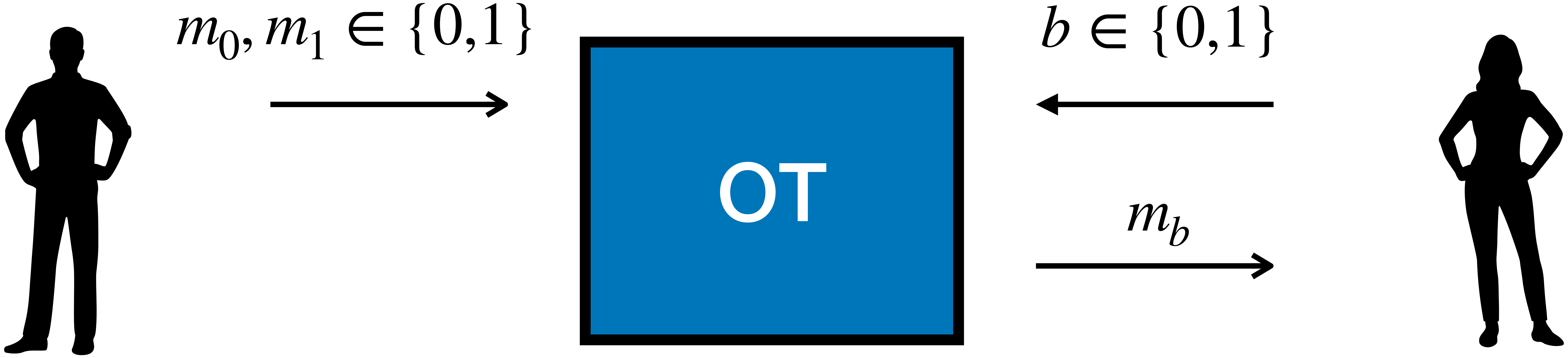
# Two-Round Maliciously-Secure Oblivious Transfer with Optimal Rate

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

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

**Akshayaram Srinivasan** *University of Toronto*

# Oblivious Transfer



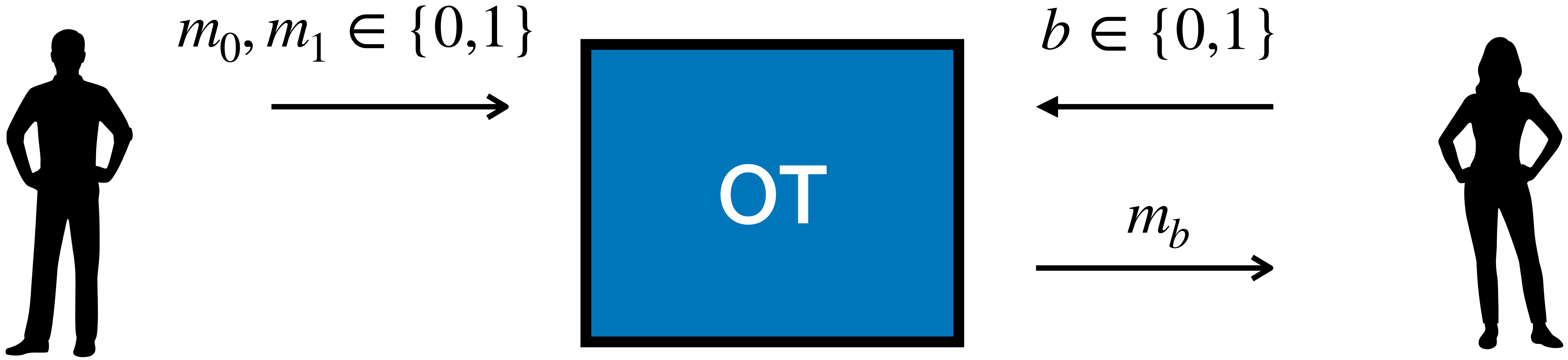
$m_0, m_1 \in \{0,1\}$

OT

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

$m_b$

# Oblivious Transfer



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

OT

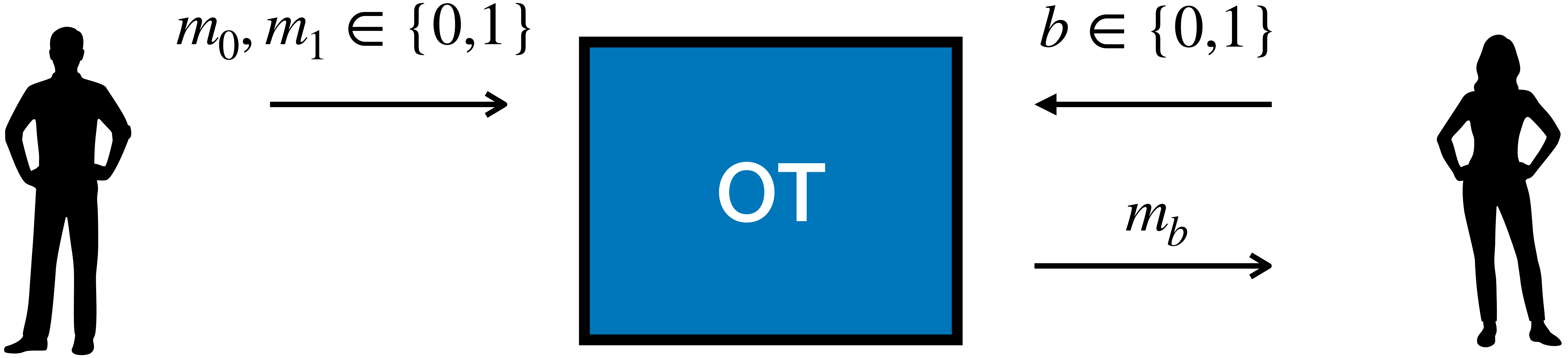
$b \in \{0,1\}$

$m_b$

**Receiver security:** b is hidden from the sender

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

# Oblivious Transfer



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

OT

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

$m_b$

**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

# How much interaction needed for OT?

**Rounds**

$\geq 2$

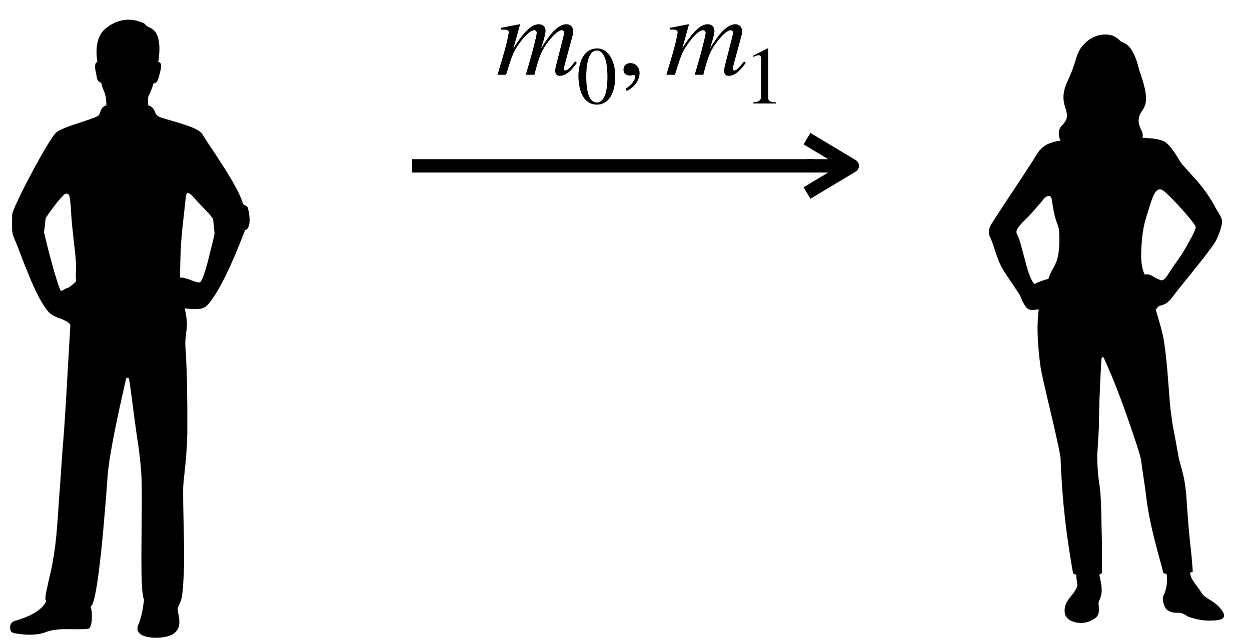
# How much interaction needed for OT?

| Rounds | Communication complexity (#bits exchanged) |
|---|---|
| $\geq 2$ | $\geq 2$ bits per OT |

