Amortizing Rate-1 OT and Applications to PIR and PSI

Melissa Chase (Microsoft Research)

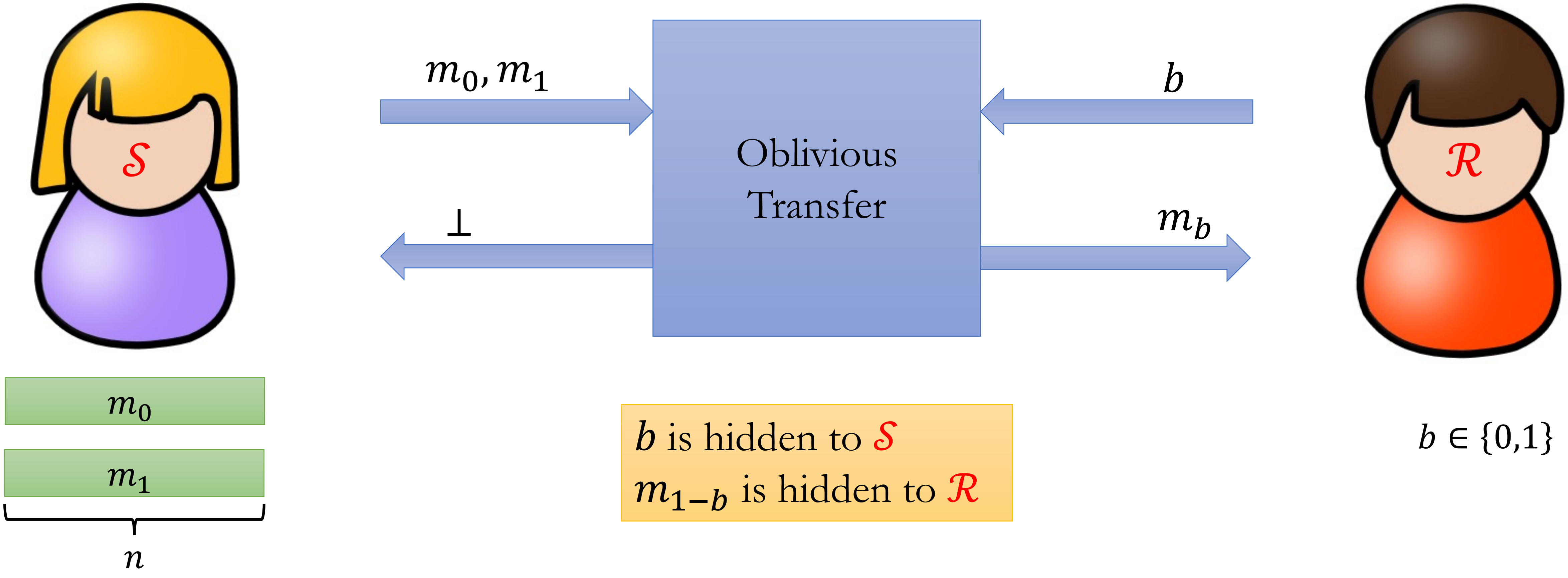
Sanjam Garg (UC Berkeley and NTT Research)

Mohammad Hajiabadi (University of Waterloo)

Jialin Li (UC Berkeley)

Peihan Miao (University of Illinois at Chicago)

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



$\mathcal{S}$

m_0, m_1

$\perp$

Oblivious Transfer

b

m_b

$\mathcal{R}$

m_0

m_1

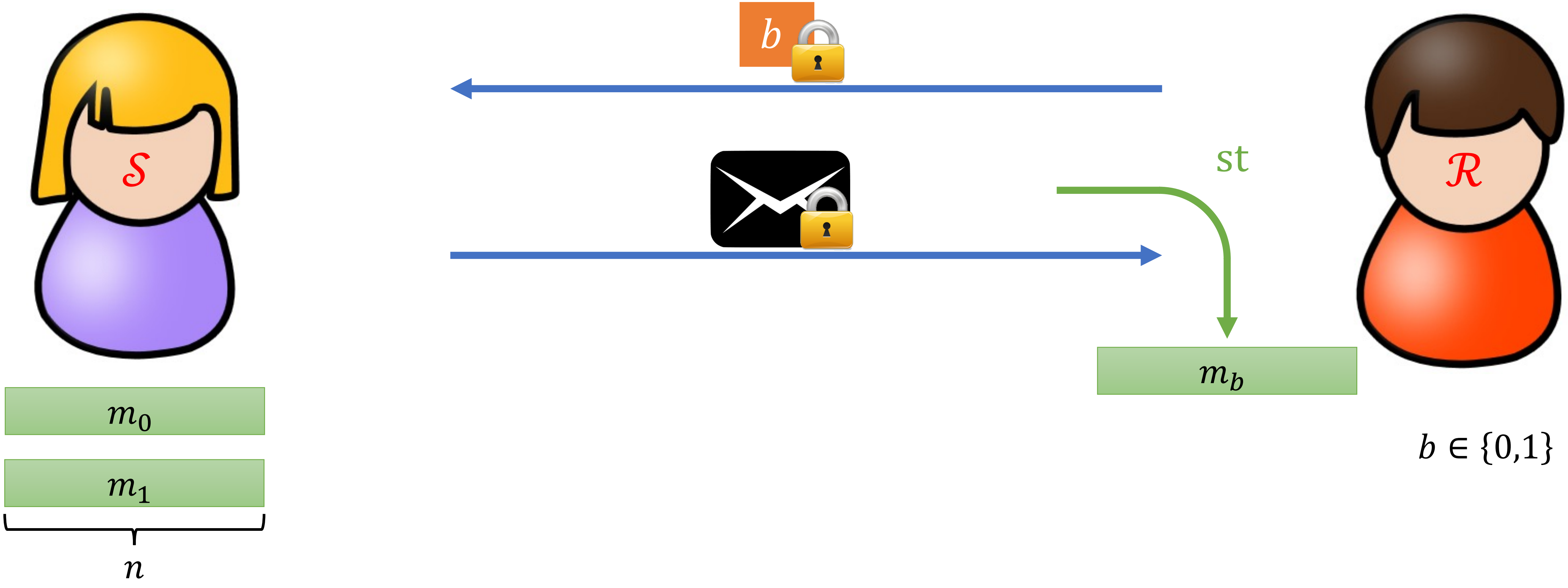
n

b is hidden to $\mathcal{S}$

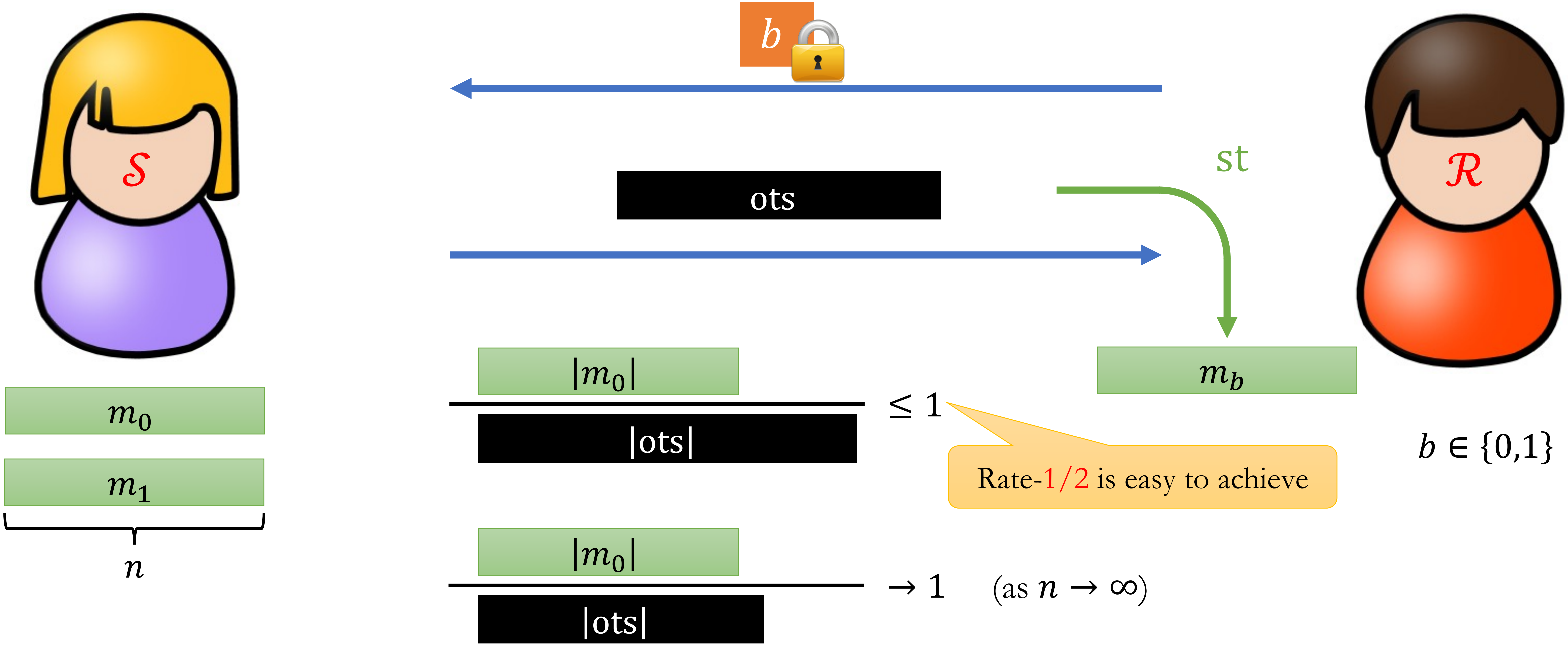
m_{1-b} is hidden to $\mathcal{R}$

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

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



Rate-1 OT [IP07, DGIMMO19, GHO20]



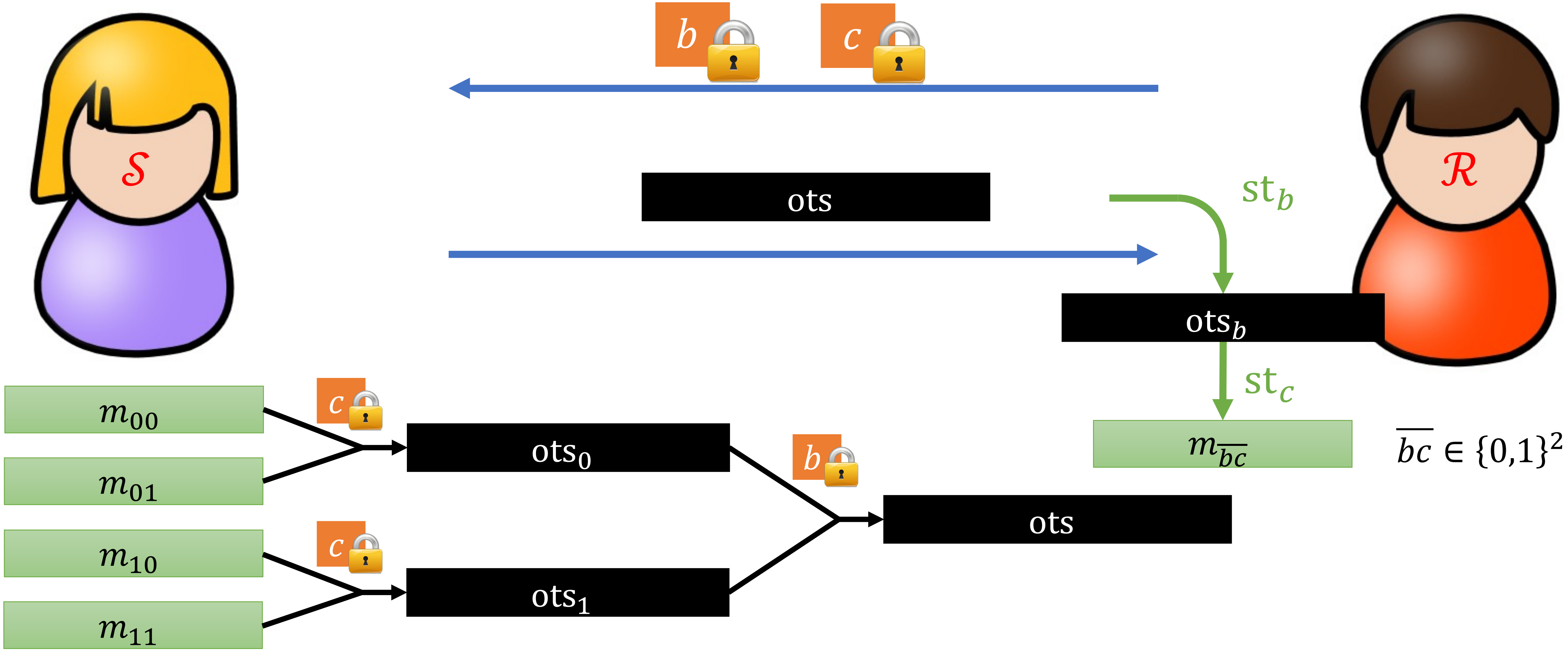
$\frac{|m_0|}{|\text{ots}|} \leq 1$

Rate-1/2 is easy to achieve

$\frac{|m_0|}{|\text{ots}|} \to 1$ (as $n \to \infty$)

Why two-message? Why rate-1?

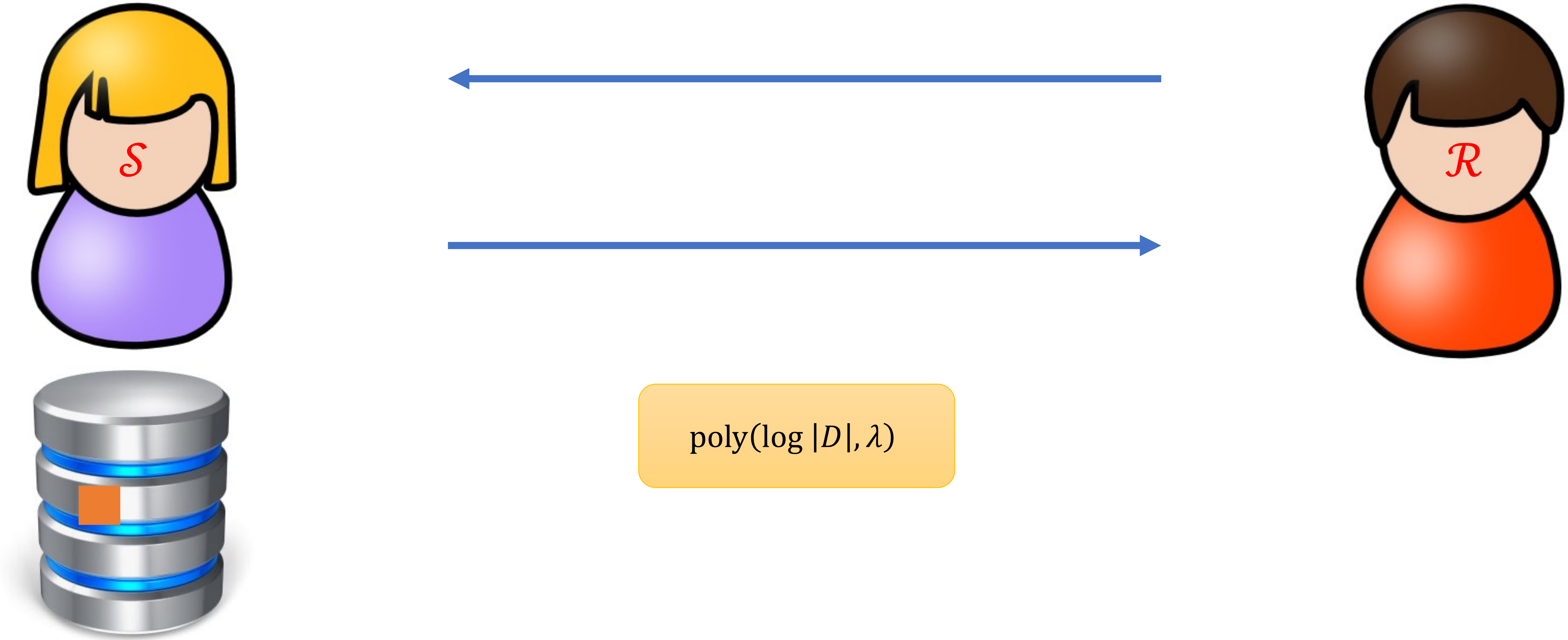
Example: 1-out-of-4 OT



Why two-message? Why rate-1?

