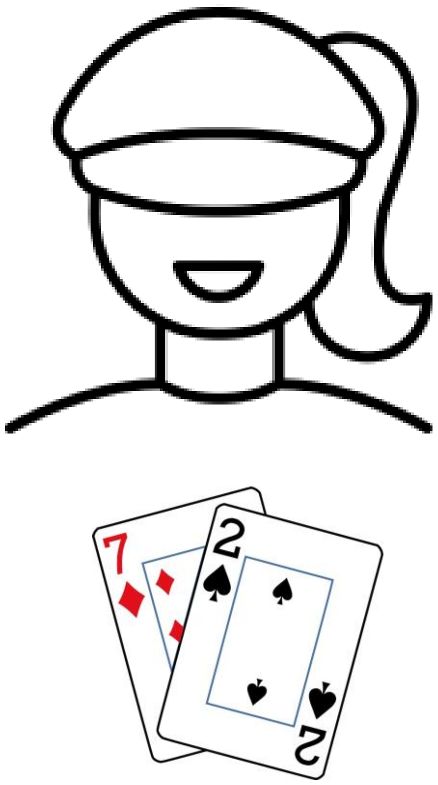
Secure Computation with Shared EPR Pairs

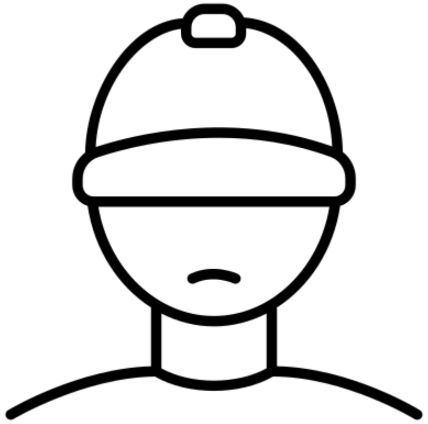
(Or: How to Teleport in Zero-Knowledge)