# How much interaction needed for OT?

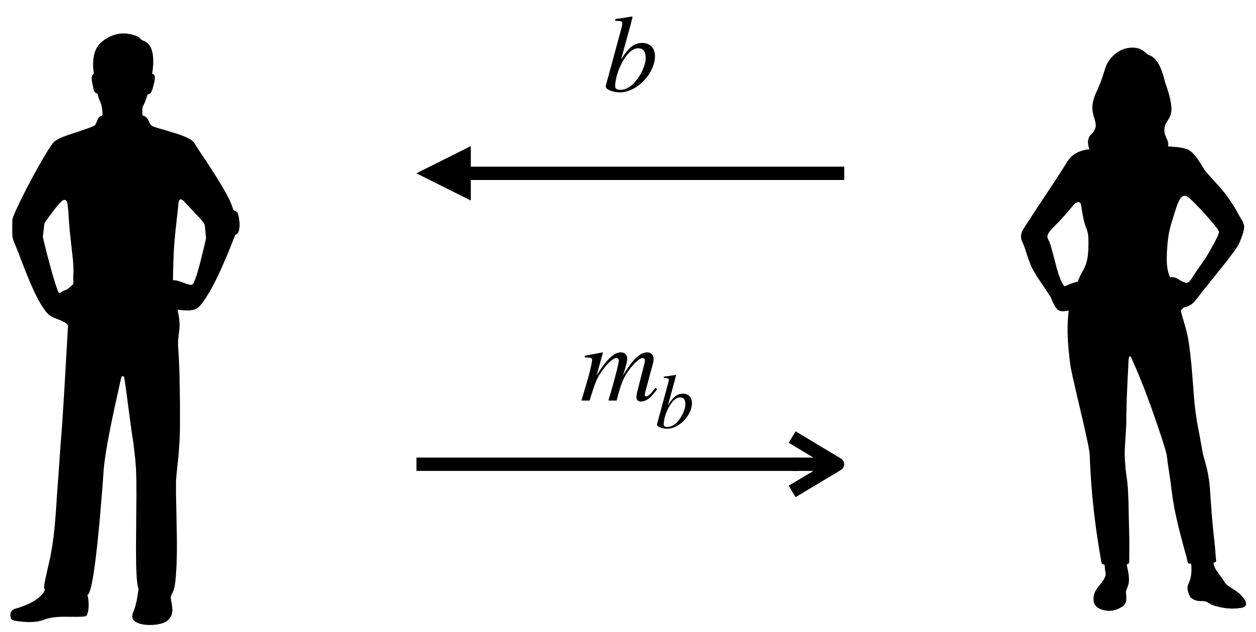
## Rounds

$\geq 2$



## Communication complexity (#bits exchanged)

$\geq 2$ bits per OT



# How much interaction needed for OT?

| **Rounds** | **Communication complexity (#bits exchanged)** |
|---|---|
| $\geq 2$ | $\geq 2$ bits per OT |

**Previous works:** [GH19,BDGM19,BBDP22,BDS23]

# How much interaction needed for OT?

| **Rounds** | **Communication complexity (#bits exchanged)** |
|---|---|
| $\geq 2$ | $\geq 2$ bits per OT |

**Previous works:** [GH19,BDGM19,BBDP22,BDS23]

**Security:** Semi-honest or one-sided malicious (e.g. SSP)

# How much interaction needed for OT?

| **Rounds** | **Communication complexity (#bits exchanged)** |
|---|---|
| $\geq 2$ | $\geq 2$ bits per OT |

**Malicious Security?**

**Previous works:** [GH19,BDGM19,BBDP22,BDS23]

**Security:** Semi-honest or one-sided malicious (e.g. SSP)

# How much interaction needed for Malicious OT?

| | **Rounds** | **Communication complexity (#bits exchanged per OT)** |
|---|---|---|
| Semi-honest<br>One-sided malicious | $\geq 2$ | $\geq 2$ |
| Malicious | | |

# How much interaction needed for Malicious OT?

| | Rounds | Communication complexity (#bits exchanged per OT) |
|---|---|---|
| Semi-honest<br>One-sided malicious | $\geq 2$ | $\geq 2$ |
| **M**alicious | $\geq 2^{*}$ | |

* In the CRS model

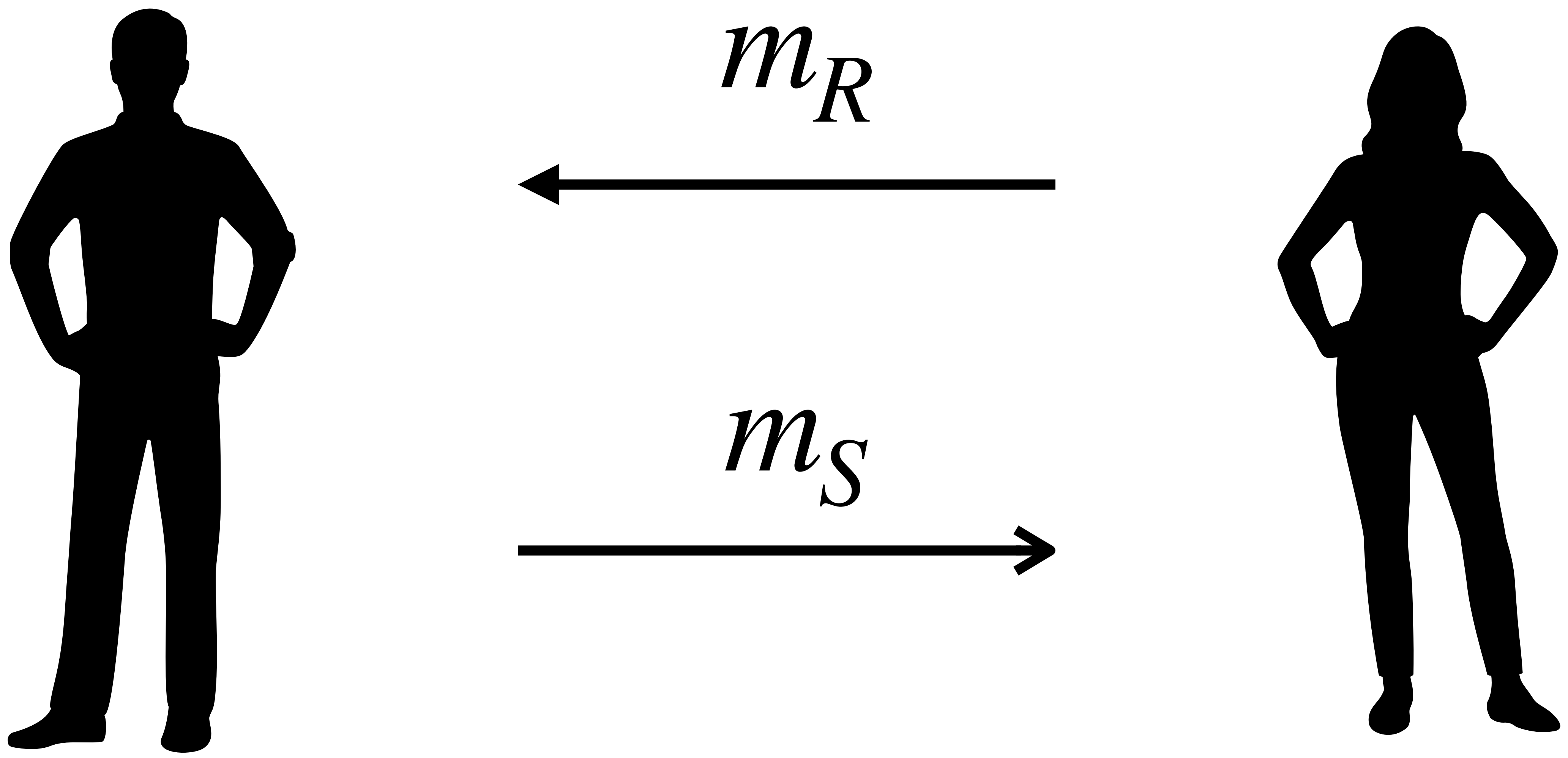
# How much interaction needed for Malicious OT?

| | Rounds | Communication complexity (#bits exchanged per OT) |
|---|---|---|
| Semi-honest<br>One-sided malicious | $\geq 2$ | $\geq 2$ |
| Malicious | $\geq 2$ * | $\geq 3$ ** |

