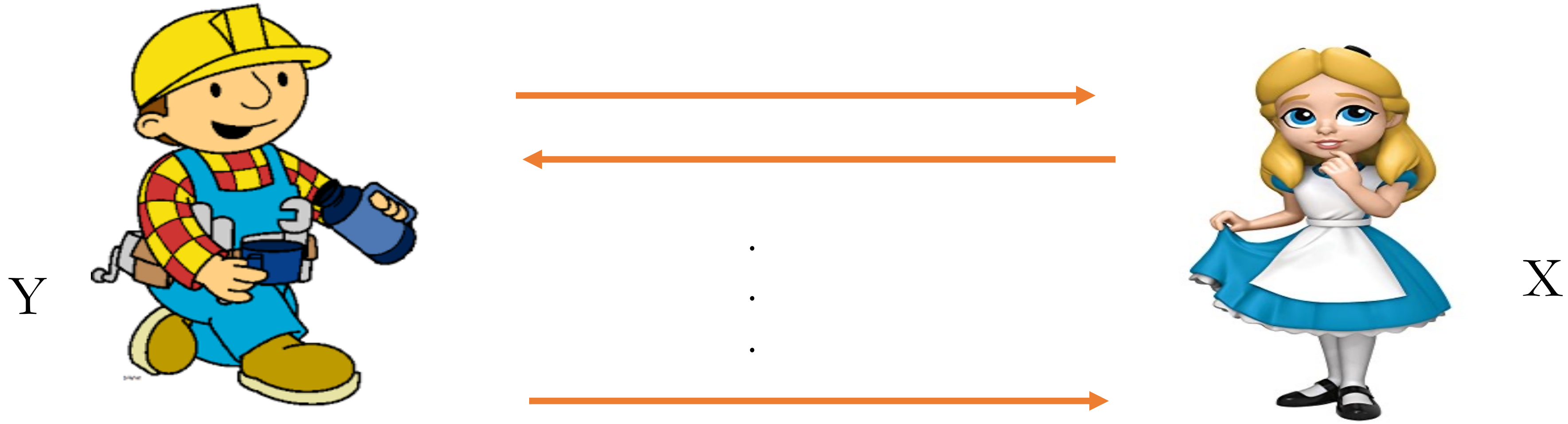
Communication-Efficient MPC for Branching Programs and Applications to PSI/PIR

Mohammad Hajiabadi

Based on work (past and ongoing) with Melissa Chase (MSR), Sanjam Garg (Berkeley) and Peihan Miao (Brown)

Secure Multi-Party Computation (MPC)

- Two-party computation for a function $f(X, Y)$



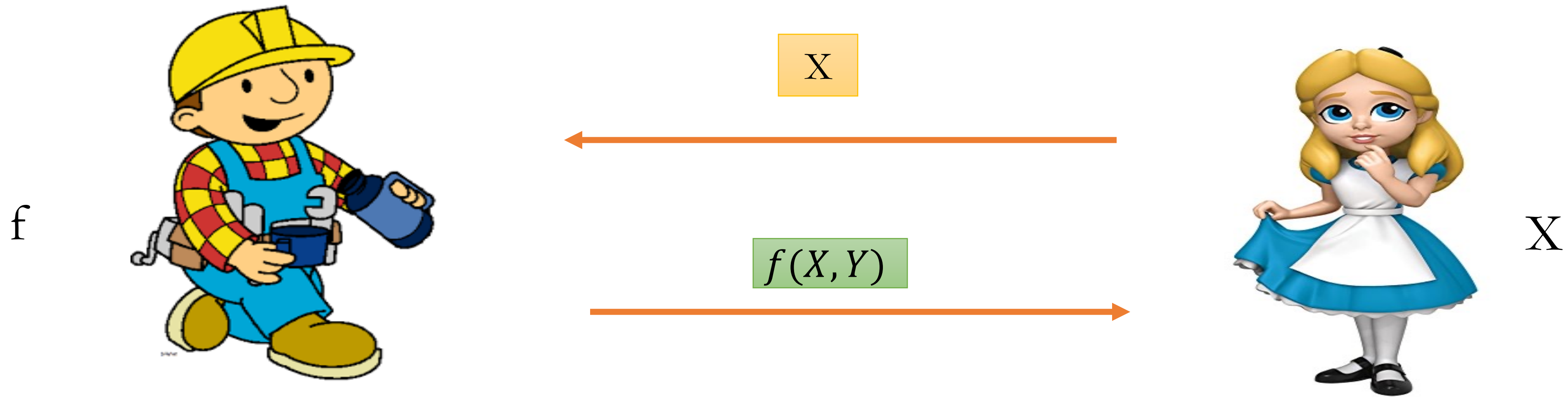
Focus:

- Two rounds
- Efficient communication: matching that of best insecure protocol

$O(Min(X, Y), |f(X, Y)|) + \lambda$, where λ is the security parameter.

Truly Laconic MPC implies FHE

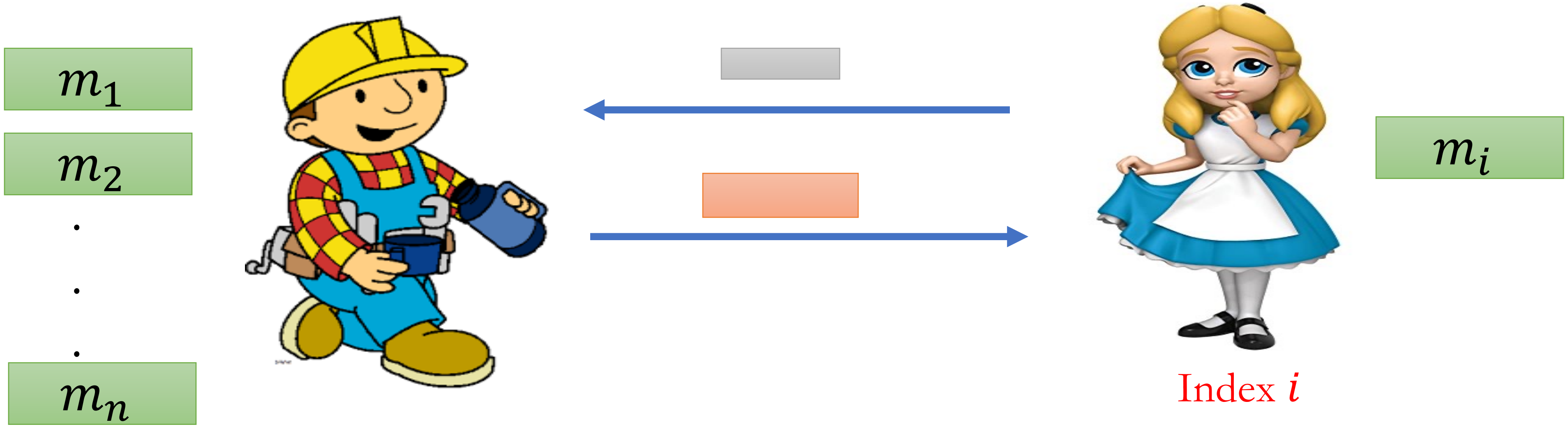
- Super communication efficient MPC for all functions implies FHE.



- If $\boxed{f(X,Y)}$ is small and we can support all functions f, this implies FHE.
- Goal: having communication-efficient MPC for special functions f and without using FHE.

Example 1: Private Information Retrieval (PIR)

- Requirement: |. | + | | << database-size
  Alice doesn't learn anything about index i, and Bob doesn't learn anything beyond m_i.



Example 2: Unbalanced PSI

$m_1, \dots, m_n$

Big Set!

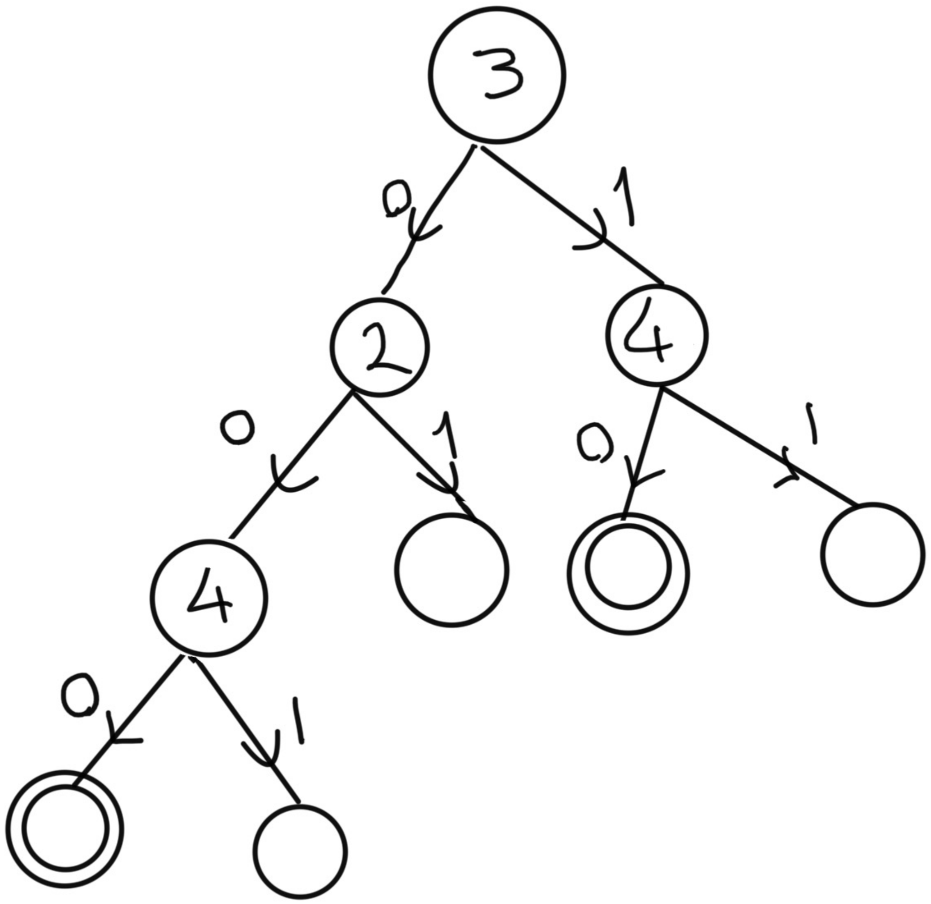
m

$m \in \{m_1, \dots, m_n\}$?