Nested OT with low communication

Applications of Rate-1 OT



$\mathrm{poly}(\log |D|, \lambda)$

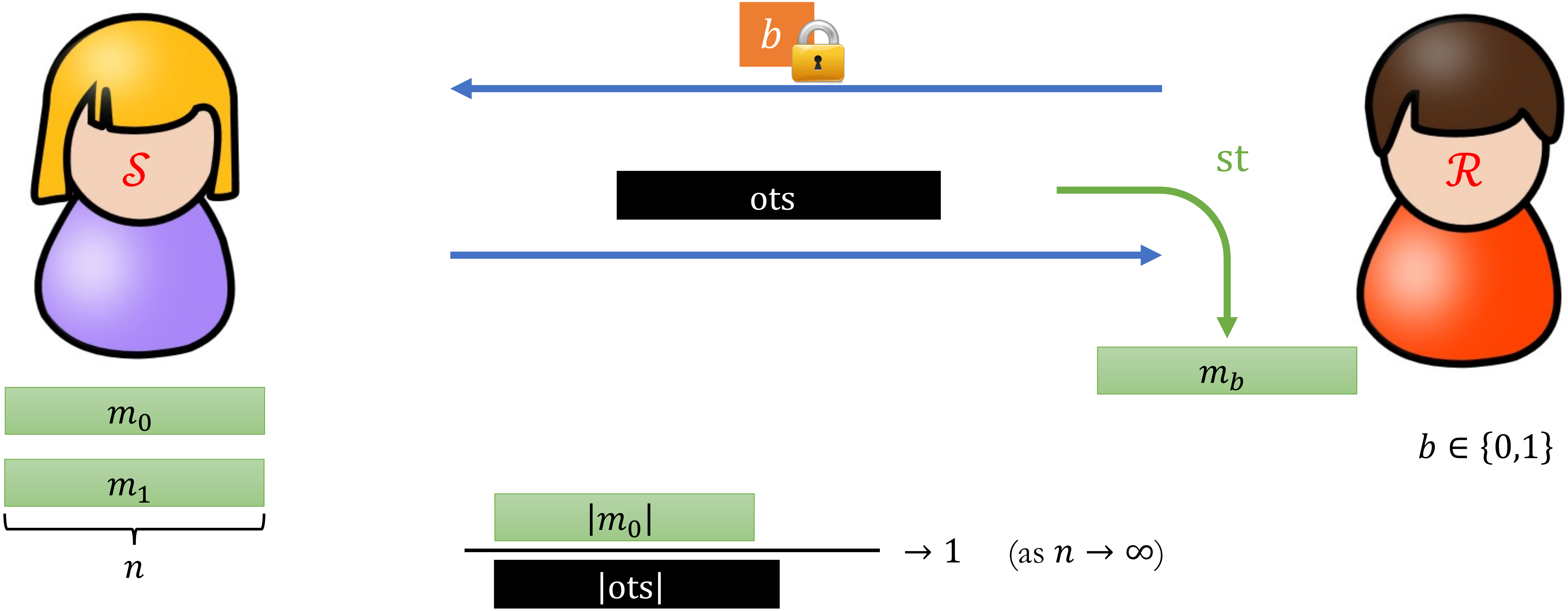
Applications of Rate-1 OT

- 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

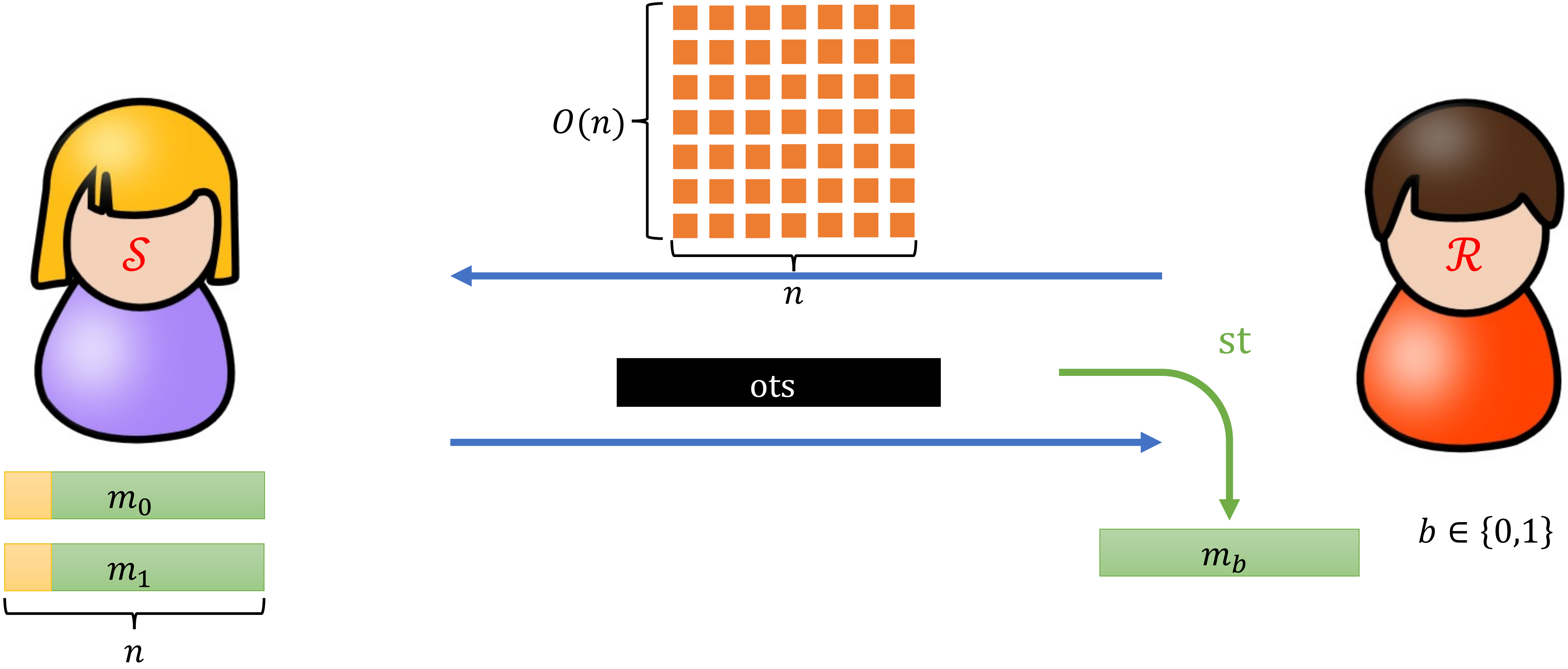
Rate-1 OT [DJ01, DGIMMO19, GHO20]



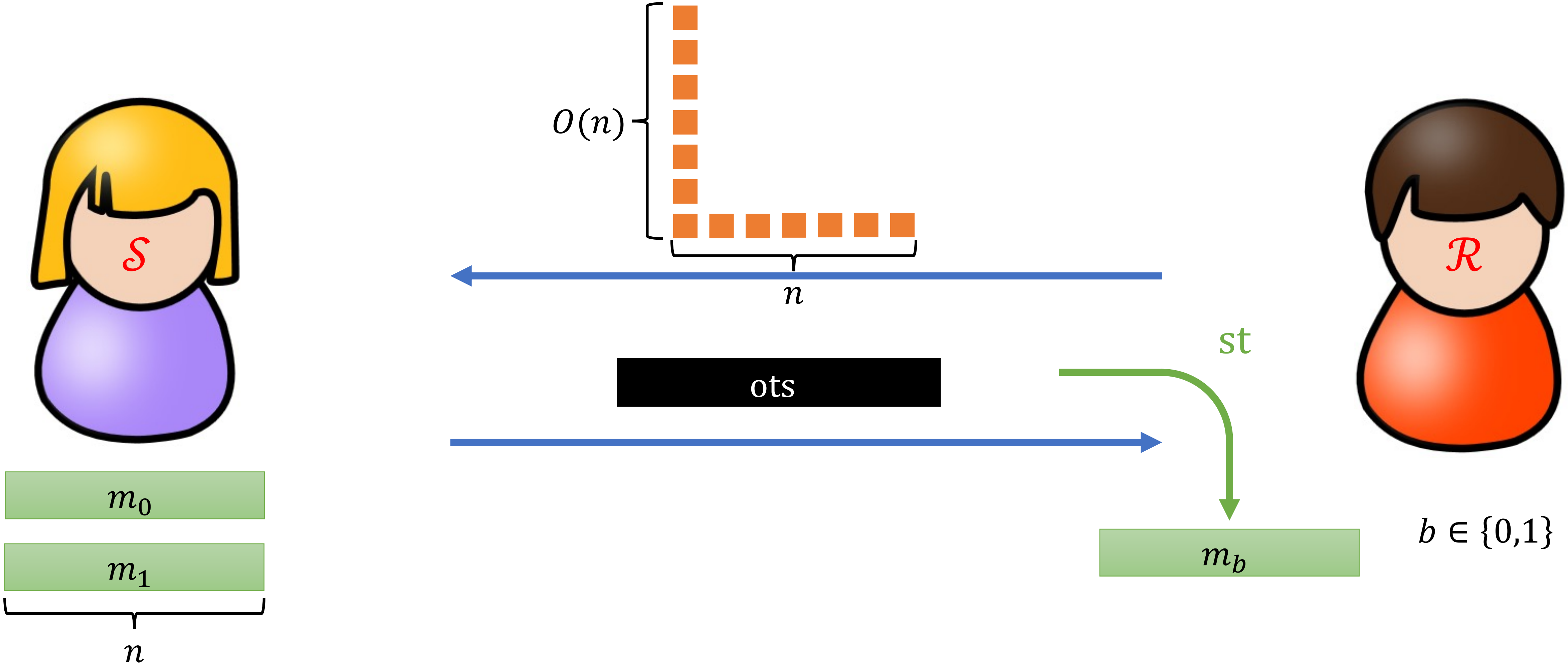
$$\frac{|m_0|}{|\text{ots}|} \to 1 \quad (\text{as } n \to \infty)$$

Receiver Communication?

Rate-1 OT from DDH [DGIMMO19]



Rate-1 OT from Power DDH [GHO20]



$\mathcal{S}$

$\mathcal{R}$

$O(n)$

n

ots

st

m_0

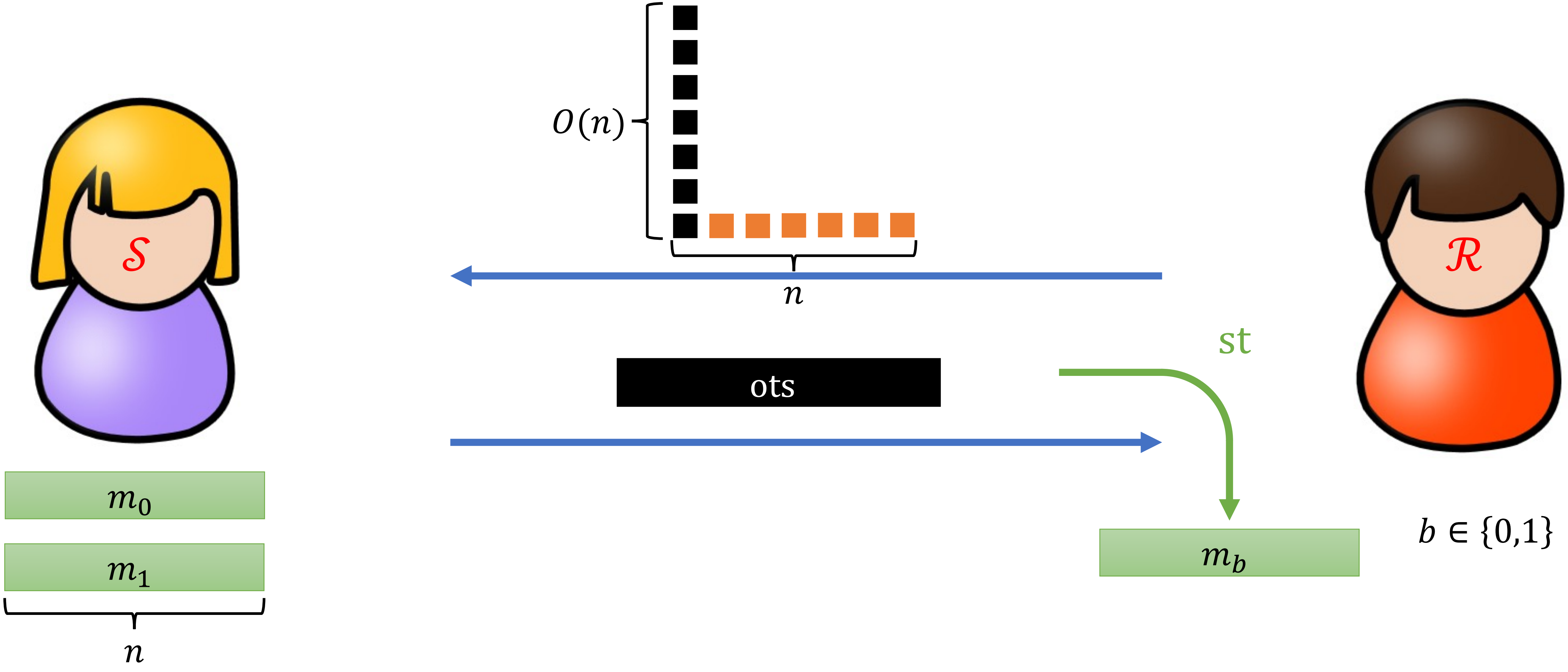
m_1

n

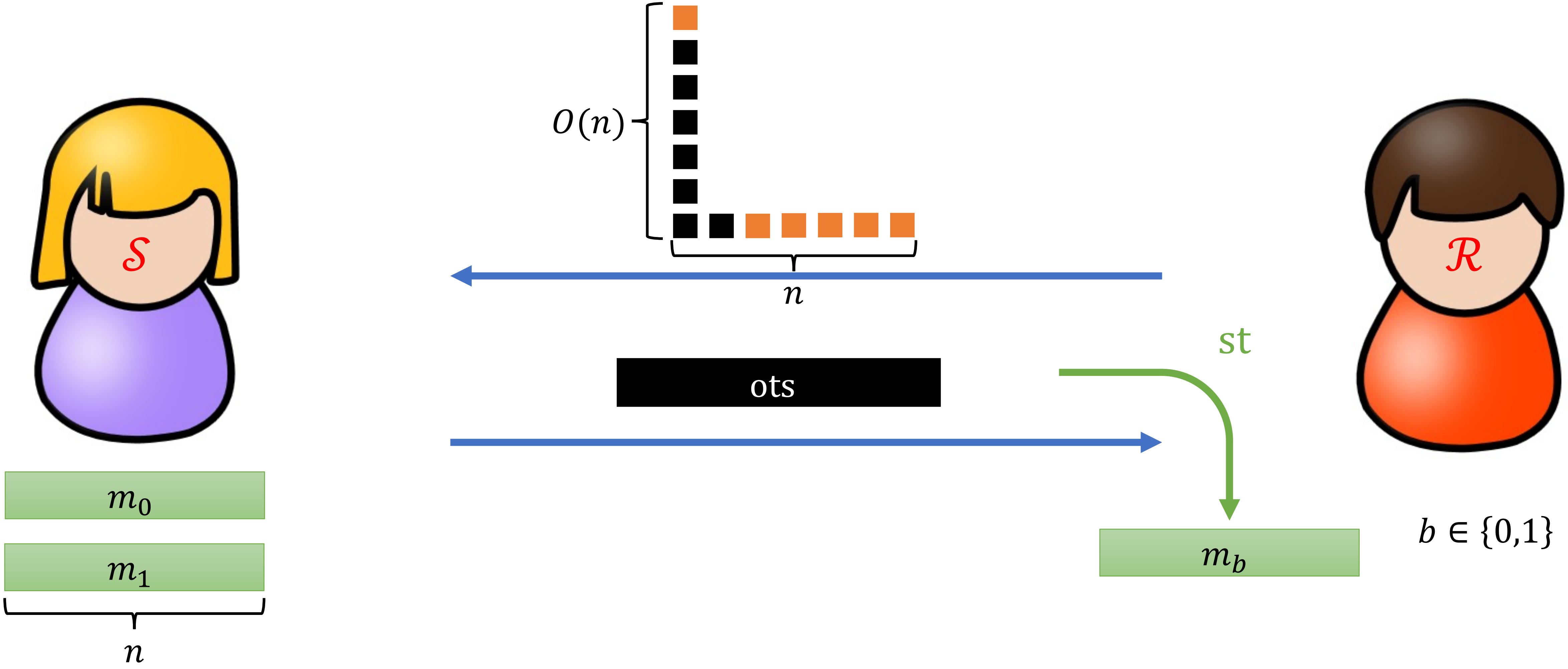
m_b

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

Rate-1 OT from Power DDH [GHO20]



Rate-1 OT from Power DDH [GHO20]



$\mathcal{S}$

$\mathcal{R}$

$O(n)$

n

ots

st

m_0

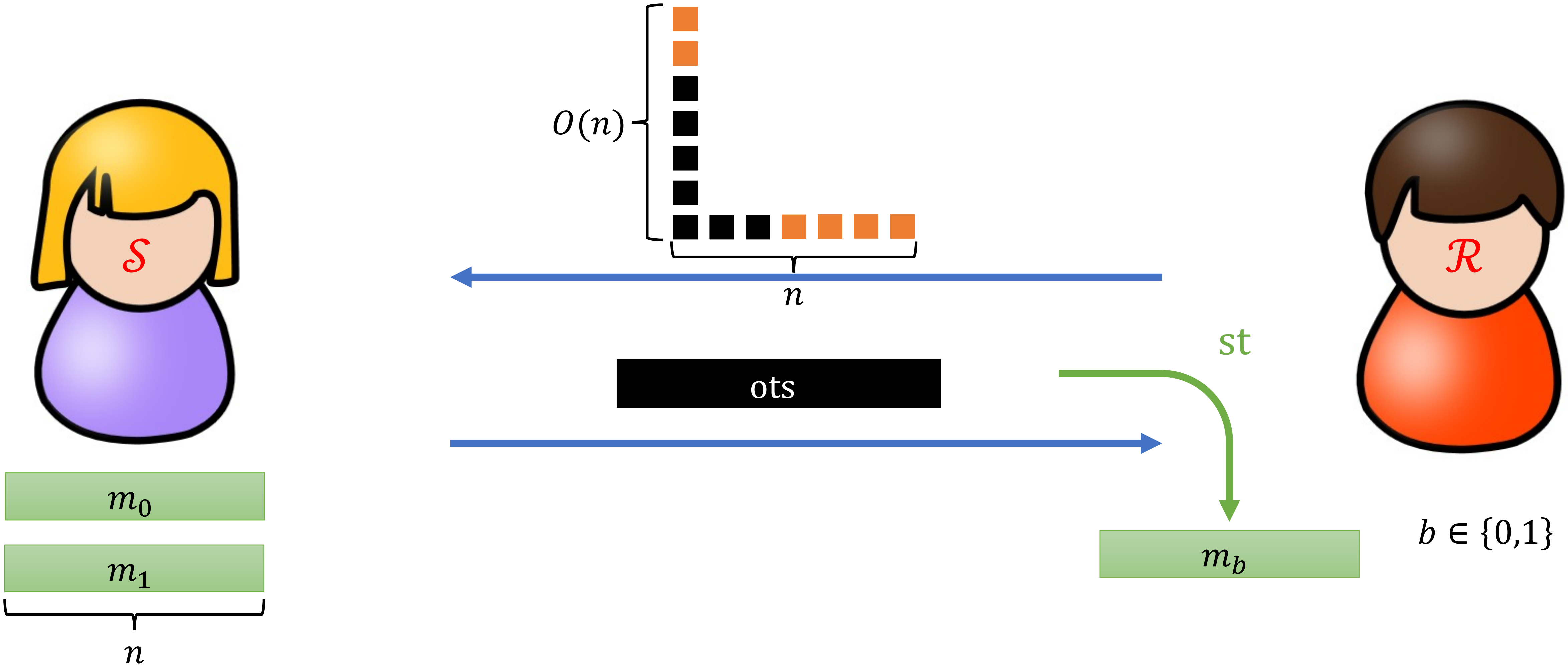
m_1

n

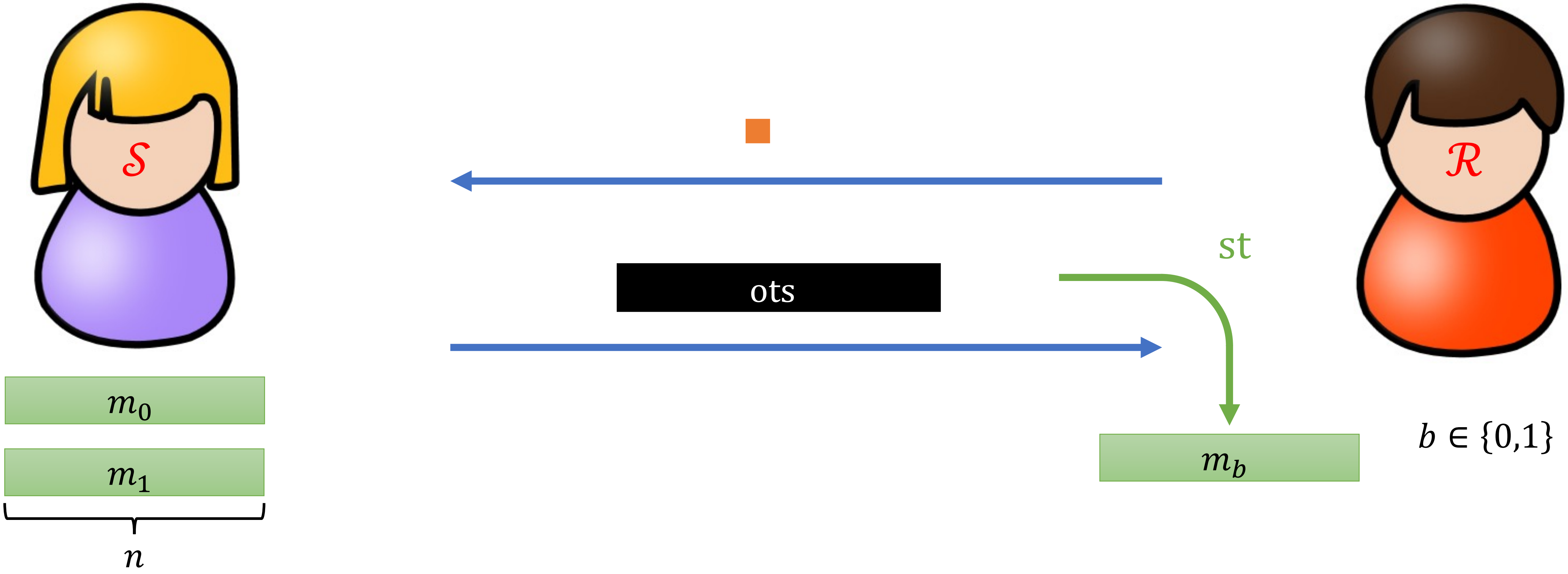
m_b

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

Rate-1 OT from Power DDH [GHO20]



Further reduce receiver communication?