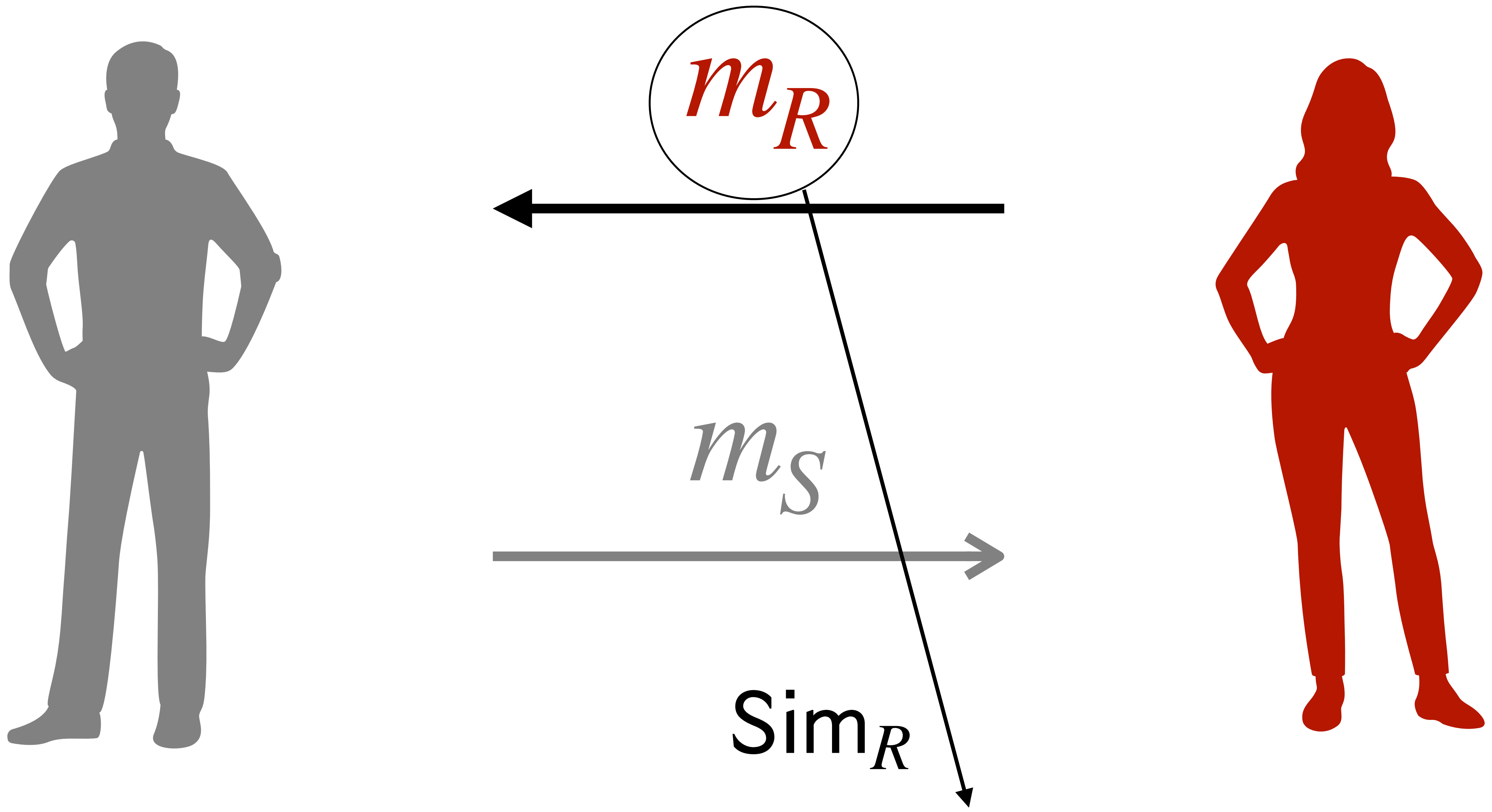
* In the CRS model

** In two rounds

# How much interaction needed for Malicious OT?



# How much interaction needed for Malicious OT?



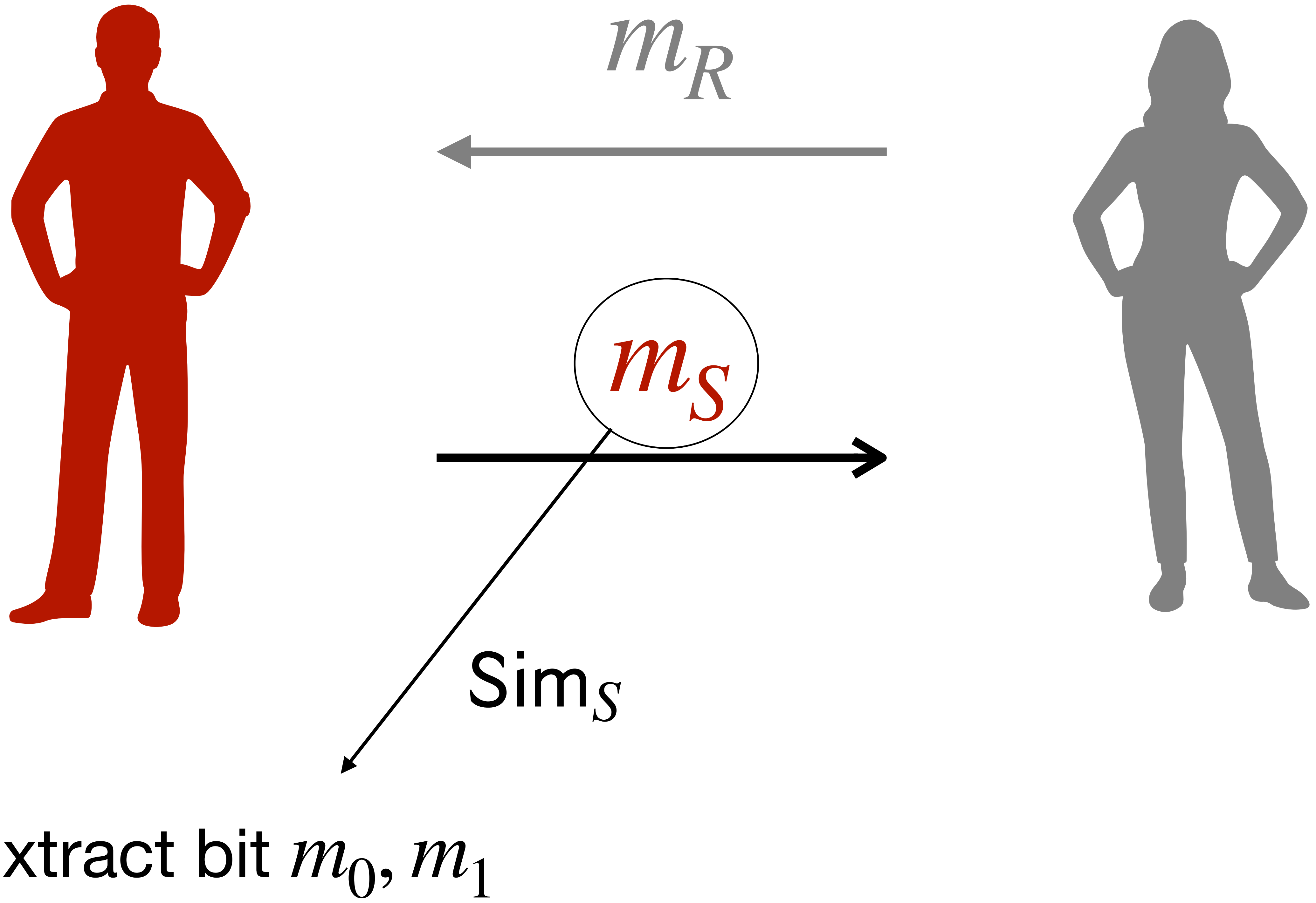
$m_R$

$m_S$

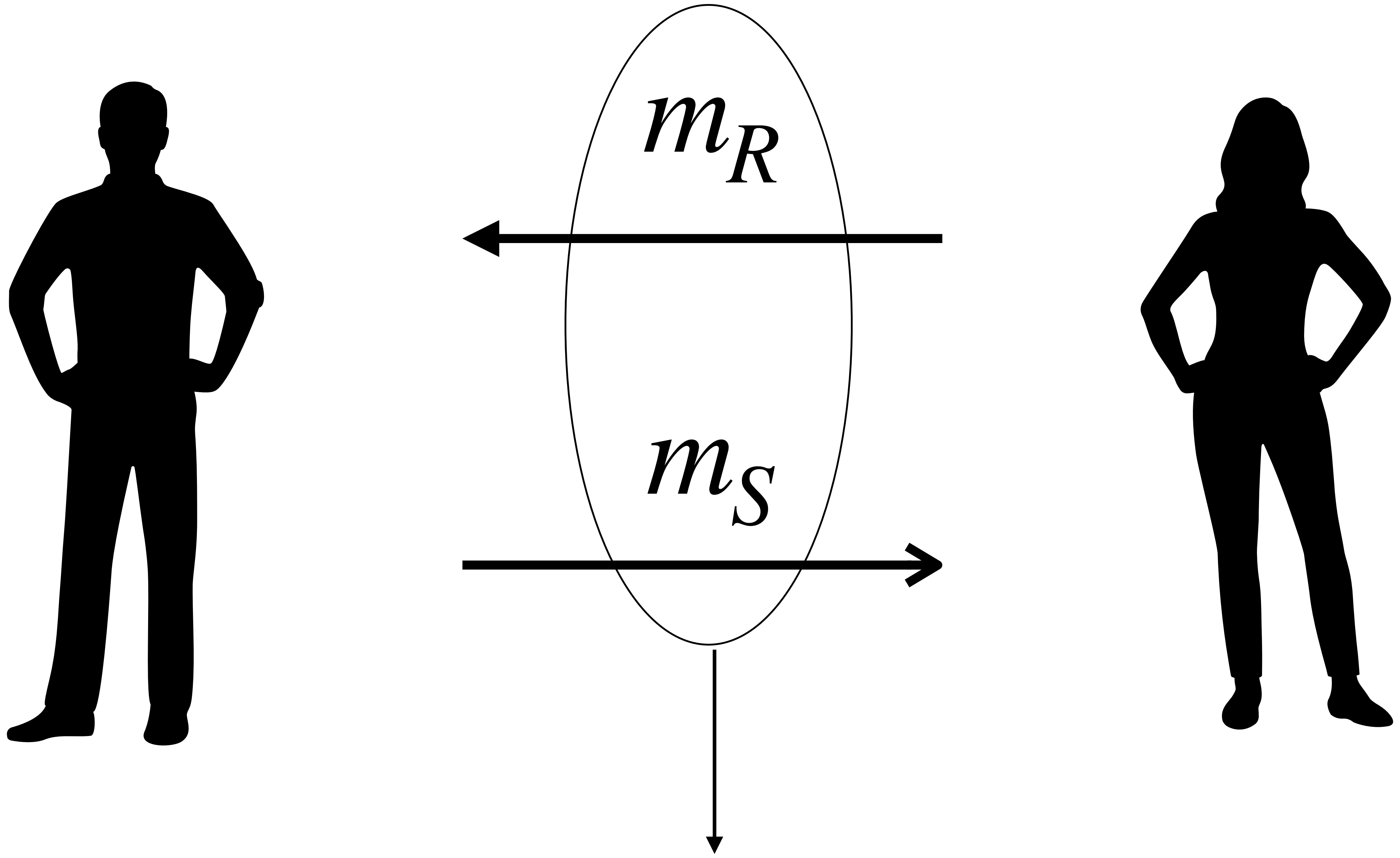
$\mathsf{Sim}_R$

Extract bit $b$

# How much interaction needed for **Malicious** OT?

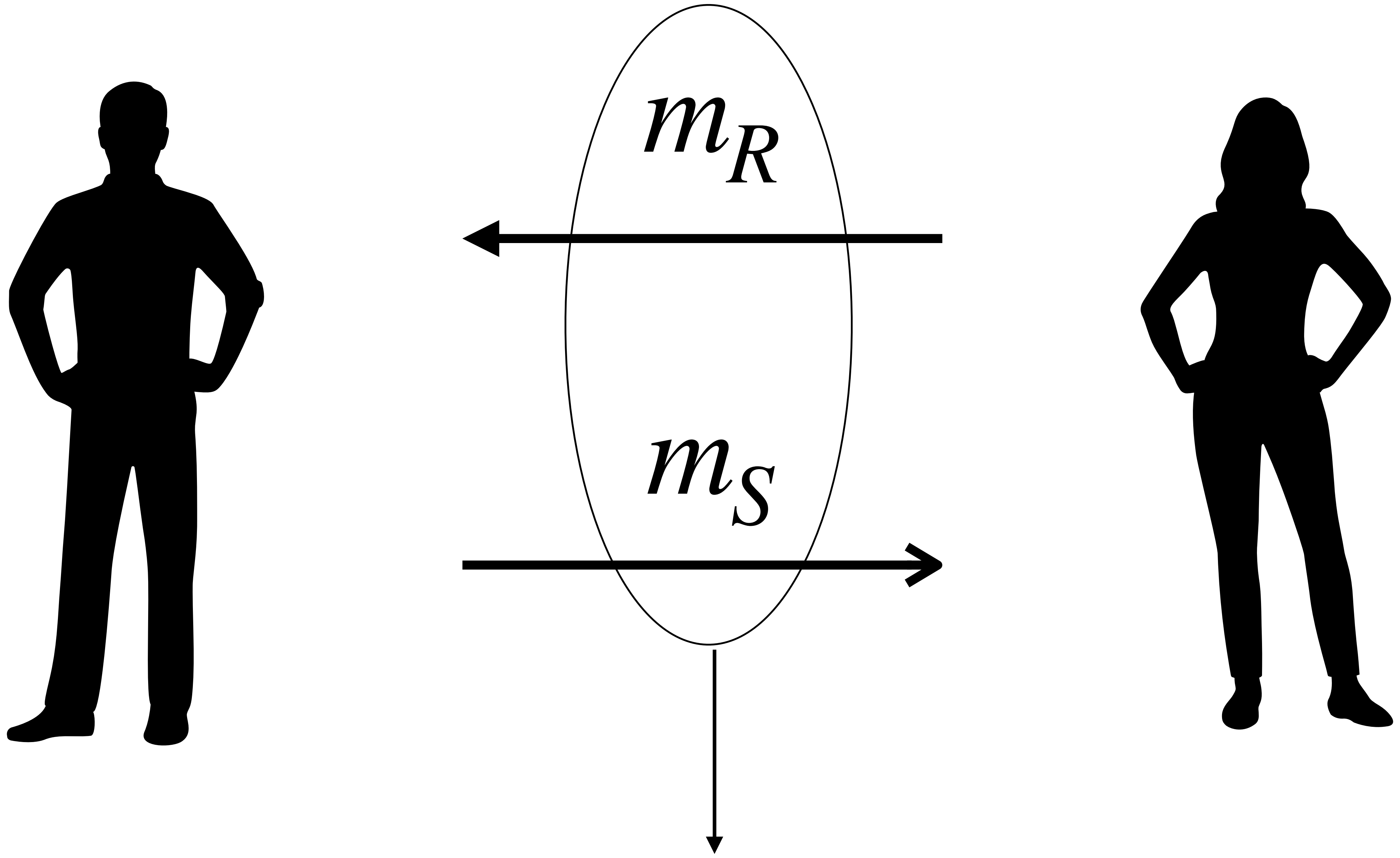


# How much interaction needed for Malicious OT?



Size $\geq |b| + |m_0| + |m_1| = 3$

# How much interaction needed for **Malicious** OT?



Size $\geq |b| + |m_0| + |m_1| = 3$

If communication is $\approx 3$ then it's optimal rate

# Malicious OT schemes with Optimal Rate

Malicious OT with optimal rate in two rounds?

# Malicious OT schemes with Optimal Rate

Malicious OT with optimal rate in two rounds?

- **LWE** via spooky FHE [DHRW16]
- **QR/DCR with long CRS** via PCGs [OSY21]
- **LPN and Random Oracle** via silent OT extensions [BCG+19]

# Malicious OT schemes with Optimal Rate

Malicious OT with optimal rate in two rounds?

- **LWE** via spooky FHE [DHRW16]
- **QR/DCR with long CRS** via PCGs [OSY21]
- **LPN and Random Oracle** via silent OT extensions [BCG+19]

Malicious two-round OT with optimal rate with a short CRS?

# Our Results

**Our Result:** Two-round batch-OT scheme:

# Our Results

**Our Result:** Two-round batch-OT scheme:

- **UC-secure against malicious adversaries under QR+LPN.**
- **Short and reusable CRS**