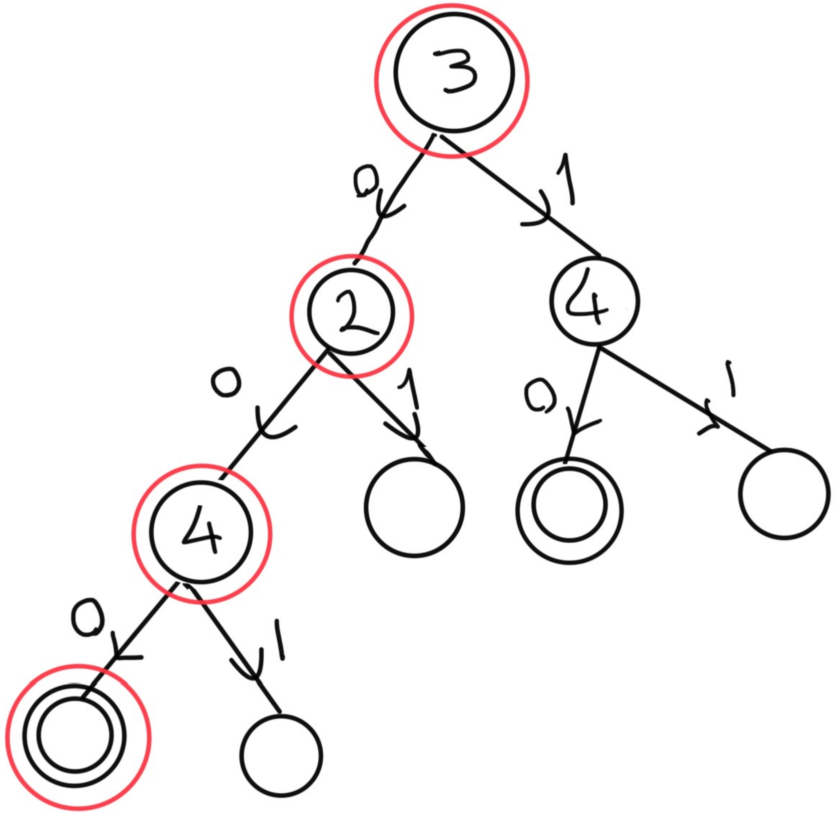
- Requirement: communication complexity $O(|m|, \lambda)$, and intendent of n
- General MPC techniques (and even most specific PSI techniques) result in communication that grows with n.

- General Theme: MPC for Branching Programs

Branching Programs

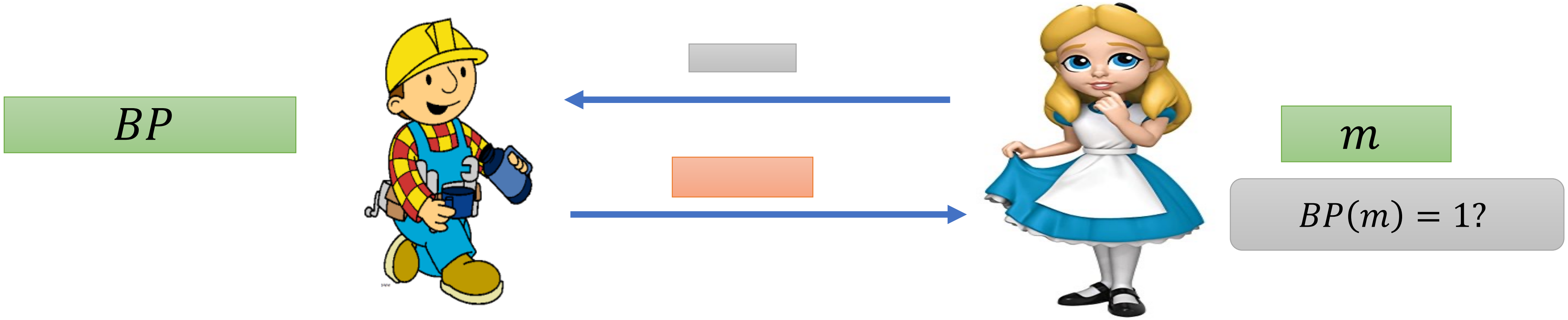


Branching Programs



X = 1000 is accepted

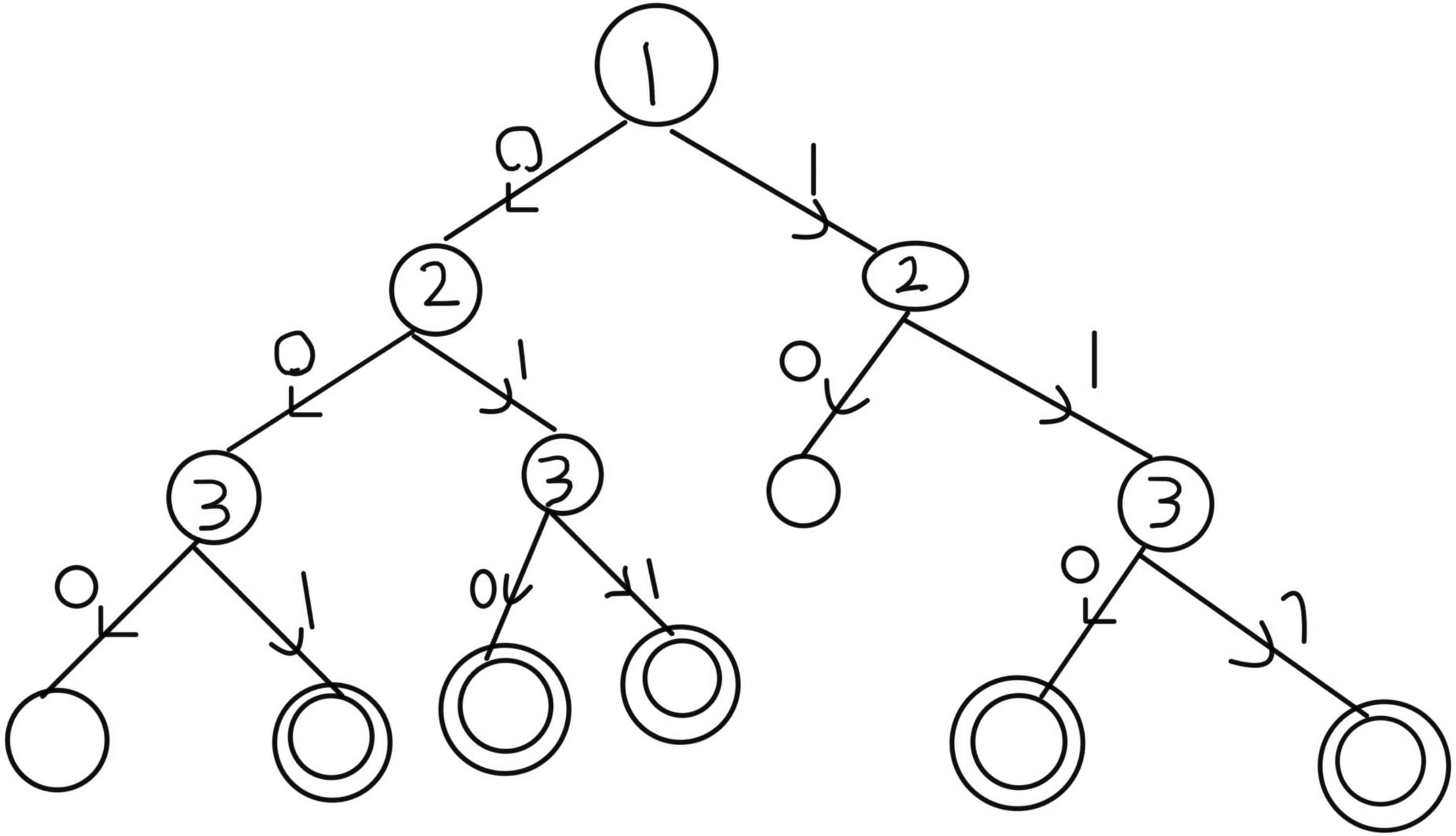
MPC for Branching Programs



- Requirement: communication complexity shouldn't grow with $|BP|$.

PIR as BP-MPC

- PIR database: S = {001,010,011,110,111}



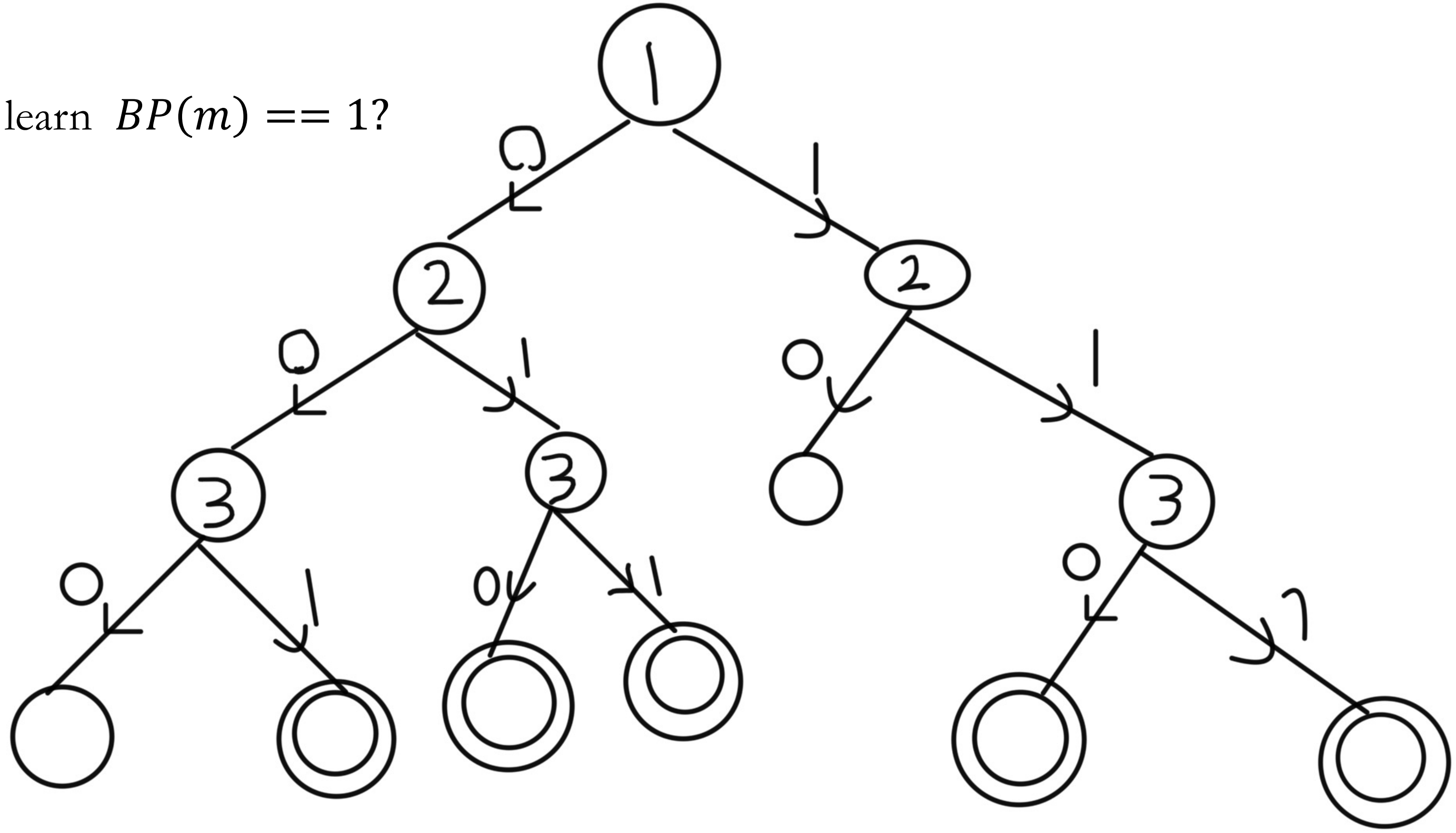
Let ℓ length of each keyword
Size of BP = $\Theta(\ell|S|)$
Depth of BP = ℓ

In general, $\ell \ll |S|$

Unbalanced PSI as BP-MPC

- Sender's set $S = \{001,010,011,110,111\}$

The senders holds BP, and the receiver wants to learn $BP(m) == 1$?

