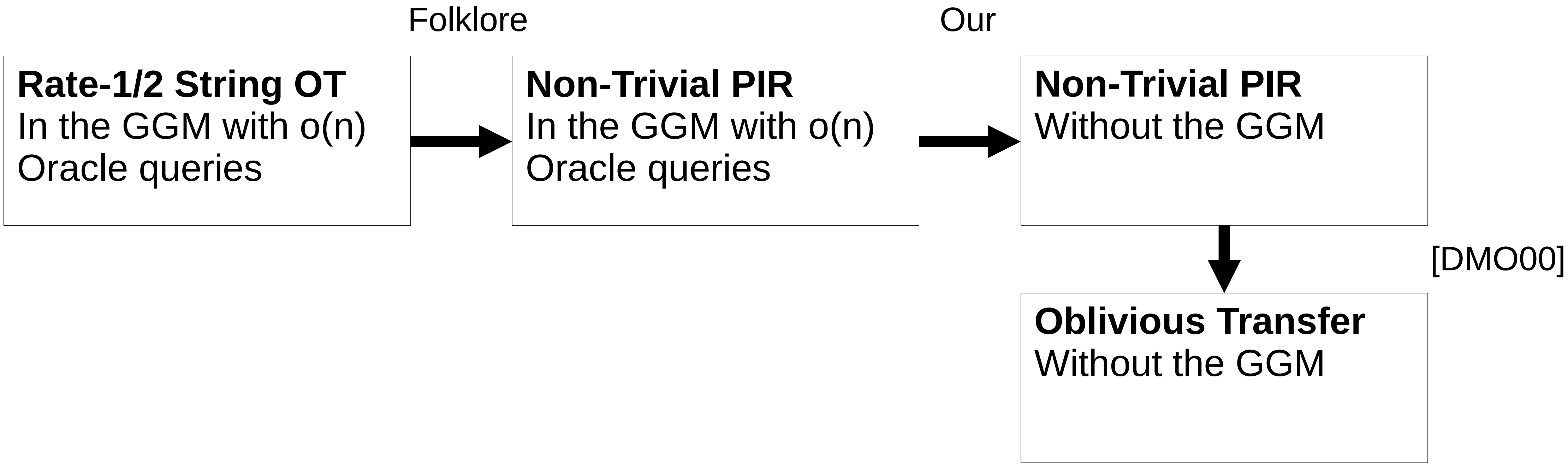
Our

Rate-1/2 String OT
In the GGM with o(n) Oracle queries

Non-Trivial PIR
In the GGM with o(n) Oracle queries

Non-Trivial PIR
Without the GGM

Consequences



Folklore

Our

[DMO00]

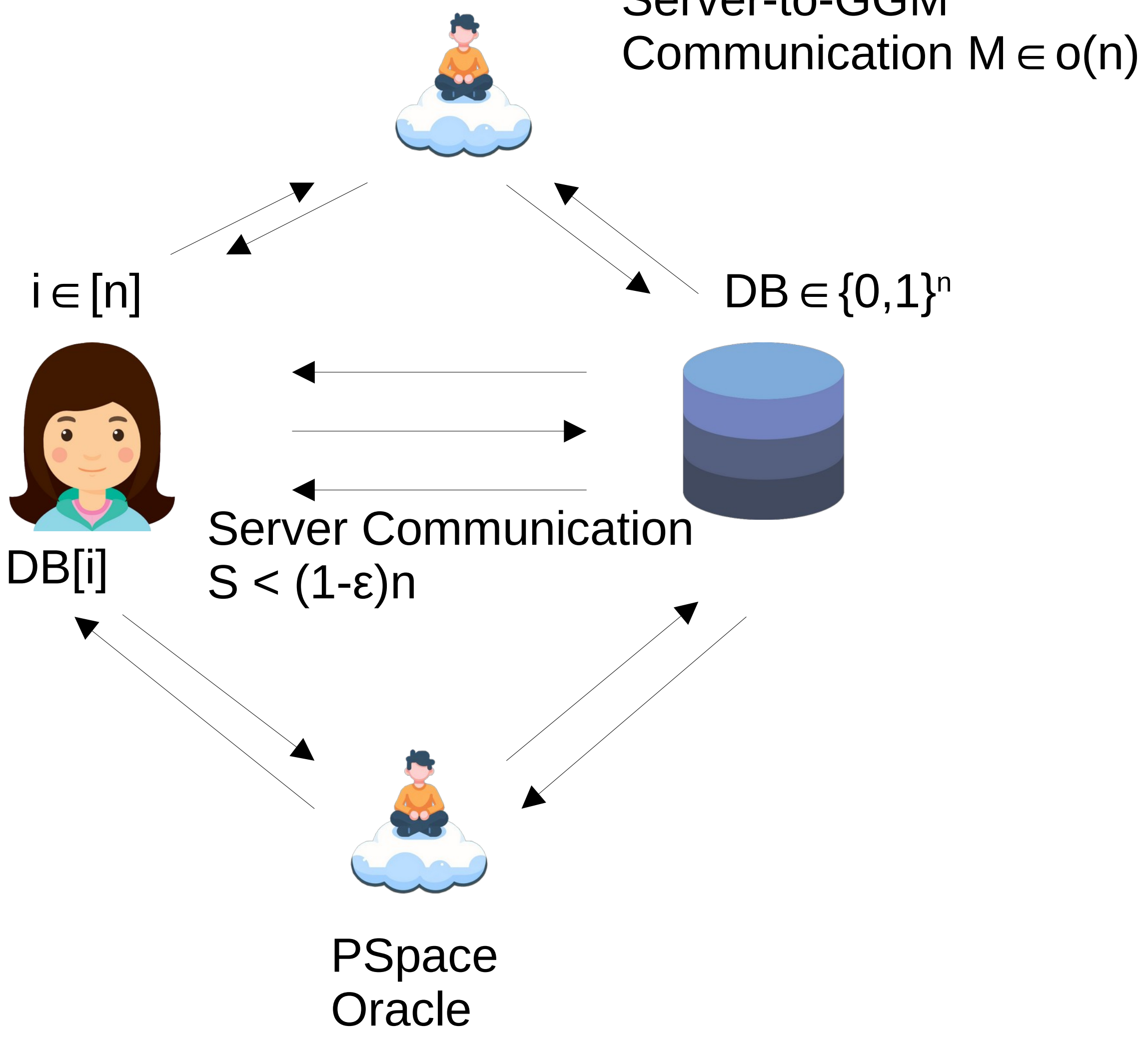
Rate-1/2 String OT
In the GGM with o(n)
Oracle queries

Non-Trivial PIR
In the GGM with o(n)
Oracle queries

Non-Trivial PIR
Without the GGM

Oblivious Transfer
Without the GGM

PIR in the GGM + PSpace



Server-to-GGM
Communication $M \in o(n)$

$i \in [n]$

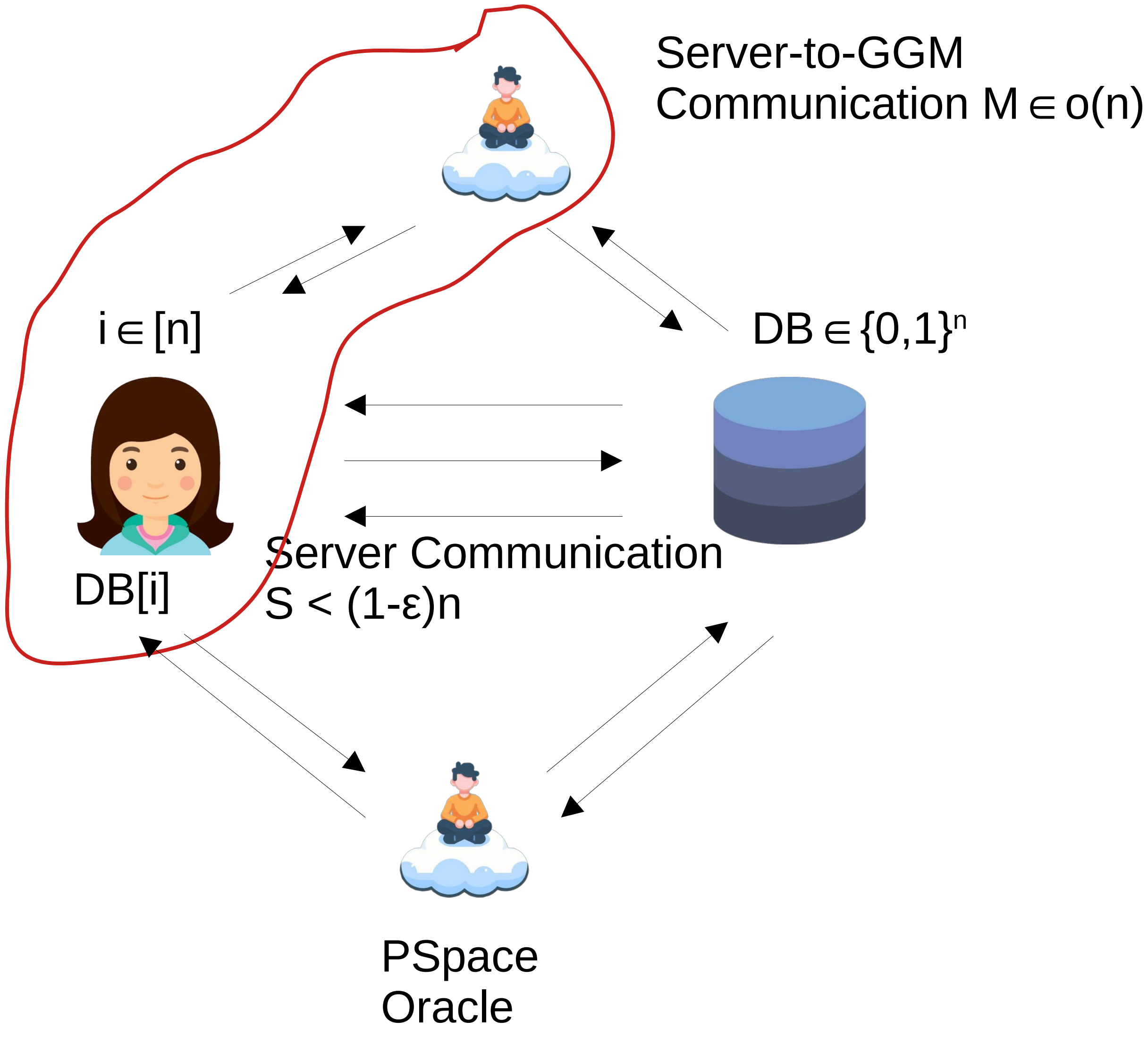
$DB \in \{0,1\}^n$

DB[i]