- **Optimal rate:** Total communication of $3k + o(k) \cdot \text{poly}(\lambda)$ for a batch $k$

# Blueprint of our Construction

OT from TDH “a la PVW”

Sender’s message:
optimal size

Receiver’s message:
large

# Blueprint of our Construction

OT from TDH “a la PVW”

Not Sender Secure!!

# Blueprint of our Construction

OT from TDH “a la PVW”

Not Sender Secure!!

Sender Security using LPN

Sender’s message:
optimal size

Receiver’s message:
large

# Blueprint of our Construction

| | | |
|---|---|---|
| OT from TDH “a la PVW” | Not Sender Secure!! | |
| Sender Security using LPN | Sender’s message:<br>optimal size | Receiver’s message:<br>large |
| Optimal upload rate via:<br>Key homomorphic TDH & LPN | Sender’s message:<br>optimal size | Receiver’s message:<br>Optimal size |

# Blueprint of our Construction

| | | |
|---|---|---|
| OT from TDH “a la PVW” | Not Sender Secure!! | |
| Sender Security using LPN | Sender’s message: optimal size | Receiver’s message: large |
| Optimal upload rate via: Key homomorphic TDH & LPN | Sender’s message: optimal size | Receiver’s message: Optimal size |
| Correct LPN errors | Our result | |

# Blueprint of our Construction

OT from TDH “a la PVW”

Not Sender Secure!!

Sender Security using LPN

Sender’s message:
optimal size

Receiver’s message:
large

Optimal upload rate via:
Key homomorphic TDH & LPN

Sender’s m
optima

Hybrid Encryption
[BBDP22,BDS23]

message:
al size

Correct LPN errors

Our result

# Blueprint of our Construction

OT from TDH “a la PVW”

Not Sender Secure!!