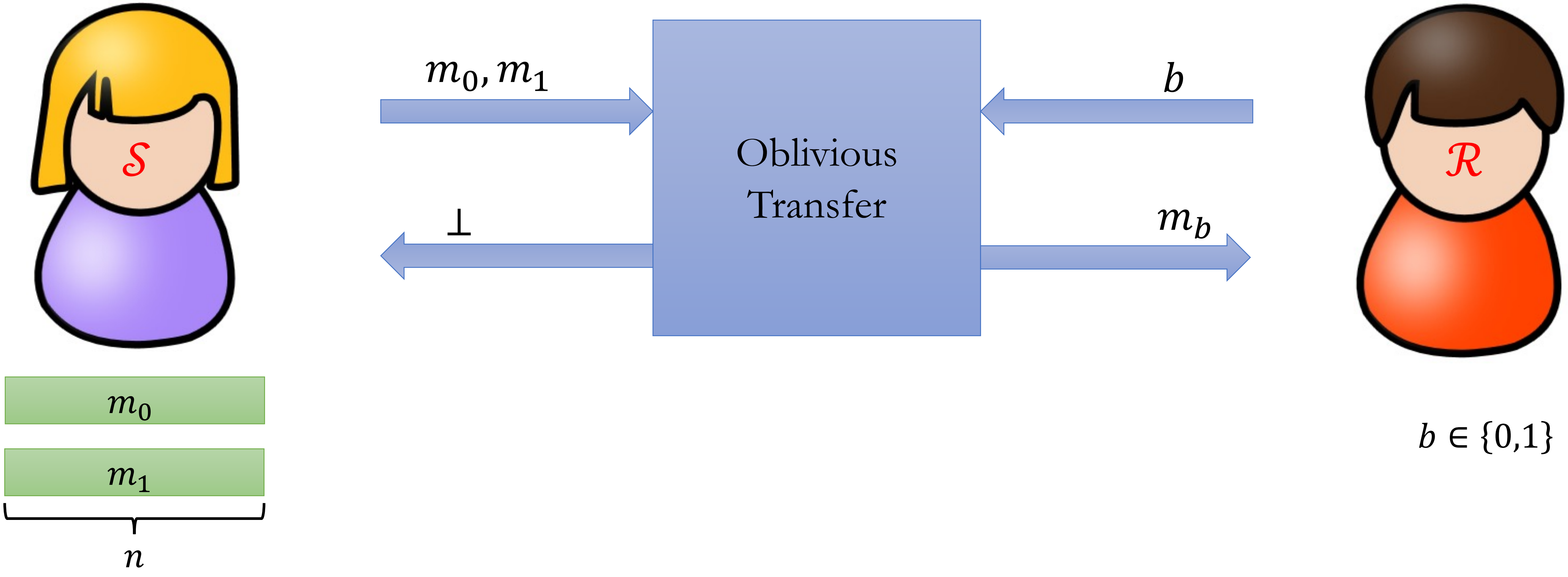


BP-MPC Realizations

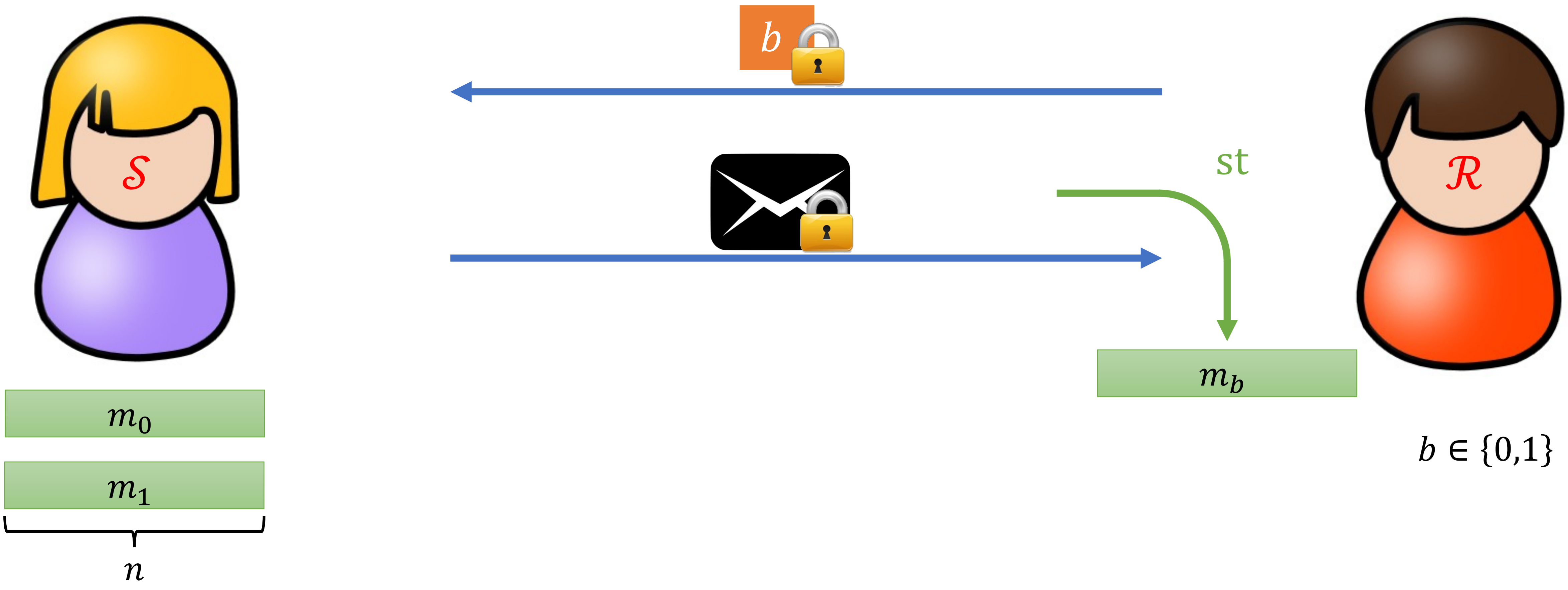
- Using generic MPC techniques (e.g., garbled circuits and OT) one can realize BP-MPC with communication that grows with the BP size.

- Insight: Using rate-1 OT, one can do BP-MPC with communication that grows only with depth of BP, and not its size.

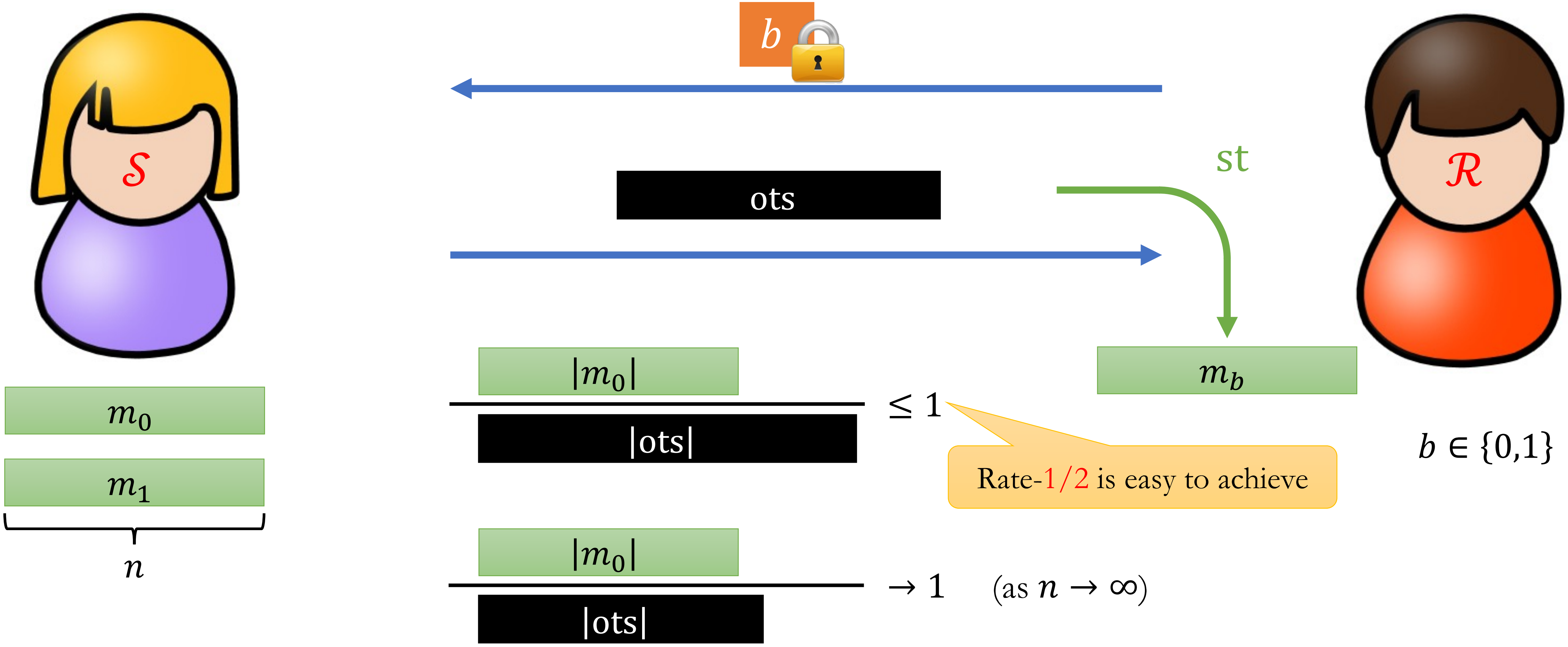
Oblivious Transfer (OT) [Rabin81, EGL82, BCR86, Kilian88]



Two-Message OT [AIR01, NP01, PVW08, HK12, DGHMW20]



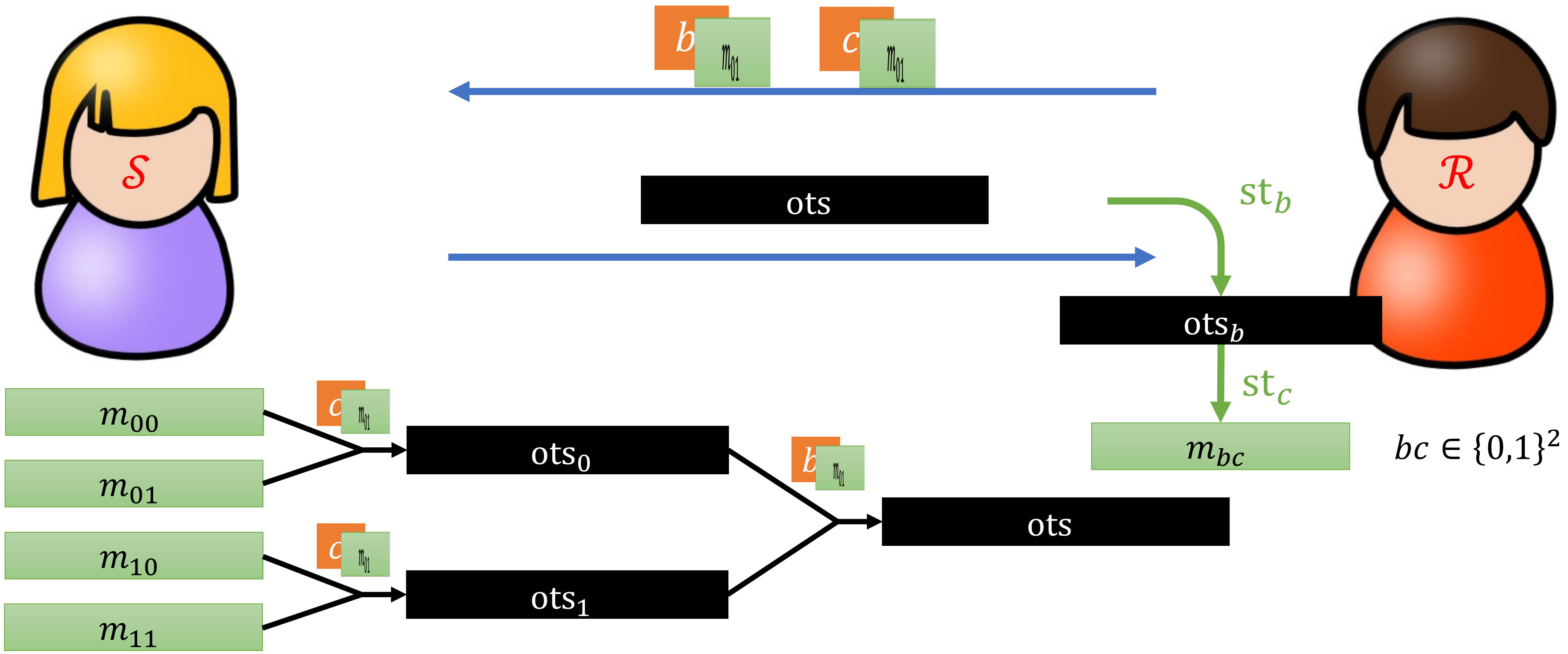
Rate-1 OT [IP07, DGIMMO19, GHO20]



Why two-message? Why rate-1?