James Bartusek — UC Berkeley

Dakshita Khurana — UIUC

Akshayaram Srinivasan — Tata Institute of Fundamental Research

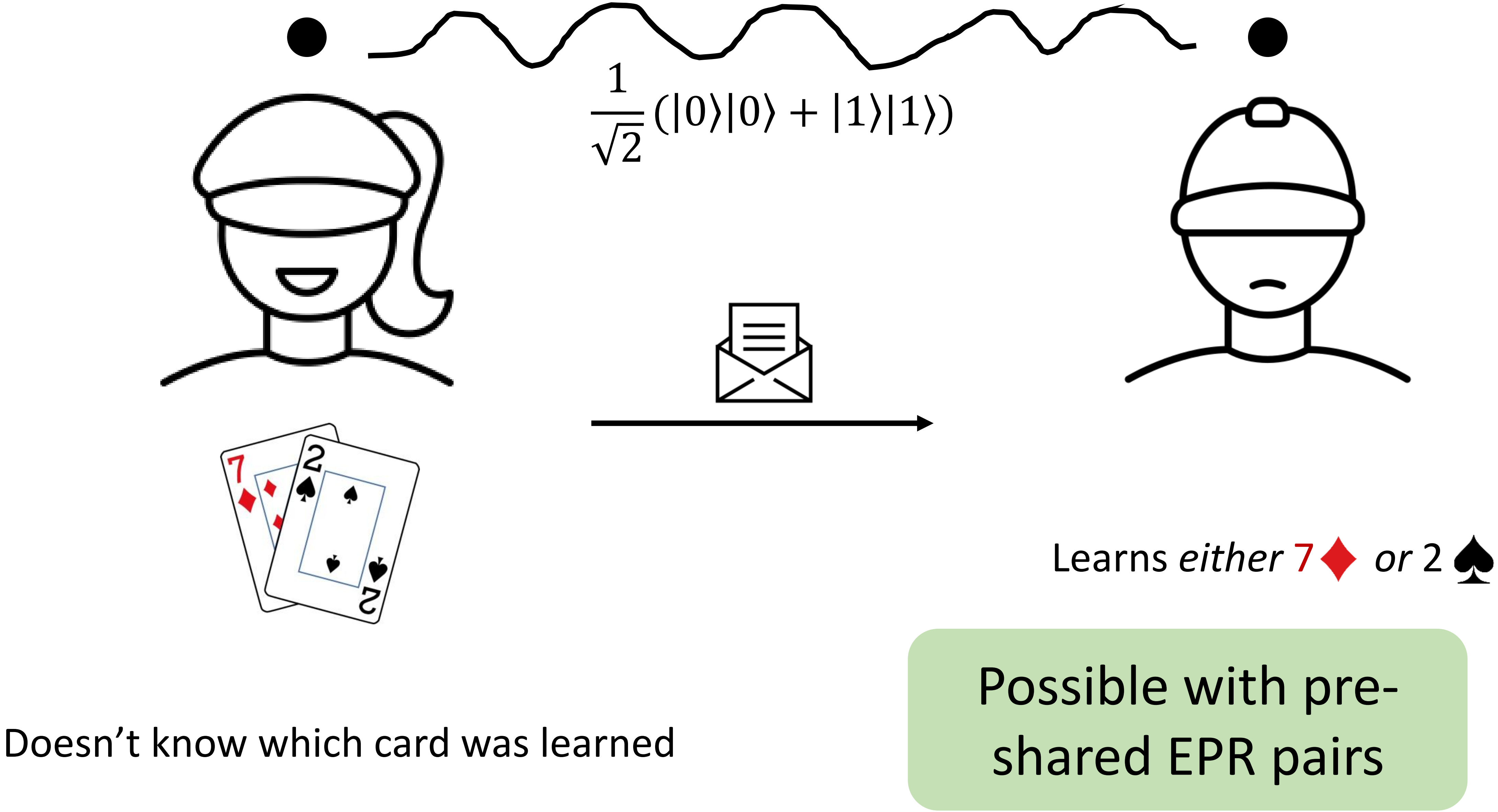




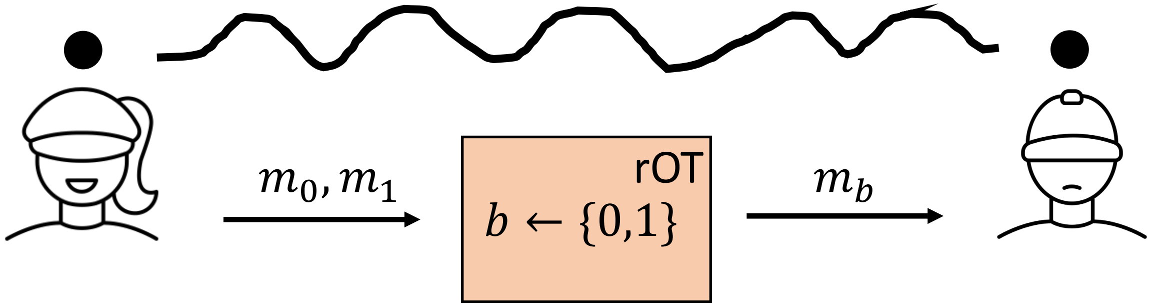
Learns *either* 7♦ *or* 2♠

Doesn’t know which card was learned

Impossible!


$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$
Learns *either* 7♦ *or* 2♠
Doesn't know which card was learned
Possible with pre-shared EPR pairs

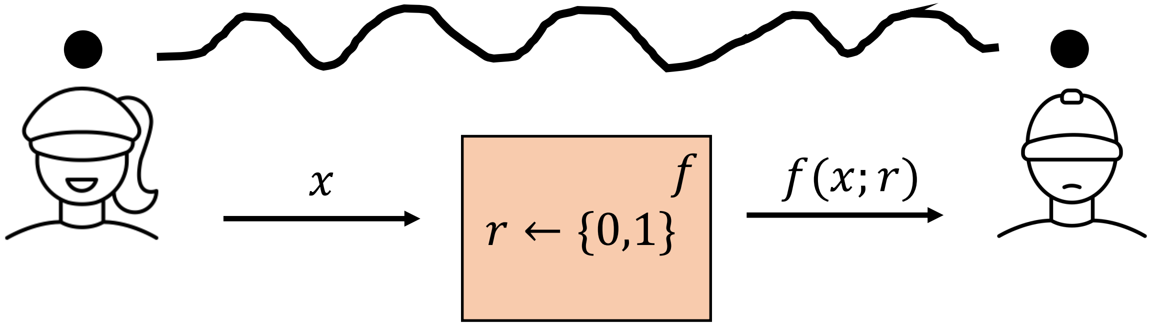
Result #1: Assuming the sub-exponential hardness of LWE, there exists a one-message random-receiver-bit string OT protocol in the shared EPR pairs model