Server Communication
$S < (1\text{-}\varepsilon)n$

PSpace
Oracle

PIR in the GGM + PSpace



Server-to-GGM
Communication $M \in o(n)$

$i \in [n]$

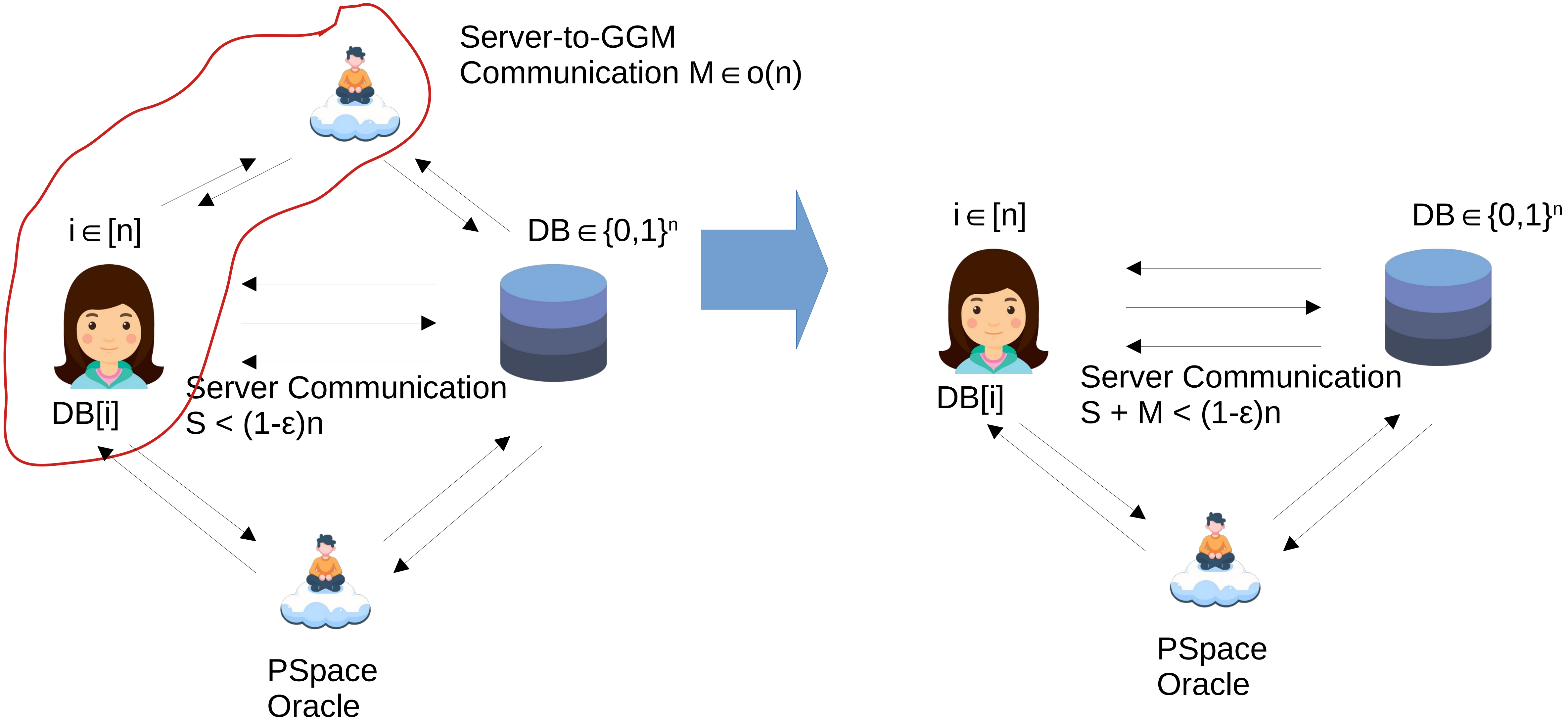
$DB \in \{0,1\}^n$

DB[i]

Server Communication
$S < (1\text{-}\varepsilon)n$

PSpace
Oracle

PIR in the GGM + PSpace



Server-to-GGM Communication $M \in o(n)$

$i \in [n]$

$\mathrm{DB} \in \{0,1\}^n$

DB[i]

Server Communication $S < (1\text{-}\varepsilon)n$

PSpace Oracle

$i \in [n]$

$\mathrm{DB} \in \{0,1\}^n$

DB[i]

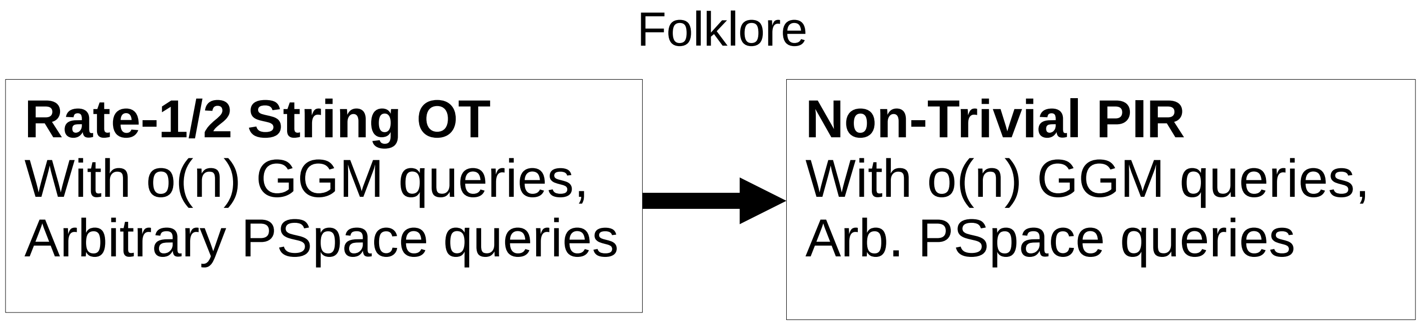
Server Communication $S + M < (1\text{-}\varepsilon)n$

PSpace Oracle

Consequences cont.

Rate-1/2 String OT
With o(n) GGM queries,
Arbitrary PSpace queries

Consequences cont.

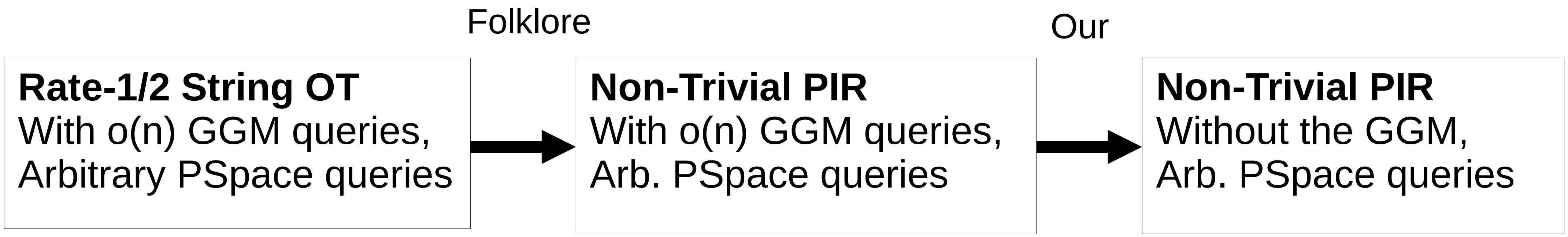


Folklore

Rate-1/2 String OT
With o(n) GGM queries,
Arbitrary PSpace queries

Non-Trivial PIR
With o(n) GGM queries,
Arb. PSpace queries

Consequences cont.



Folklore

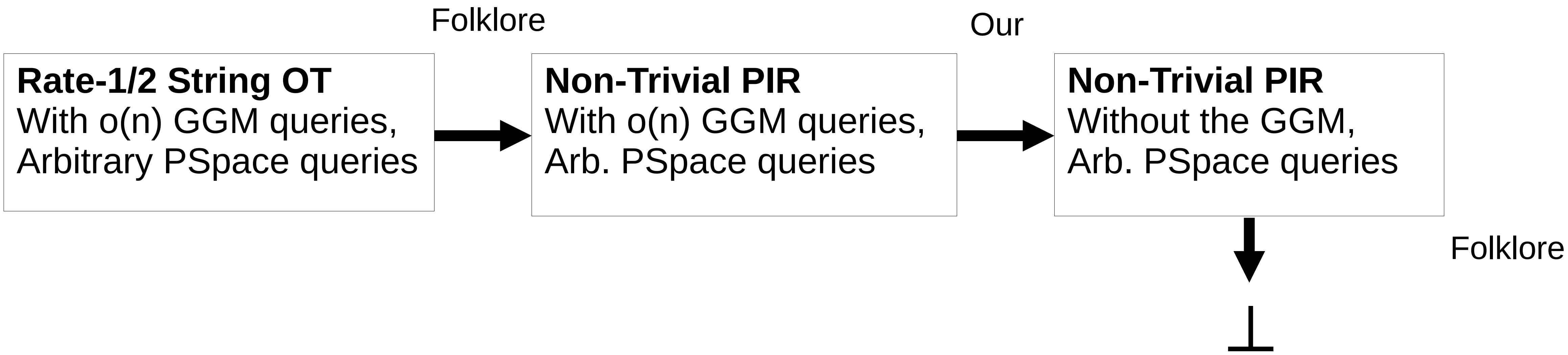
Our

Rate-1/2 String OT
With o(n) GGM queries,
Arbitrary PSpace queries

Non-Trivial PIR
With o(n) GGM queries,
Arb. PSpace queries

Non-Trivial PIR
Without the GGM,
Arb. PSpace queries

Consequences cont.