$\mathcal{S}$

$\mathcal{R}$

🟧

ots

st

m_0

m_1

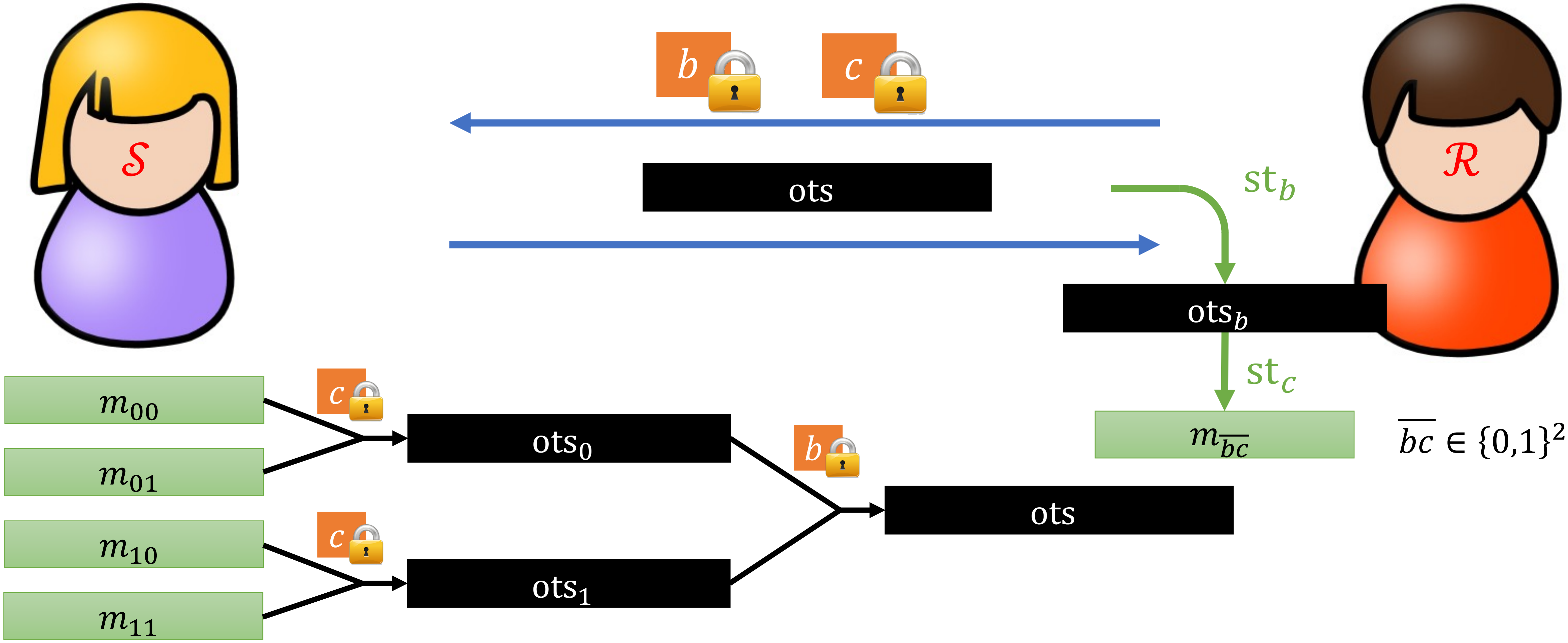
n

m_b

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

Why do we care?

Example: 1-out-of-4 OT



$\mathcal{S}$

b

c

ots

$\mathcal{R}$

st_b

ots_b

st_c

$m_{\overline{bc}}$

$\overline{bc} \in \{0,1\}^2$

m_{00}

m_{01}

m_{10}

m_{11}

c

ots_0

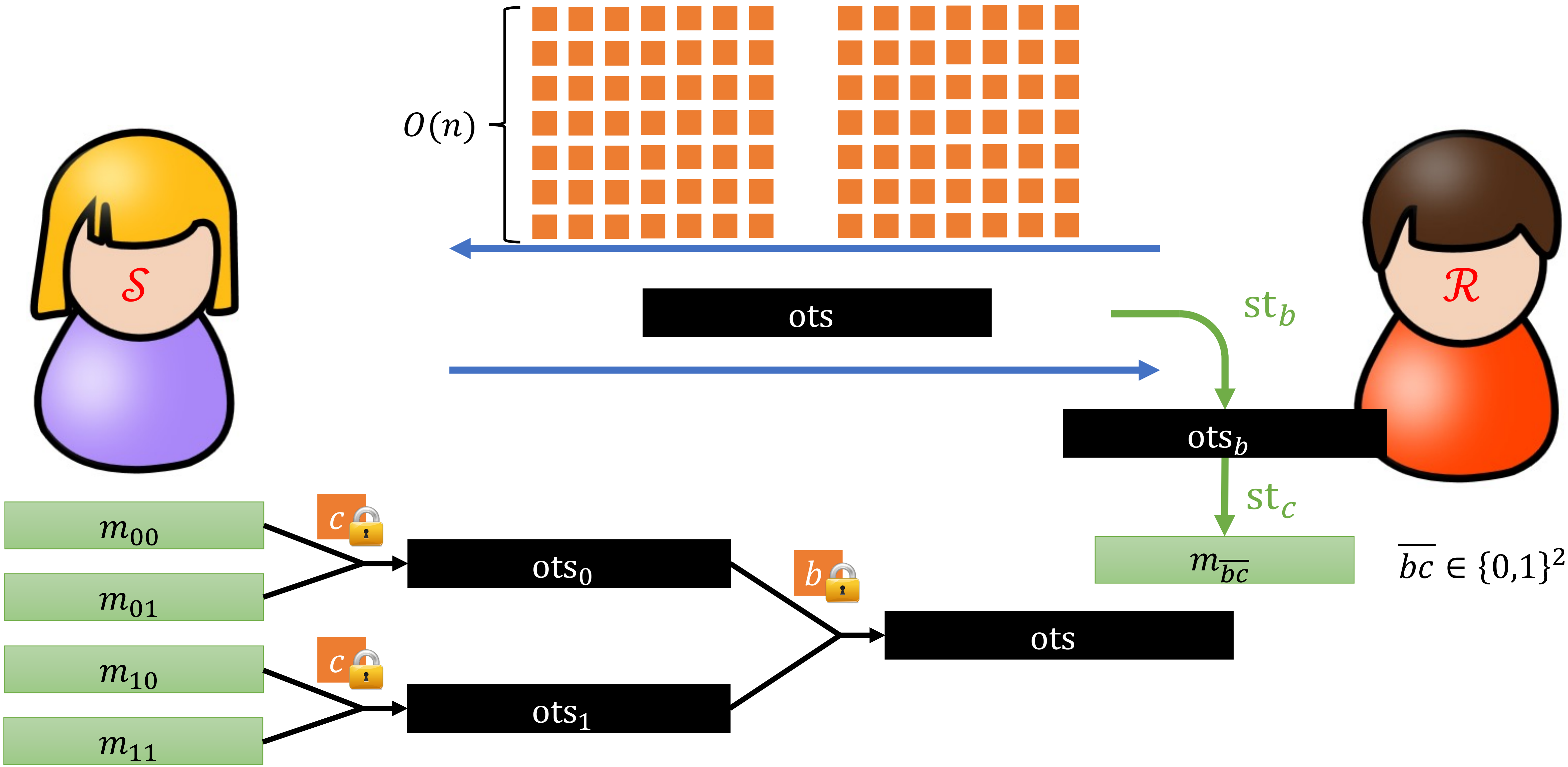
c

ots_1

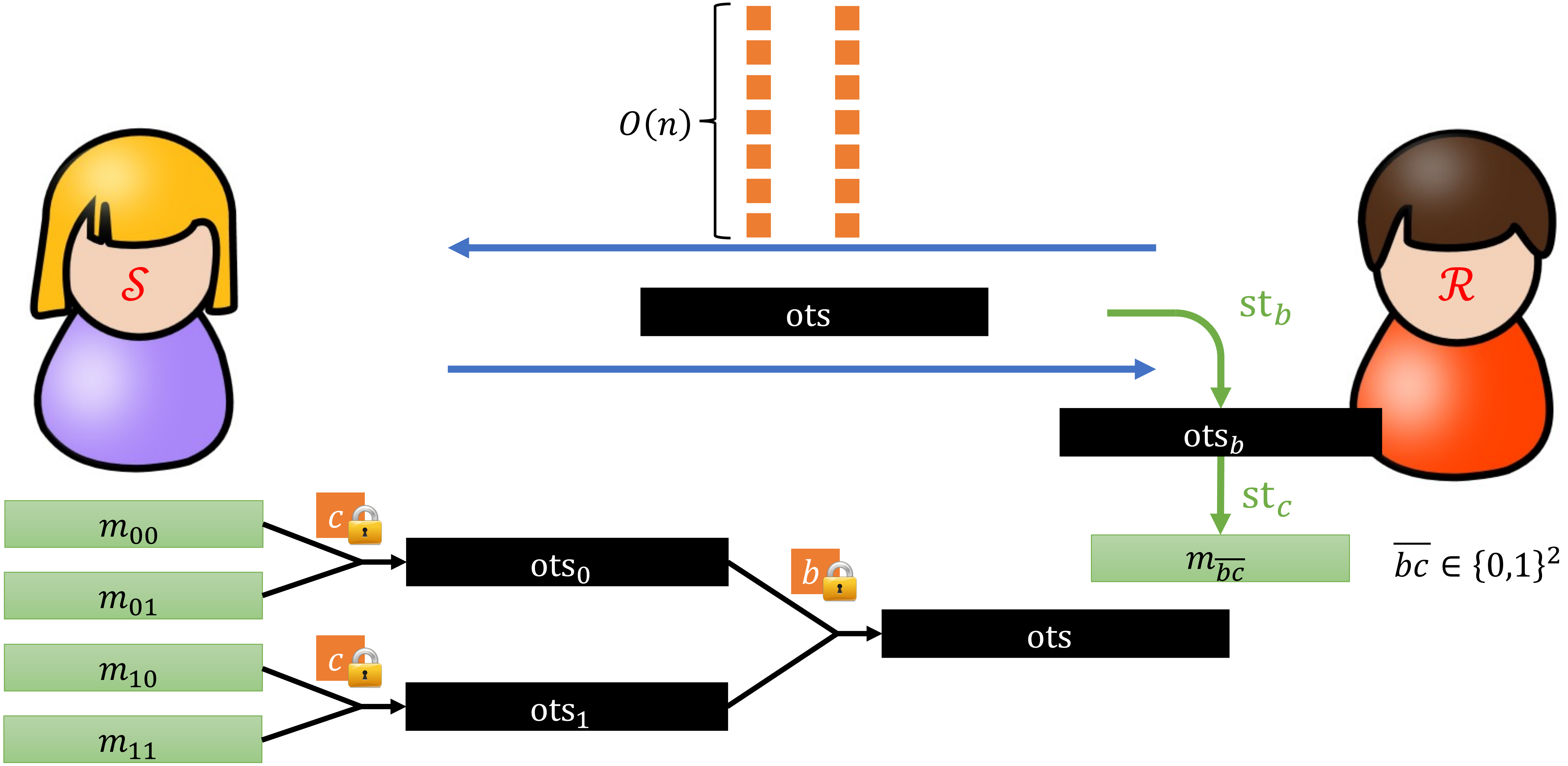
b

ots

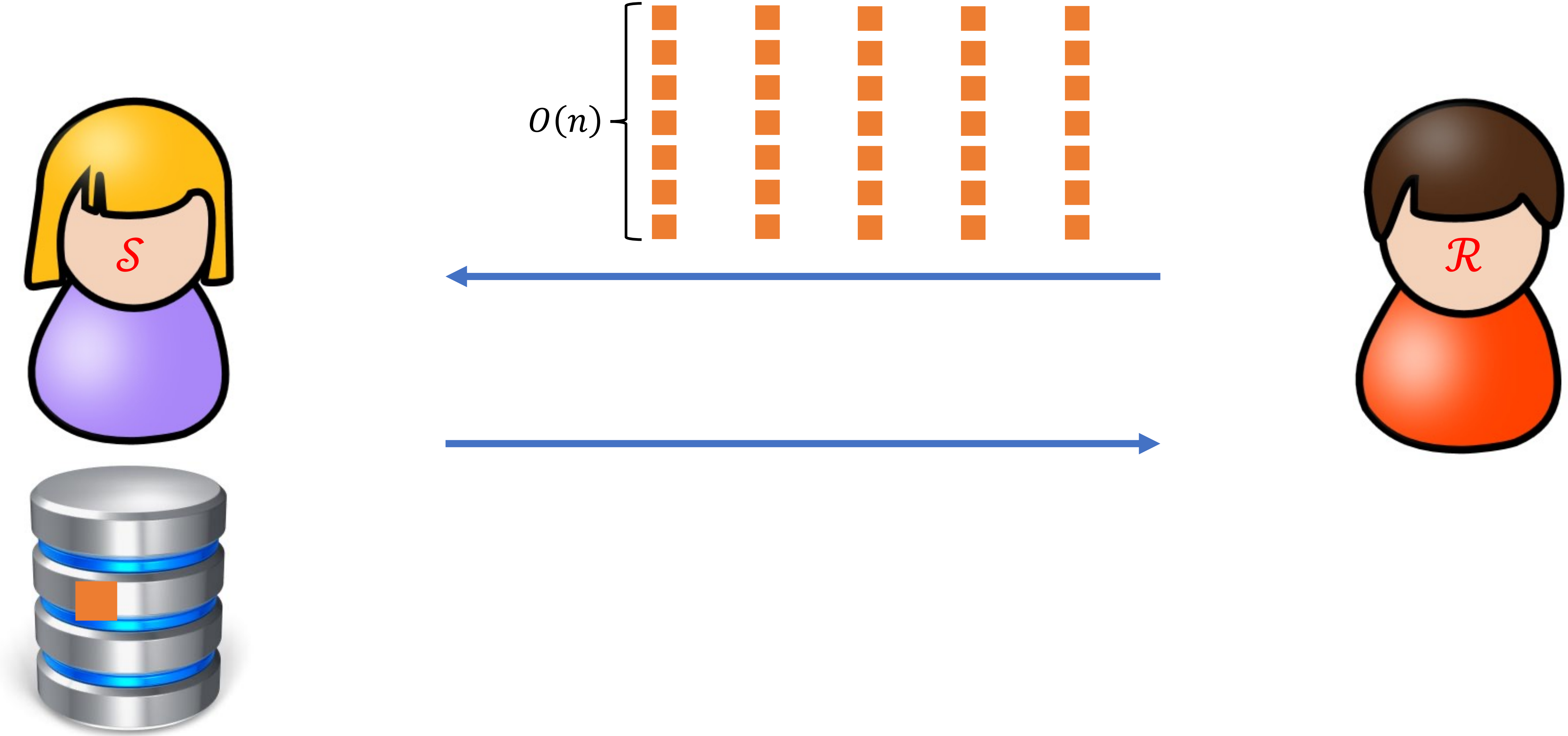
1-out-of-4 OT from DDH [DGIMMO19]