Reason: $2 \times 2 = 4$

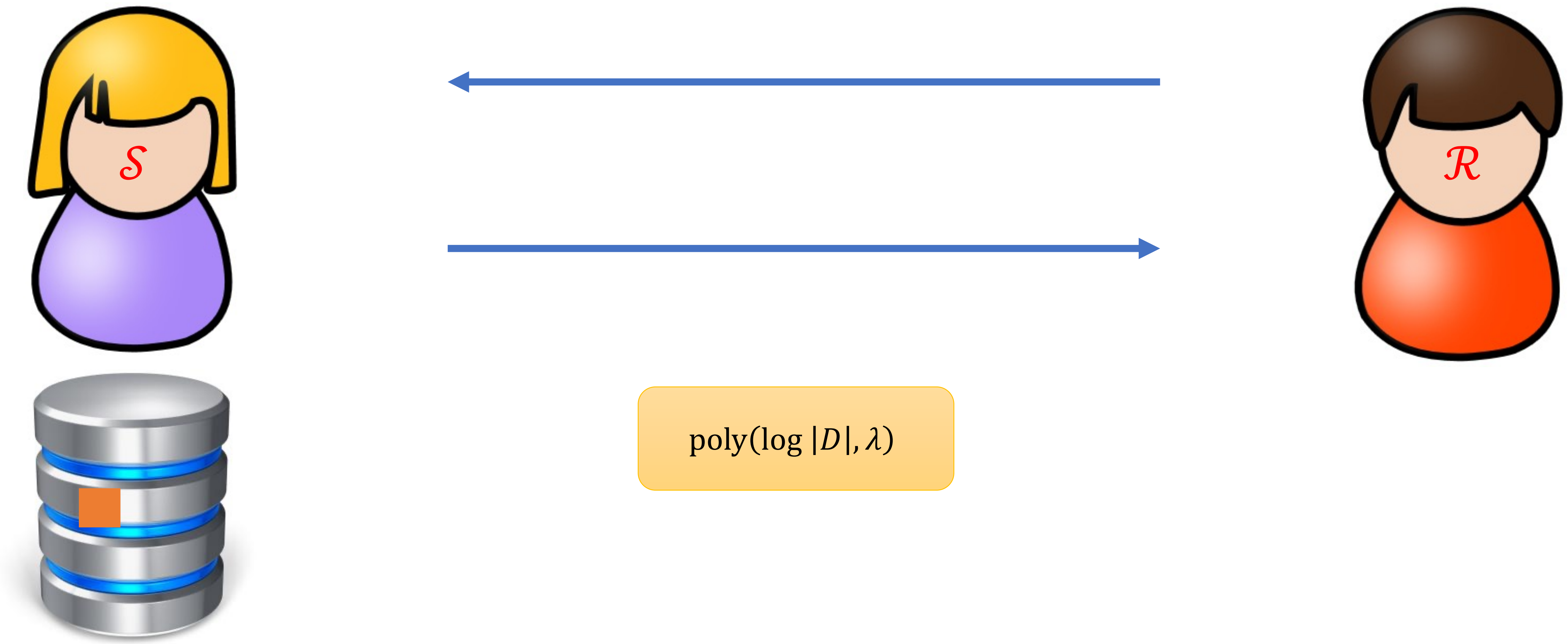
Example: 1-out-of-4 OT



Why two-message? Why rate-1?

Nested OT with low communication

Applications of Rate-1 OT



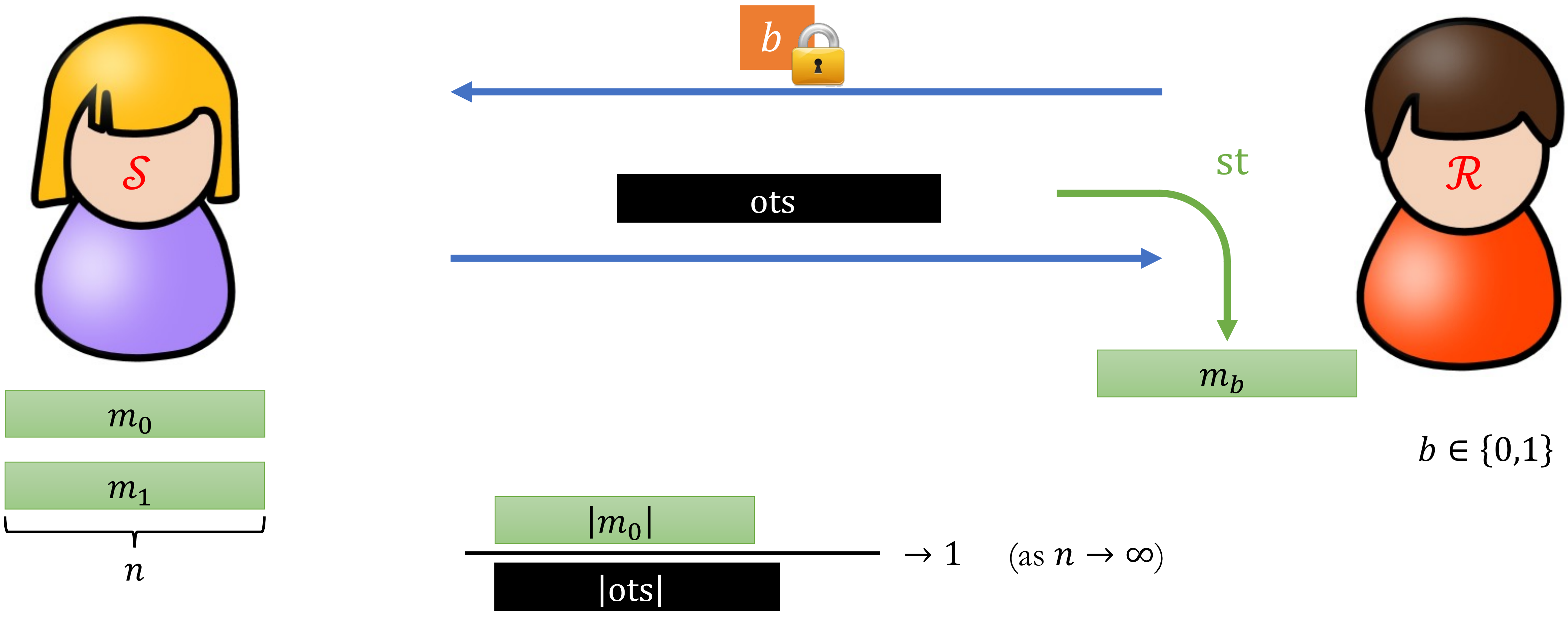
Applications of Rate-1 OT

- Semi-compact homomorphic encryption for branching programs [IP07]
  - Single-server private information retrieval **(PIR)** [KO97] with poly-logarithmic communication
  - Unbalanced private set intersection **(PSI)** with poly-logarithmic communication in the size of the larger set
  - Secure inference on decision trees with communication linear in the tree depth
- Lossy trapdoor functions [PW08, HO12] with optimal rate [DGIMMO19]

Can we achieve Rate-1 OT?

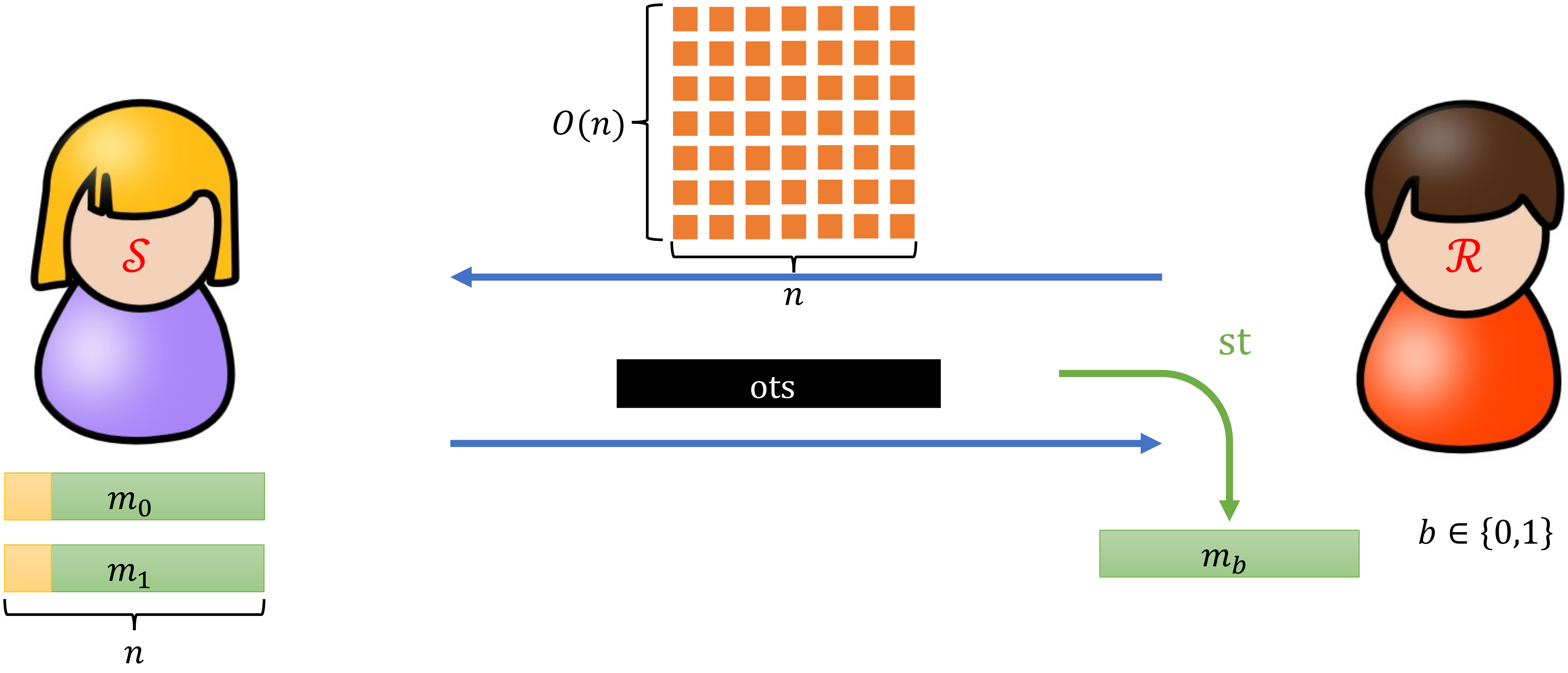
- Damgård-Jurik Cryptosystem [DJ01] from DCR
- Trapdoor Hash Functions [DGIMMO19] from DDH/QR/LWE/DCR
- Our results: rate-1 OT with better communication complexity for receivers.