Folklore

Rate-1/2 String OT
With o(n) GGM queries,
Arbitrary PSpace queries

Our

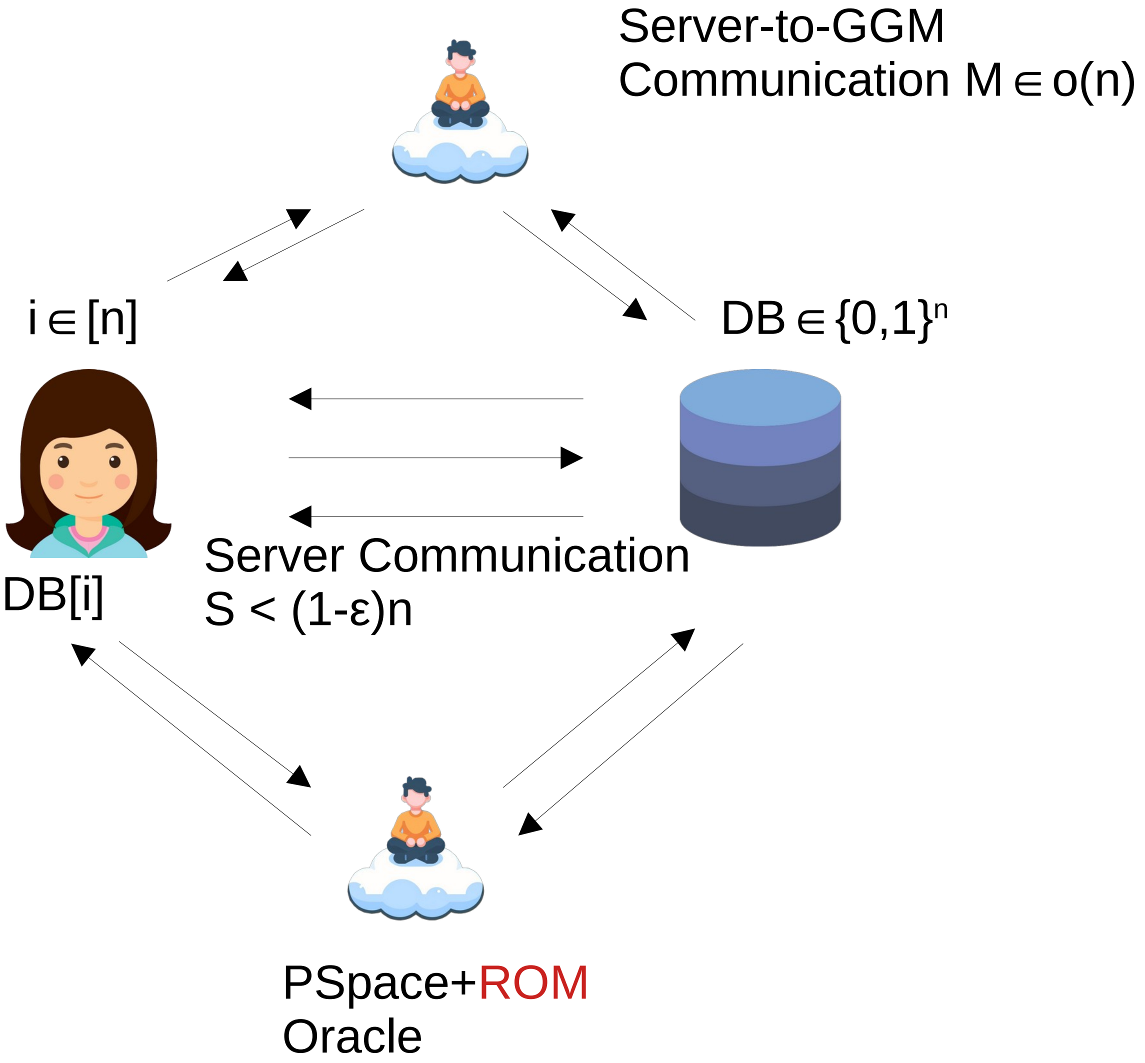
Non-Trivial PIR
With o(n) GGM queries,
Arb. PSpace queries

Non-Trivial PIR
Without the GGM,
Arb. PSpace queries

Folklore

$\perp$

PIR in the GGM + PSpace + ROM



Server-to-GGM
Communication $M \in o(n)$

$i \in [n]$

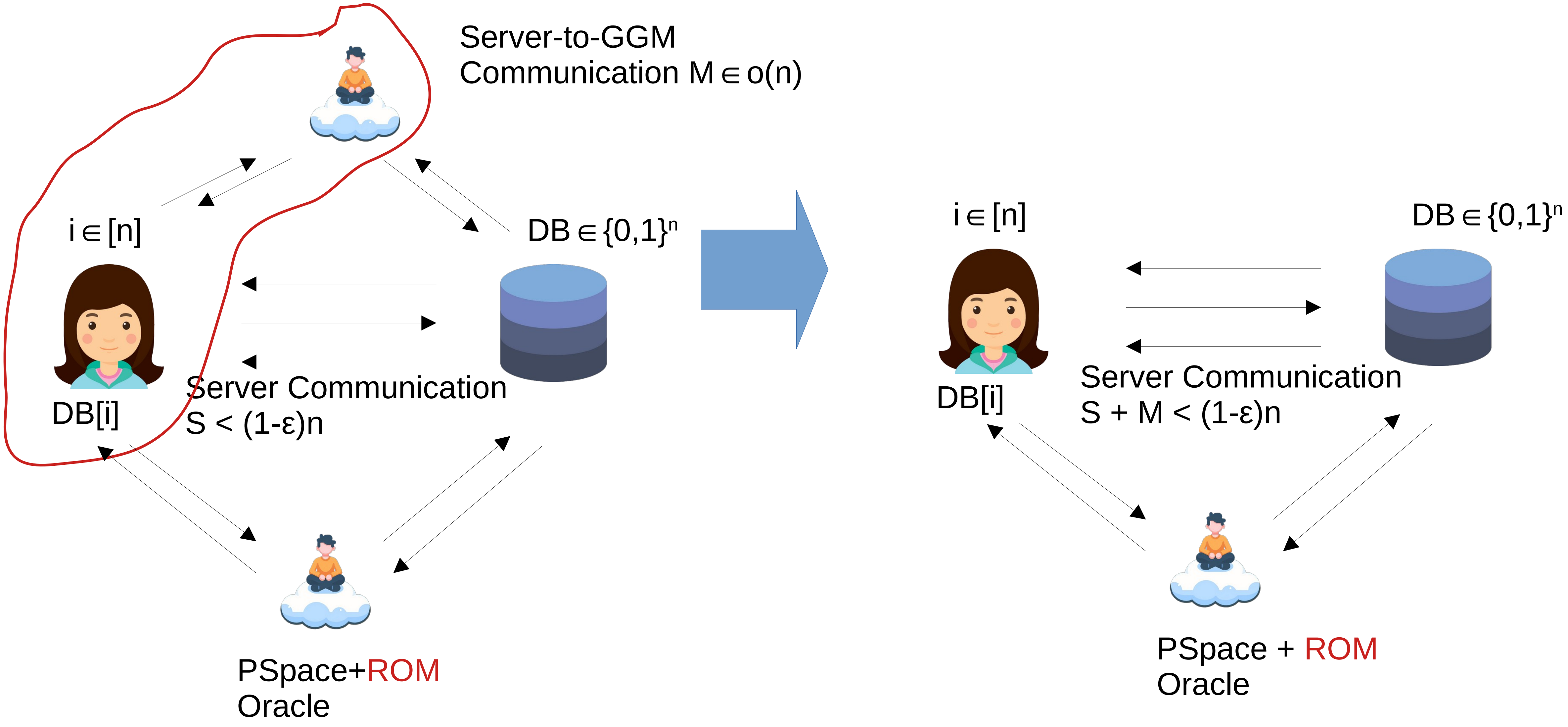
$DB \in \{0,1\}^n$

Server Communication
$S < (1-\varepsilon)n$

DB[i]

PSpace+ROM
Oracle

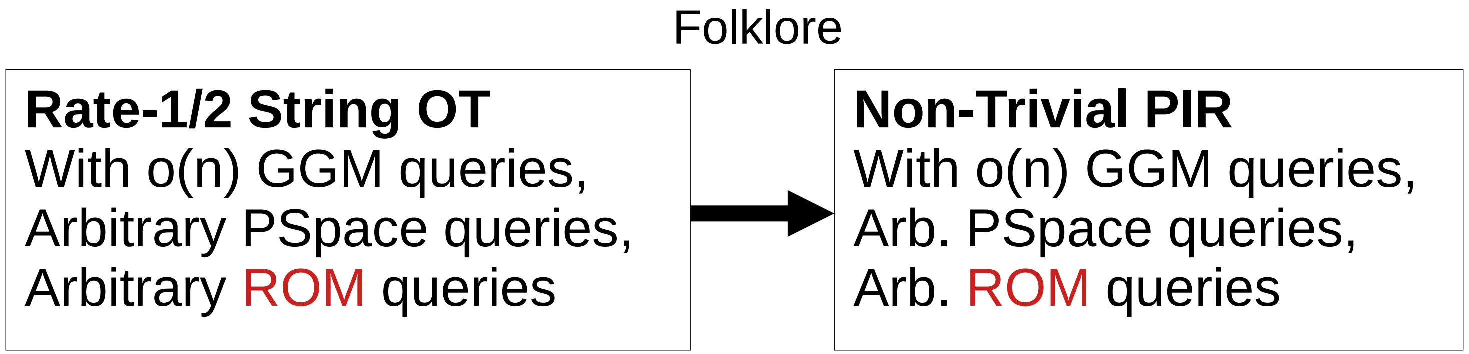
PIR in the GGM + PSpace + ROM



Consequences cont. (2)

Rate-1/2 String OT
With o(n) GGM queries,
Arbitrary PSpace queries,
Arbitrary ROM queries

Consequences cont. (2)

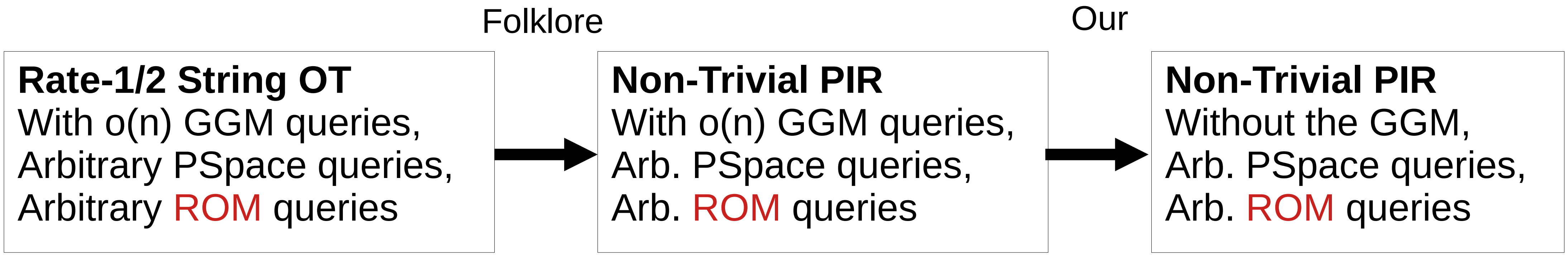


Folklore

Rate-1/2 String OT
With o(n) GGM queries,
Arbitrary PSpace queries,
Arbitrary ROM queries

Non-Trivial PIR
With o(n) GGM queries,
Arb. PSpace queries,
Arb. ROM queries

Consequences cont. (2)