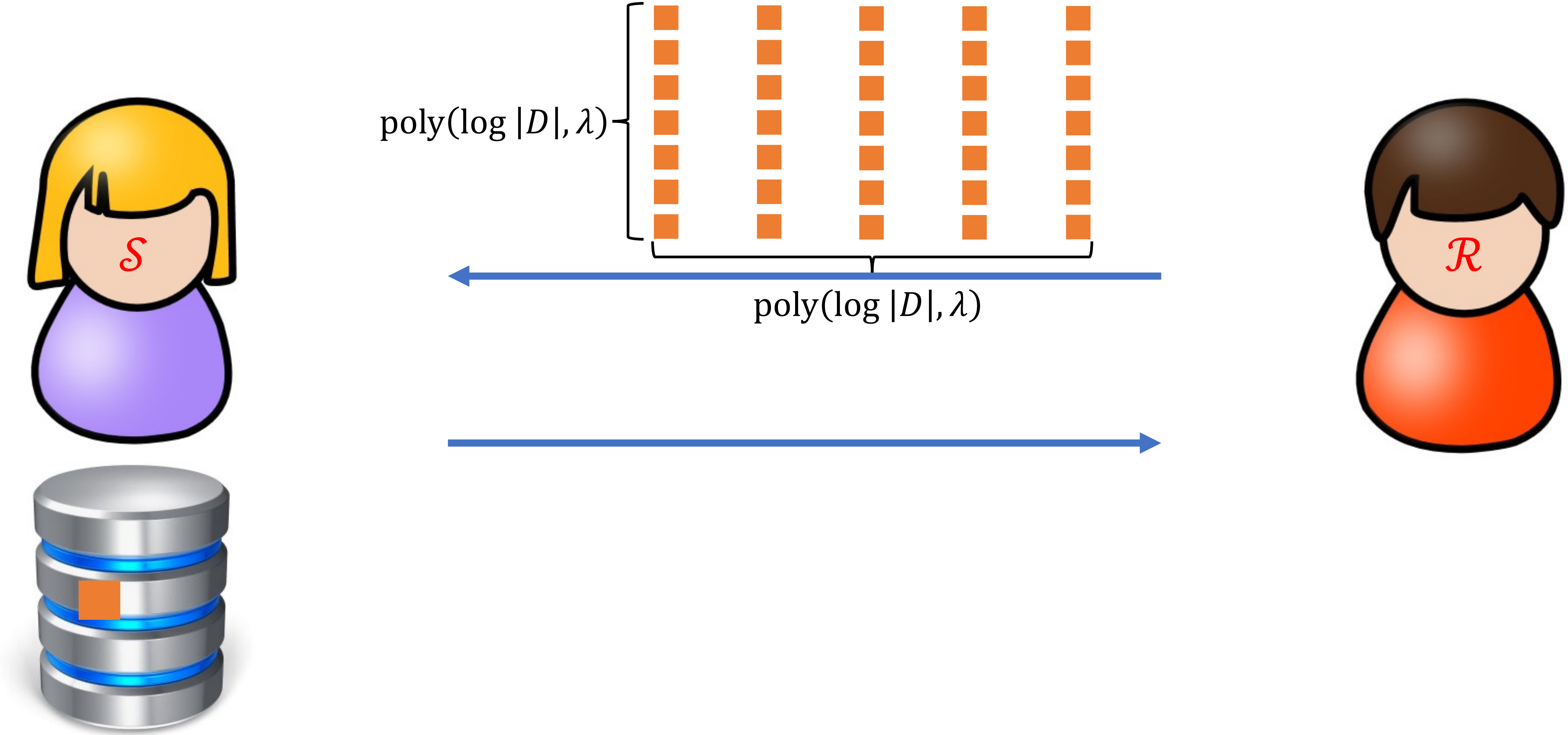
1-out-of-4 OT from Power DDH [DGIMMO19]



Applications from Power DDH [GHO20]



Applications from Power DDH [GHO20]



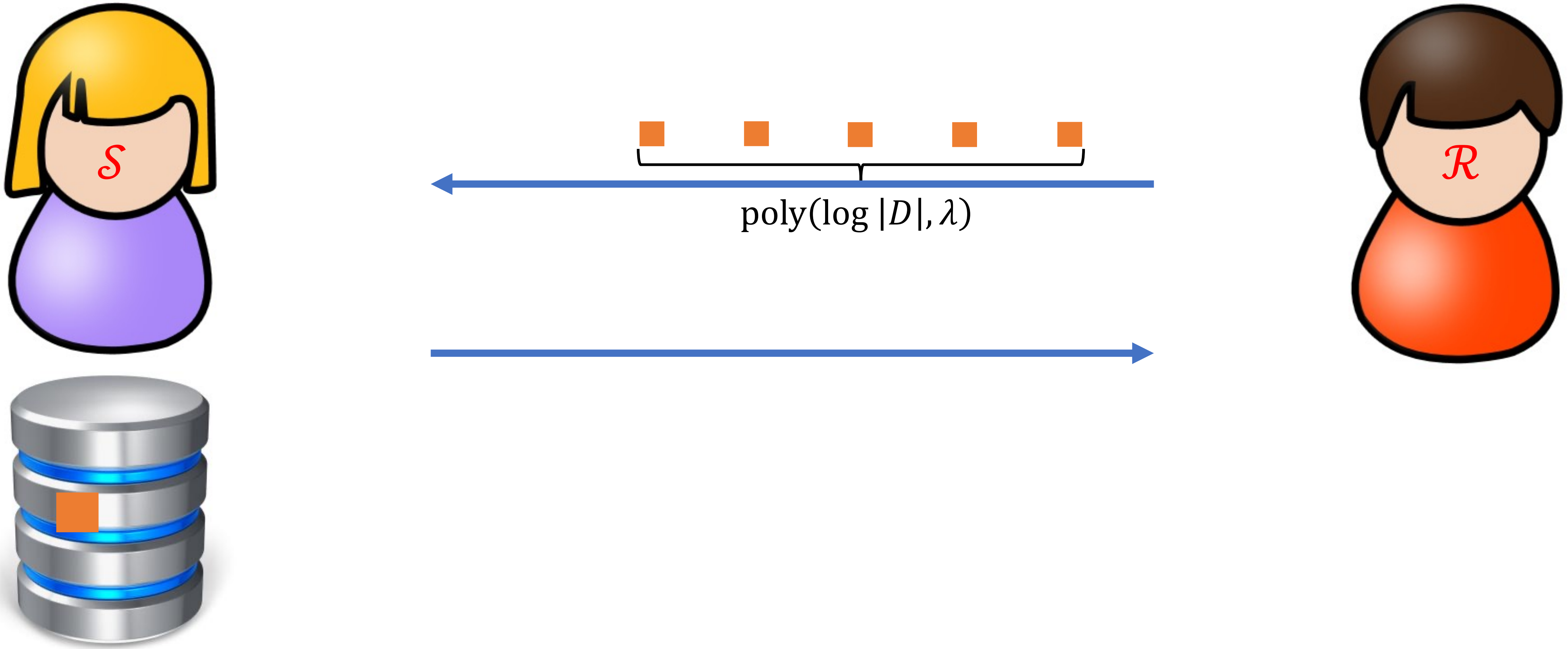
$\mathcal{S}$

$\mathcal{R}$

$\text{poly}(\log |D|, \lambda)$

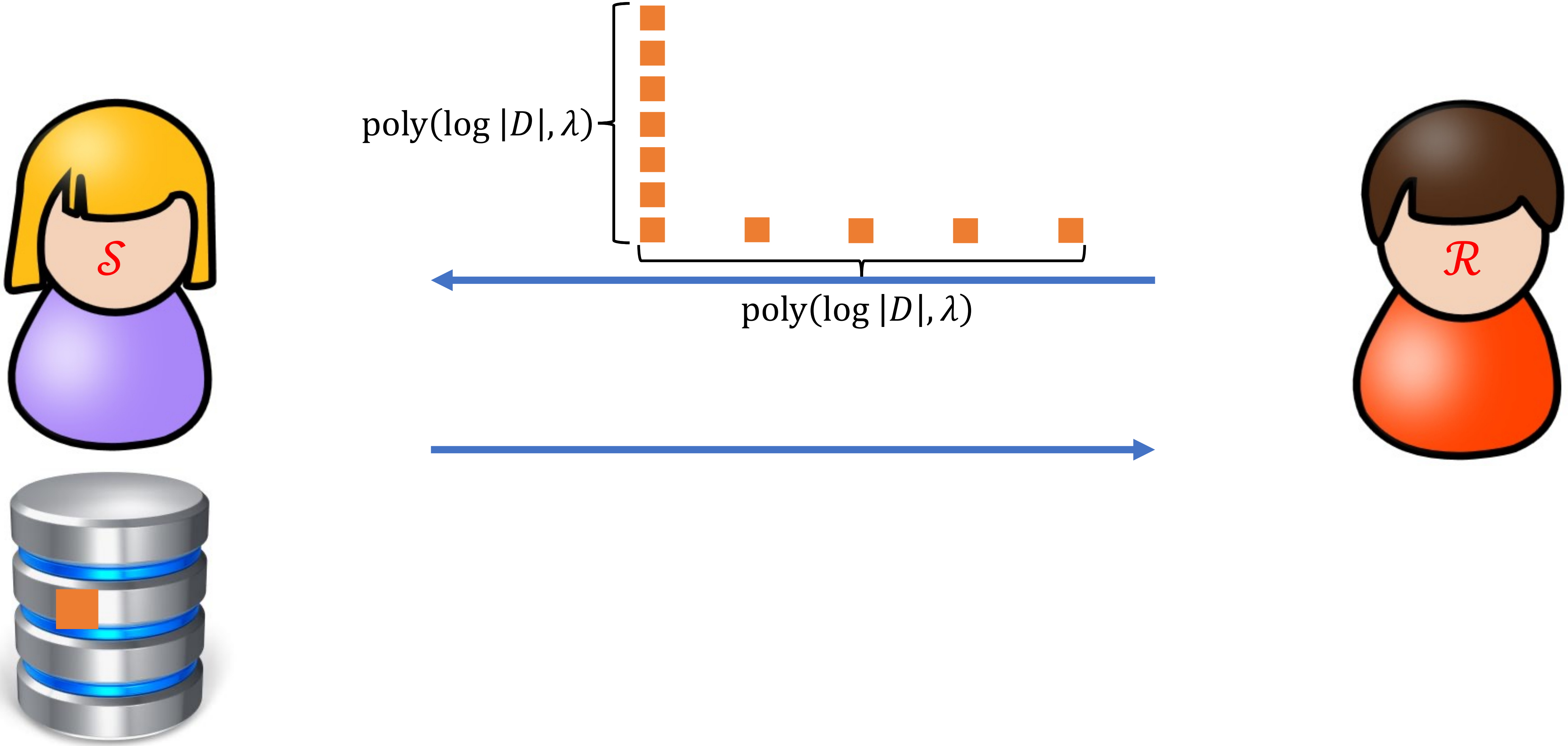
$\text{poly}(\log |D|, \lambda)$

Reduce receiver communication?

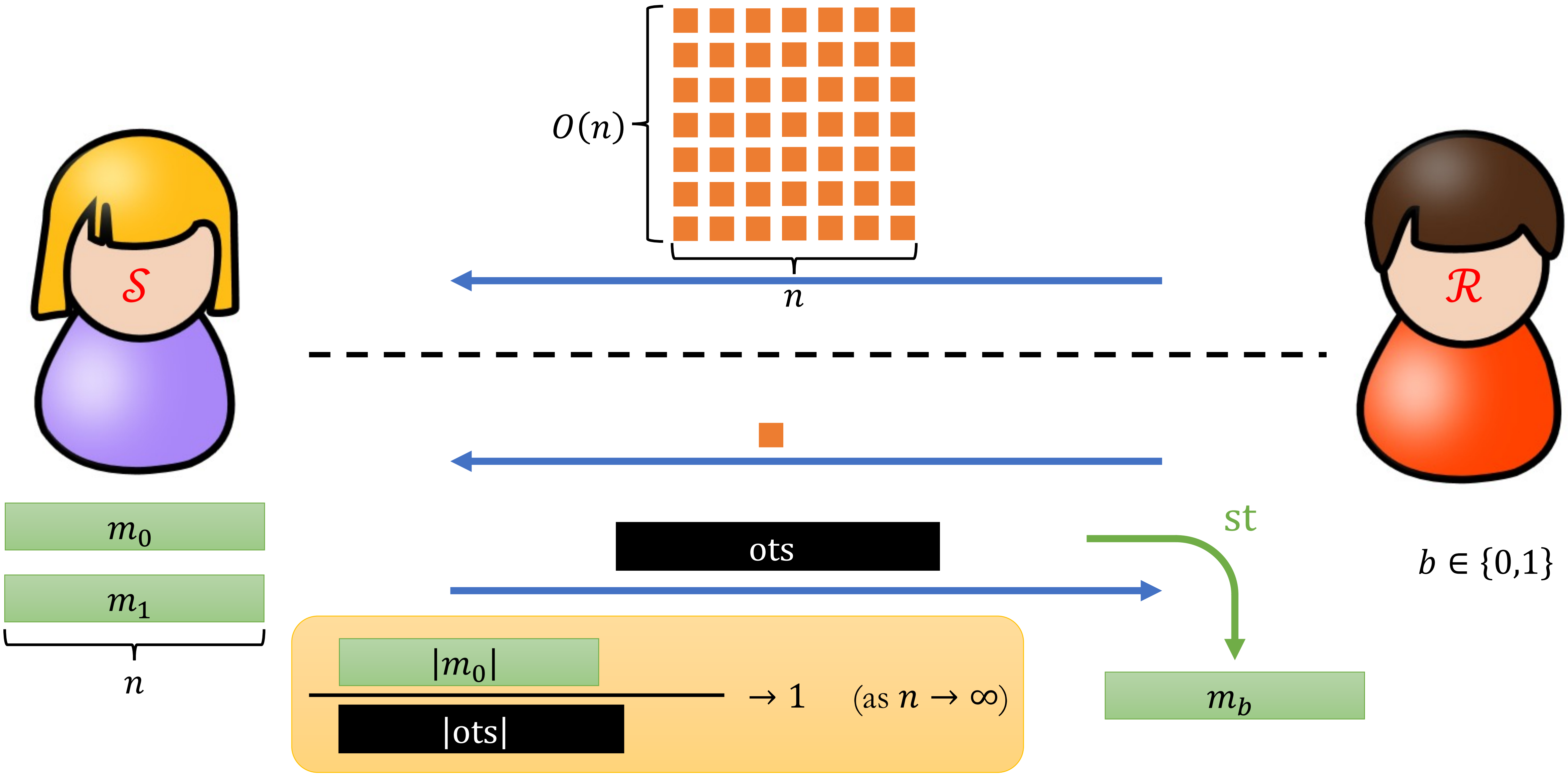


$\text{poly}(\log |D|, \lambda)$

Reduce receiver communication?


$\mathcal{S}$
$\mathcal{R}$
$\text{poly}(\log|D|, \lambda)$
$\text{poly}(\log|D|, \lambda)$

Our Results: Amortized Rate-1 OT



$O(n)$

n

$\mathcal{S}$

$\mathcal{R}$

m_0

m_1

n

ots

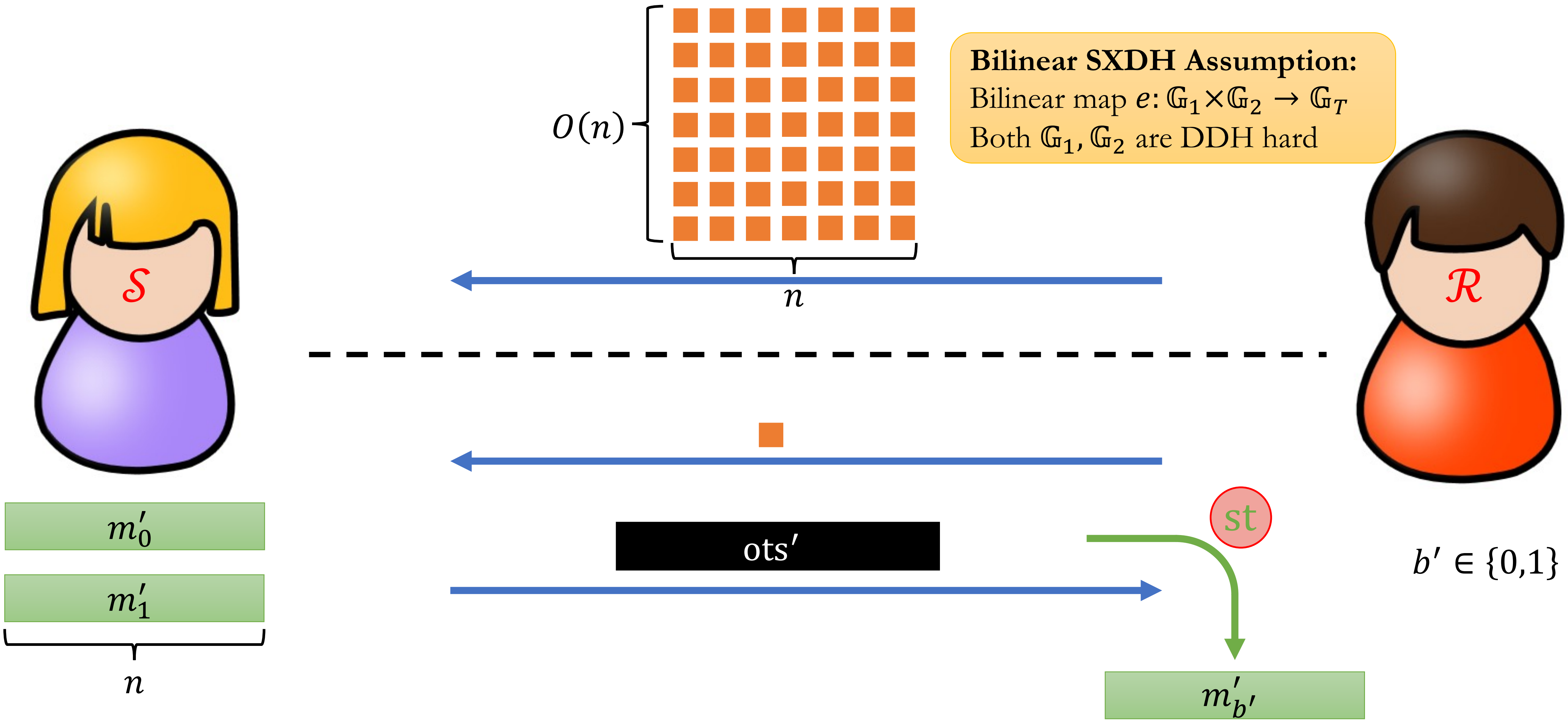
st

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

m_b

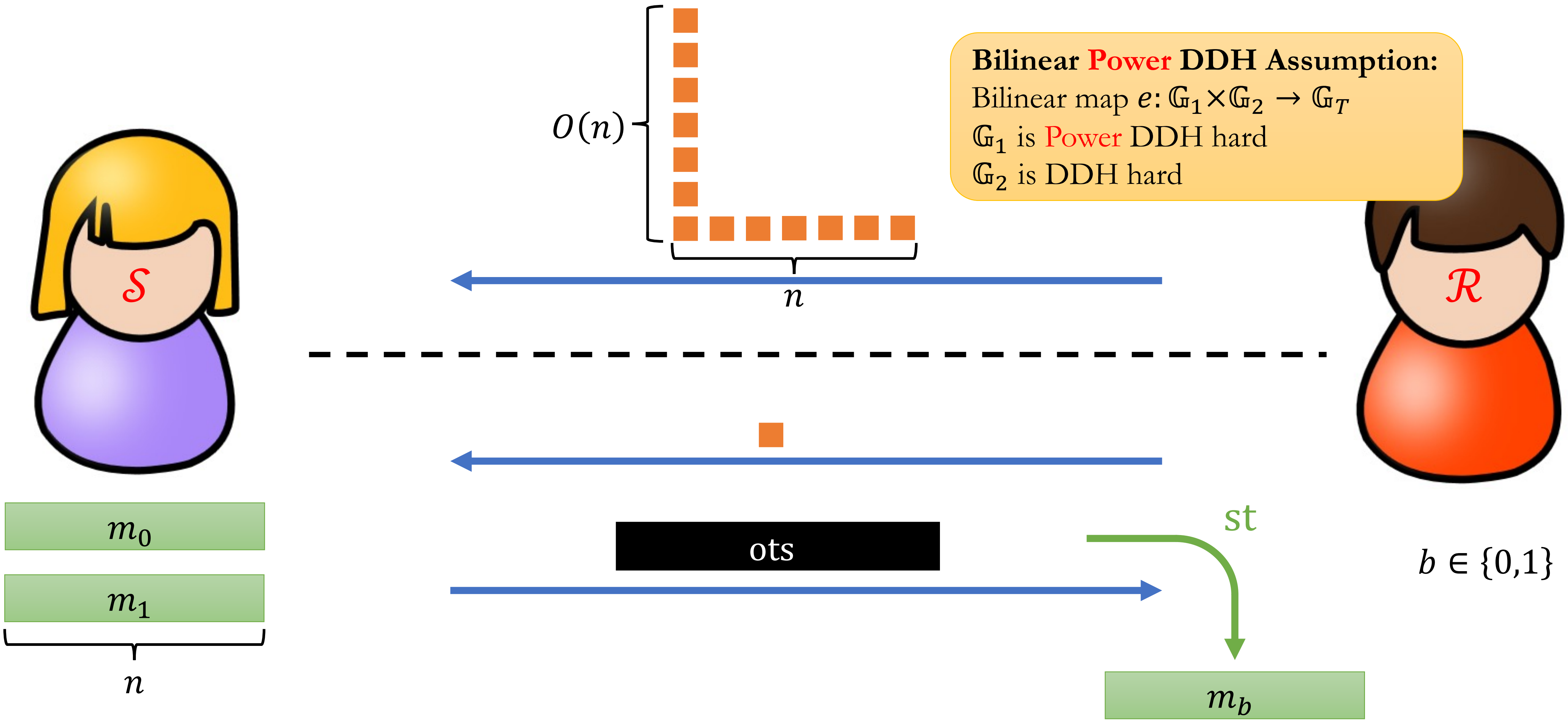
$$\frac{|m_0|}{|\mathrm{ots}|} \to 1 \quad (\text{as } n \to \infty)$$