Prior work: [Agarwal, **B**, Khurana, Kumar 23] gave a one-message random-receiver-bit *bit* OT protocol in the shared EPR pairs model using a *random oracle*

Corollary #1: Assuming the sub-exponential hardness of LWE, there exists a one-message secure computation protocol for any unidirectional classical functionality

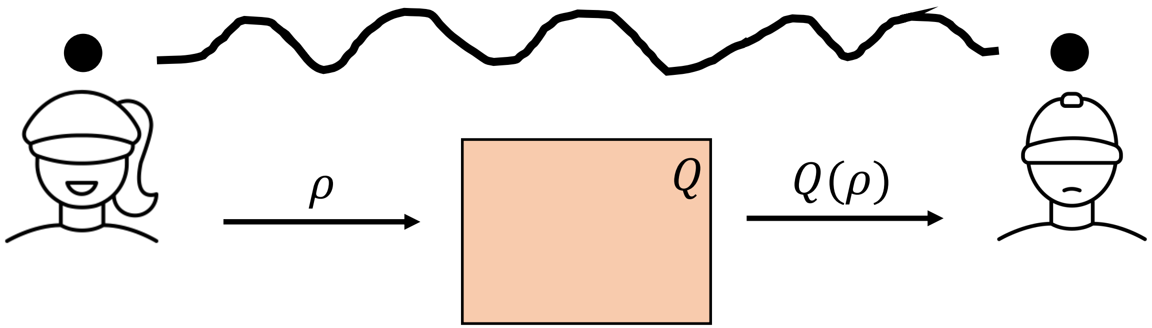
[Garg, Ishai, Kushilevitz, Ostrovsky, Sahai 15]



Prior work: [GIKOS 15] and [Agarwal, Ishai, Kushilevitz, Narayanan, Prabhakaran, Prabhakaran, Rosen 20 / 21] study one-message protocols for unidirectional classical functionalities in a *noisy channel model*

Corollary #2: Assuming the sub-exponential hardness of LWE, there exists a one-message secure computation protocol for any unidirectional quantum functionality

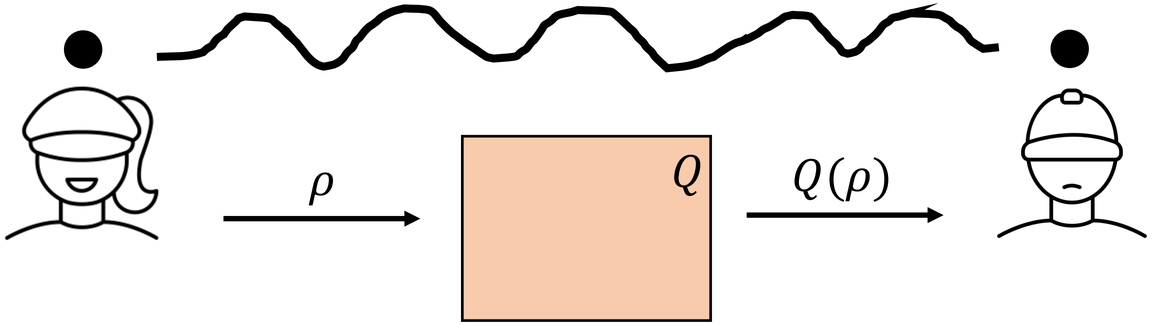
[**B**, Coladangelo, Khurana, Ma 21]



"Secure teleportation through Q"

Corollary #2: Assuming the sub-exponential hardness of LWE, there exists a one-message secure computation protocol for any unidirectional *quantum* functionality

[**B**, Coladangelo, Khurana, Ma 21]