Folklore

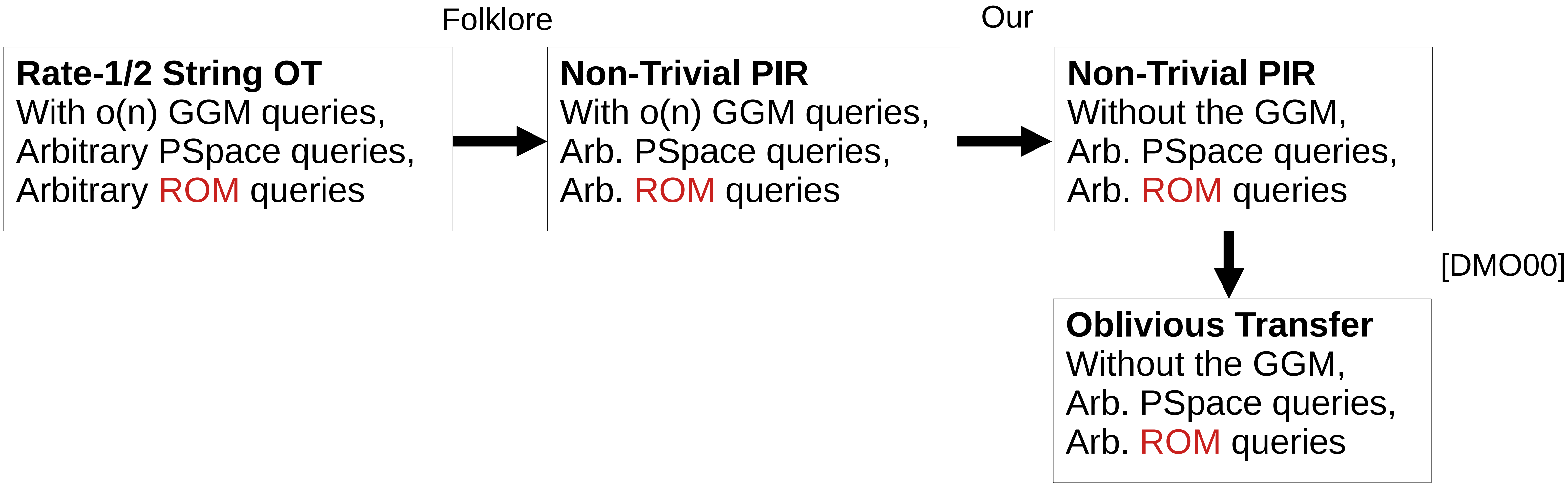
Our

Rate-1/2 String OT
With o(n) GGM queries,
Arbitrary PSpace queries,
Arbitrary ROM queries

Non-Trivial PIR
With o(n) GGM queries,
Arb. PSpace queries,
Arb. ROM queries

Non-Trivial PIR
Without the GGM,
Arb. PSpace queries,
Arb. ROM queries

Consequences cont. (2)



Folklore

Our

[DMO00]

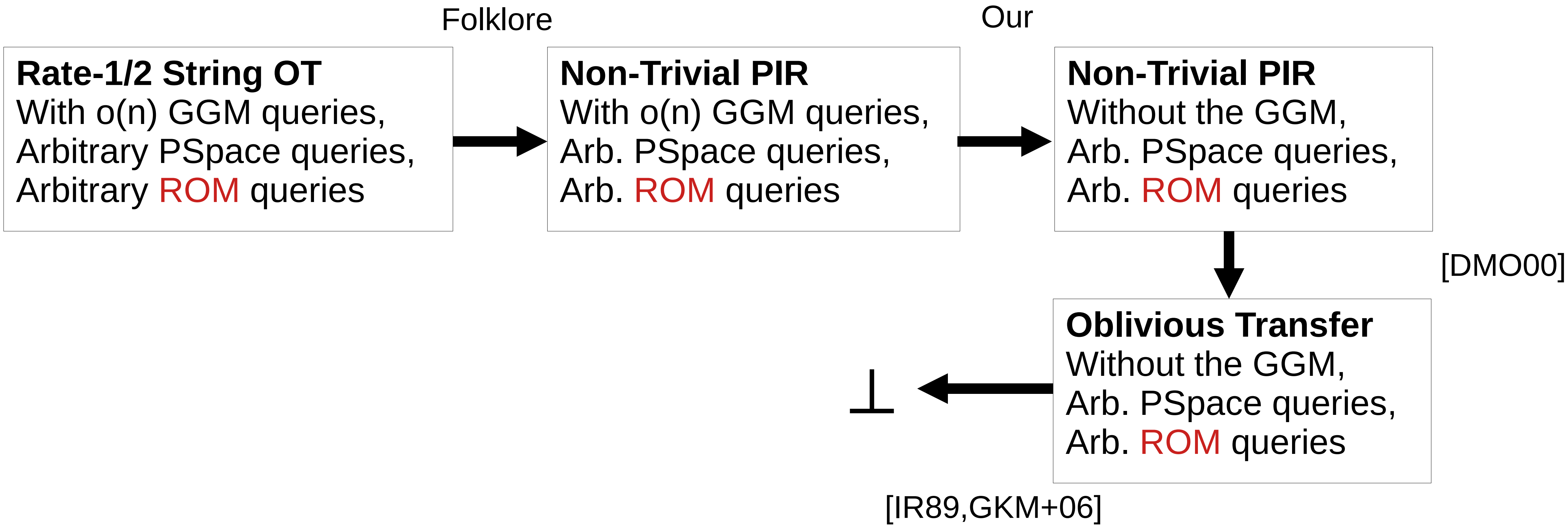
Rate-1/2 String OT
With o(n) GGM queries,
Arbitrary PSpace queries,
Arbitrary ROM queries

Non-Trivial PIR
With o(n) GGM queries,
Arb. PSpace queries,
Arb. ROM queries

Non-Trivial PIR
Without the GGM,
Arb. PSpace queries,
Arb. ROM queries

Oblivious Transfer
Without the GGM,
Arb. PSpace queries,
Arb. ROM queries

Consequences cont. (2)



Folklore

Our

Rate-1/2 String OT
With o(n) GGM queries,
Arbitrary PSpace queries,
Arbitrary ROM queries

Non-Trivial PIR
With o(n) GGM queries,
Arb. PSpace queries,
Arb. ROM queries

Non-Trivial PIR
Without the GGM,
Arb. PSpace queries,
Arb. ROM queries

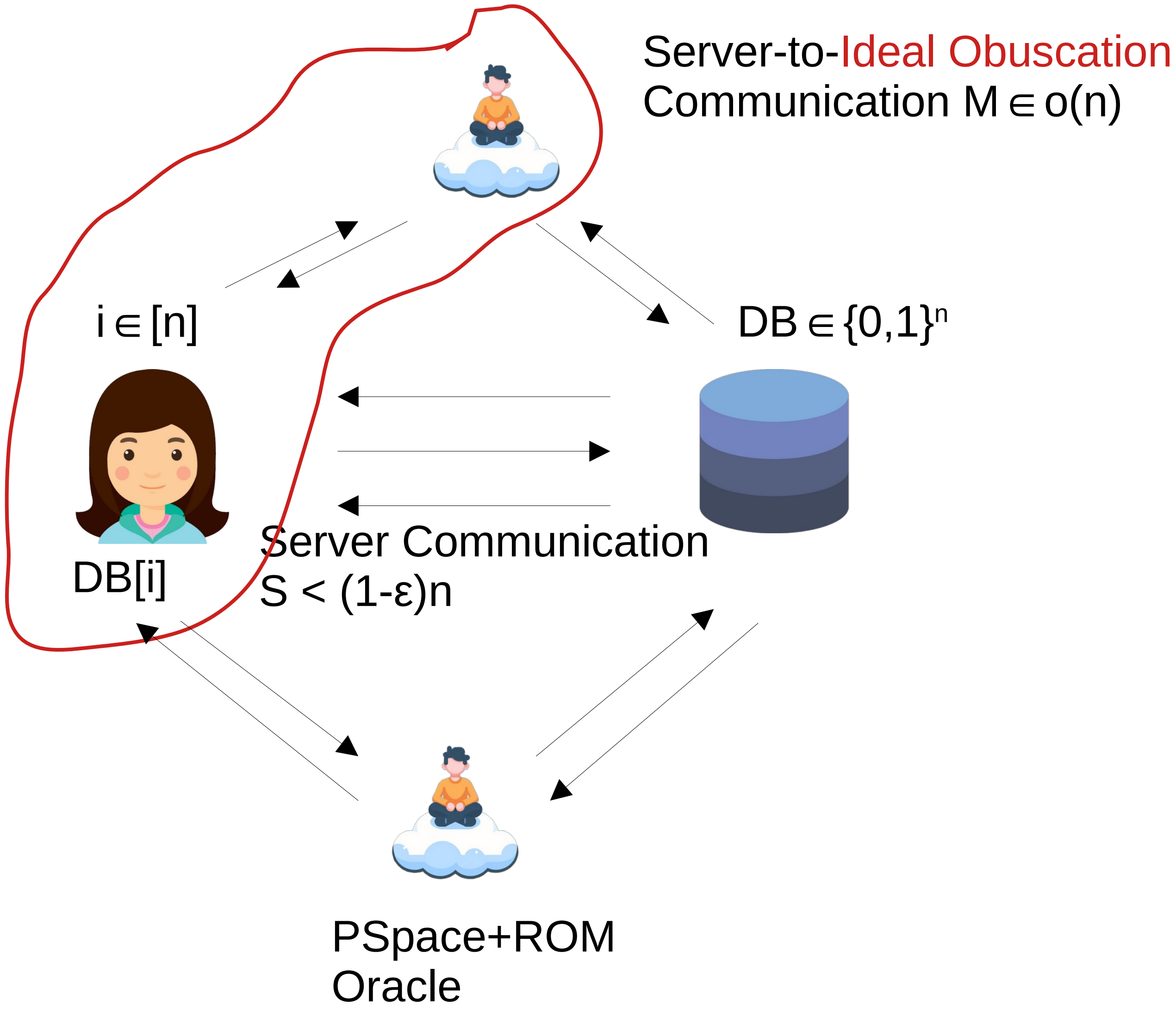
[DMO00]

Oblivious Transfer
Without the GGM,
Arb. PSpace queries,
Arb. ROM queries

$\perp$

[IR89,GKM+06]