Our Results: Amortized Rate-1 OT



Bilinear SXDH Assumption:
Bilinear map $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$
Both $\mathbb{G}_1, \mathbb{G}_2$ are DDH hard

Our Results: Amortized Rate-1 OT



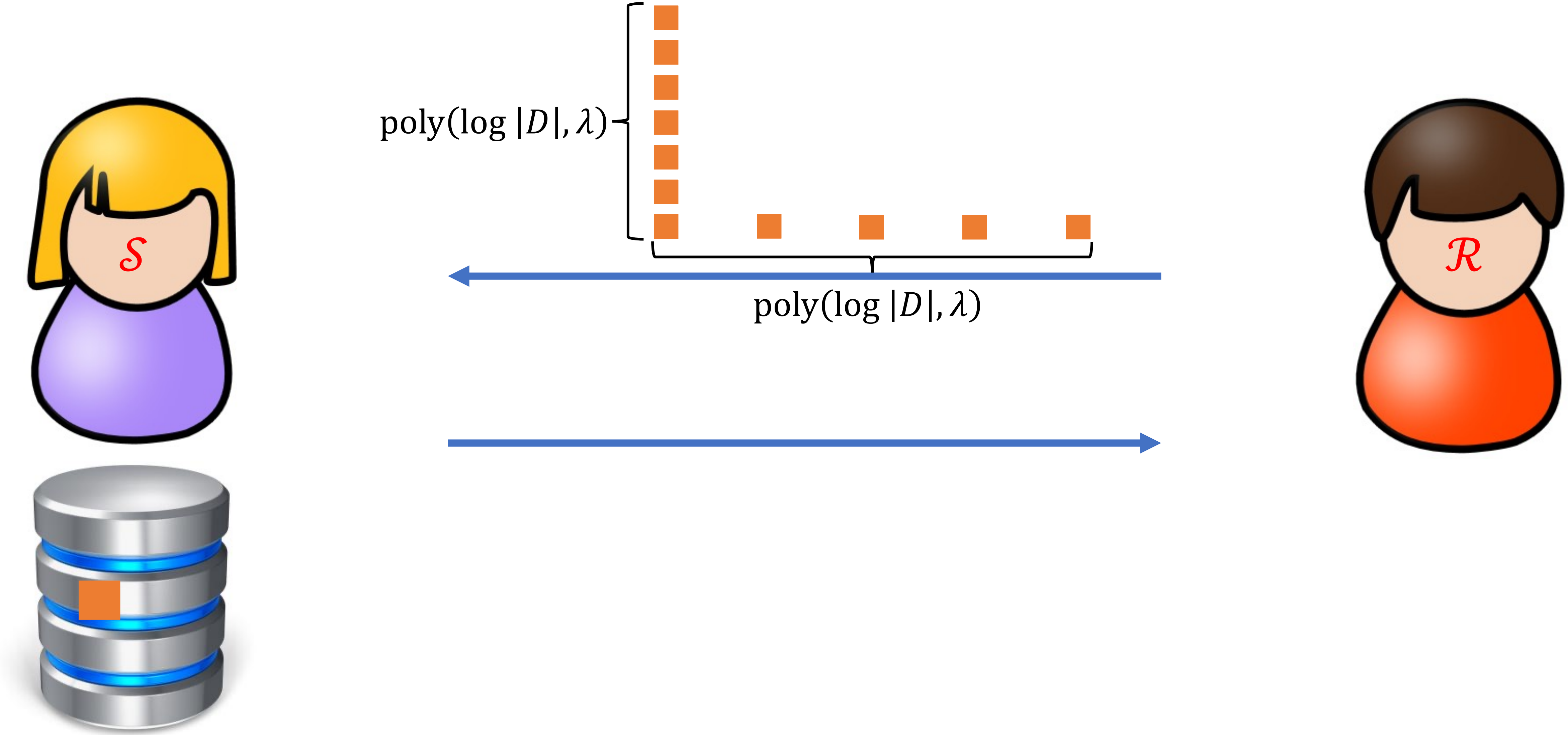
Bilinear Power DDH Assumption:

Bilinear map $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$

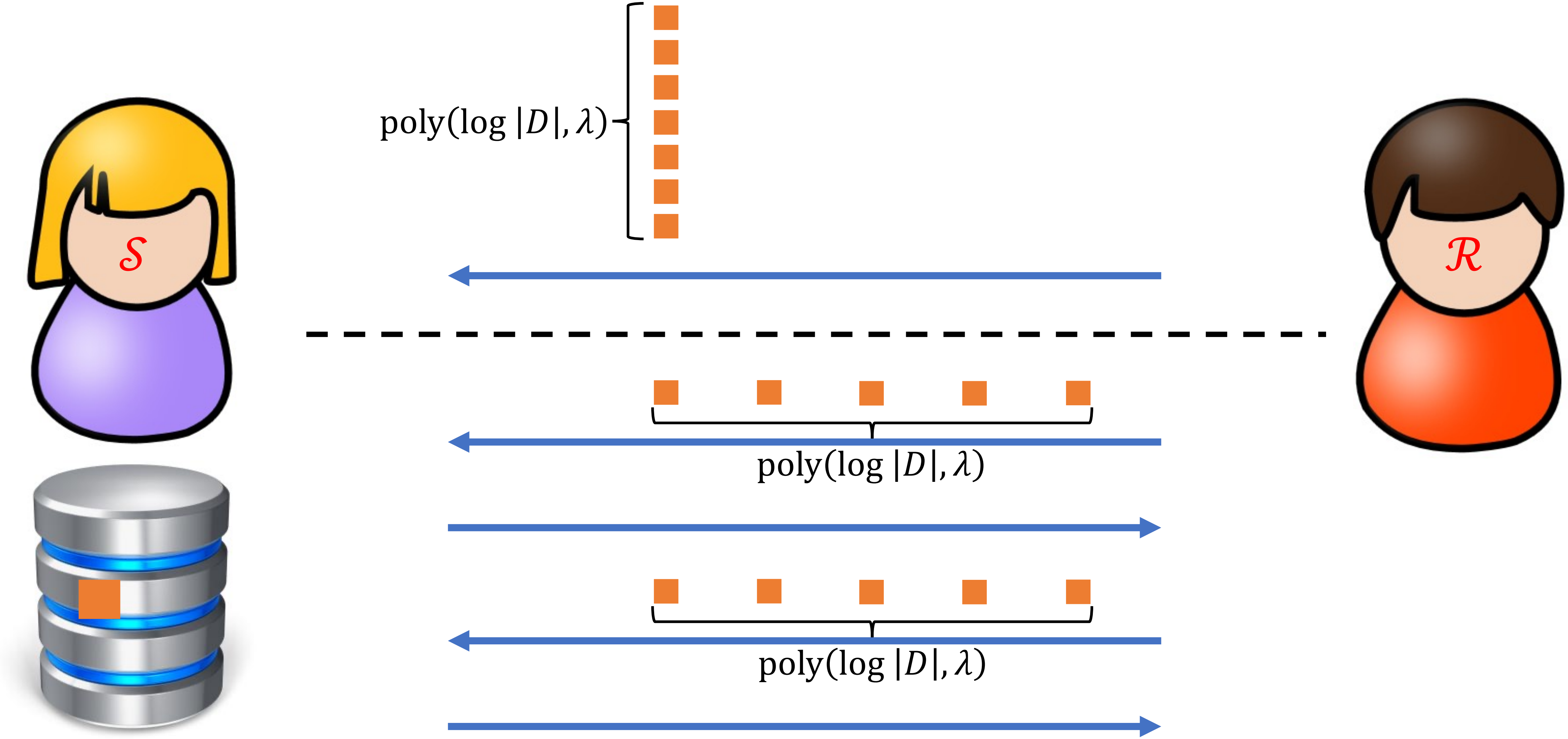
$\mathbb{G}_1$ is Power DDH hard

$\mathbb{G}_2$ is DDH hard

Our Results: Applications from Bilinear Power DDH



Our Results: Applications from Bilinear Power DDH


$\text{poly}(\log|D|,\lambda)$
$\mathcal{S}$
$\mathcal{R}$
$\text{poly}(\log|D|,\lambda)$
$\text{poly}(\log|D|,\lambda)$

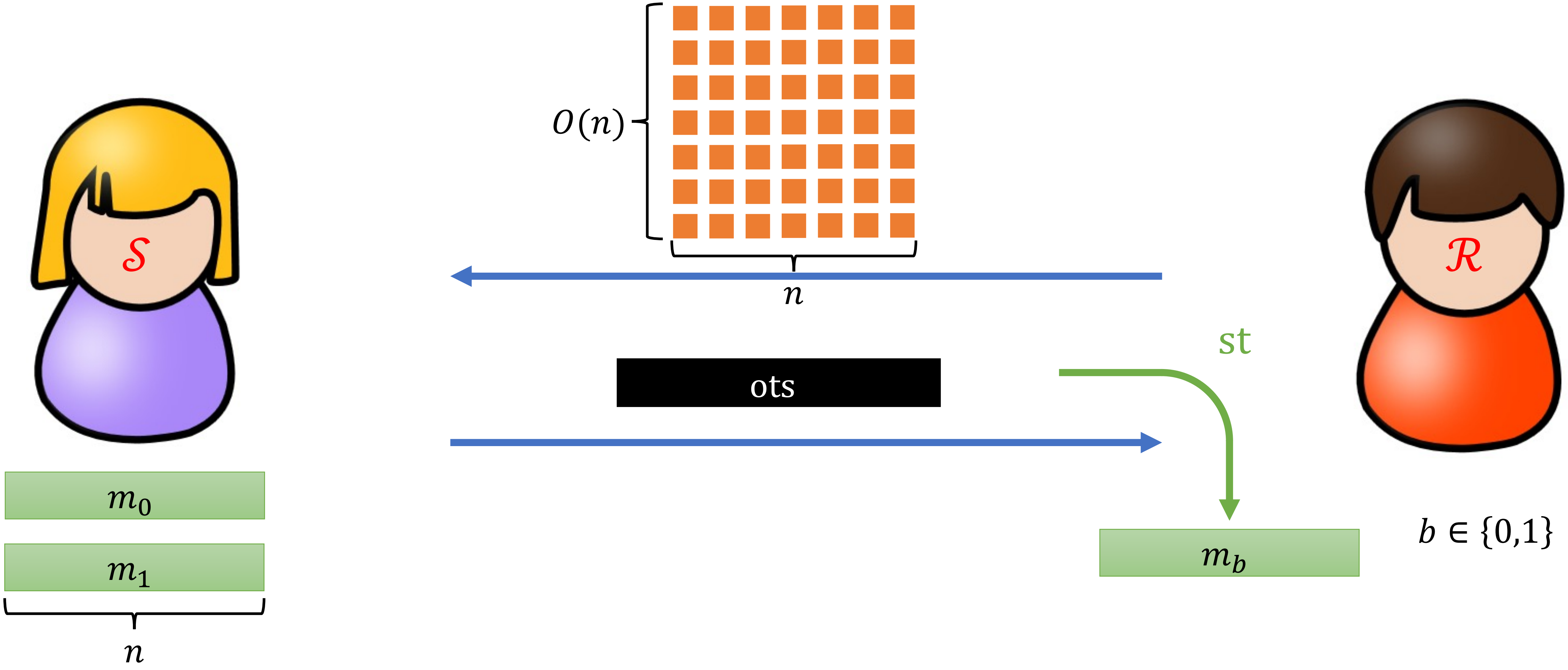
Summary

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

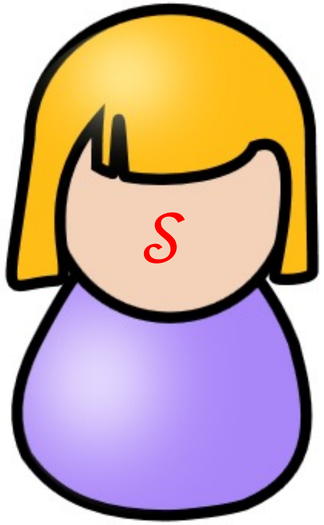
Outline

- Rate-1 OT from DDH [DGIMMO19]
- Amortized Rate-1 OT from Bilinear SXDH
- Optimizations

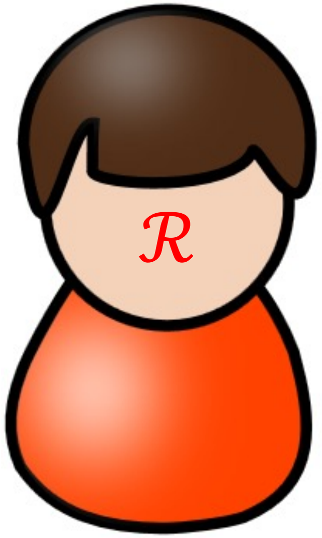
Rate-1 OT from DDH [DGIMMO19]



Rate-1 OT from DDH [DGIMMO19]



$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$ek =$	$g_{0,1}^{\rho} \cdot g^{1-b}$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho} \cdot g^{b}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$
$b = 0$:	$g_{0,1}^{\rho} \cdot g$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$
$b = 1$:	$g_{0,1}^{\rho}$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho} \cdot g$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$



m_0

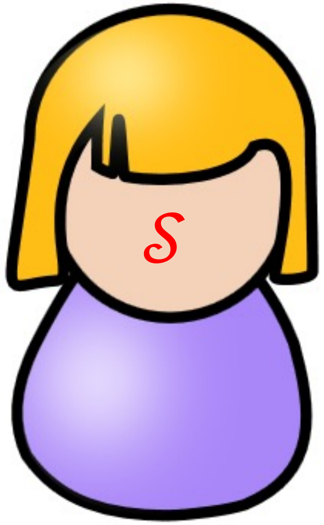
m_1

$\underbrace{\qquad\qquad}_{n}$

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

Rate-1 OT from DDH [DGIMMO19]

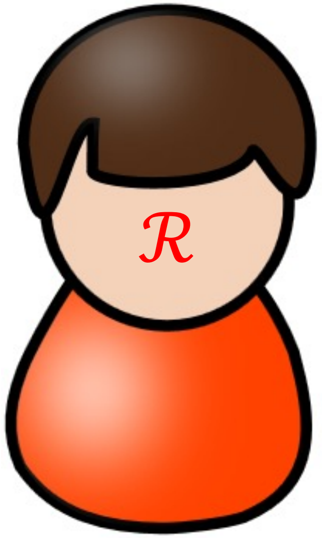
$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$ek =$	$g_{0,1}^{\rho} \cdot g$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$



m_0

m_1

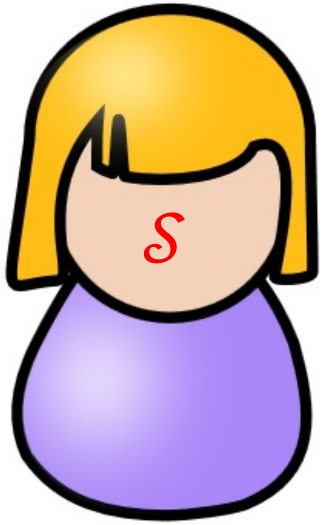
n

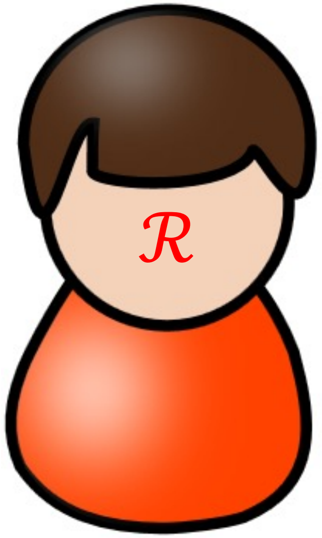


$b = 0$

Rate-1 OT from DDH [DGIMMO19]

$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$ek =$	$g_{0,1}^{\rho} \cdot g$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$





$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$m =$		m_0						m_1				
$ek =$	$g_{0,1}^{\rho} \cdot g$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$