Sender Security using LPN

Sender’s message:
optimal size

Receiver’s message:
large

Optimal upload rate via:
Key homomorphic TDH & LPN

Sender’s message:
optimal size

Receiver’s message:
Optimal size

Correct LPN errors

Our result

# Trapdoor hash functions [DGI+19]

- **Hash:** $\mathsf{H}(\mathsf{hk}, \mathbf{x}) \rightarrow \mathsf{h}$

# Trapdoor hash functions [DGI+19]

- **Hash:** $\mathsf{H}(\mathsf{hk}, \mathbf{x}) \rightarrow \mathsf{h}$
- **KeyGen with respect to** $f$**:** $(\mathsf{ek}, \mathsf{td})$

$\mathsf{Enc}(\mathsf{ek}, \mathbf{x})$ $\mathsf{Dec}(\mathsf{td}, h)$

# Trapdoor hash functions [DGI+19]

- **Hash:** $\mathrm{H}(\mathrm{hk}, \mathbf{x}) \rightarrow \mathrm{h}$
- **KeyGen with respect to $f$:** $(\mathrm{ek}, \mathrm{td})$

$\mathrm{Enc}(\mathrm{ek}, \mathbf{x})$

$\mathrm{Dec}(\mathrm{td}, h)$

Additive shares of $f(\mathbf{x})$

$$\mathrm{Enc}(\mathrm{ek}, \mathbf{x}) \oplus \mathrm{Dec}(\mathrm{td}, h) = f(\mathbf{x})$$

# Trapdoor hash functions [DGI+19]

- **Hash:** $\text{H}(\text{hk}, \mathbf{x}) \rightarrow \text{h}$
- **KeyGen with respect to $f$:** $(\text{ek}, \text{td})$

$\text{Enc}(\text{ek}, \mathbf{x})$ ↘

$\text{Dec}(\text{td}, h)$ ↙

Additive shares of $f(\mathbf{x})$

$$\text{Enc}(\text{ek}, \mathbf{x}) \oplus \text{Dec}(\text{td}, h) = f(\mathbf{x})$$

**Security:** ek hides $f$

# Trapdoor hash functions [DGI+19]

- **Hash:** $\mathsf{H}(\mathsf{hk}, \mathbf{x}) \to \mathsf{h}$
- **KeyGen with respect to $f$:** $(\mathsf{ek}, \mathsf{td})$

$\mathsf{Enc}(\mathsf{ek}, \mathbf{x})$

$\mathsf{Dec}(\mathsf{td}, h)$

Additive shares of $f(\mathbf{x})$

$$\mathsf{Enc}(\mathsf{ek}, \mathbf{x}) \oplus \mathsf{Dec}(\mathsf{td}, h) = f(\mathbf{x})$$

**Security:** ek hides $f$

**Instantiations:** DDH, LWE, QR

# Trapdoor hash functions [DGI+19]

- **Hash:** $\mathsf{H}(\mathsf{hk}, \mathbf{x}) \rightarrow \mathsf{h}$
- **KeyGen with respect to $f$:** $(\mathsf{ek}, \mathsf{td})$

$\mathsf{Enc}(\mathsf{ek}, \mathbf{x})$ $\mathsf{Dec}(\mathsf{td}, h)$ Additive shares of $f(\mathbf{x})$

$$\mathsf{Enc}(\mathsf{ek}, \mathbf{x}) \oplus \mathsf{Dec}(\mathsf{td}, h) = f(\mathbf{x})$$

**Security:** ek hides $f$

**Instantiations:** DDH, LWE, QR

*Perfect correctness*

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t} \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

**Receiver** $(b)$**:**

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t} \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

**Receiver** $(b)$**:**

$\xleftarrow{\text{ek}}$

- ek encodes $b \cdot \mathbf{t}$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t} \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)

$$\xleftarrow{\quad \text{ek} \quad}$$

**Receiver** $(b)$**:**

- ek encodes $b \cdot \mathbf{t}$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t} \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_0 = \mathsf{Enc}(\mathsf{ek}, \mathbf{r}) \oplus \mu_0$
- $w_1 = \mathsf{Enc}(\mathsf{ek}, \mathbf{r}) \oplus \langle \mathbf{t}, \mathbf{r} \rangle \oplus \mu_1$

$$\xleftarrow{\mathsf{ek}}$$

**Receiver** $(b)$**:**

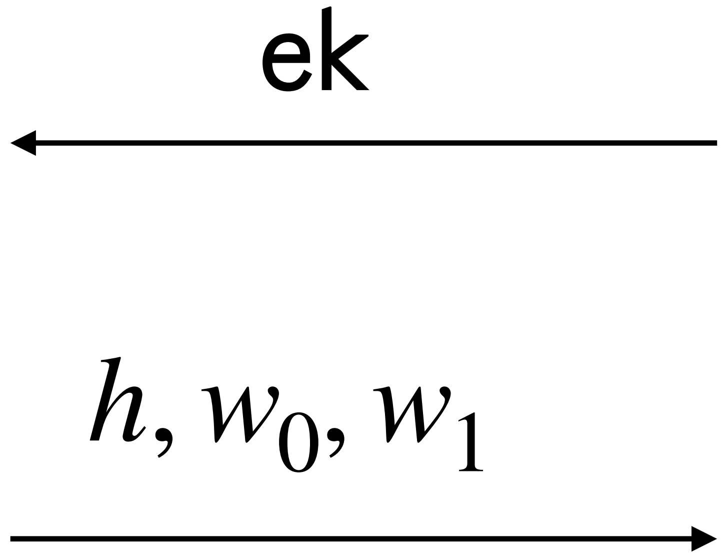
- ek encodes $b \cdot \mathbf{t}$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t} \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_0 = \mathsf{Enc}(\mathsf{ek}, \mathbf{r}) \oplus \mu_0$
- $w_1 = \mathsf{Enc}(\mathsf{ek}, \mathbf{r}) \oplus \langle \mathbf{t}, \mathbf{r} \rangle \oplus \mu_1$



ek

$h, w_0, w_1$

**Receiver** $(b)$**:**

- ek encodes $b \cdot \mathbf{t}$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t} \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_0 =$ Enc(ek, $\mathbf{r}$) $\oplus \mu_0$
- $w_1 =$ Enc(ek, $\mathbf{r}$) $\oplus \langle \mathbf{t}, \mathbf{r} \rangle \oplus \mu_1$

$\xleftarrow{\text{ek}}$

$\xrightarrow{h, w_0, w_1}$

**Receiver** $(b)$**:**

- ek encodes $b \cdot \mathbf{t}$

- Enc(ek, $\mathbf{r}$) $\oplus$ Dec(h, td) $= b \cdot \langle \mathbf{t}, \mathbf{r} \rangle$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t} \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_0 =$ Enc(ek, $\mathbf{r}$) $\oplus \mu_0$
- $w_1 =$ Enc(ek, $\mathbf{r}$) $\oplus \langle \mathbf{t}, \mathbf{r} \rangle \oplus \mu_1$

$\xleftarrow{\quad \text{ek} \quad}$

$\xrightarrow{\quad h, w_0, w_1 \quad}$

**Receiver** $(b)$**:**

- ek encodes $b \cdot \mathbf{t}$

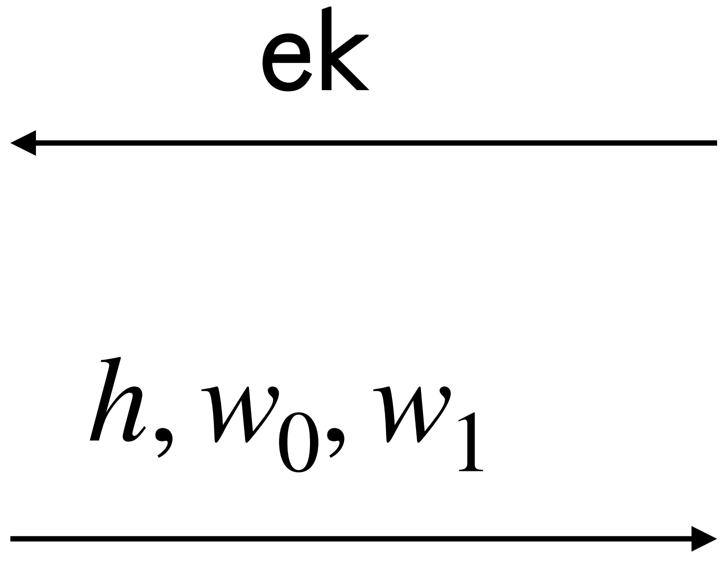
- Enc(ek, $\mathbf{r}$) $\oplus$ Dec(h, td) $= b \cdot \langle \mathbf{t}, \mathbf{r} \rangle$
- **Correct:** For $w_b$, the shift $\langle \mathbf{t}, \mathbf{r} \rangle$ cancels out.

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t} \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- $\mathsf{h} \leftarrow \mathsf{H}(\mathsf{hk}, \mathbf{r})$
- $w_0 = \mathsf{Enc}(\mathsf{ek}, \mathbf{r}) \oplus \mu_0$
- $w_1 = \mathsf{Enc}(\mathsf{ek}, \mathbf{r}) \oplus \langle \mathbf{t}, \mathbf{r} \rangle \oplus \mu_1$



ek

$h, w_0, w_1$

**Receiver** $(b)$**:**

- ek encodes $b \cdot \mathbf{t}$

- $\mathsf{Enc}(\mathsf{ek}, \mathbf{r}) \oplus \mathsf{Dec}(\mathsf{h}, \mathsf{td}) = b \cdot \langle \mathbf{t}, \mathbf{r} \rangle$
- **Correct:** For $w_b$, the shift $\langle \mathbf{t}, \mathbf{r} \rangle$ cancels out.
- **Secure:** For $w_{1-b}$, the shift $\langle \mathbf{t}, \mathbf{r} \rangle$ hides $\mu_{1-b}$ (by LHL).