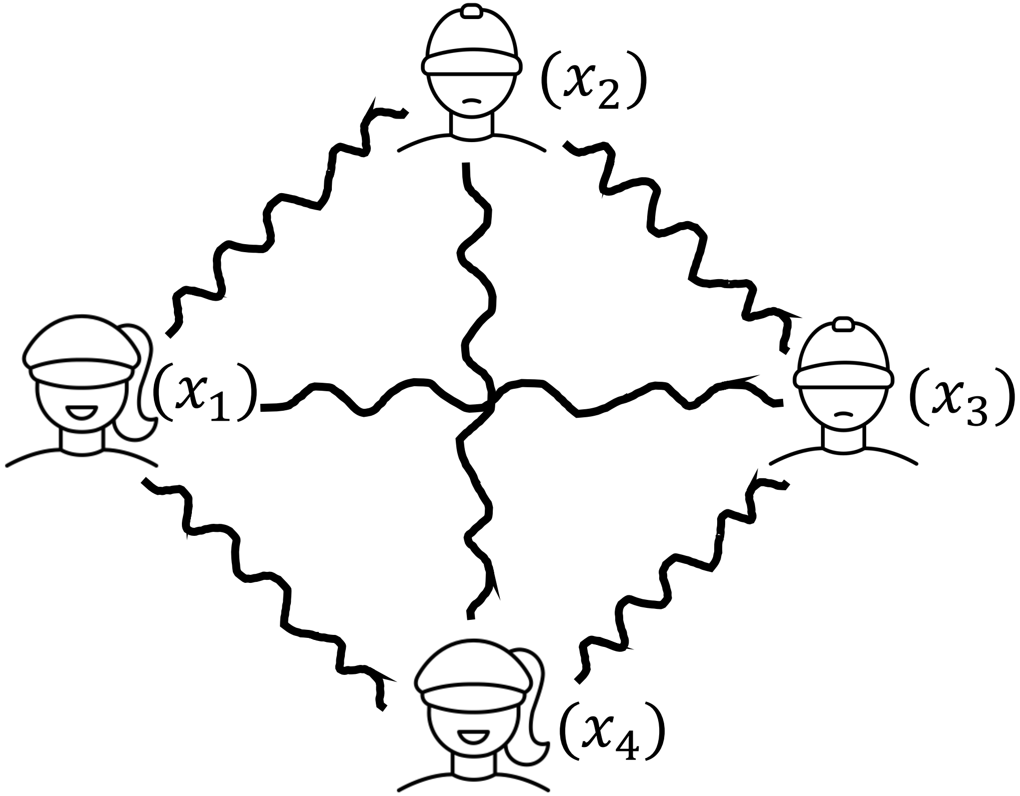


Special cases:

- NIZK for QMA. Prior work [Morimae, Yamakawa 22] gave a protocol in the shared EPR pairs model using a *random oracle*.
- Non-interactive zero-knowledge state synthesis.

Result #2: There exists two-round MPC in the shared EPR pairs model from (the black-box use of) hash functions

Goal: compute $f(x_1, x_2, x_3, x_4)$

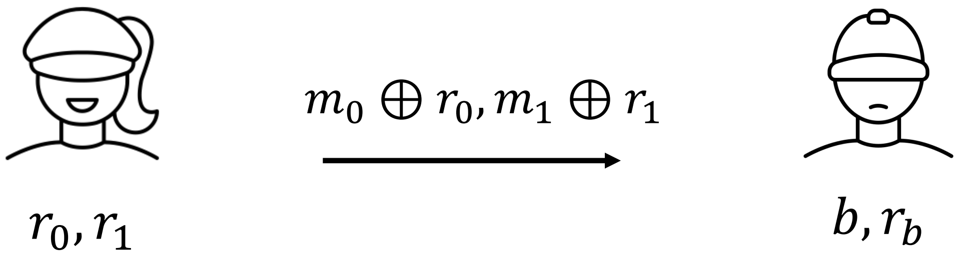


Prior work:

- Two-round MPC in the CRS model with public-key assumptions …, [Garg, Srinivasan 18], [Benhamouda, Lin 18]
- Multi-round MPC without public-key assumptions …, [Grilo, Lin, Song, Vaikuntanathan 21], [**B**, Coladangelo, Khurana, Ma 21]