Rate-1 OT [DJ01, DGIMMO19, GHO20]

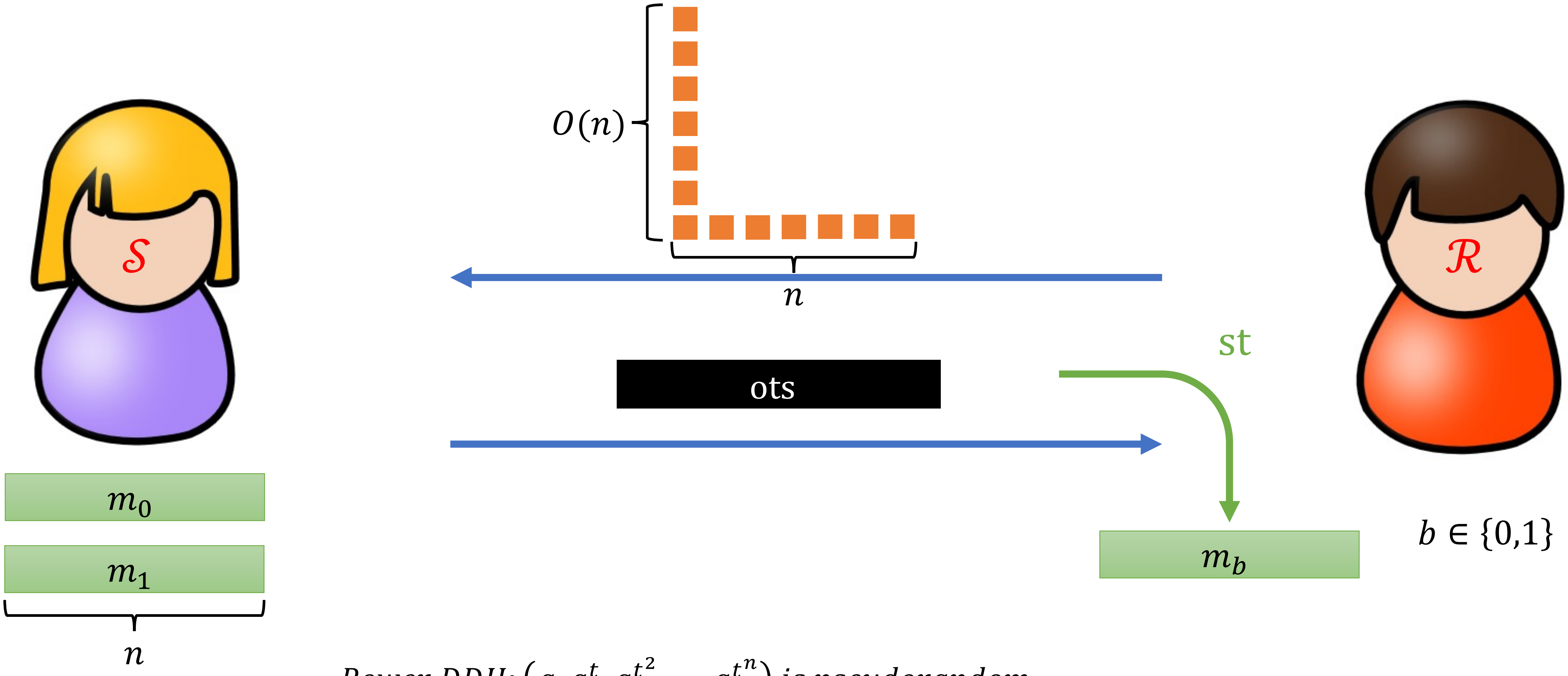


Receiver Communication?

Rate-1 OT from DDH [DGIMMO19]

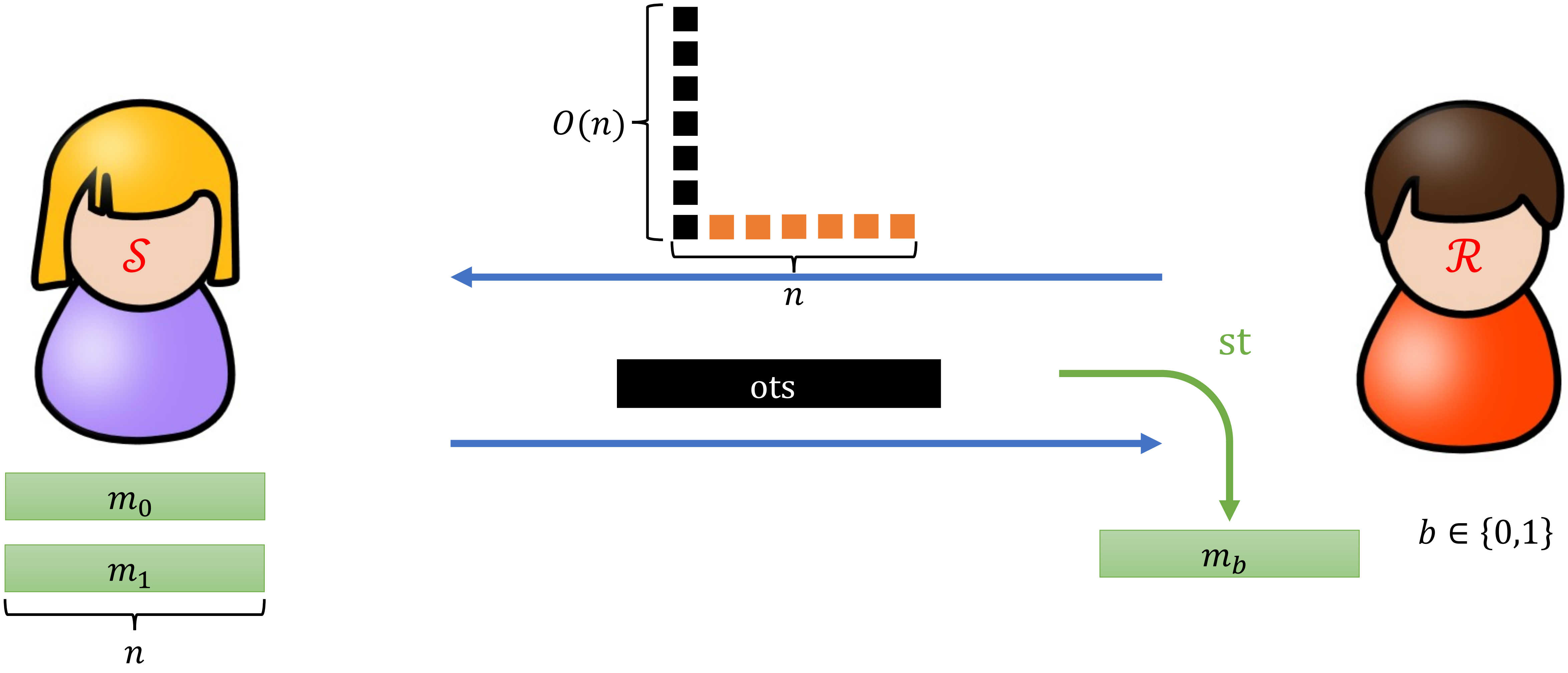


Rate-1 OT from Power DDH [GHO20]