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t} \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_0 =$ Enc(ek, $\mathbf{r}$) $\oplus \mu_0$
- $w_1 =$ Enc(ek, $\mathbf{r}$) $\oplus \langle \mathbf{t}, \mathbf{r} \rangle \oplus \mu_1$

$$\xleftarrow{\text{ek}}$$

$$\xrightarrow{h, w_0, w_1}$$

**Receiver** $(b)$**:**

- ek encodes $b \cdot \mathbf{t}$

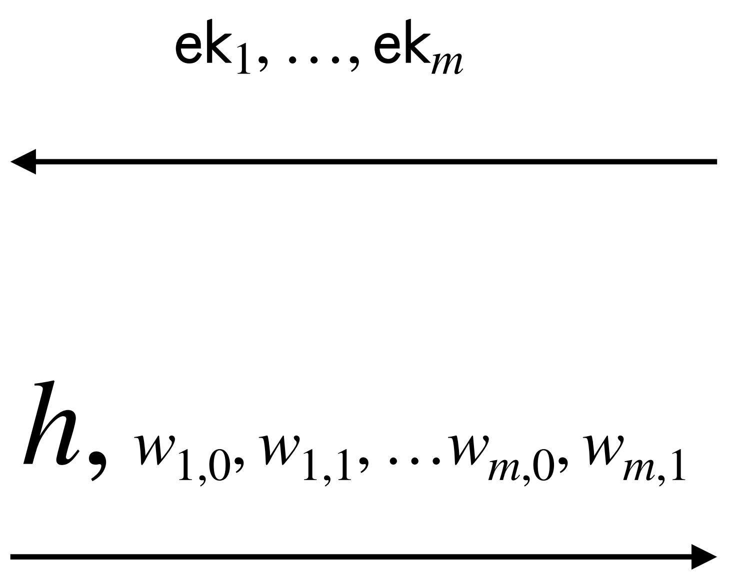
- **Sender's rate:** Not optimal.

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_{i,0}, \mu_{i,1})_{i \in [m]}$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_{1,0} =$ Enc(ek$_1$, $\mathbf{r}$) $\oplus \mu_{1,0}$
- $w_{1,1} =$ Enc(ek$_1$, $\mathbf{r}$) $\oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} =$ Enc(ek$_m$, $\mathbf{r}$) $\oplus \mu_{m,0}$
- $w_{m,1} =$ Enc(ek$_m$, $\mathbf{r}$) $\oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus \mu_{m,1}$



**Receiver** $(b_1, \ldots, b_m)$**:**

- ek$_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- ek$_m$ encodes $b_m \cdot \mathbf{t}_m$

- **Sender's rate:** Not optimal.
- **Solution: Batch OTs**
- Reuse $\mathbf{r}$ (and h) for several ek$_i$ encoding $b_i \cdot \mathbf{t}_i$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_{i,0}, \mu_{i,1})_{i\in[m]}$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_{1,0} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \mu_{1,0}$
- $w_{1,1} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \mu_{m,0}$
- $w_{m,1} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus \mu_{m,1}$

$$\xleftarrow{\mathsf{ek}_1, \ldots, \mathsf{ek}_m}$$

$$\xrightarrow{h,\ w_{1,0}, w_{1,1}, \ldots w_{m,0}, w_{m,1}}$$

**Receiver** $(b_1, \ldots, b_m)$**:**

- $\mathsf{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\mathsf{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

- **Sender's rate:** Not optimal.
- **Solution: Batch OTs**
- Reuse $\mathbf{r}$ (and h) for several $\mathsf{ek}_i$ encoding $b_i \cdot \mathbf{t}_i$
- **Sender's rate:** Optimal!

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_{i,0}, \mu_{i,1})_{i \in [m]}$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_{1,0} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \mu_{1,0}$
- $w_{1,1} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \mu_{m,0}$
- $w_{m,1} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus \mu_{m,1}$

$\xleftarrow{\mathsf{ek}_1, \ldots, \mathsf{ek}_m}$

**Receiver** $(b_1, \ldots, b_m)$**:**

- $\mathsf{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\mathsf{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

**Problem!**

- **Sender's rate:** Not optimal.
- **Solution: Batch OTs**
- Reuse $\mathbf{r}$ (and h) for several $\mathsf{ek}_i$ encoding $b_i \cdot \mathbf{t}_i$
- **Sender's rate:** Optimal!

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_{i,0}, \mu_{i,1})_{i \in [m]}$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_{1,0} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \mu_{1,0}$
- $w_{1,1} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \mu_{m,0}$
- $w_{m,1} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus \mu_{m,1}$

$\xleftarrow{\mathsf{ek}_1, \ldots, \mathsf{ek}_m}$

$\xrightarrow{h,\ w_{1,0}, w_{1,1}, \ldots w_{m,0}, w_{m,1}}$

**Receiver** $(b_1, \ldots, b_m)$**:**

- $\mathsf{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\mathsf{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

- For LHL $L > m$.

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_{i,0}, \mu_{i,1})_{i \in [m]}$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- $\mathsf{h} \leftarrow \mathsf{H}(\mathsf{hk}, \mathbf{r})$
- $w_{1,0} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \mu_{1,0}$
- $w_{1,1} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \mu_{m,0}$
- $w_{m,1} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus \mu_{m,1}$

$\xleftarrow{\mathsf{ek}_1, \ldots, \mathsf{ek}_m}$

$\xrightarrow{h, w_{1,0}, w_{1,1}, \ldots w_{m,0}, w_{m,1}}$

**Receiver** $(b_1, \ldots, b_m)$**:**

- $\mathsf{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\mathsf{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

- For LHL $L > m$.
- Each $\mathsf{ek}_i$ grows with $|t_i|$. That is $|\mathsf{ek}_i| = \Omega(m)$.

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_{i,0}, \mu_{i,1})_{i \in [m]}$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- $\mathsf{h} \leftarrow \mathsf{H}(\mathsf{hk}, \mathbf{r})$
- $w_{1,0} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \mu_{1,0}$
- $w_{1,1} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \mu_{m,0}$
- $w_{m,1} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus \mu_{m,1}$

$$\xleftarrow{\quad \mathsf{ek}_1, \ldots, \mathsf{ek}_m \quad}$$

$$\xrightarrow{\quad h, \ w_{1,0}, w_{1,1}, \ldots w_{m,0}, w_{m,1} \quad}$$

**Receiver** $(b_1, \ldots, b_m)$**:**

- $\mathsf{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\mathsf{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

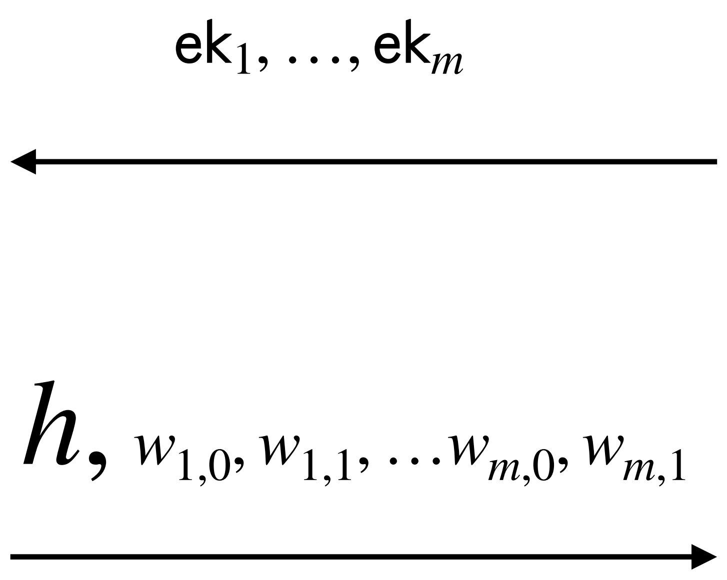
- For LHL $L > m$.
- Each $\mathsf{ek}_i$ grows with $|t_i|$. That is $|\mathsf{ek}_i| = \Omega(m)$.
- Receiver's rate will be a problem!

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_{i,0}, \mu_{i,1})_{i \in [m]}$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_{1,0} = \text{Enc}(\text{ek}_1, \mathbf{r}) \oplus \mu_{1,0}$
- $w_{1,1} = \text{Enc}(\text{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \text{Enc}(\text{ek}_m, \mathbf{r}) \oplus \mu_{m,0}$
- $w_{m,1} = \text{Enc}(\text{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus \mu_{m,1}$

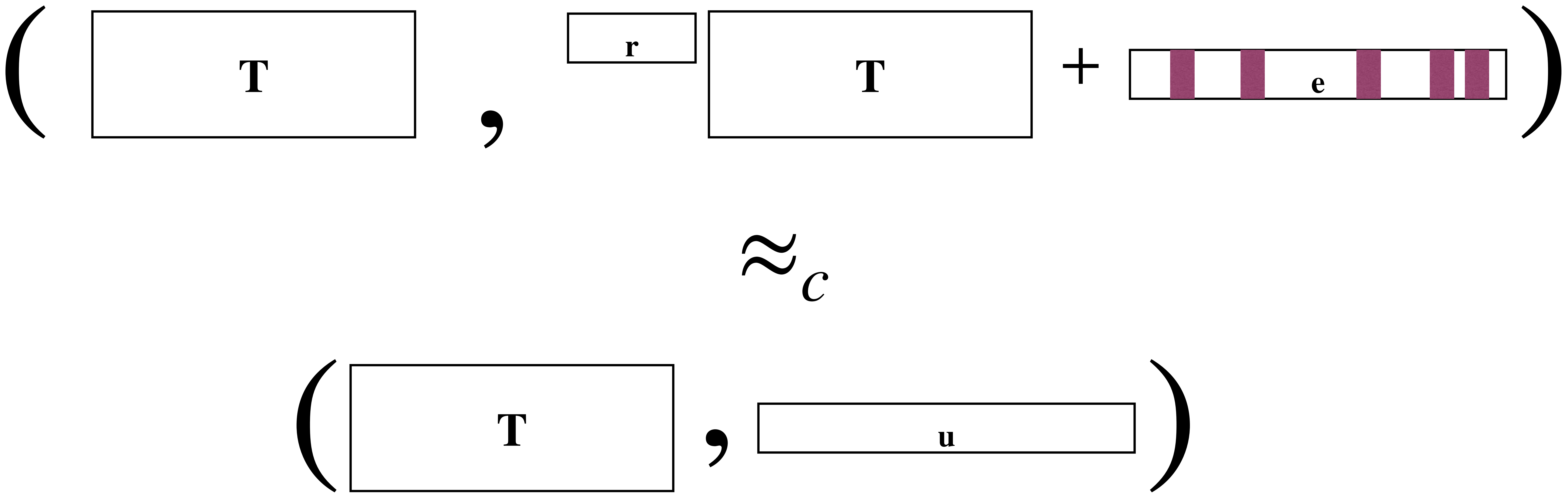


**Receiver** $(b_1, \ldots, b_m)$**:**

- $\text{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\text{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