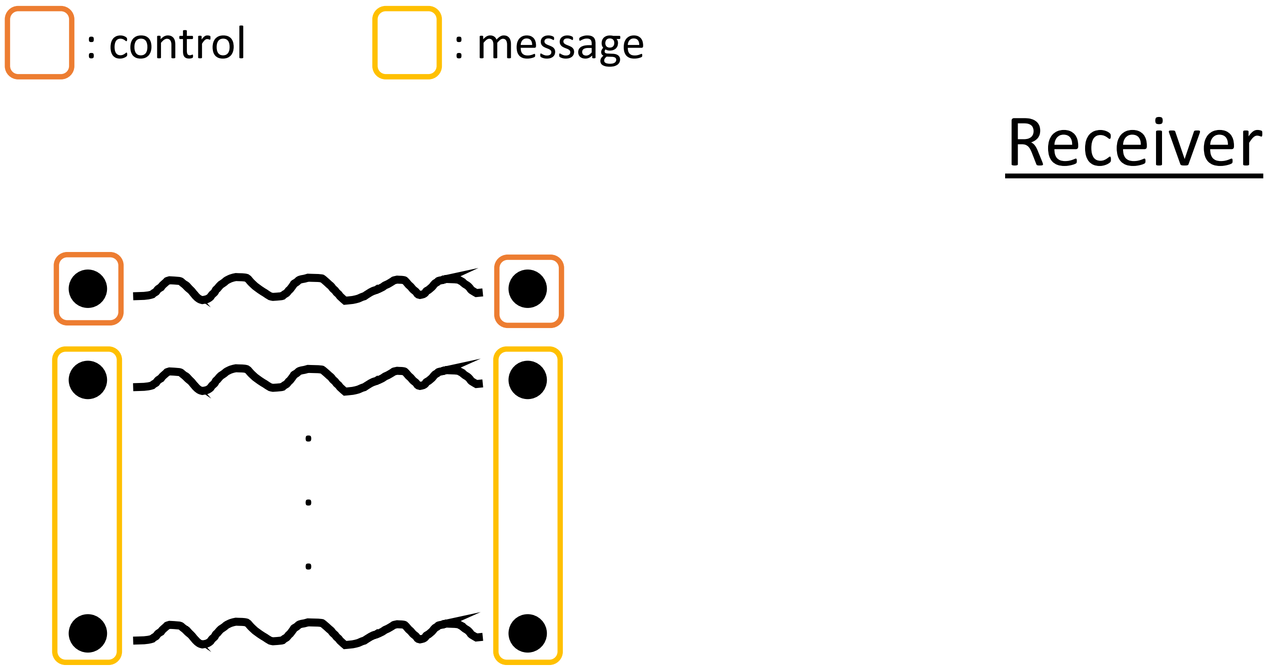
The One-Message OT Protocol

Via OT correlations:



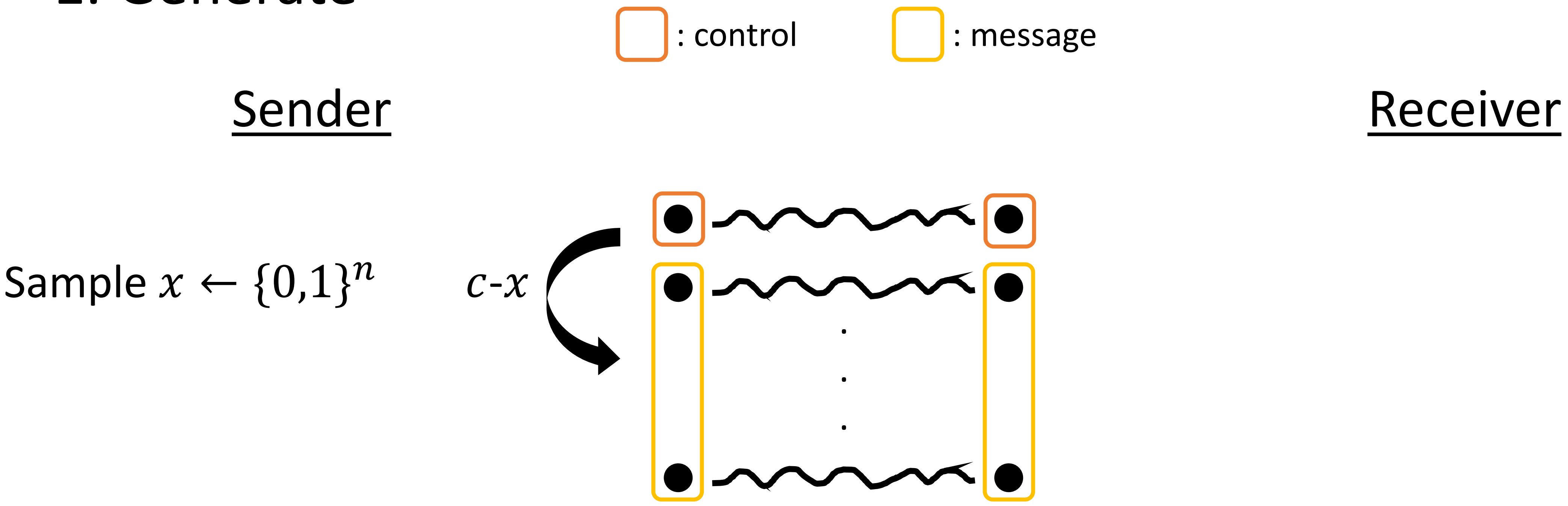
1. Generate: use shared EPR pairs to generate insecure correlations
2. Delete: run a deletion protocol to obtain weakly secure correlations
3. Combine: obtain one strongly secure correlation from many weakly secure correlations