PIR in the Simulatable Oracle + PSpace + ROM



Server-to-Ideal Obuscation
Communication $M \in o(n)$

$i \in [n]$

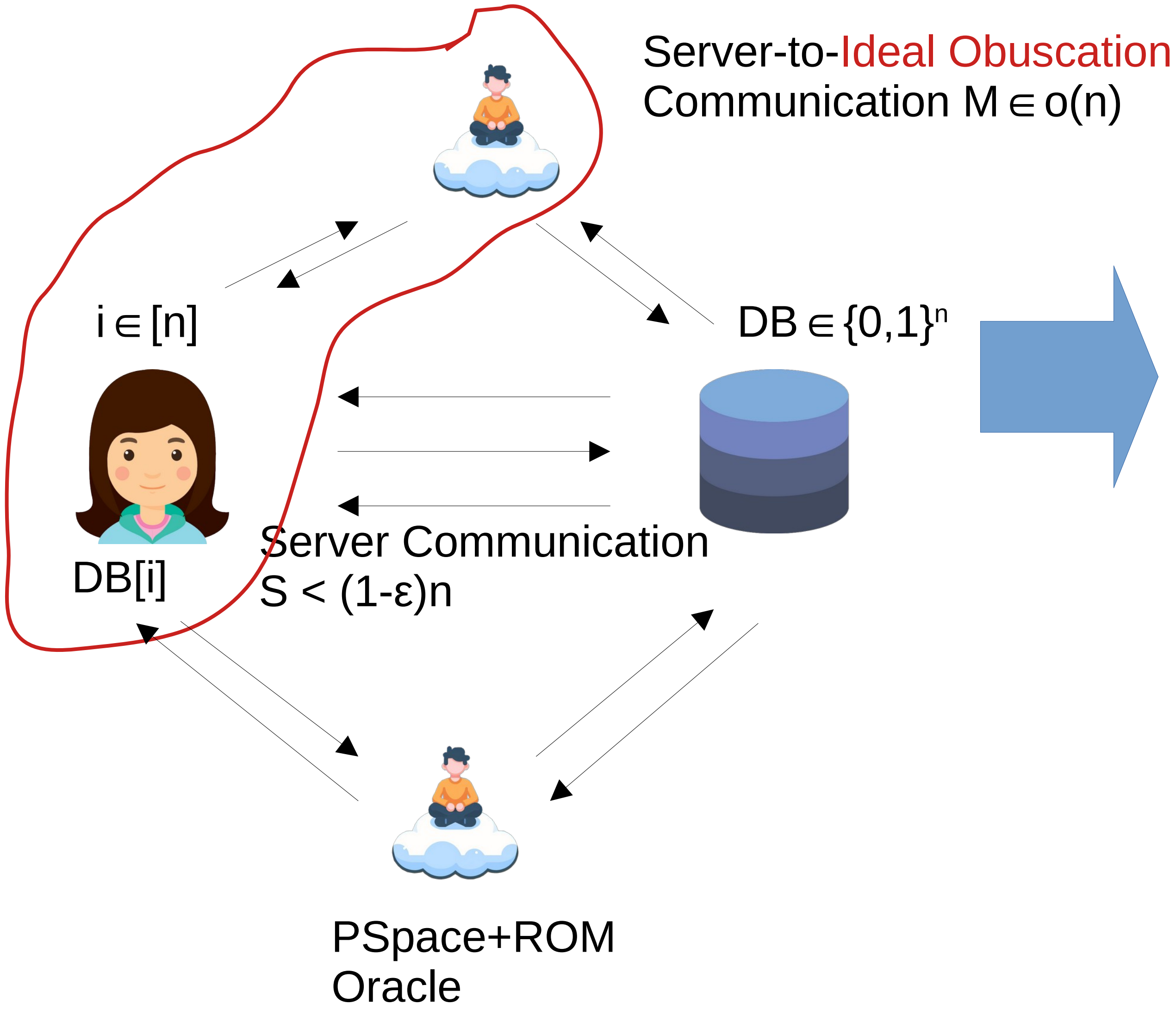
$DB \in \{0,1\}^n$

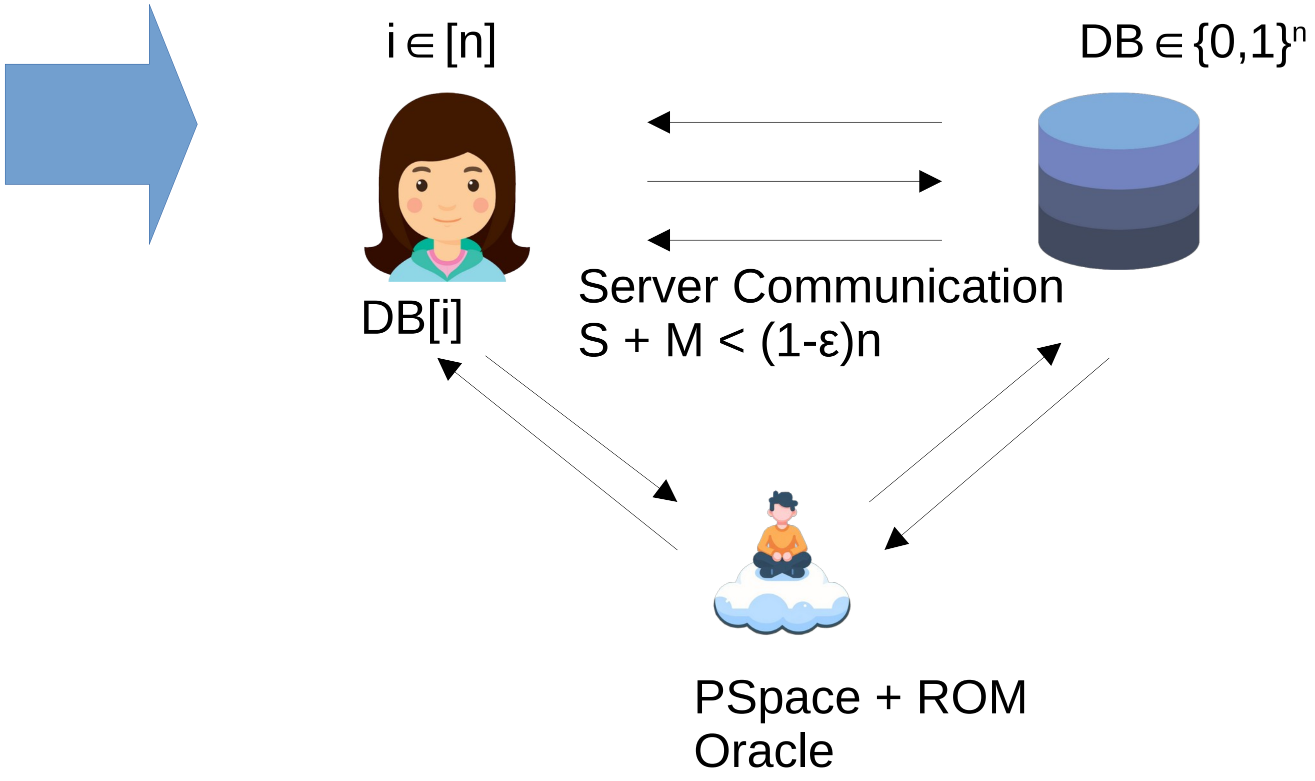
DB[i]

Server Communication
$S < (1-\varepsilon)n$

PSpace+ROM
Oracle

PIR in the Simulatable Oracle + PSpace + ROM

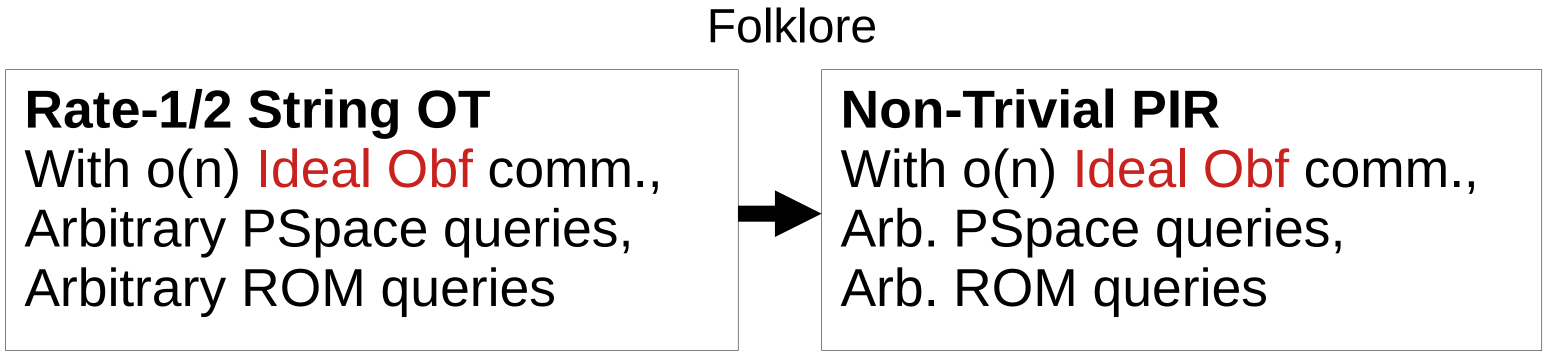




Consequences cont. (3)

Rate-1/2 String OT
With o(n) Ideal Obf comm.,
Arbitrary PSpace queries,
Arbitrary ROM queries

Consequences cont. (3)

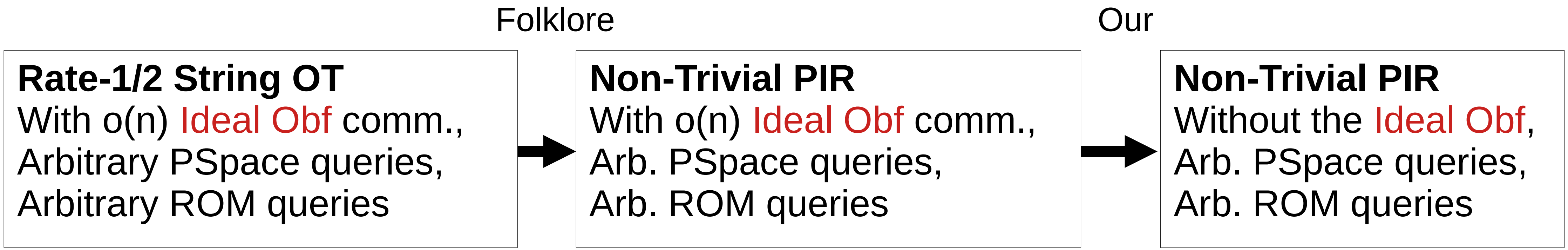


Folklore

Rate-1/2 String OT
With o(n) Ideal Obf comm.,
Arbitrary PSpace queries,
Arbitrary ROM queries

Non-Trivial PIR
With o(n) Ideal Obf comm.,
Arb. PSpace queries,
Arb. ROM queries

Consequences cont. (3)