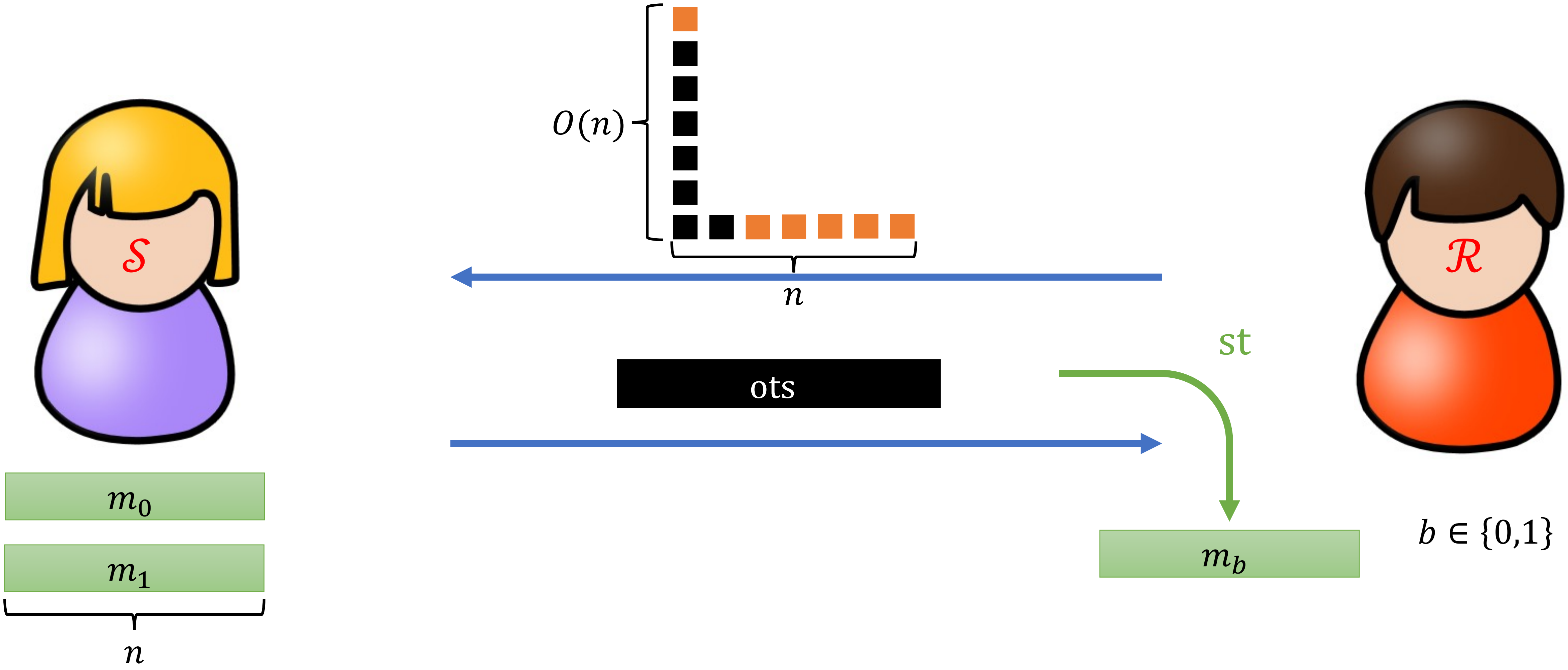


Power DDH: $(g, g^t, g^{t^2}, \dots, g^{t^n})$ *is pseudorandom*

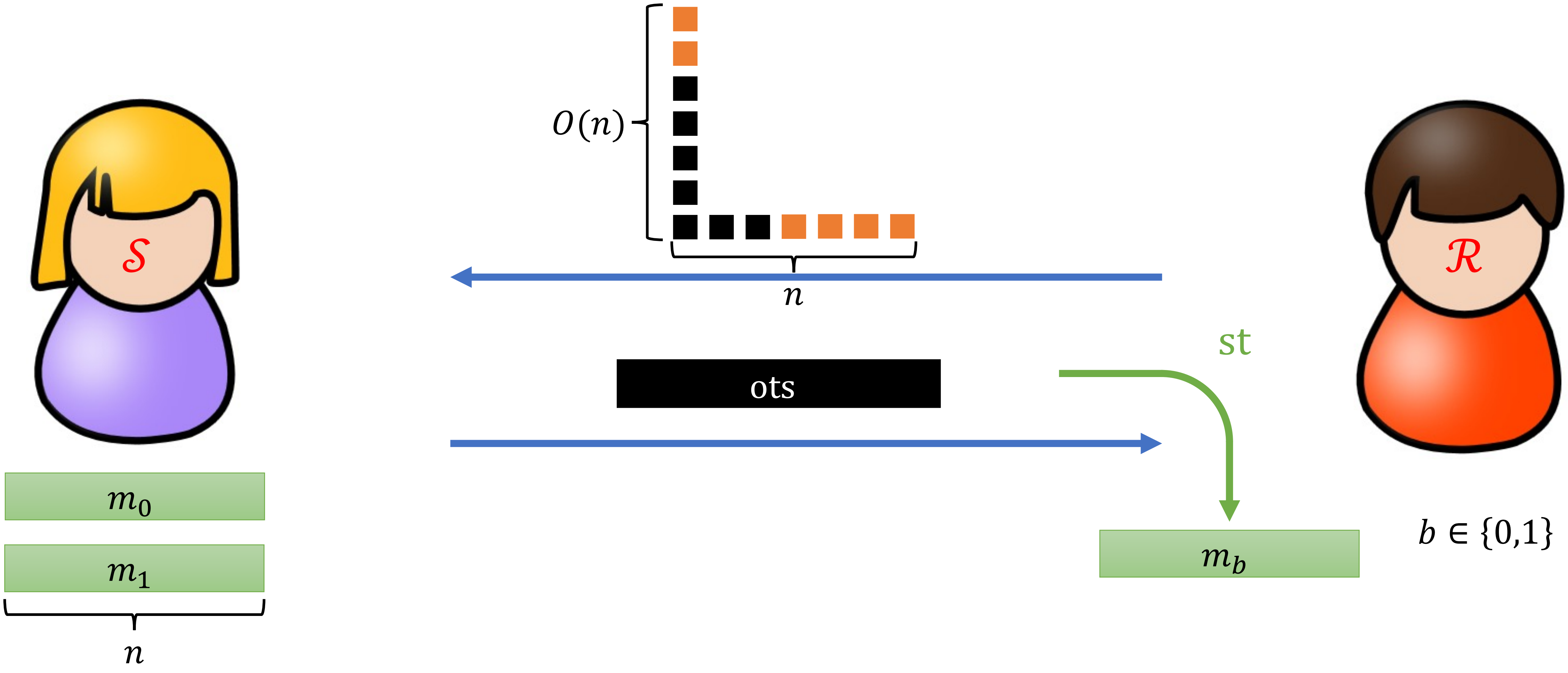
Rate-1 OT from Power DDH [GHO20]



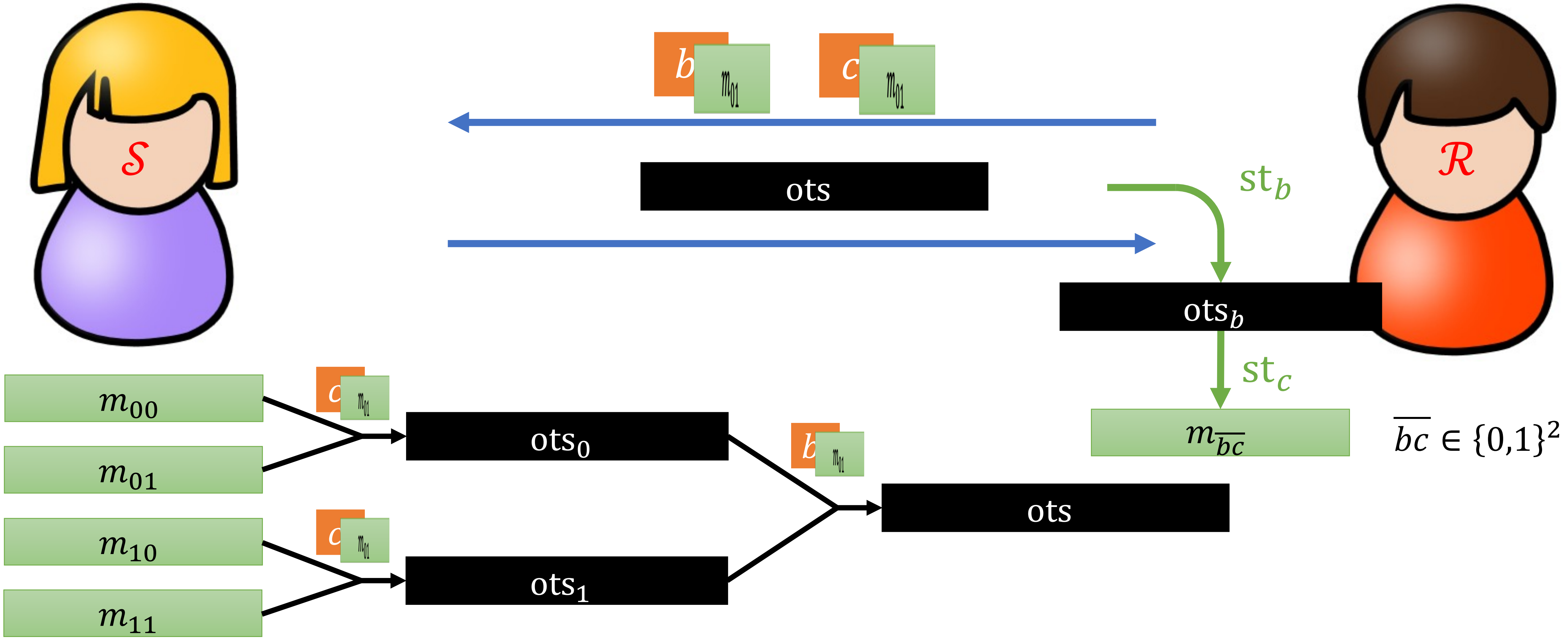
Rate-1 OT from Power DDH [GHO20]



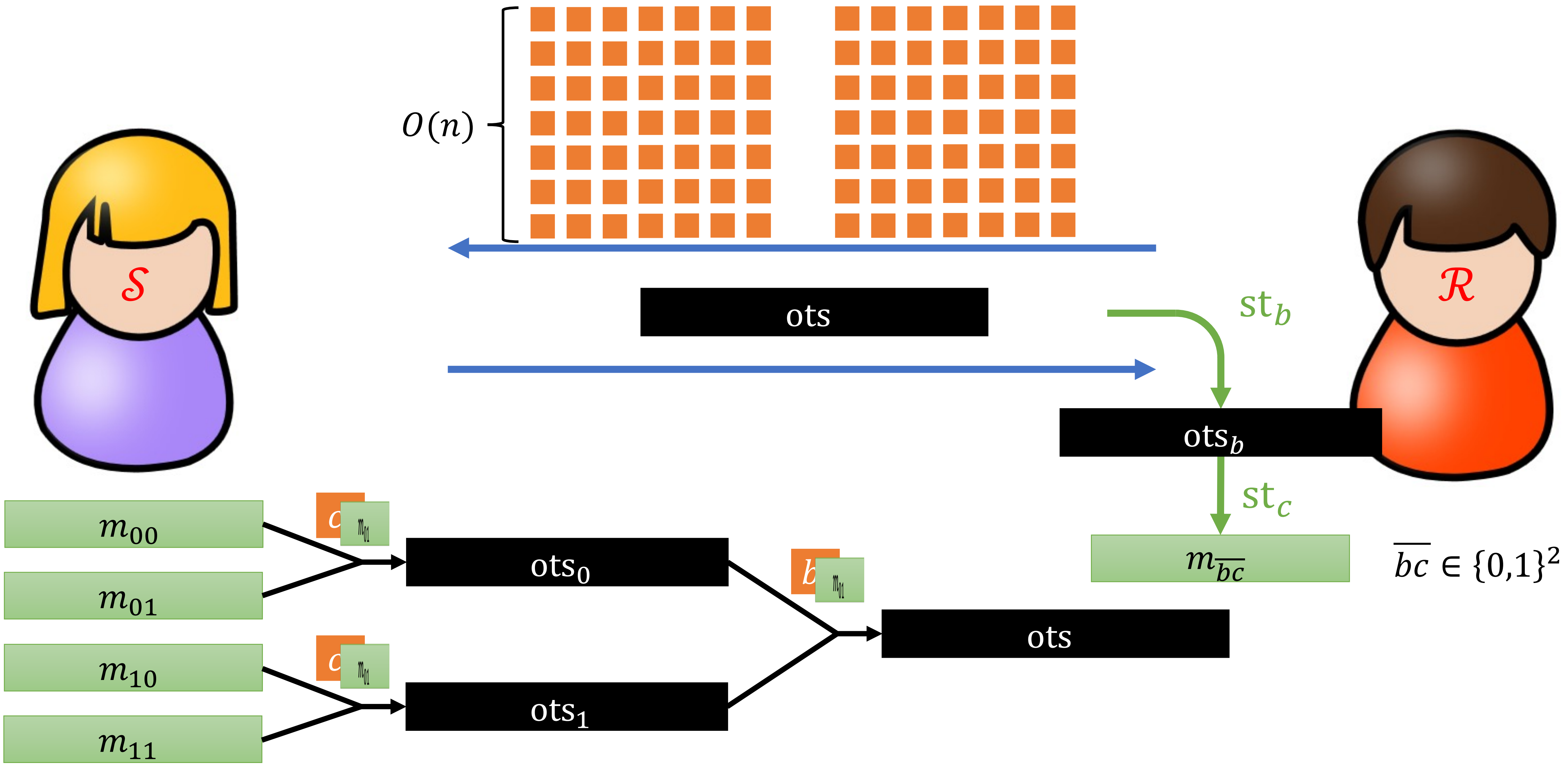
Rate-1 OT from Power DDH [GHO20]