1. Generate



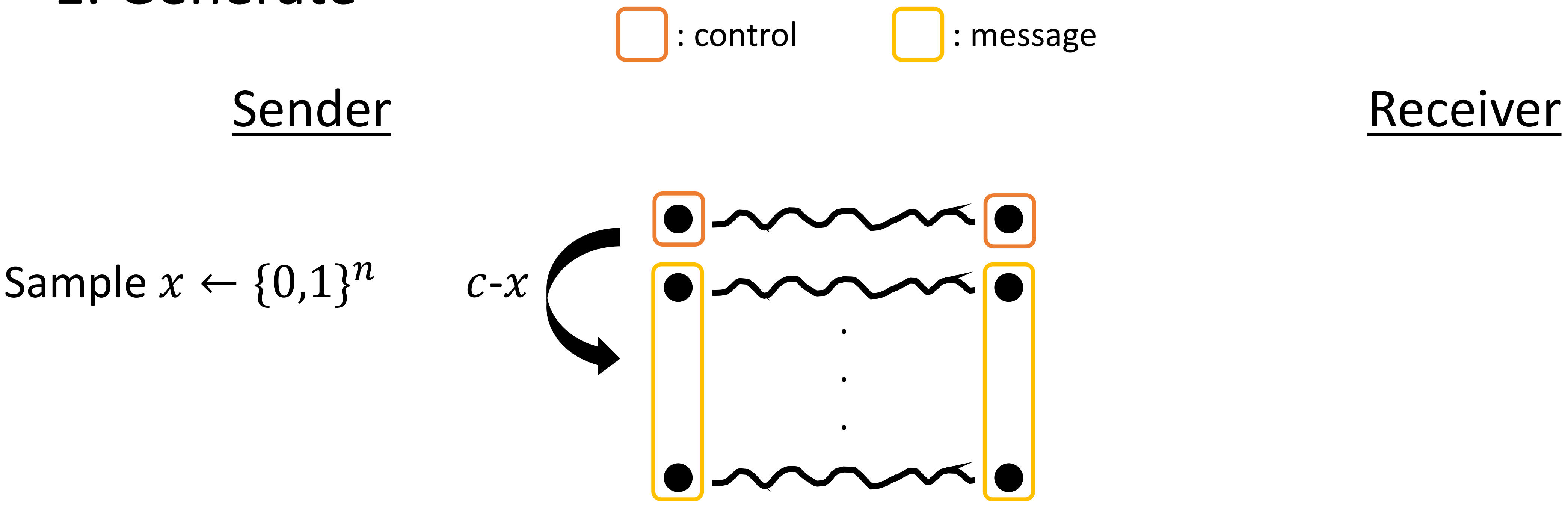
$$\sum_{b\in\{0,1\},v\in\{0,1\}^n} |b\rangle_{S_{ctl}}|v\rangle_{S_{msg}}|b\rangle_{R_{ctl}}|v\rangle_{R_{msg}}$$

1. Generate



$$\sum_{b\in\{0,1\}, v\in\{0,1\}^n} |b\rangle_{S_{ctl}} |v \oplus b \cdot x\rangle_{S_{msg}} |b\rangle_{R_{ctl}} |v\rangle_{R_{msg}}$$