Folklore

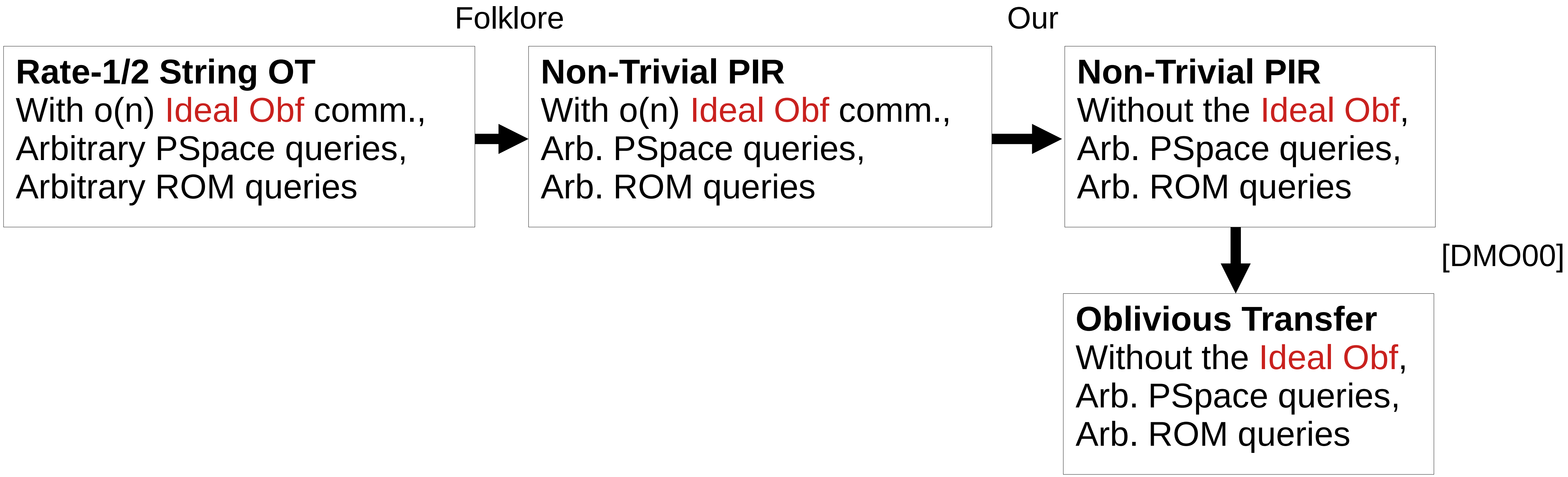
Our

Rate-1/2 String OT
With o(n) Ideal Obf comm.,
Arbitrary PSpace queries,
Arbitrary ROM queries

Non-Trivial PIR
With o(n) Ideal Obf comm.,
Arb. PSpace queries,
Arb. ROM queries

Non-Trivial PIR
Without the Ideal Obf,
Arb. PSpace queries,
Arb. ROM queries

Consequences cont. (3)



Folklore

Our

Rate-1/2 String OT
With o(n) Ideal Obf comm.,
Arbitrary PSpace queries,
Arbitrary ROM queries

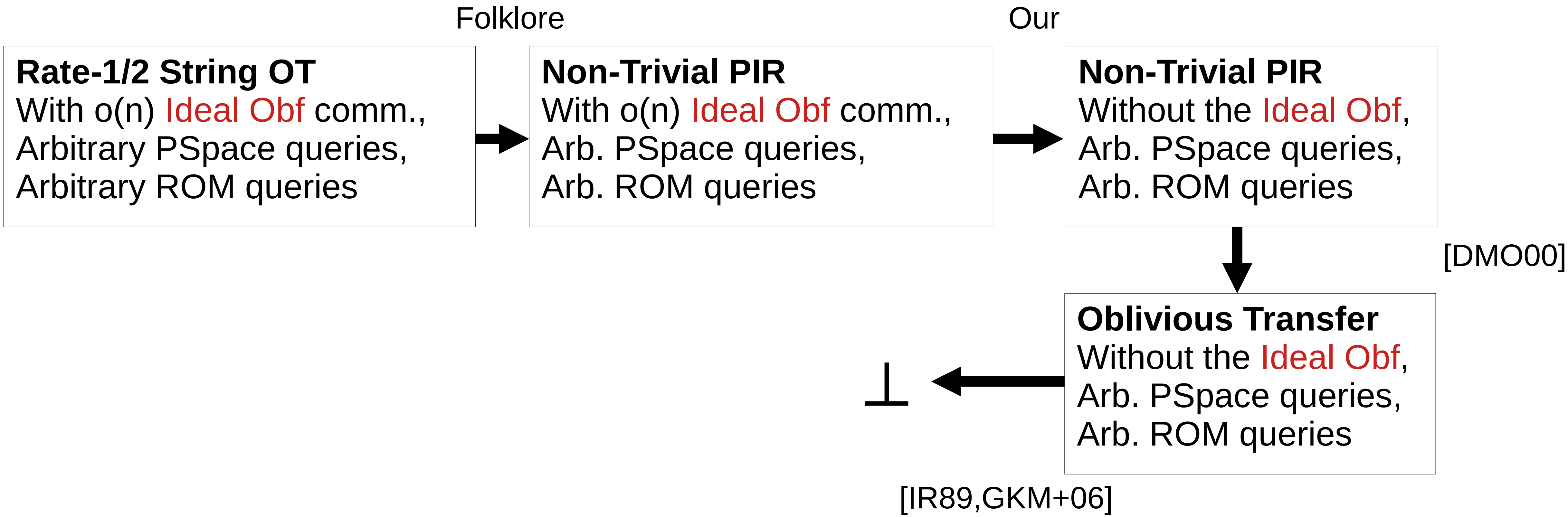
Non-Trivial PIR
With o(n) Ideal Obf comm.,
Arb. PSpace queries,
Arb. ROM queries

Non-Trivial PIR
Without the Ideal Obf,
Arb. PSpace queries,
Arb. ROM queries

[DMO00]

Oblivious Transfer
Without the Ideal Obf,
Arb. PSpace queries,
Arb. ROM queries

Consequences cont. (3)



Folklore

Our

Rate-1/2 String OT
With o(n) Ideal Obf comm.,
Arbitrary PSpace queries,
Arbitrary ROM queries

Non-Trivial PIR
With o(n) Ideal Obf comm.,
Arb. PSpace queries,
Arb. ROM queries

Non-Trivial PIR
Without the Ideal Obf,
Arb. PSpace queries,
Arb. ROM queries

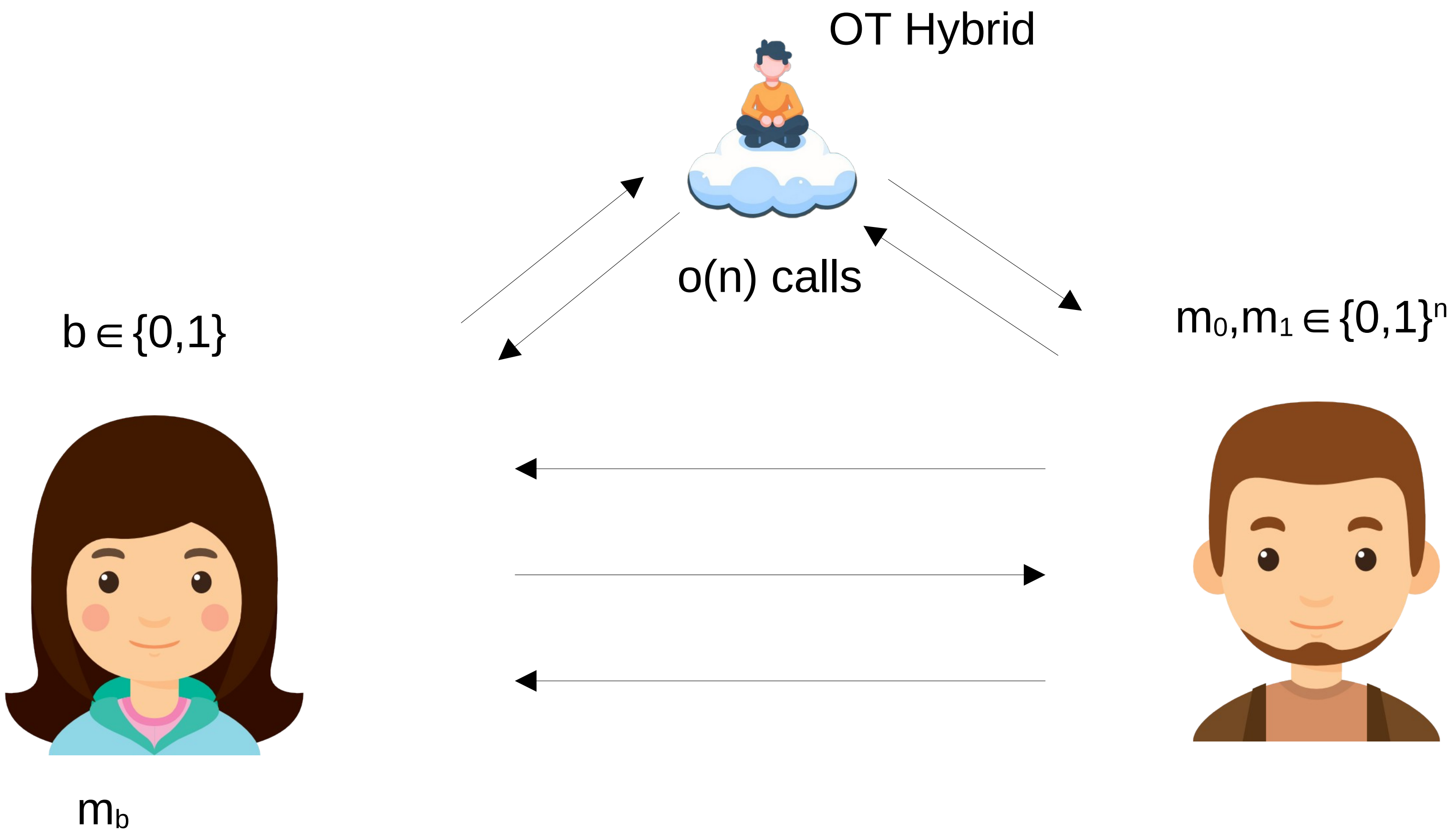
[DMO00]

Oblivious Transfer
Without the Ideal Obf,
Arb. PSpace queries,
Arb. ROM queries

$\perp$

[IR89,GKM+06]

OT Extensions (Weak Variant)