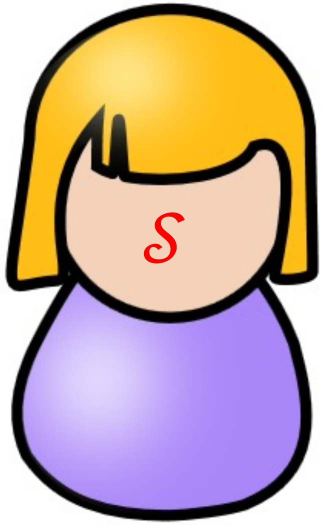
$$h = \langle hk, m \rangle = \prod_{i \in [2n]} hk[i]^{m[i]}$$

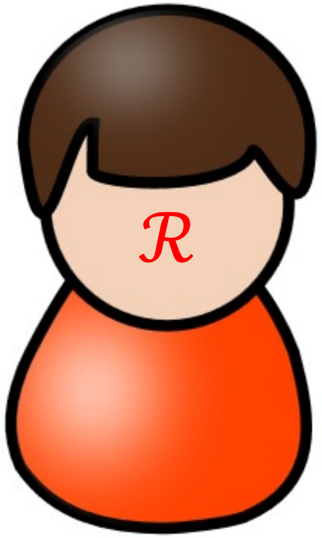
$$e = \langle ek, m \rangle = \prod_{i \in [2n]} ek[i]^{m[i]}$$

$b = 0$

Rate-1 OT from DDH [DGIMMO19]

$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$ek =$	$g_{0,1}^{\rho} \cdot g$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$





$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$m =$	0	0	1	0	1	1	1	0	1	1	0	1
$ek =$	$g_{0,1}^{\rho} \cdot g$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$

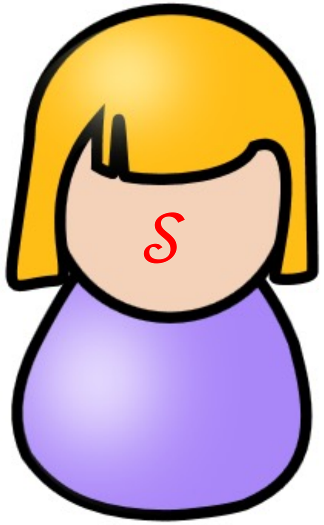
$$h = \langle hk, m \rangle = \prod_{i \in [2n]} hk[i]^{m[i]}$$

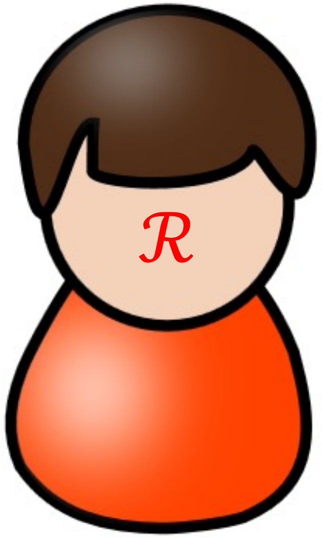
$$e = \langle ek, m \rangle = \prod_{i \in [2n]} ek[i]^{m[i]}$$

$b = 0$

Rate-1 OT from DDH [DGIMMO19]

$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$ek =$	$g_{0,1}^{\rho} \cdot g$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$





$b = 0$

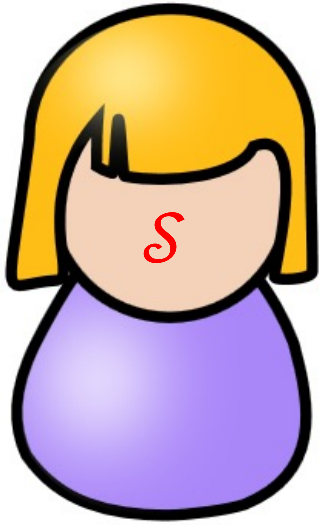
$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$m =$	0	0	1	0	1	1	1	0	1	1	0	1
$ek =$	$g_{0,1}^{\rho} \cdot g$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$

$$h = \langle hk, m \rangle = \prod_{i \in [2n]} hk[i]^{m[i]}$$

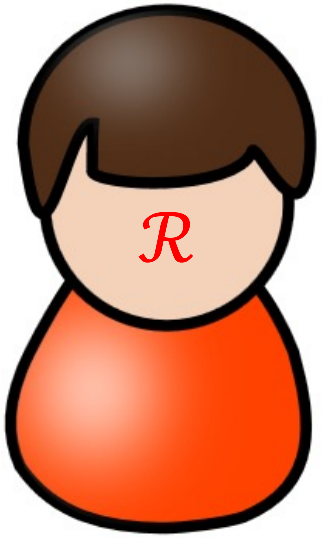
$$e = \langle ek, m \rangle = \prod_{i \in [2n]} ek[i]^{m[i]}$$

$m_0[1] = 0$: $e = h^{\rho}$

Rate-1 OT from DDH [DGIMMO19]



$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$ek =$	$g_{0,1}^{\rho} \cdot g$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$



$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$m =$	1	0	1	0	1	1	1	0	1	1	0	1
$ek =$	$g_{0,1}^{\rho} \cdot g$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$

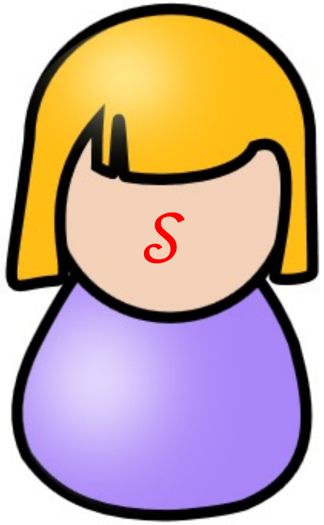
$$h = \langle hk, m \rangle = \prod_{i \in [2n]} hk[i]^{m[i]}$$

$$e = \langle ek, m \rangle = \prod_{i \in [2n]} ek[i]^{m[i]}$$

$b = 0$

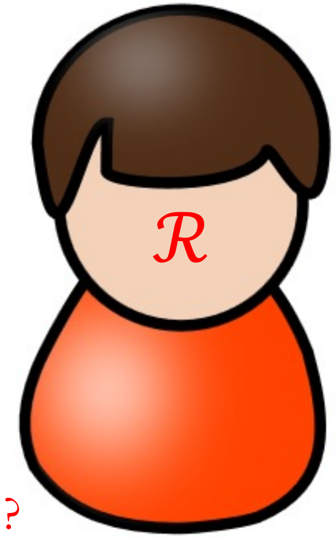
$m_0[1] = 1$: $e = h^{\rho} \cdot g$

Rate-1 OT from DDH [DGIMMO19]



$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$ek =$	$g_{0,1}^{\rho}$ $\cdot g$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$

h, e



$e = h^{\rho}$ or $h^{\rho} \cdot g$?

$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$m =$	1	0	1	0	1	1	1	0	1	1	0	1
$ek =$	$g_{0,1}^{\rho}$ $\cdot g$	$g_{0,2}^{\rho}$	.	.	.	$g_{0,n}^{\rho}$	$g_{1,1}^{\rho}$	$g_{1,2}^{\rho}$	.	.	.	$g_{1,n}^{\rho}$

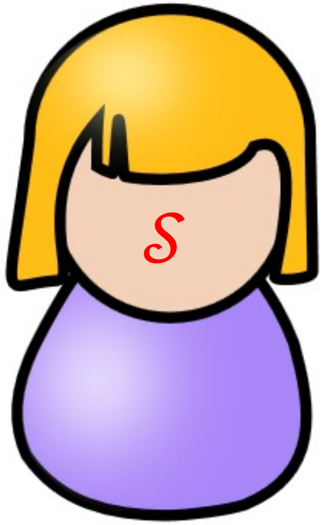
$$h = \langle hk, m \rangle = \prod_{i \in [2n]} hk[i]^{m[i]}$$

$$e = \langle ek, m \rangle = \prod_{i \in [2n]} ek[i]^{m[i]}$$

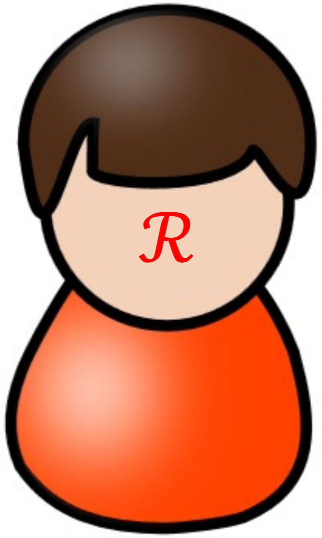
$b = 0$

$e = h^{\rho}$ or $h^{\rho} \cdot g$

Rate-1 OT from DDH [DGIMMO19]



$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$ek_1 =$	$g_{0,1}^{\rho_1} \cdot g$	$g_{0,2}^{\rho_1}$	.	.	.	$g_{0,n}^{\rho_1}$	$g_{1,1}^{\rho_1}$	$g_{1,2}^{\rho_1}$	.	.	.	$g_{1,n}^{\rho_1}$
$ek_2 =$	$g_{0,1}^{\rho_2}$	$g_{0,2}^{\rho_2} \cdot g$	.	.	.	$g_{0,n}^{\rho_2}$	$g_{1,1}^{\rho_2}$	$g_{1,2}^{\rho_2}$	.	.	.	$g_{1,n}^{\rho_2}$
							⋮					
$ek_n =$	$g_{0,1}^{\rho_n}$	$g_{0,2}^{\rho_n}$	.	.	.	$g_{0,n}^{\rho_n} \cdot g$	$g_{1,1}^{\rho_n}$	$g_{1,2}^{\rho_n}$	.	.	.	$g_{1,n}^{\rho_n}$



$m =$	m_0	m_1

$b = 0$

$$h = \langle hk, m \rangle$$
$$e_1 = \langle ek_1, m \rangle$$
$$e_2 = \langle ek_2, m \rangle$$
$$\vdots$$
$$e_n = \langle ek_n, m \rangle$$

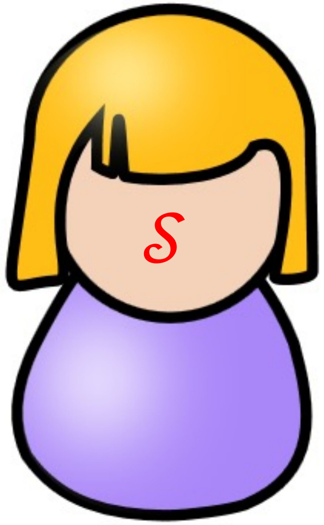
$h, e_1, e_2, \ldots, e_n$

$(n+1)$ group elements!

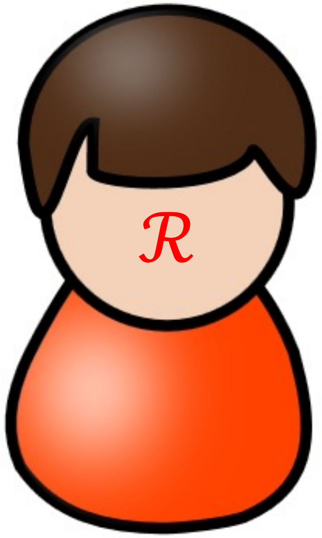
Goal: 1 group element + n bits

$e_1 = h^{\rho_1}$ or $h^{\rho_1} \cdot g$?
$e_2 = h^{\rho_2}$ or $h^{\rho_2} \cdot g$?
$\vdots$
$e_n = h^{\rho_n}$ or $h^{\rho_n} \cdot g$?

Rate-1 OT from DDH [DGIMMO19]



$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$ek_1 =$	$g_{0,1}^{\rho_1} \cdot g$	$g_{0,2}^{\rho_1}$	.	.	.	$g_{0,n}^{\rho_1}$	$g_{1,1}^{\rho_1}$	$g_{1,2}^{\rho_1}$	.	.	.	$g_{1,n}^{\rho_1}$
$ek_2 =$	$g_{0,1}^{\rho_2}$	$g_{0,2}^{\rho_2} \cdot g$	.	.	.	$g_{0,n}^{\rho_2}$	$g_{1,1}^{\rho_2}$	$g_{1,2}^{\rho_2}$	.	.	.	$g_{1,n}^{\rho_2}$
							$\vdots$					
$ek_n =$	$g_{0,1}^{\rho_n}$	$g_{0,2}^{\rho_n}$	.	.	.	$g_{0,n}^{\rho_n} \cdot g$	$g_{1,1}^{\rho_n}$	$g_{1,2}^{\rho_n}$	.	.	.	$g_{1,n}^{\rho_n}$



$m =$	m_0	m_1

$b = 0$

$h = \langle hk, m \rangle$

$e_1 = \langle ek_1, m \rangle \rightarrow b_1$

$e_2 = \langle ek_2, m \rangle \rightarrow b_2$

$\vdots$

$e_n = \langle ek_n, m \rangle \rightarrow b_n$

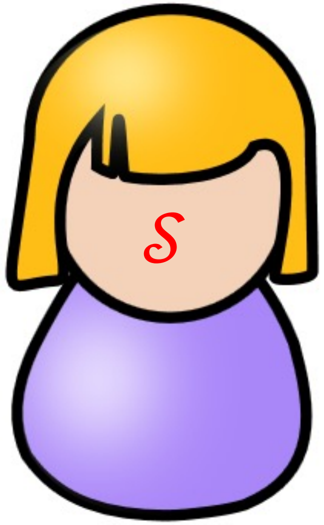
$h, b_1, b_2, \dots, b_n$

Goal: 1 group element + n bits

Rate-1 OT from DDH [DGIMMO19]

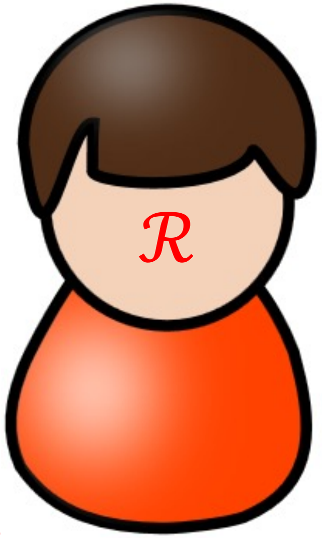
$$hk = \begin{array}{|c|c|c|c|c|c|}\hline g_{0,1} & g_{0,2} & . & . & . & g_{0,n} \\ \hline \end{array}\ \begin{array}{|c|c|c|c|c|c|}\hline g_{1,1} & g_{1,2} & . & . & . & g_{1,n} \\ \hline \end{array}$$

$$ek = \begin{array}{|c|c|c|c|c|c|}\hline g_{0,1}^{\rho} \cdot g & g_{0,2}^{\rho} & . & . & . & g_{0,n}^{\rho} \\ \hline \end{array}\ \begin{array}{|c|c|c|c|c|c|}\hline g_{1,1}^{\rho} & g_{1,2}^{\rho} & . & . & . & g_{1,n}^{\rho} \\ \hline \end{array}$$



$$\xleftarrow{\qquad\qquad\qquad\qquad}$$

$$\xrightarrow{h,\ \Phi(e)}$$



$\Phi(e) = \Phi(h^{\rho})$ or $\Phi(h^{\rho} \cdot g)$?

$b = 0$

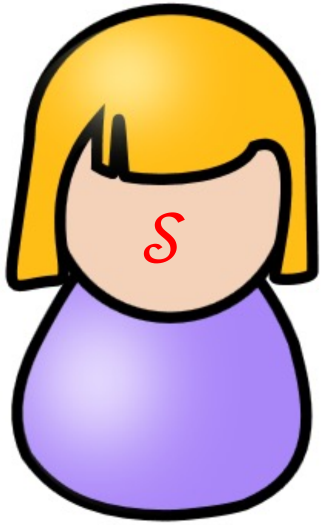
$$m = \begin{array}{|c|c|}\hline m_0 & m_1 \\ \hline \end{array}$$

$h = \langle hk, m \rangle$
$e = \langle ek, m \rangle$

$e = h^{\rho}$ or $h^{\rho} \cdot g$

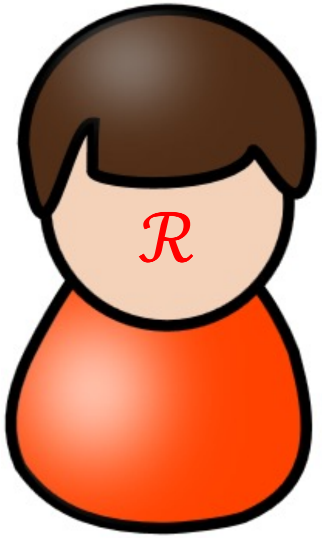
$\Phi\colon \mathbb{G} \to \{0,1\}$ such that
$\forall v \in \mathbb{G},\ \ \Phi(v) \neq \Phi(v \cdot g)$
(can be achieved by [BGI16])

Rate-1 OT from DDH [DGIMMO19]



$hk =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$ek_1 =$	$g_{0,1}^{\rho_1} \cdot g$	$g_{0,2}^{\rho_1}$	.	.	.	$g_{0,n}^{\rho_1}$	$g_{1,1}^{\rho_1}$	$g_{1,2}^{\rho_1}$	.	.	.	$g_{1,n}^{\rho_1}$
$ek_2 =$	$g_{0,1}^{\rho_2}$	$g_{0,2}^{\rho_2} \cdot g$	.	.	.	$g_{0,n}^{\rho_2}$	$g_{1,1}^{\rho_2}$	$g_{1,2}^{\rho_2}$	.	.	.	$g_{1,n}^{\rho_2}$
						⋮						
$ek_n =$	$g_{0,1}^{\rho_n}$	$g_{0,2}^{\rho_n}$	.	.	.	$g_{0,n}^{\rho_n} \cdot g$	$g_{1,1}^{\rho_n}$	$g_{1,2}^{\rho_n}$	.	.	.	$g_{1,n}^{\rho_n}$

←



$m =$	m_0	m_1

$b = 0$

$$h = \langle hk, m \rangle$$
$$e_1 = \langle ek_1, m \rangle \xrightarrow{\Phi} b_1$$
$$e_2 = \langle ek_2, m \rangle \longrightarrow b_2$$
$$\vdots$$
$$e_n = \langle ek_n, m \rangle \longrightarrow b_n$$

$h, b_1, b_2, \ldots, b_n$ →

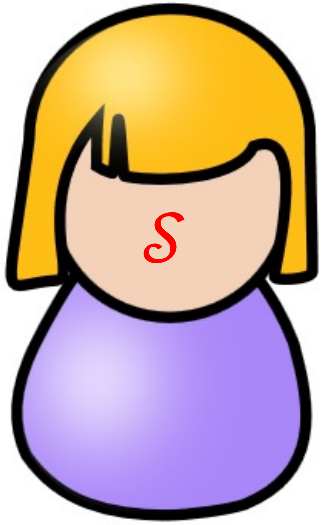
Outline

- Rate-1 OT from DDH [DGIMMO19]