1. Generate



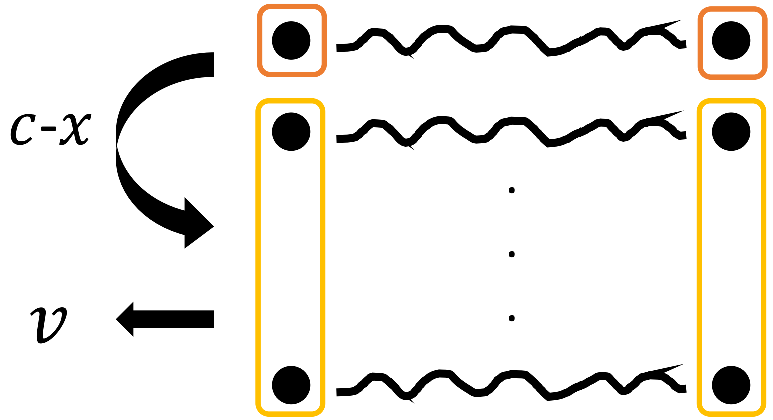
$$\sum_{b \in \{0,1\}, v \in \{0,1\}^n} |b\rangle_{S_{ctl}} |v\rangle_{S_{msg}} |b\rangle_{R_{ctl}} |v \oplus b \cdot x\rangle_{R_{msg}}$$

1. Generate

: control : message

Sender **Receiver**

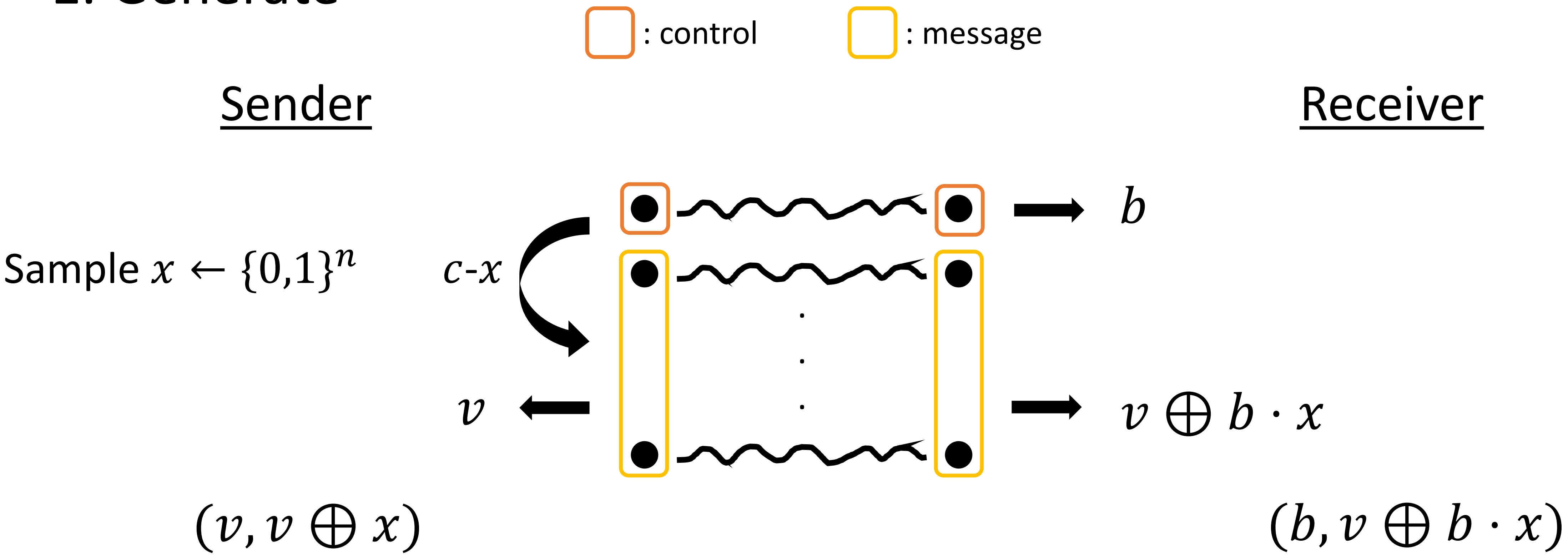
Sample $x \leftarrow \{0,1\}^n$



$(v, v \oplus x)$

$$\sum_{b\in\{0,1\}} |b\rangle_{S_{ctl}}|v\rangle_{S_{msg}}|b\rangle_{R_{ctl}}|v \oplus b \cdot x\rangle_{R_{msg}}$$