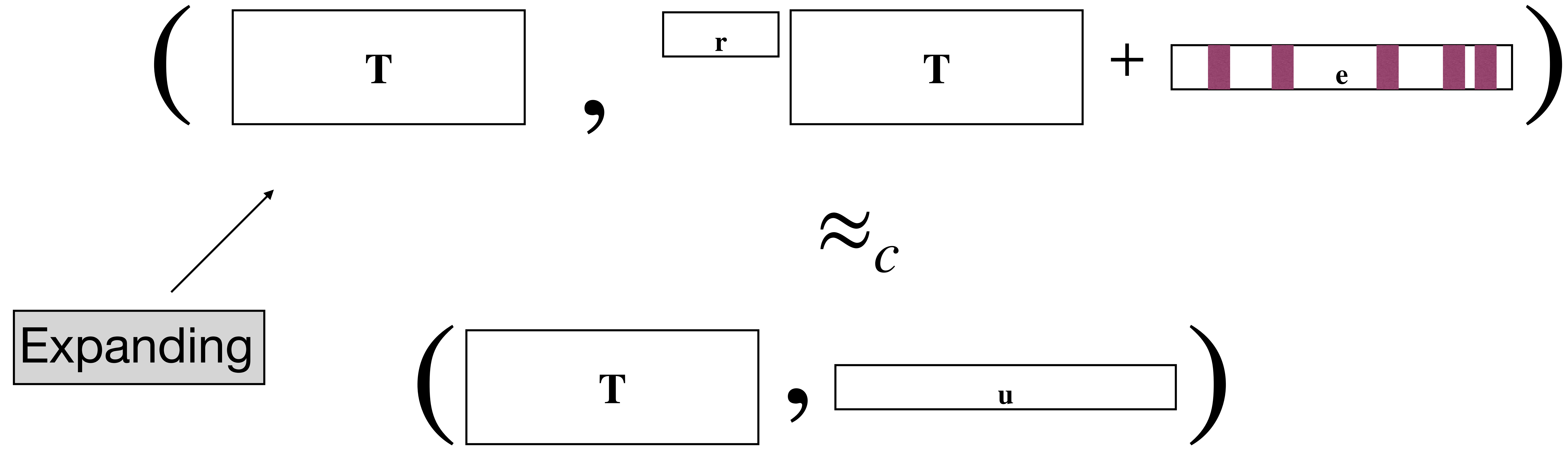
- For LHL $L > m$.
- Each $\text{ek}_i$ grows with $|t_i|$. That is $|\text{ek}_i| = \Omega(m)$.
- Receiver's rate will be a problem!
- **Solution:** Make $L$ independent of $m$.

# Learning Parity with Noise



$\mathbf{T} \leftarrow \{0,1\}^{n \times m}$, $\mathbf{r} \leftarrow \{0,1\}^{n}$, $\mathbf{u} \leftarrow \{0,1\}^{m}$ and $\mathbf{e} \leftarrow \mathsf{Ber}(p)^{m}$

# Learning Parity with Noise



Expanding

$\mathbf{T} \leftarrow \{0,1\}^{n\times m}$, $\mathbf{r} \leftarrow \{0,1\}^{n}$, $\mathbf{u} \leftarrow \{0,1\}^{m}$ and $\mathbf{e} \leftarrow \mathrm{Ber}(p)^{m}$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t} \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h ← H(hk, $\mathbf{r}$)
- $w_0 = \mathsf{Enc}(\mathsf{ek}, \mathbf{r}) \oplus e_0 \oplus \mu_0$
- $w_1 = \mathsf{Enc}(\mathsf{ek}, \mathbf{r}) \oplus \langle \mathbf{t}, \mathbf{r} \rangle \oplus e_1 \oplus \mu_1$

$e_0, e_1 \leftarrow \mathsf{Ber}(p)$

$$\xleftarrow{\quad \mathsf{ek} \quad}$$

$$\xrightarrow{\quad h, w_0, w_1 \quad}$$

**Receiver** $(b)$**:**

- ek encodes $b \cdot \mathbf{t}$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t} \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_0 =$ Enc(ek, $\mathbf{r}$) $\oplus e_0 \oplus \mu_0$
- $w_1 =$ Enc(ek, $\mathbf{r}$) $\oplus \langle \mathbf{t}, \mathbf{r} \rangle \oplus e_1 \oplus \mu_1$

$e_0, e_1 \leftarrow$ Ber$(p)$

$$\xleftarrow{\quad\text{ek}\quad}$$

$$\xrightarrow{\quad h, w_0, w_1\quad}$$

**Receiver** $(b)$**:**

- ek encodes $b \cdot \mathbf{t}$

**Sender security:** via LPN

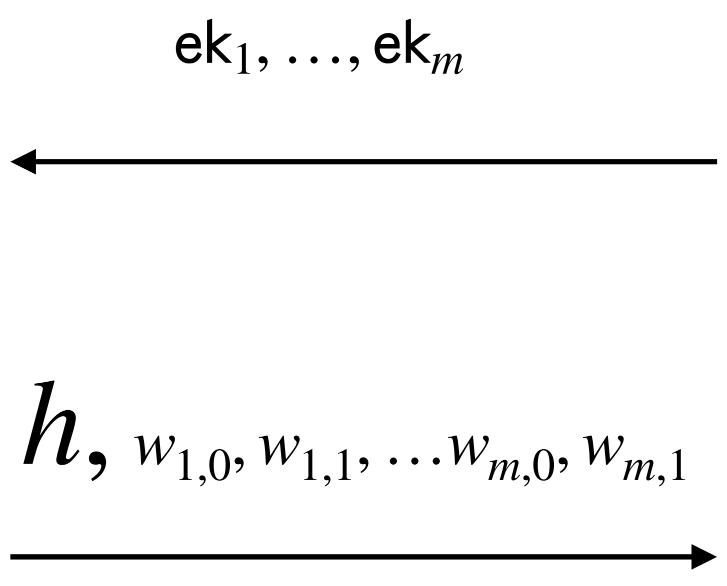
Since $\left(\mathbf{t_i}, \langle \mathbf{t_i}, \mathbf{r} \rangle \oplus e_{i,1-b_i}\right) \approx_c (\mathbf{t_i}, \mathbf{u_i})$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_{1,0} = \text{Enc}(\text{ek}_1, \mathbf{r}) \oplus e_{1,0} \oplus \mu_{1,0}$
- $w_{1,1} = \text{Enc}(\text{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus e_{1,1} \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \text{Enc}(\text{ek}_m, \mathbf{r}) \oplus e_{m,0} \oplus \mu_{m,0}$
- $w_{m,1} = \text{Enc}(\text{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus e_{m,1} \oplus \mu_{m,1}$



$\text{ek}_1, \ldots, \text{ek}_m$

$h,\ w_{1,0}, w_{1,1}, \ldots w_{m,0}, w_{m,1}$

**Receiver** $(b_1, \ldots, b_m)$**:**

- $\text{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\text{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

**Sender security:** via LPN

Since $\left(\mathbf{t_i}, \langle \mathbf{t_i}, \mathbf{r} \rangle \oplus e_{i,1-b_i}\right) \approx_c (\mathbf{t_i}, \mathbf{u_i})$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h ← H(hk, $\mathbf{r}$)

**Leak on $\mathbf{r}$**

- $w_{1,0} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus e_{1,0} \oplus \mu_{1,0}$
- $w_{1,1} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus e_{1,1} \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus e_{m,0} \oplus \mu_{m,0}$
- $w_{m,1} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus e_{m,1} \oplus \mu_{m,1}$

$\xleftarrow{\mathsf{ek}_1, \ldots, \mathsf{ek}_m}$

$\xrightarrow{h,\ w_{1,0}, w_{1,1}, \ldots w_{m,0}, w_{m,1}}$

**Receiver** $(b_1, \ldots, b_m)$**:**

- $\mathsf{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\mathsf{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

**Sender security:** via LPN

Since $\left(\mathbf{t_i}, \langle \mathbf{t_i}, \mathbf{r} \rangle \oplus e_{i,1-b_i}\right) \approx_c (\mathbf{t_i}, \mathbf{u_i})$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h ← H(hk, $\mathbf{r}$)