- Amortized Rate-1 OT from Bilinear SXDH

- Optimizations

Amortized Rate-1 OT from Bilinear SXDH



$M =$	$g_{0,1}$	$g_{0,2}$	.	.	.	$g_{0,n}$	$g_{1,1}$	$g_{1,2}$	.	.	.	$g_{1,n}$
$vk_1 =$	$g_{0,1}^{\rho} \cdot g$	$g_{0,2}^{\rho_1}$	.	.	.	$g_{0,n}^{\rho_1}$	$g_{1,1}^{\rho_1} \cdot g$	$g_{1,2}^{\rho_1}$	.	.	.	$g_{1,n}^{\rho_1}$
$vk_2 =$	$g_{0,1}^{\rho_2}$	$g_{0,2}^{\rho_2} \cdot g$	.	.	.	$g_{0,n}^{\rho_2}$	$g_{1,1}^{\rho_2}$	$g_{1,2}^{\rho_2} \cdot g$	.	.	.	$g_{1,n}^{\rho_2}$
						$\vdots$						
$vk_n =$	$g_{0,1}^{\rho_n}$	$g_{0,2}^{\rho_n}$	.	.	.	$g_{0,n}^{\rho_n} \cdot g$	$g_{1,1}^{\rho_n}$	$g_{1,2}^{\rho_n}$	.	.	.	$g_{1,n}^{\rho_n} \cdot g$

$\in \mathbb{G}_1$

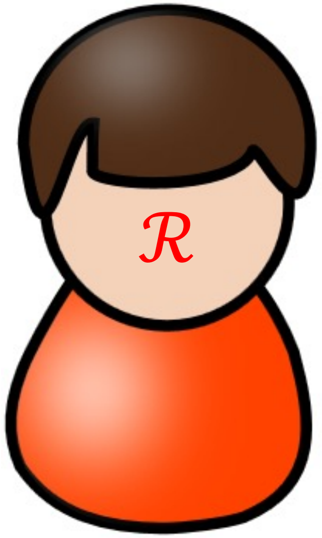
e

u $\in \mathbb{G}_2$

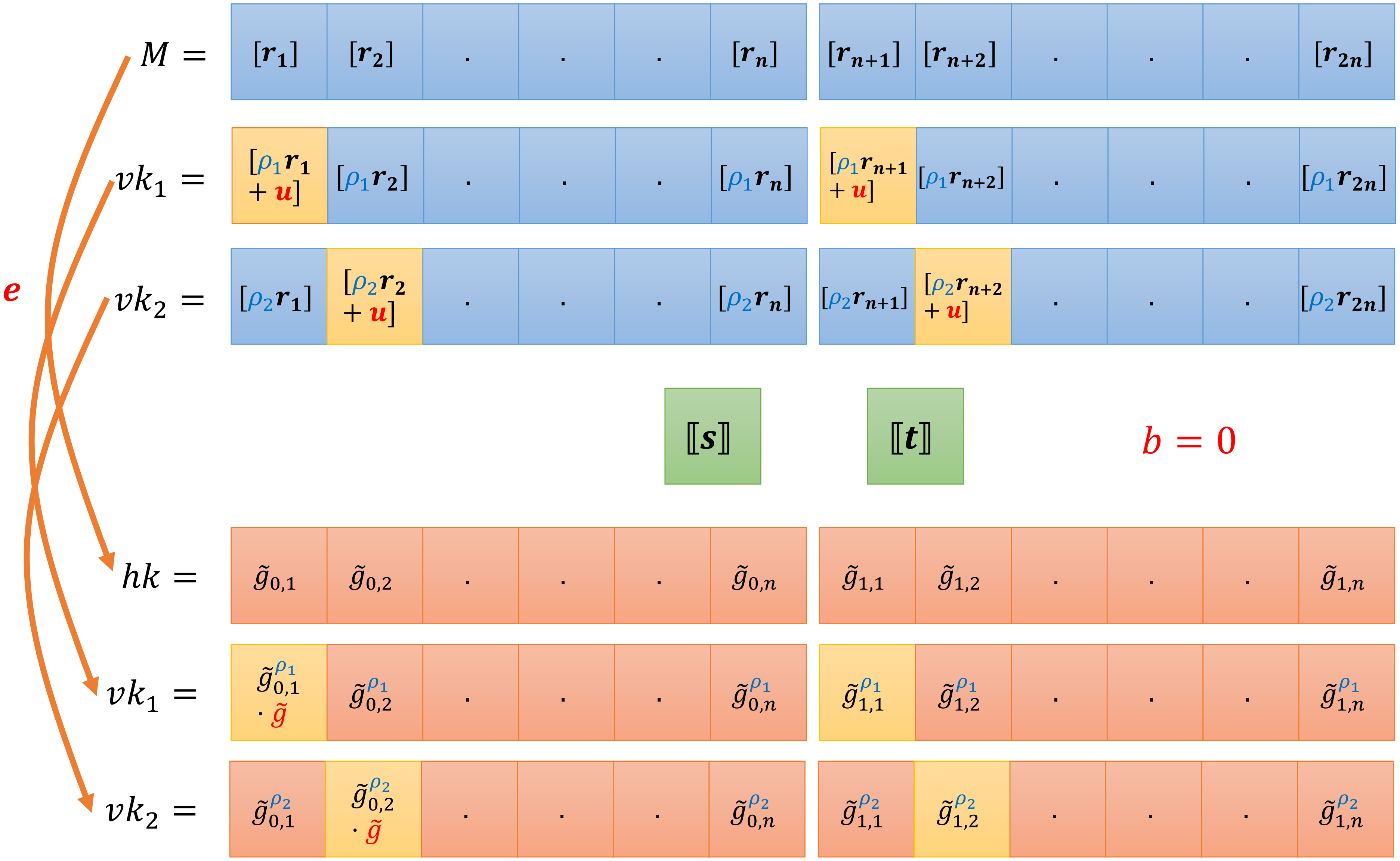
$b = 0$

$hk =$	$\tilde{g}_{0,1}$	$\tilde{g}_{0,2}$	.	.	.	$\tilde{g}_{0,n}$	$\tilde{g}_{1,1}$	$\tilde{g}_{1,2}$	.	.	.	$\tilde{g}_{1,n}$
$ek_1 =$	$\tilde{g}_{0,1}^{\rho_1} \cdot \tilde{g}$	$\tilde{g}_{0,2}^{\rho_1}$	.	.	.	$\tilde{g}_{0,n}^{\rho_1}$	$\tilde{g}_{1,1}^{\rho_1}$	$\tilde{g}_{1,2}^{\rho_1}$	.	.	.	$\tilde{g}_{1,n}^{\rho_1}$
$ek_2 =$	$\tilde{g}_{0,1}^{\rho_2}$	$\tilde{g}_{0,2}^{\rho_2} \cdot \tilde{g}$	.	.	.	$\tilde{g}_{0,n}^{\rho_2}$	$\tilde{g}_{1,1}^{\rho_2}$	$\tilde{g}_{1,2}^{\rho_2}$	.	.	.	$\tilde{g}_{1,n}^{\rho_2}$

$\in \mathbb{G}_T$



Amortized Rate-1 OT from Bilinear SXDH



$M =$	$[\boldsymbol{r}_1]$	$[\boldsymbol{r}_2]$	.	.	.	$[\boldsymbol{r}_n]$	$[\boldsymbol{r}_{n+1}]$	$[\boldsymbol{r}_{n+2}]$	.	.	.	$[\boldsymbol{r}_{2n}]$
$vk_1 =$	$[\rho_1\boldsymbol{r}_1 + \boldsymbol{u}]$	$[\rho_1\boldsymbol{r}_2]$	.	.	.	$[\rho_1\boldsymbol{r}_n]$	$[\rho_1\boldsymbol{r}_{n+1} + \boldsymbol{u}]$	$[\rho_1\boldsymbol{r}_{n+2}]$	.	.	.	$[\rho_1\boldsymbol{r}_{2n}]$
$vk_2 =$	$[\rho_2\boldsymbol{r}_1]$	$[\rho_2\boldsymbol{r}_2 + \boldsymbol{u}]$	.	.	.	$[\rho_2\boldsymbol{r}_n]$	$[\rho_2\boldsymbol{r}_{n+1}]$	$[\rho_2\boldsymbol{r}_{n+2} + \boldsymbol{u}]$	.	.	.	$[\rho_2\boldsymbol{r}_{2n}]$

$[\![\boldsymbol{s}]\!]$ $[\![\boldsymbol{t}]\!]$ $b = 0$

$hk =$	$\tilde{g}_{0,1}$	$\tilde{g}_{0,2}$	.	.	.	$\tilde{g}_{0,n}$	$\tilde{g}_{1,1}$	$\tilde{g}_{1,2}$	.	.	.	$\tilde{g}_{1,n}$
$vk_1 =$	$\tilde{g}_{0,1}^{\rho_1} \cdot \tilde{g}$	$\tilde{g}_{0,2}^{\rho_1}$	.	.	.	$\tilde{g}_{0,n}^{\rho_1}$	$\tilde{g}_{1,1}^{\rho_1}$	$\tilde{g}_{1,2}^{\rho_1}$	.	.	.	$\tilde{g}_{1,n}^{\rho_1}$
$vk_2 =$	$\tilde{g}_{0,1}^{\rho_2}$	$\tilde{g}_{0,2}^{\rho_2} \cdot \tilde{g}$	.	.	.	$\tilde{g}_{0,n}^{\rho_2}$	$\tilde{g}_{1,1}^{\rho_2}$	$\tilde{g}_{1,2}^{\rho_2}$	.	.	.	$\tilde{g}_{1,n}^{\rho_2}$

$\boldsymbol{r}_i, \boldsymbol{u} \xleftarrow{\$} \binom{\mathbb{Z}_p}{\mathbb{Z}_p}$

$[\boldsymbol{r}] := \binom{g^{r[0]}}{g^{r[1]}}$

$\rho_i \xleftarrow{\$} \mathbb{Z}_p$

$\boldsymbol{s}, \boldsymbol{t} \xleftarrow{\$} \binom{\mathbb{Z}_p}{\mathbb{Z}_p}$ s.t.

$\boldsymbol{s} \cdot \boldsymbol{u} = 1$

$\boldsymbol{t} \cdot \boldsymbol{u} = 0$

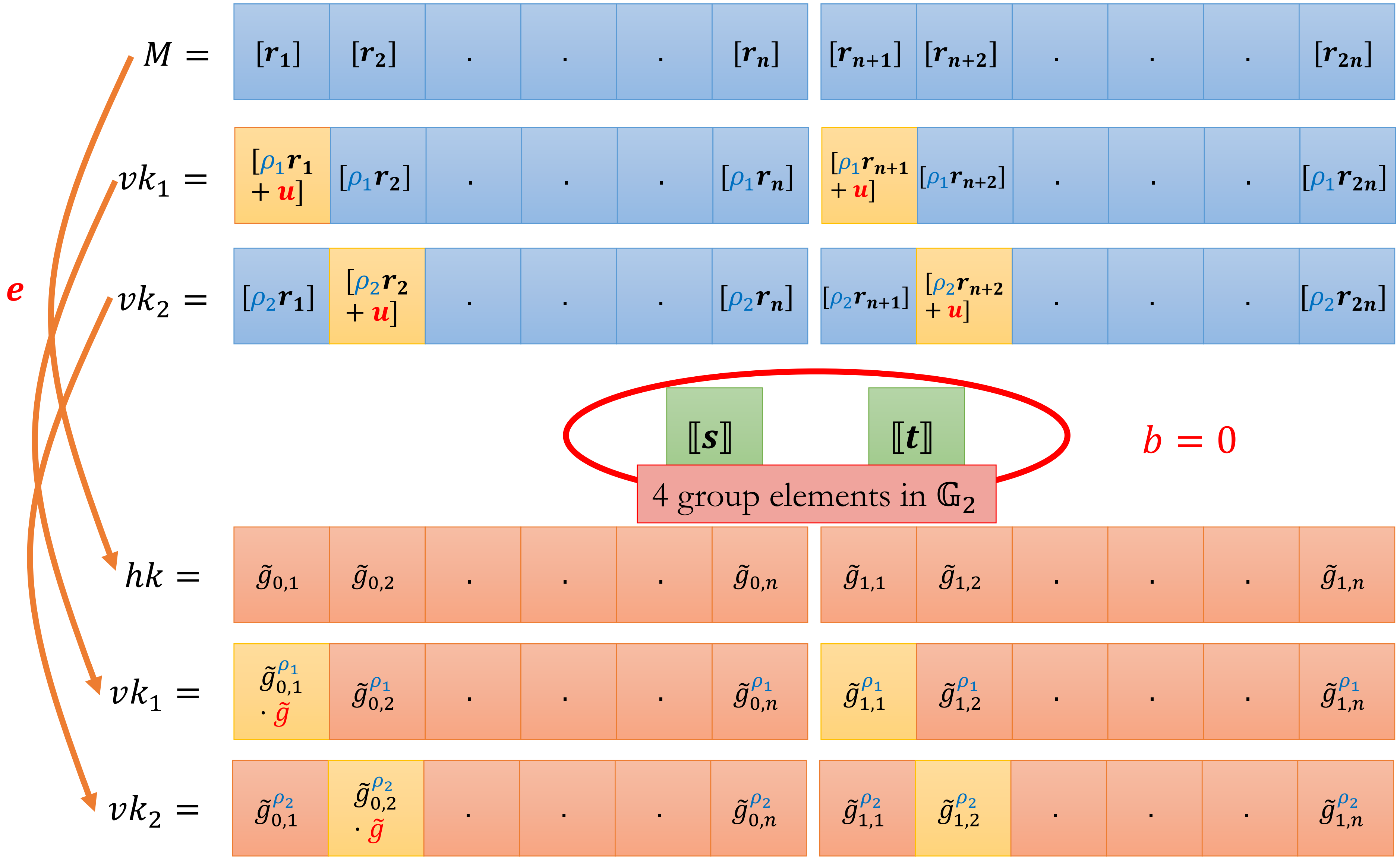
$[\![\boldsymbol{s}]\!] := \binom{h^{s[0]}}{h^{s[1]}}$

$$\boldsymbol{e}([\boldsymbol{r}], [\![\boldsymbol{s}]\!]) \coloneqq \boldsymbol{e}\left(g^{r[0]}, h^{s[0]}\right) \cdot \boldsymbol{e}\left(g^{r[1]}, h^{s[1]}\right)$$

Outline

- Rate-1 OT from DDH [DGIMMO19]
- Amortized Rate-1 OT from Bilinear SXDH
- Optimizations

Amortized Rate-1 OT from Bilinear SXDH



$M =$	$[\boldsymbol{r}_1]$	$[\boldsymbol{r}_2]$	.	.	.	$[\boldsymbol{r}_n]$	$[\boldsymbol{r}_{n+1}]$	$[\boldsymbol{r}_{n+2}]$	.	.	.	$[\boldsymbol{r}_{2n}]$
$vk_1 =$	$[\rho_1 \boldsymbol{r}_1 + \boldsymbol{u}]$	$[\rho_1 \boldsymbol{r}_2]$	.	.	.	$[\rho_1 \boldsymbol{r}_n]$	$[\rho_1 \boldsymbol{r}_{n+1} + \boldsymbol{u}]$	$[\rho_1 \boldsymbol{r}_{n+2}]$	.	.	.	$[\rho_1 \boldsymbol{r}_{2n}]$
$vk_2 =$	$[\rho_2 \boldsymbol{r}_1]$	$[\rho_2 \boldsymbol{r}_2 + \boldsymbol{u}]$	.	.	.	$[\rho_2 \boldsymbol{r}_n]$	$[\rho_2 \boldsymbol{r}_{n+1}]$	$[\rho_2 \boldsymbol{r}_{n+2} + \boldsymbol{u}]$	.	.	.	$[\rho_2 \boldsymbol{r}_{2n}]$

$[\![\boldsymbol{s}]\!]$ $[\![\boldsymbol{t}]\!]$

4 group elements in $\mathbb{G}_2$

$b = 0$

$hk =$	$\tilde{g}_{0,1}$	$\tilde{g}_{0,2}$	.	.	.	$\tilde{g}_{0,n}$	$\tilde{g}_{1,1}$	$\tilde{g}_{1,2}$	.	.	.	$\tilde{g}_{1,n}$
$vk_1 =$	$\tilde{g}_{0,1}^{\rho_1} \cdot \tilde{g}$	$\tilde{g}_{0,2}^{\rho_1}$	.	.	.	$\tilde{g}_{0,n}^{\rho_1}$	$\tilde{g}_{1,1}^{\rho_1}$	$\tilde{g}_{1,2}^{\rho_1}$	.	.	.	$\tilde{g}_{1,n}^{\rho_1}$
$vk_2 =$	$\tilde{g}_{0,1}^{\rho_2}$	$\tilde{g}_{0,2}^{\rho_2} \cdot \tilde{g}$	.	.	.	$\tilde{g}_{0,n}^{\rho_2}$	$\tilde{g}_{1,1}^{\rho_2}$	$\tilde{g}_{1,2}^{\rho_2}$	.	.	.	$\tilde{g}_{1,n}^{\rho_2}$

$\boldsymbol{r}_i, \boldsymbol{u} \overset{\$}{\leftarrow} \begin{pmatrix} \mathbb{Z}_p \\ \mathbb{Z}_p \end{pmatrix}$

$[\boldsymbol{r}] := \begin{pmatrix} g^{r[0]} \\ g^{r[1]} \end{pmatrix}$

$\rho_i \overset{\$}{\leftarrow} \mathbb{Z}_p$

$\boldsymbol{s}, \boldsymbol{t} \overset{\$}{\leftarrow} \begin{pmatrix} \mathbb{Z}_p \\ \mathbb{Z}_p \end{pmatrix}$ s.t.