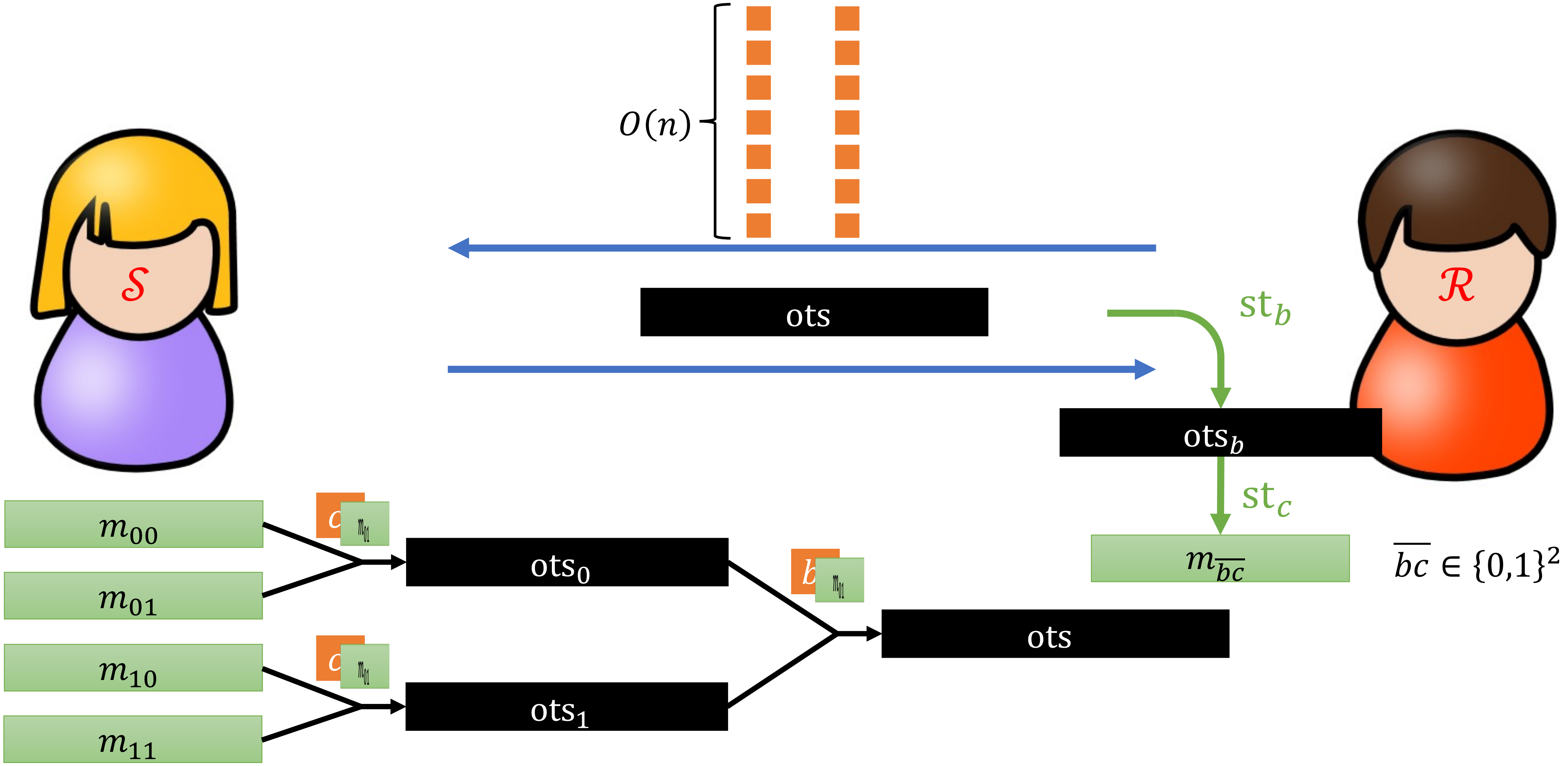
Example: 1-out-of-4 OT



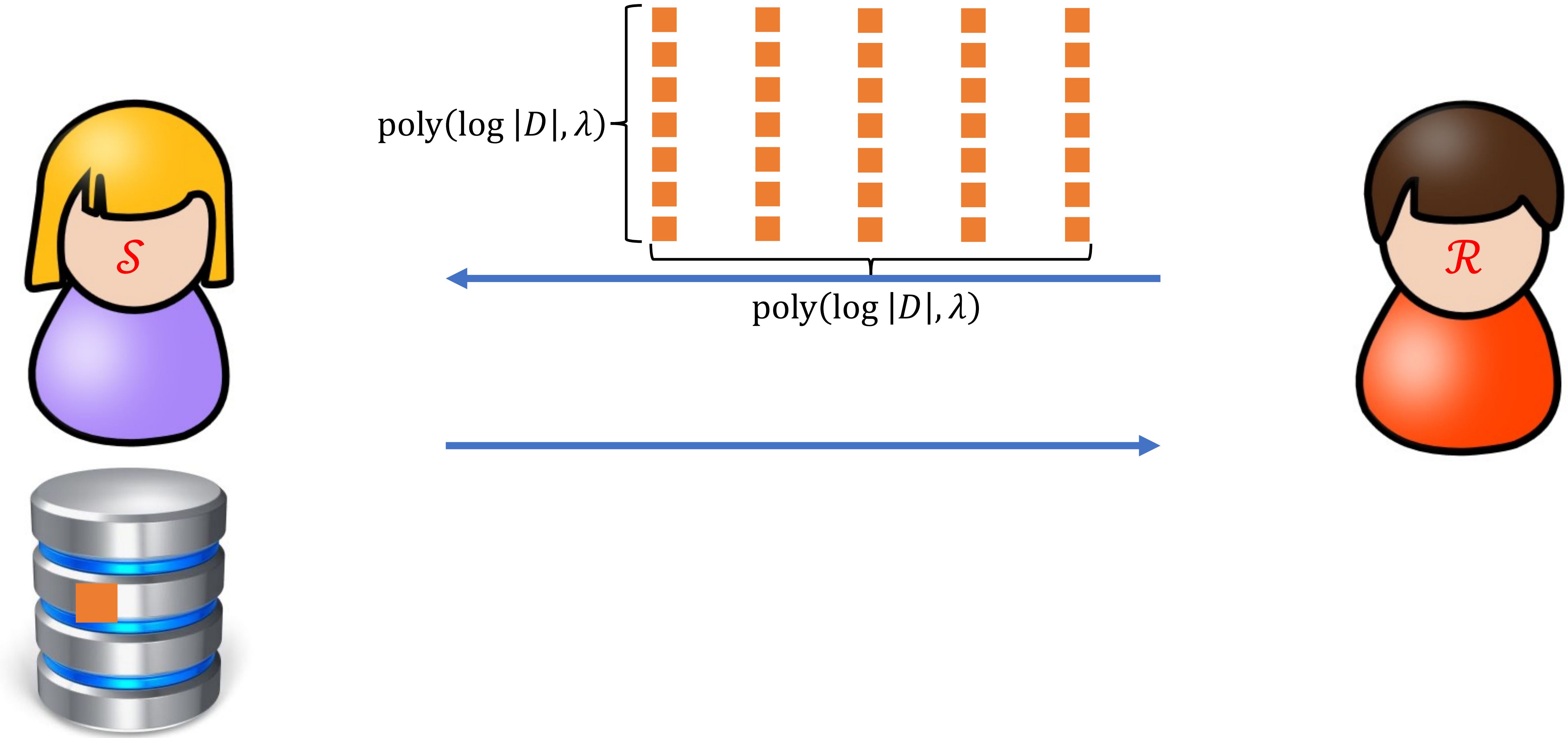
1-out-of-4 OT from DDH [DGIMMO19]



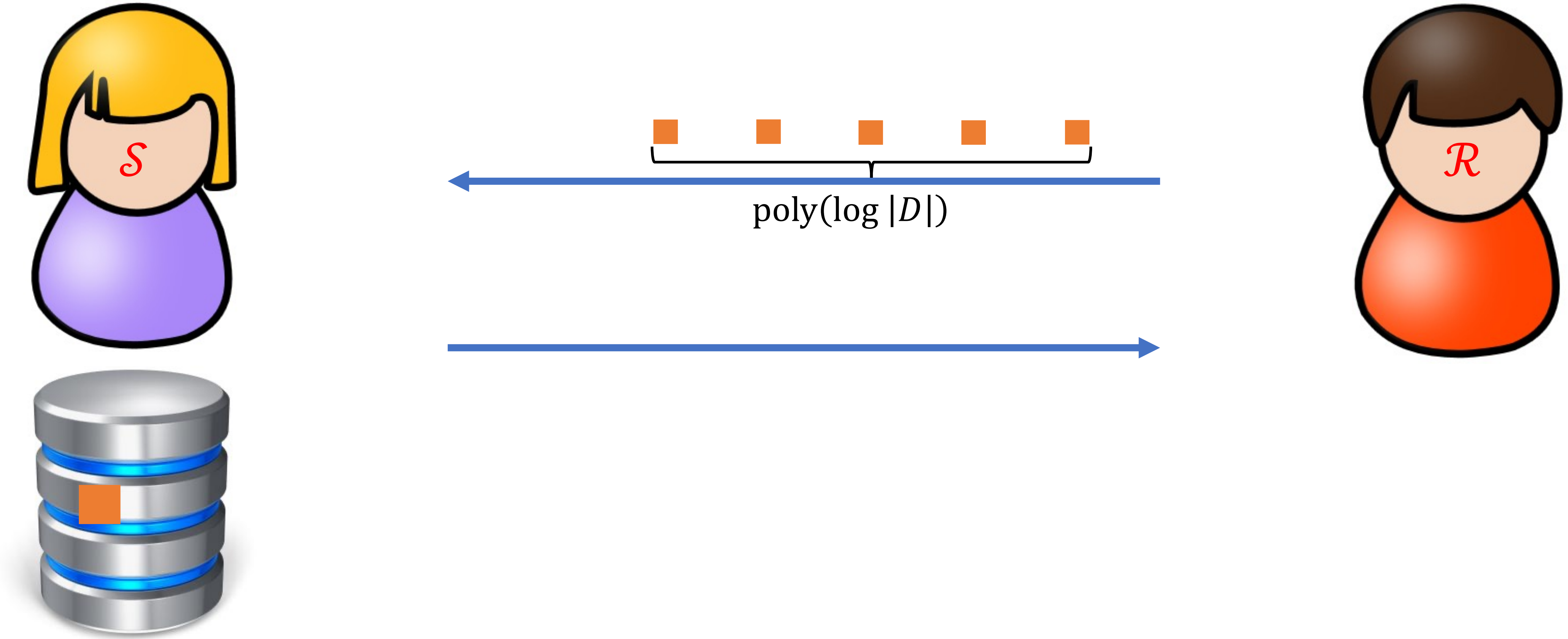
1-out-of-4 OT from Power DDH [DGIMMO19]



Applications from Power DDH [GHO20]