**Leak on $\mathbf{r}$**

- $w_{1,0} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus e_{1,0} \oplus \mu_{1,0}$
- $w_{1,1} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus e_{1,1} \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus e_{m,0} \oplus \mu_{m,0}$
- $w_{m,1} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus e_{m,1} \oplus \mu_{m,1}$

$\mathsf{ek}_1, \ldots, \mathsf{ek}_m$ ←

$h, w_{1,0}, w_{1,1}, \ldots w_{m,0}, w_{m,1}$ →

**Receiver** $(b_1, \ldots, b_m)$**:**

- ek$_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- ek$_m$ encodes $b_m \cdot \mathbf{t}_m$

**Sender security:** via (entropic?) LPN

Since $\left(\mathbf{t_i}, \langle \mathbf{t_i}, \mathbf{r} \rangle \oplus e_{i,1-b_i}\right) \approx_c (\mathbf{t_i}, \mathbf{u_i})$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_{1,0} = \text{Enc}(\text{ek}_1, \mathbf{r}) \oplus e_{1,0} \oplus \mu_{1,0}$
- $w_{1,1} = \text{Enc}(\text{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus e_{1,1} \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \text{Enc}(\text{ek}_m, \mathbf{r}) \oplus e_{m,0} \oplus \mu_{m,0}$
- $w_{m,1} = \text{Enc}(\text{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus e_{m,1} \oplus \mu_{m,1}$

**Leak on $\mathbf{r}$**

$\text{ek}_1, \ldots, \text{ek}_m$ ←

$h, w_{1,0}, w_{1,1}, \ldots w_{m,0}, w_{m,1}$ →

**Receiver** $(b_1, \ldots, b_m)$**:**

- $\text{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\text{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

**Sender security:** via LPN

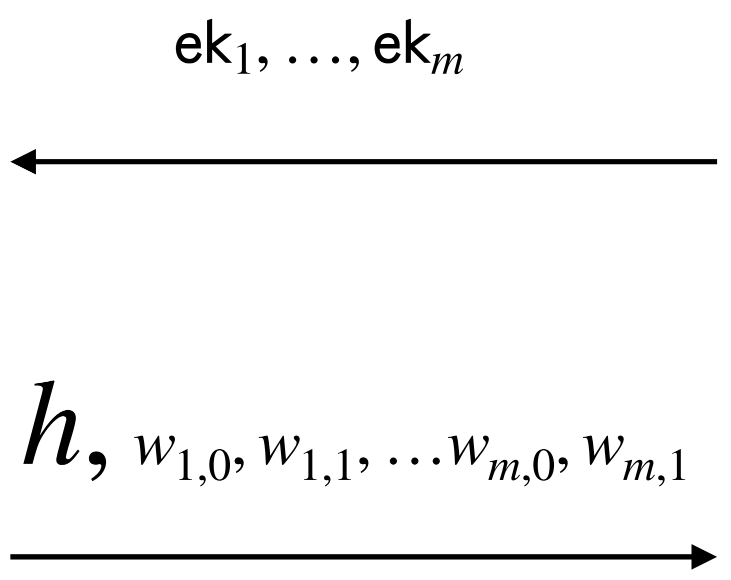
Since $\left(\mathbf{t_i}, \langle \mathbf{t_i}, \mathbf{r} \rangle \oplus e_{i,1-b_i}\right) \approx_c \left(\mathbf{t_i}, \mathbf{u_i}\right)$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- $\mathsf{h} \leftarrow \mathsf{H}(\mathsf{hk}, \mathbf{r})$
- $w_{1,0} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus e_{1,0} \oplus \mu_{1,0}$
- $w_{1,1} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus e_{1,1} \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus e_{m,0} \oplus \mu_{m,0}$
- $w_{m,1} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus e_{m,1} \oplus \mu_{m,1}$



**Receiver** $(b_1, \ldots, b_m)$**:**

- $\mathsf{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\mathsf{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- $\mathsf{h} \leftarrow \mathsf{H}(\mathsf{hk}, \mathbf{r})$
- $w_{1,0} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus e_{1,0} \oplus \mu_{1,0}$
- $w_{1,1} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus e_{1,1} \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus e_{m,0} \oplus \mu_{m,0}$
- $w_{m,1} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus e_{m,1} \oplus \mu_{m,1}$

$$\xleftarrow{\quad \mathsf{ek}_1, \ldots, \mathsf{ek}_m \quad}$$

$$\xrightarrow{\quad h,\ w_{1,0}, w_{1,1}, \ldots w_{m,0}, w_{m,1} \quad}$$

**Receiver** $(b_1, \ldots, b_m)$**:**

- $\mathsf{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\mathsf{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

**Faulty correctness**

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

## Sender $(\mu_0, \mu_1)$:

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_{1,0} = \text{Enc}(\text{ek}_1, \mathbf{r}) \oplus e_{1,0} \oplus \mu_{1,0}$
- $w_{1,1} = \text{Enc}(\text{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus e_{1,1} \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \text{Enc}(\text{ek}_m, \mathbf{r}) \oplus e_{m,0} \oplus \mu_{m,0}$
- $w_{m,1} = \text{Enc}(\text{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus e_{m,1} \oplus \mu_{m,1}$

$$\xleftarrow{\quad \text{ek}_1, \ldots, \text{ek}_m \quad}$$

$$\xrightarrow{\quad h,\ w_{1,0}, w_{1,1}, \ldots w_{m,0}, w_{m,1} \quad}$$

## Receiver $(b_1, \ldots, b_m)$:

- $\text{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\text{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

**2PC**

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- $\mathsf{h} \leftarrow \mathsf{H}(\mathsf{hk}, \mathbf{r})$
- $w_{1,0} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus e_{1,0} \oplus \mu_{1,0}$
- $w_{1,1} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus e_{1,1} \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus e_{m,0} \oplus \mu_{m,0}$
- $w_{m,1} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus e_{m,1} \oplus \mu_{m,1}$

$$\xleftarrow{\mathsf{ek}_1, \ldots, \mathsf{ek}_m}$$

$$\xrightarrow{h,\ w_{1,0}, w_{1,1}, \ldots w_{m,0}, w_{m,1}}$$

**Receiver** $(b_1, \ldots, b_m)$**:**

- $\mathsf{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\mathsf{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

**2PC**

**Communication overhead:**

$\sim$ (Hamming weight of error)

# OT from TDH for linear functions

**CRS:** hk, $\mathbf{t}_1, \ldots, \mathbf{t}_m \leftarrow \{0,1\}^L$

**Sender** $(\mu_0, \mu_1)$**:**

- $\mathbf{r} \leftarrow \{0,1\}^L$
- h $\leftarrow$ H(hk, $\mathbf{r}$)
- $w_{1,0} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus e_{1,0} \oplus \mu_{1,0}$
- $w_{1,1} = \mathsf{Enc}(\mathsf{ek}_1, \mathbf{r}) \oplus \langle \mathbf{t}_1, \mathbf{r} \rangle \oplus e_{1,1} \oplus \mu_{1,1}$
- $\vdots$
- $w_{m,0} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus e_{m,0} \oplus \mu_{m,0}$
- $w_{m,1} = \mathsf{Enc}(\mathsf{ek}_m, \mathbf{r}) \oplus \langle \mathbf{t}_m, \mathbf{r} \rangle \oplus e_{m,1} \oplus \mu_{m,1}$

$$\xleftarrow{\mathsf{ek}_1, \ldots, \mathsf{ek}_m}$$

$$\xrightarrow{h,\ w_{1,0}, w_{1,1}, \ldots w_{m,0}, w_{m,1}}$$

**Receiver** $(b_1, \ldots, b_m)$**:**

- $\mathsf{ek}_1$ encodes $b_1 \cdot \mathbf{t}_1$
- $\vdots$
- $\mathsf{ek}_m$ encodes $b_m \cdot \mathbf{t}_m$

**2PC**

**Communication overhead:**

$\sim$ (Hamming weight of error)

$\uparrow$

Set as $m^\epsilon$

# Malicious security against senders

**Malicious security:**

- Almost for free → Perfect correctness of TDH

# Malicious security against senders

**Malicious security:**

- Almost for free → Perfect correctness of TDH

- h of $\mathbf{r}$ are well-formed. → **2PC**

**Communication overhead:**

$\sim |\mathbf{r}|$

↑

Set as $m^{\epsilon}$

# Recap

- This talk: two-round maliciously-sender secure OT with optimal download rate from QR + LPN.

# Recap

- This talk: two-round maliciously-sender secure OT with optimal download rate from QR + LPN.

↓

- Main Result: two-round maliciously-secure OT with optimal rate from QR + LPN.

# Recap

- **This talk:** two-round maliciously-sender secure OT with optimal download rate from QR + LPN.

↓

- **Main Result:** two-round maliciously-secure OT with optimal rate from QR + LPN.
- **Main insight:** how to use TDH with LPN for improved communication and security.

# Recap

- This talk: two-round maliciously-sender secure OT with optimal download rate from QR + LPN.

↓

- Main Result: two-round maliciously-secure OT with optimal rate from QR + LPN.
- Main insight: how to use TDH with LPN for improved communication and security.

**Thanks!**

# Two-Round Maliciously-Secure Oblivious Transfer with Optimal Rate

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

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

**Akshayaram Srinivasan** *University of Toronto*