OT Hybrid

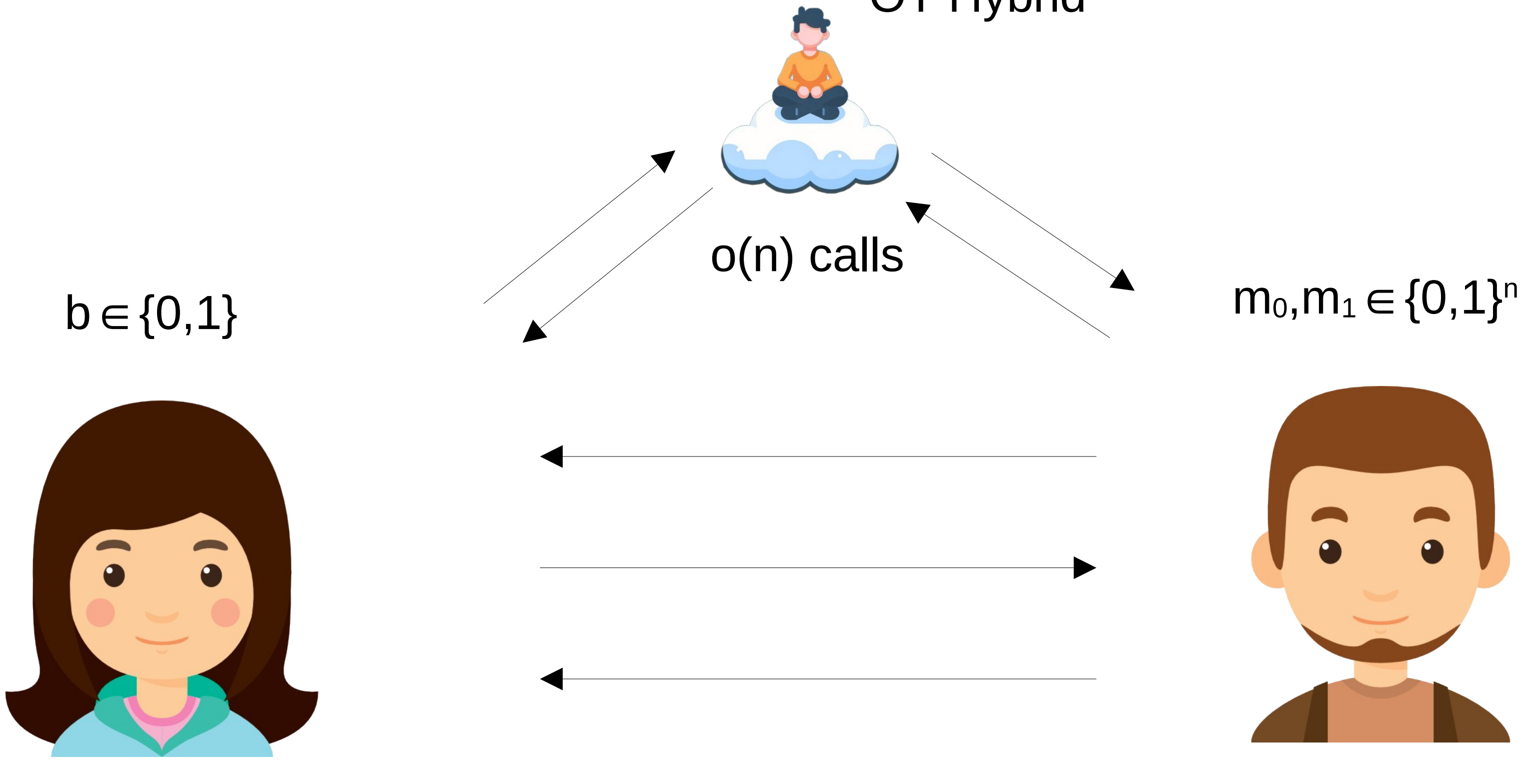
o(n) calls

$b \in \{0,1\}$

$m_0, m_1 \in \{0,1\}^n$

m_b

OT Extensions (Weak Variant)



OT Hybrid

o(n) calls

$b \in \{0,1\}$

$m_0, m_1 \in \{0,1\}^n$

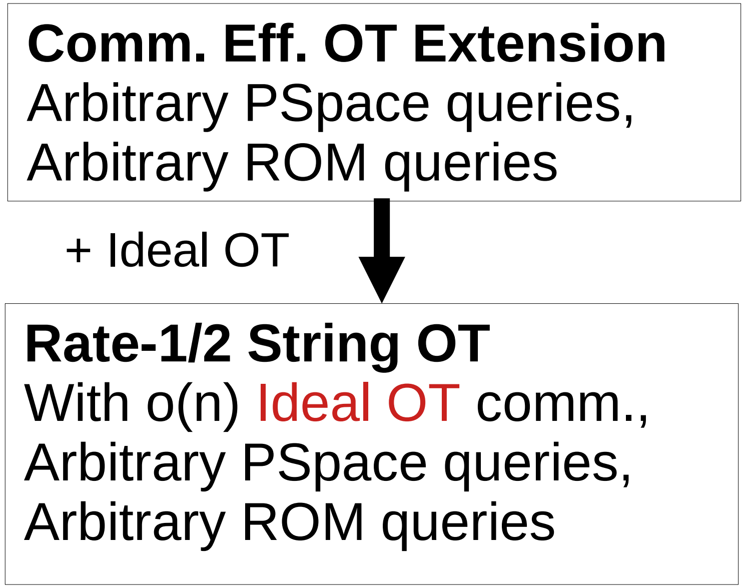
m_b

Communication < $(1-\varepsilon)2n$

OT Extension Consequences

Comm. Eff. OT Extension
Arbitrary PSpace queries,
Arbitrary ROM queries

OT Extension Consequences

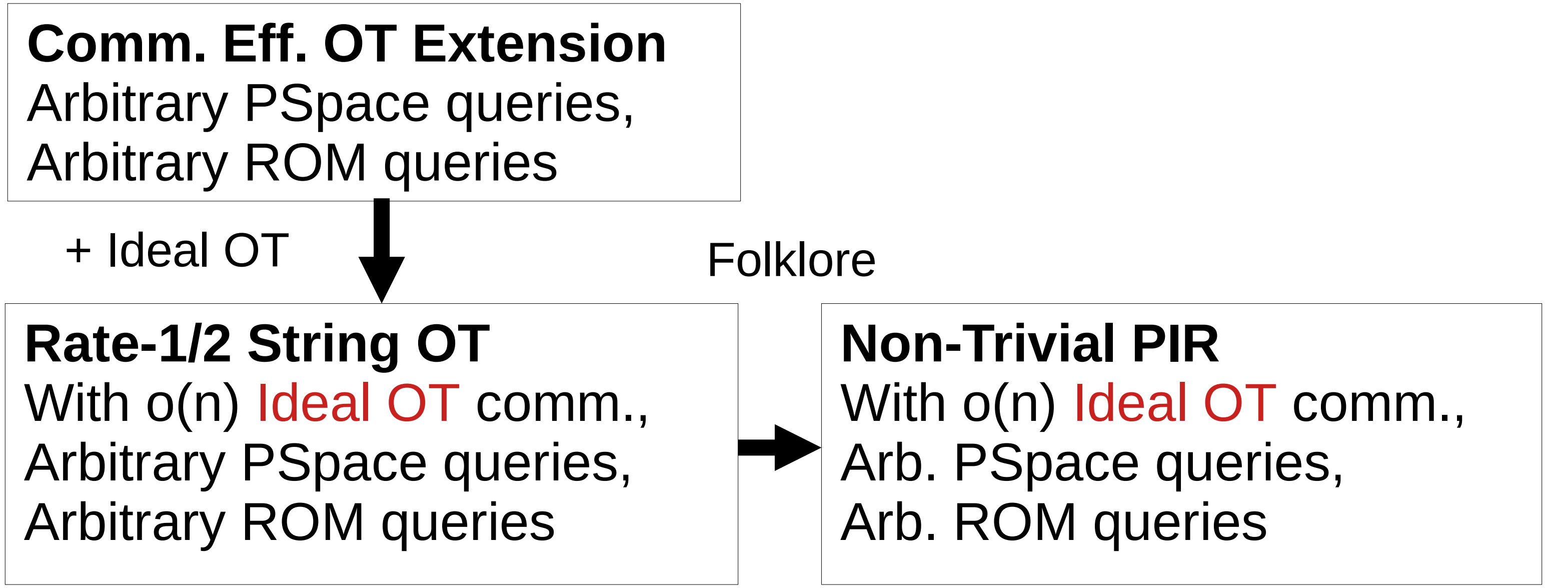


Comm. Eff. OT Extension
Arbitrary PSpace queries,
Arbitrary ROM queries

+ Ideal OT

Rate-1/2 String OT
With o(n) Ideal OT comm.,
Arbitrary PSpace queries,
Arbitrary ROM queries

OT Extension Consequences



Comm. Eff. OT Extension
Arbitrary PSpace queries,
Arbitrary ROM queries

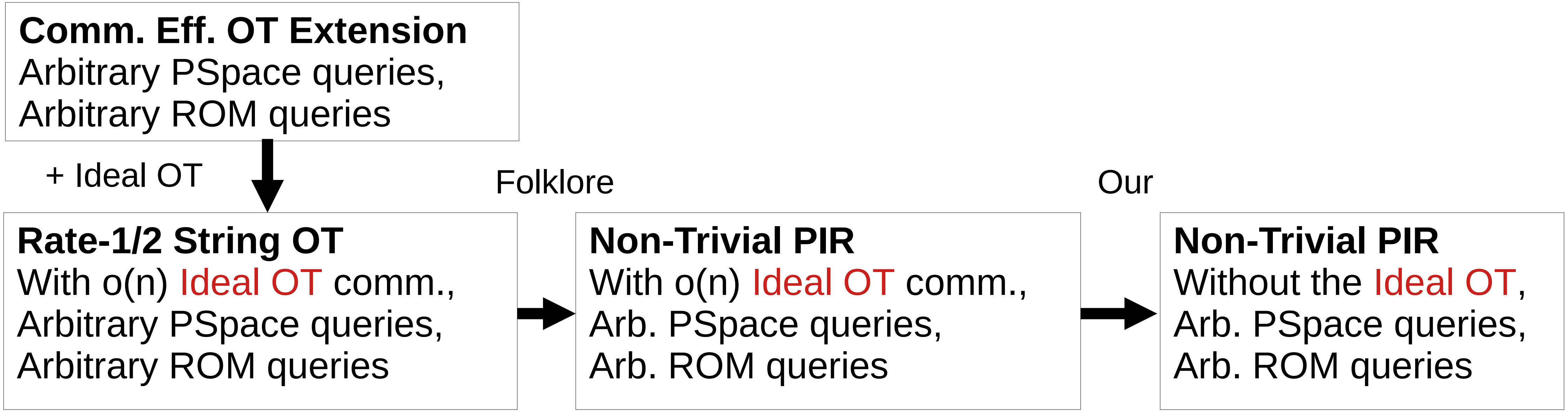
+ Ideal OT

Rate-1/2 String OT
With o(n) Ideal OT comm.,
Arbitrary PSpace queries,
Arbitrary ROM queries

Folklore

Non-Trivial PIR
With o(n) Ideal OT comm.,
Arb. PSpace queries,
Arb. ROM queries

OT Extension Consequences



Comm. Eff. OT Extension
Arbitrary PSpace queries,
Arbitrary ROM queries

+ Ideal OT

Rate-1/2 String OT
With o(n) Ideal OT comm.,
Arbitrary PSpace queries,
Arbitrary ROM queries