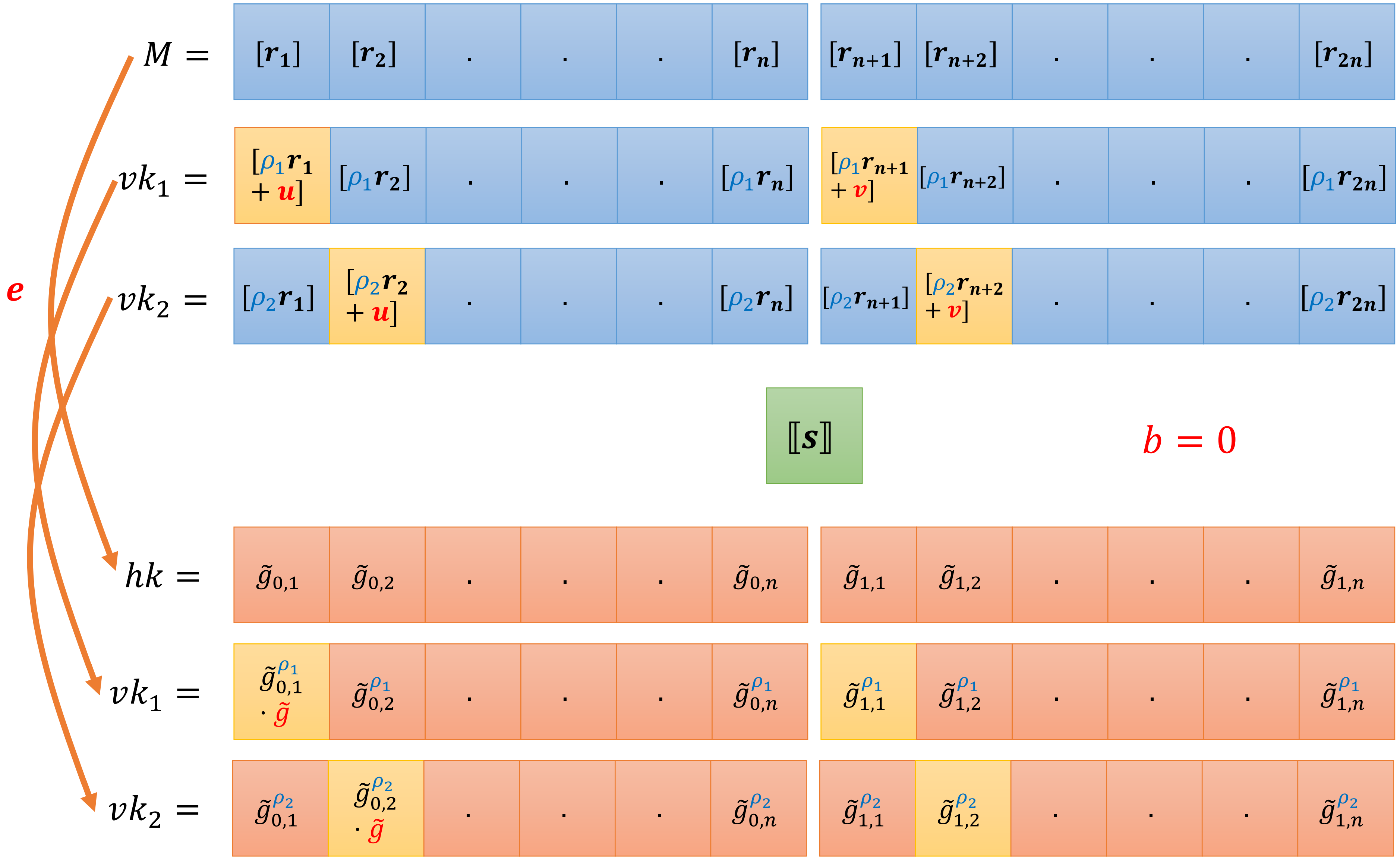
$\boldsymbol{s} \cdot \boldsymbol{u} = 1$

$\boldsymbol{t} \cdot \boldsymbol{u} = 0$

$[\![\boldsymbol{s}]\!] := \begin{pmatrix} h^{s[0]} \\ h^{s[1]} \end{pmatrix}$

$$\boldsymbol{e}([\boldsymbol{r}], [\![\boldsymbol{s}]\!]) \coloneqq \boldsymbol{e}\left(g^{r[0]}, h^{s[0]}\right) \cdot \boldsymbol{e}\left(g^{r[1]}, h^{s[1]}\right)$$

From 4 to 3 Group Elements in $\mathbb{G}_2$



$M =$	$[\boldsymbol{r}_1]$	$[\boldsymbol{r}_2]$	.	.	.	$[\boldsymbol{r}_n]$	$[\boldsymbol{r}_{n+1}]$	$[\boldsymbol{r}_{n+2}]$	.	.	.	$[\boldsymbol{r}_{2n}]$
$vk_1 =$	$[\rho_1 \boldsymbol{r}_1 + \boldsymbol{u}]$	$[\rho_1 \boldsymbol{r}_2]$	.	.	.	$[\rho_1 \boldsymbol{r}_n]$	$[\rho_1 \boldsymbol{r}_{n+1} + \boldsymbol{v}]$	$[\rho_1 \boldsymbol{r}_{n+2}]$	.	.	.	$[\rho_1 \boldsymbol{r}_{2n}]$
$vk_2 =$	$[\rho_2 \boldsymbol{r}_1]$	$[\rho_2 \boldsymbol{r}_2 + \boldsymbol{u}]$	.	.	.	$[\rho_2 \boldsymbol{r}_n]$	$[\rho_2 \boldsymbol{r}_{n+1}]$	$[\rho_2 \boldsymbol{r}_{n+2} + \boldsymbol{v}]$	.	.	.	$[\rho_2 \boldsymbol{r}_{2n}]$

$\llbracket \boldsymbol{s} \rrbracket$

$b = 0$

$hk =$	$\tilde{g}_{0,1}$	$\tilde{g}_{0,2}$	.	.	.	$\tilde{g}_{0,n}$	$\tilde{g}_{1,1}$	$\tilde{g}_{1,2}$	.	.	.	$\tilde{g}_{1,n}$
$vk_1 =$	$\tilde{g}_{0,1}^{\rho_1} \cdot \tilde{g}$	$\tilde{g}_{0,2}^{\rho_1}$	.	.	.	$\tilde{g}_{0,n}^{\rho_1}$	$\tilde{g}_{1,1}^{\rho_1}$	$\tilde{g}_{1,2}^{\rho_1}$	.	.	.	$\tilde{g}_{1,n}^{\rho_1}$
$vk_2 =$	$\tilde{g}_{0,1}^{\rho_2}$	$\tilde{g}_{0,2}^{\rho_2} \cdot \tilde{g}$	.	.	.	$\tilde{g}_{0,n}^{\rho_2}$	$\tilde{g}_{1,1}^{\rho_2}$	$\tilde{g}_{1,2}^{\rho_2}$	.	.	.	$\tilde{g}_{1,n}^{\rho_2}$

$$\boldsymbol{r}_i, \boldsymbol{u}, \boldsymbol{v} \overset{\$}{\leftarrow} \begin{pmatrix}\mathbb{Z}_p\\ \mathbb{Z}_p\\ \mathbb{Z}_p\end{pmatrix}$$

$$[\boldsymbol{r}] := \begin{pmatrix} g^{r[0]}\\ g^{r[1]}\\ g^{r[2]}\end{pmatrix}$$

$$\rho_i \overset{\$}{\leftarrow} \mathbb{Z}_p$$

$$\boldsymbol{s} \overset{\$}{\leftarrow} \begin{pmatrix}\mathbb{Z}_p\\ \mathbb{Z}_p\\ \mathbb{Z}_p\end{pmatrix} \text{ s.t.}$$

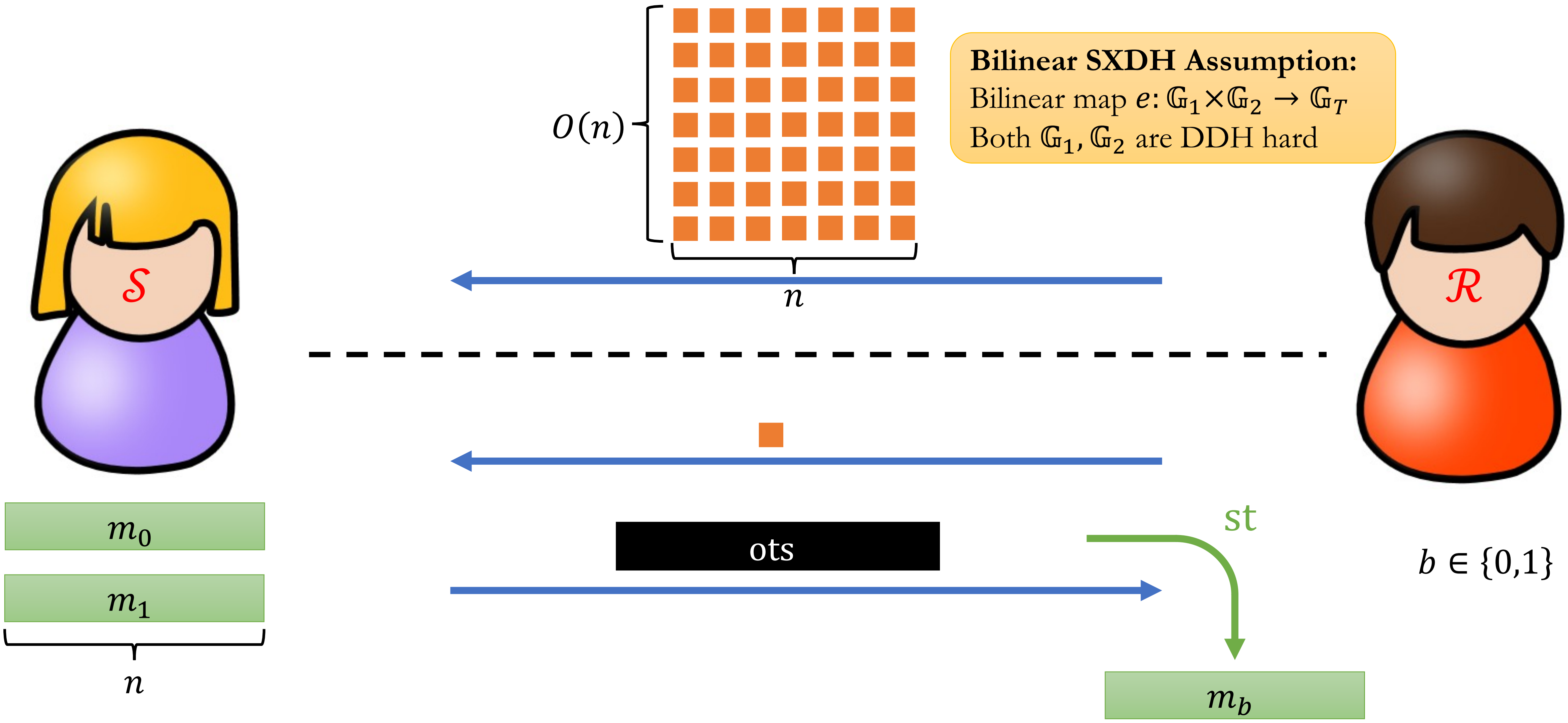
$$\boldsymbol{s} \cdot \boldsymbol{u} = 1$$

$$\boldsymbol{s} \cdot \boldsymbol{v} = 0$$

$$\llbracket \boldsymbol{s} \rrbracket := \begin{pmatrix} h^{s[0]}\\ h^{s[1]}\\ h^{s[2]}\end{pmatrix}$$

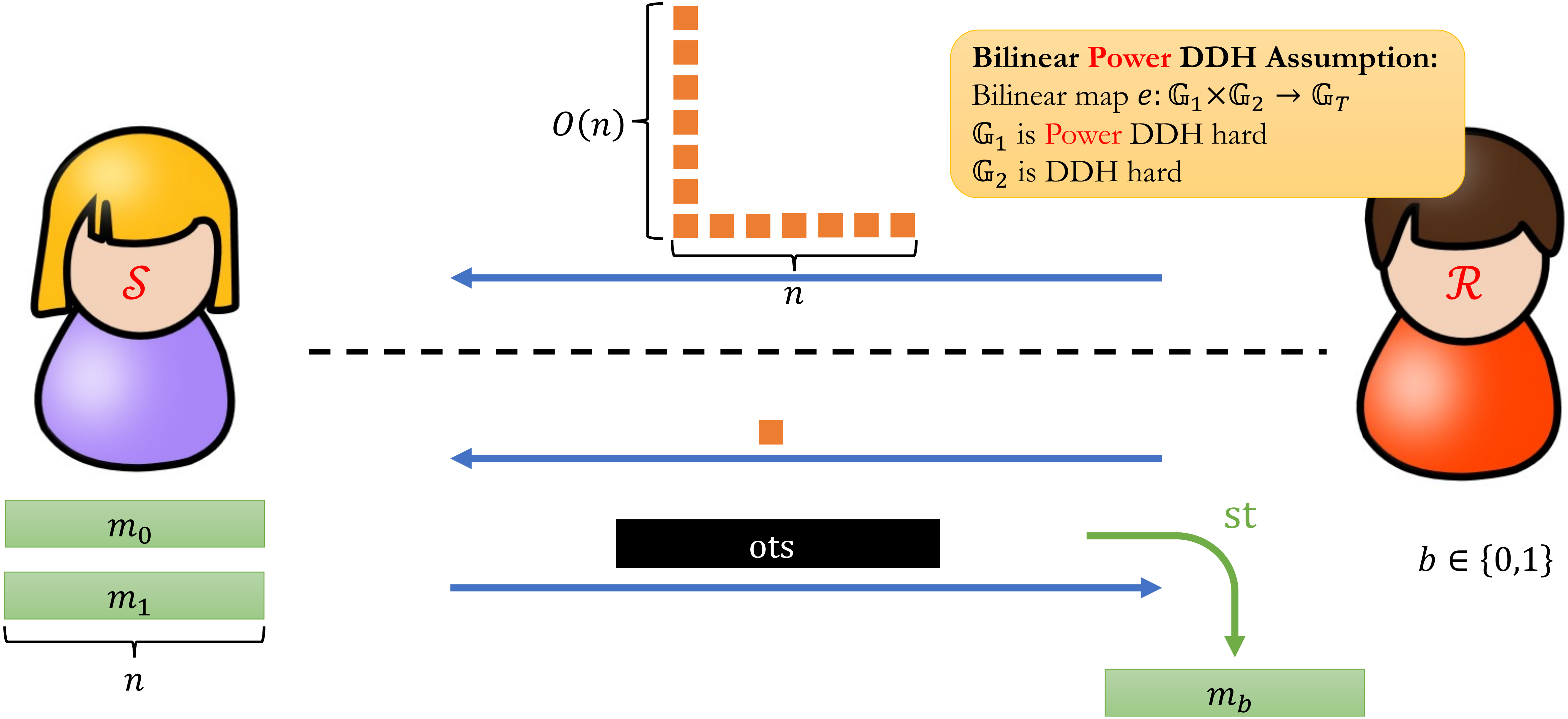
$$\boldsymbol{e}([\boldsymbol{r}], \llbracket \boldsymbol{s} \rrbracket) := \boldsymbol{e}\left(g^{r[0]}, h^{s[0]}\right) \cdot \boldsymbol{e}\left(g^{r[1]}, h^{s[1]}\right) \cdot \boldsymbol{e}\left(g^{r[2]}, h^{s[2]}\right)$$

Summary: Amortized Rate-1 OT



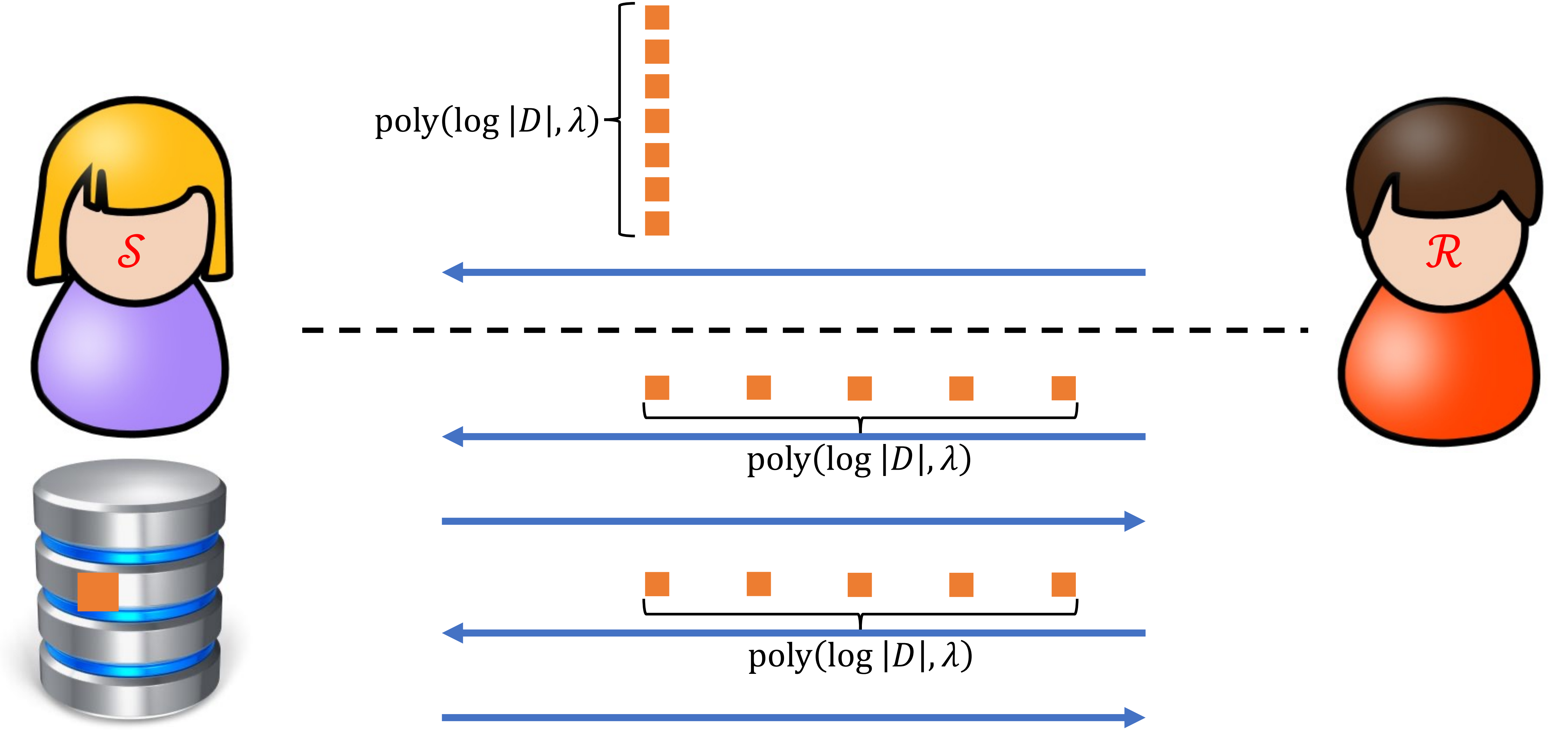
Bilinear SXDH Assumption:
Bilinear map $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$
Both $\mathbb{G}_1, \mathbb{G}_2$ are DDH hard

Summary: Amortized Rate-1 OT



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

Summary: Applications (PIR & PSI)



Open Problems

- Amortized Rate-1 OT from other assumptions

- Amortized Rate-1 OT extension

- Applications
    - More applications of amortized Rate-1 OT
    - Concretely efficient implementation of the applications

Thank you!