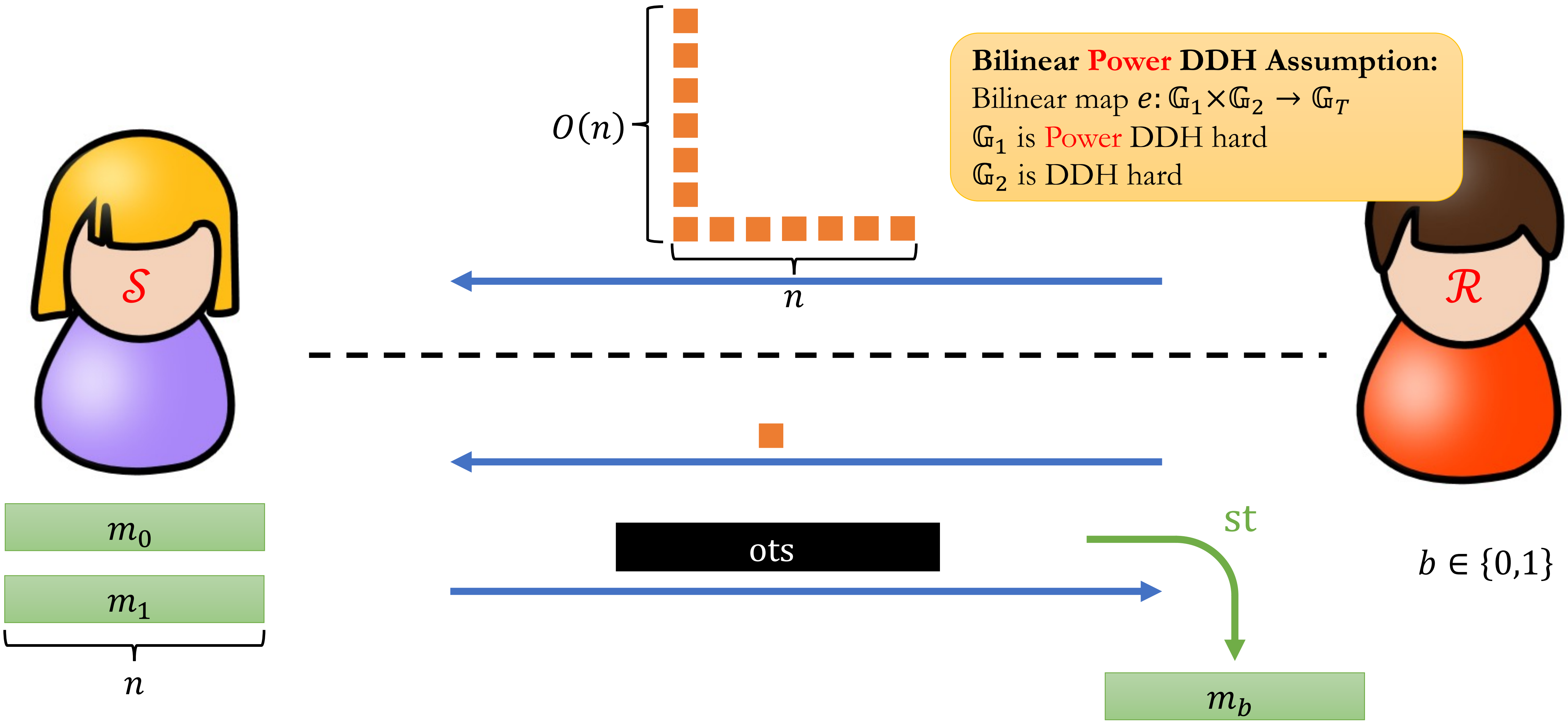


Reduce receiver communication?

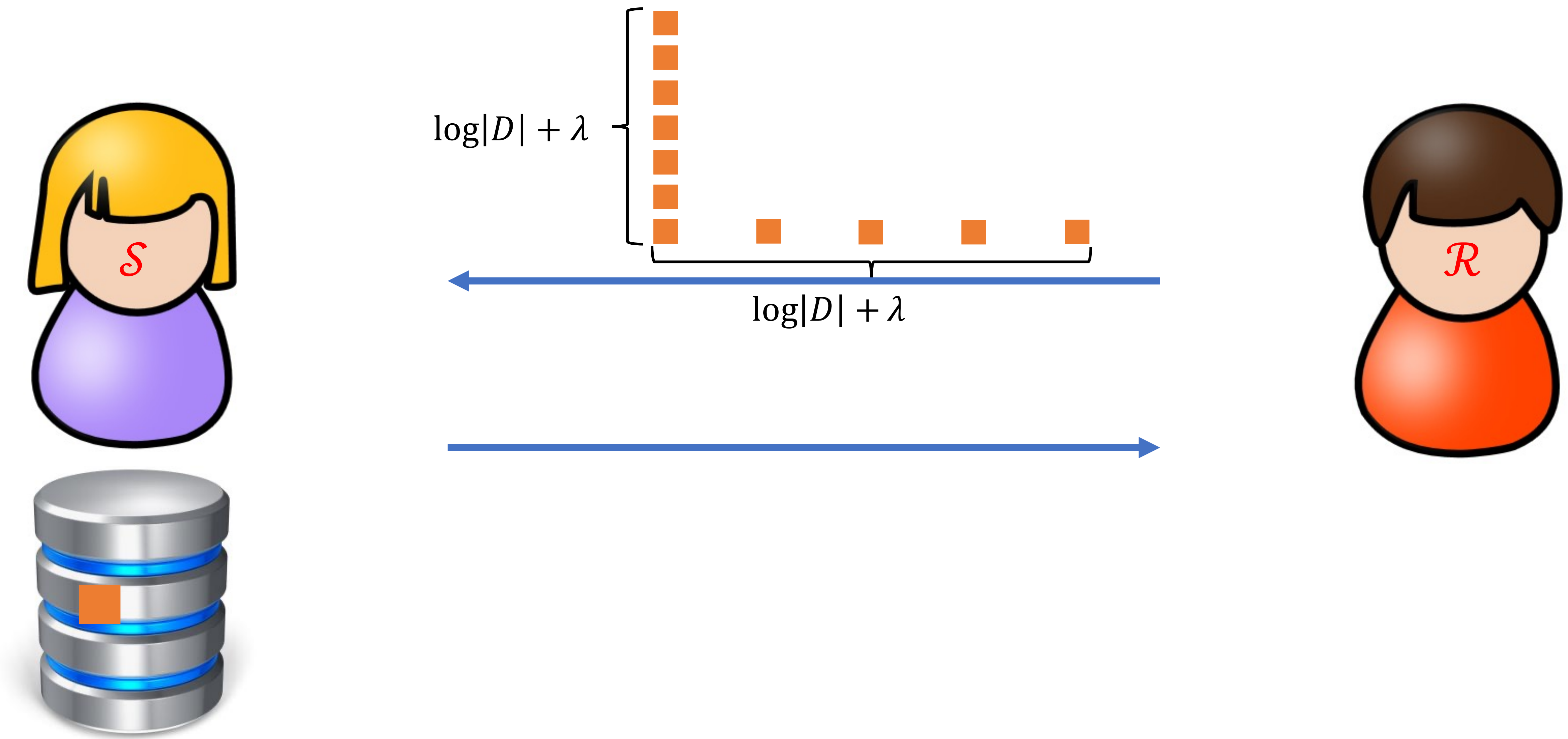


Our Results: Amortized Rate-1 OT

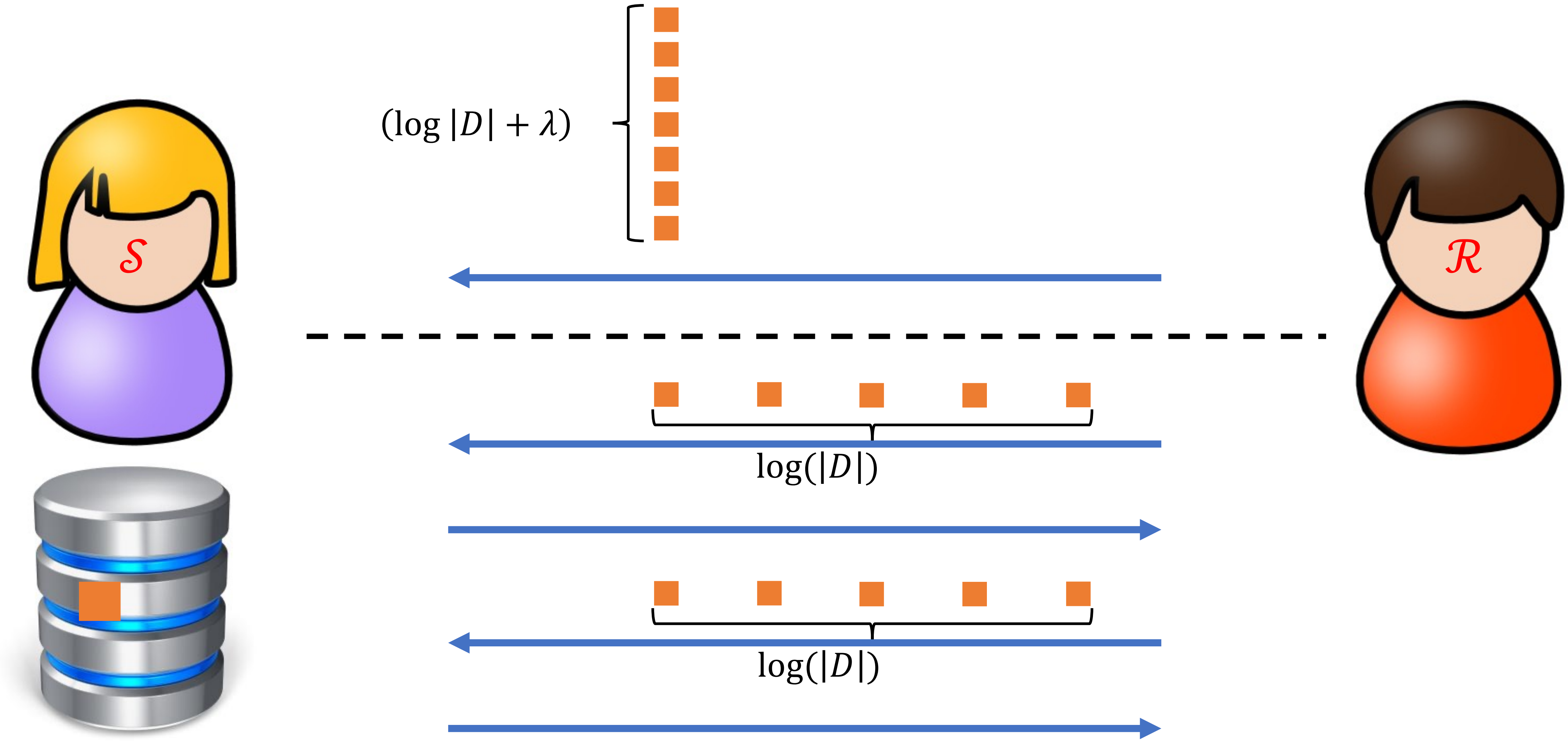
Bilinear Power DDH Assumption:
Bilinear map $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$
$\mathbb{G}_1$ is Power DDH hard
$\mathbb{G}_2$ is DDH hard



Our Results: Applications from Bilinear Power DDH



Our Results: Applications from Bilinear Power DDH



Summary

Problem	Work	Receiver Offline	Receiver Online	Assumption
Rate-1 OT	[DGIMMO19]	N/A	$O(n^2)$	DDH
Amortized Rate-1 OT	Ours	$O(n^2)$	$O(1)$	Bilinear SXDH
Rate-1 OT	[GHO20]	N/A	$O(n)$	Power DDH
Amortized Rate-1 OT	Ours	$O(n)$	$O(1)$	Bilinear Power DDH
Single-Server PIR	[GHO20]	N/A	$O(\lambda \cdot \log^2 N)$	Power DDH
Single-Server PIR	Ours	$O(\lambda \cdot \log N)$	$O(\log N)$	Bilinear Power DDH
Unbalanced PSI	[GHO20]	N/A	$O(\lambda \cdot \log^2 N \cdot m)$	Power DDH
Unbalanced PSI	Ours	$O(\lambda \cdot \log N)$	$O(\log N \cdot m)$	Bilinear Power DDH

More optimizations in the paper!

Open Problems

- Amortized Rate-1 OT from other assumptions
- Amortized Rate-1 OT extension (ongoing work)
- Applications
  - More applications of amortized Rate-1 OT
  - Concretely efficient implementation of the applications

Thank you!