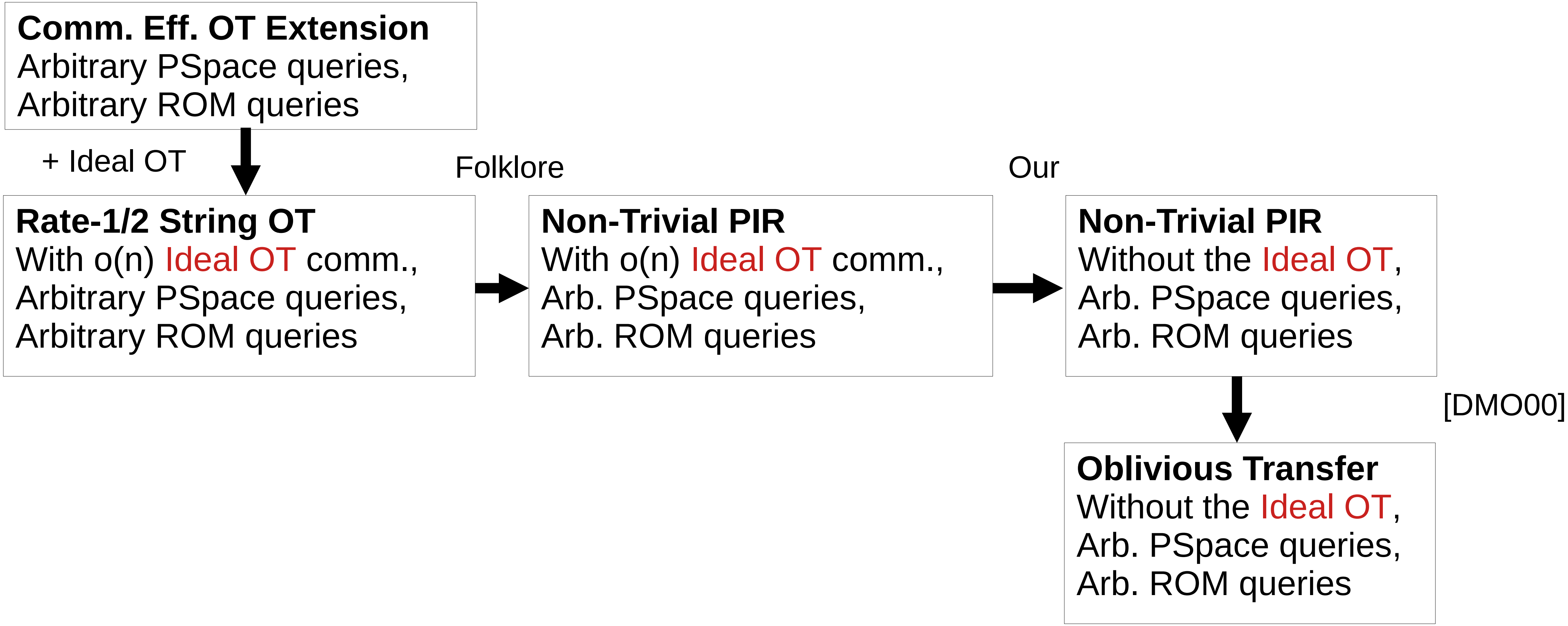
Folklore

Non-Trivial PIR
With o(n) Ideal OT comm.,
Arb. PSpace queries,
Arb. ROM queries

Our

Non-Trivial PIR
Without the Ideal OT,
Arb. PSpace queries,
Arb. ROM queries

OT Extension Consequences



Comm. Eff. OT Extension
Arbitrary PSpace queries,
Arbitrary ROM queries

+ Ideal OT

Rate-1/2 String OT
With o(n) Ideal OT comm.,
Arbitrary PSpace queries,
Arbitrary ROM queries

Folklore

Non-Trivial PIR
With o(n) Ideal OT comm.,
Arb. PSpace queries,
Arb. ROM queries

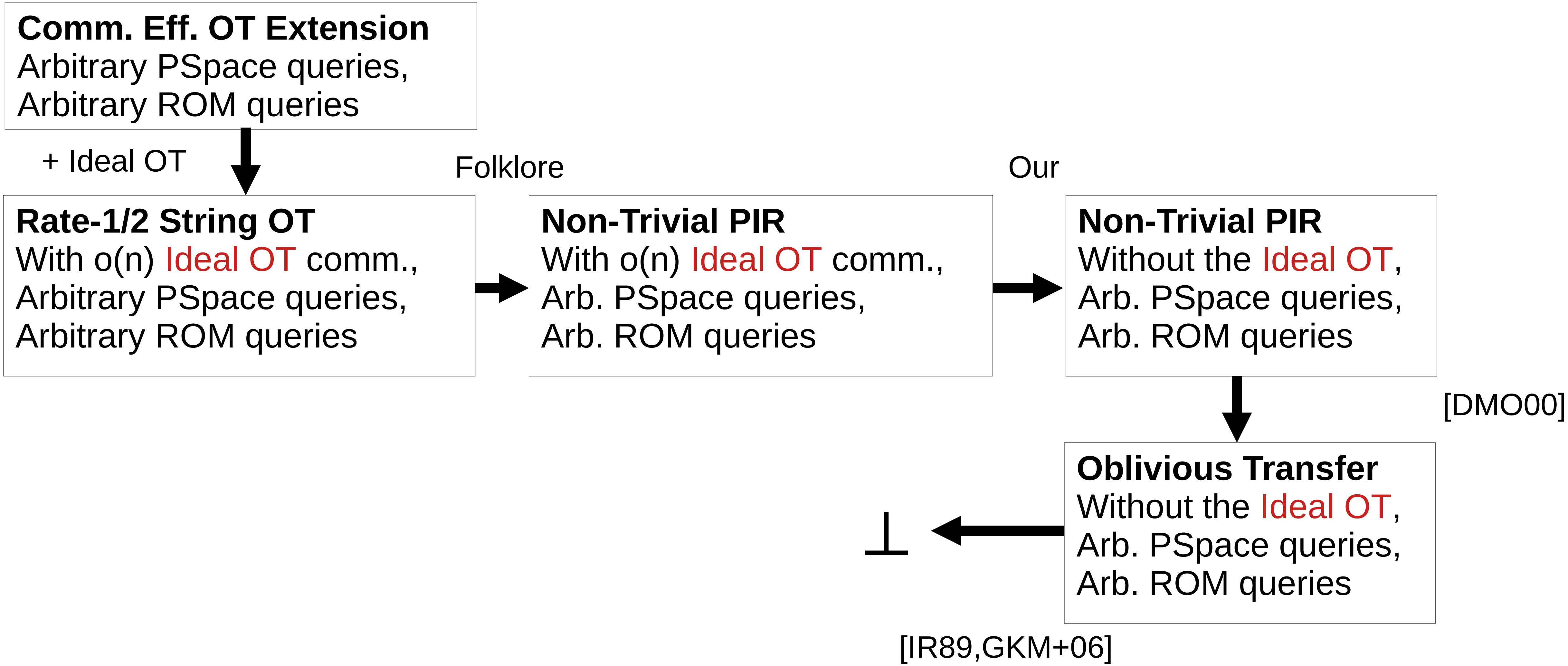
Our

Non-Trivial PIR
Without the Ideal OT,
Arb. PSpace queries,
Arb. ROM queries

[DMO00]

Oblivious Transfer
Without the Ideal OT,
Arb. PSpace queries,
Arb. ROM queries

OT Extension Consequences



Comm. Eff. OT Extension
Arbitrary PSpace queries,
Arbitrary ROM queries

+ Ideal OT

Rate-1/2 String OT
With o(n) Ideal OT comm.,
Arbitrary PSpace queries,
Arbitrary ROM queries

Folklore

Non-Trivial PIR
With o(n) Ideal OT comm.,
Arb. PSpace queries,
Arb. ROM queries

Our

Non-Trivial PIR
Without the Ideal OT,
Arb. PSpace queries,
Arb. ROM queries

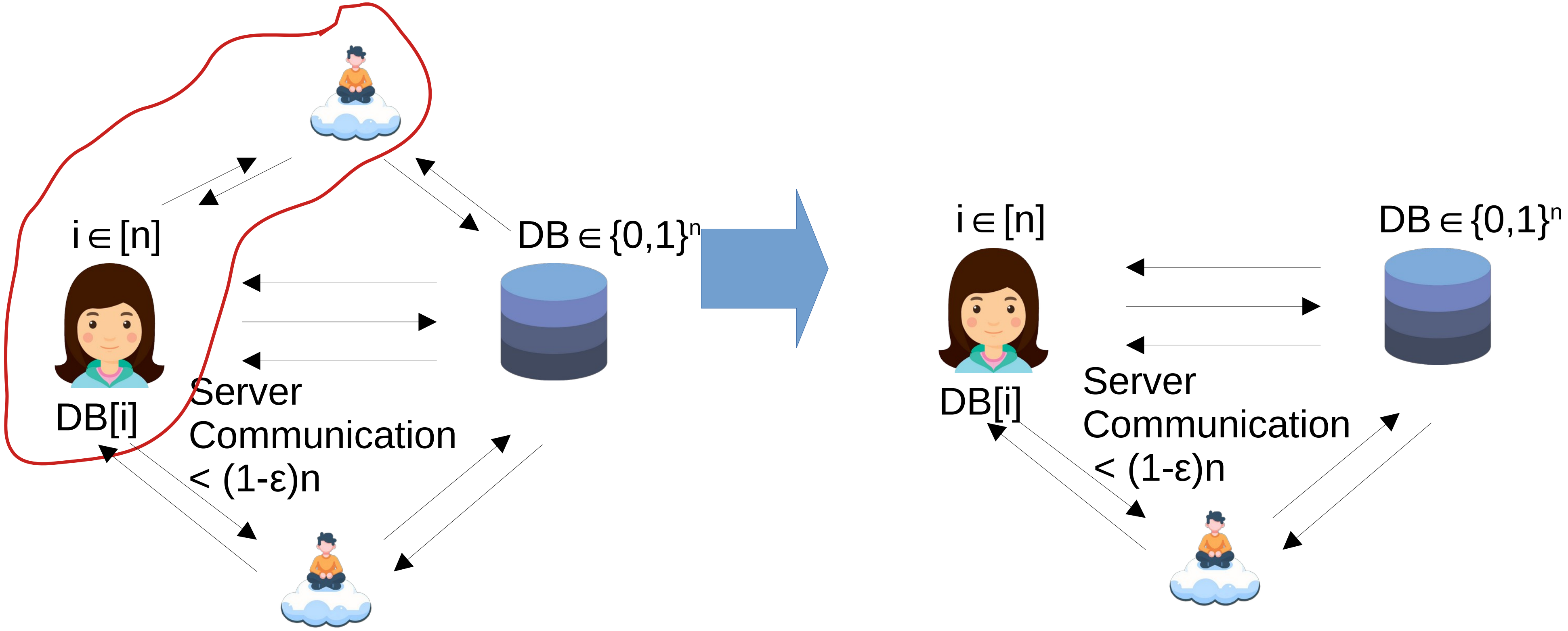
[DMO00]

Oblivious Transfer
Without the Ideal OT,
Arb. PSpace queries,
Arb. ROM queries

$\perp$

[IR89,GKM+06]

Thank you!


i ∈ [n]
DB ∈ {0,1}ⁿ
DB[i]
Server
Communication
< (1-ε)n
i ∈ [n]
DB ∈ {0,1}ⁿ
DB[i]
Server
Communication
< (1-ε)n