1. Generate



$$|b\rangle_{S_{ctl}} |v\rangle_{S_{msg}} |b\rangle_{R_{ctl}} |v \oplus b \cdot x\rangle_{R_{msg}}$$

1. Generate

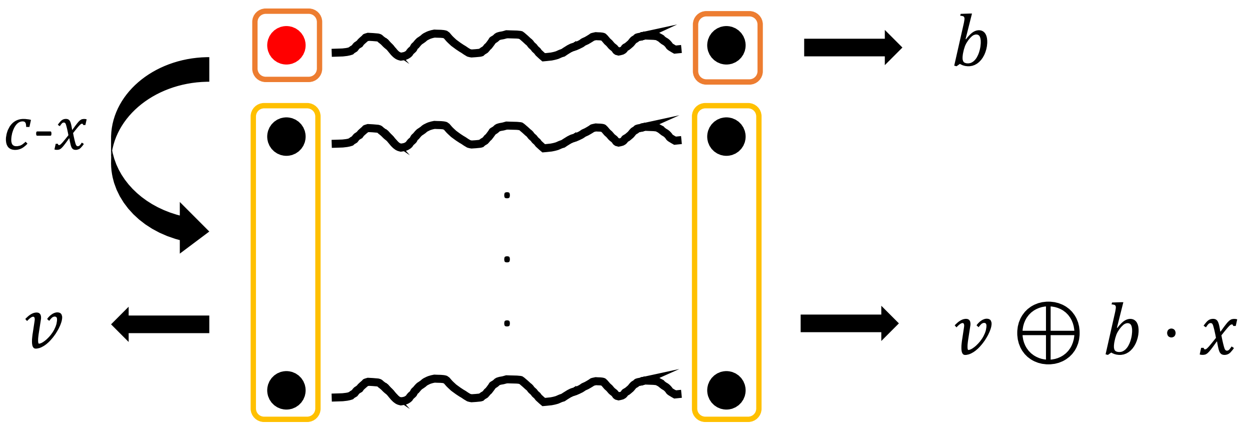
: control : message

Sender

Insecure, because S_{ctl} holds the receiver's bit b

Receiver

Sample $x \leftarrow \{0,1\}^n$



$(v, v \oplus x)$

$(b, v \oplus b \cdot x)$

$$|b\rangle_{S_{ctl}} |v\rangle_{S_{msg}} |b\rangle_{R_{ctl}} |v \oplus b \cdot x\rangle_{R_{msg}}$$

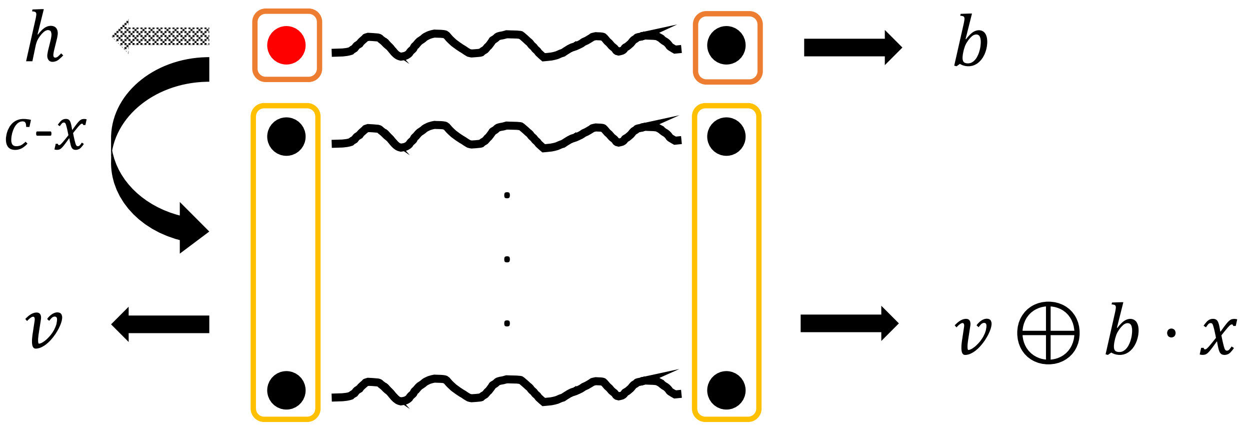
Idea: ask Sender to "delete" b by measuring S_{ctl} in the Hadamard basis

2. Delete

: control : message

Sender **Receiver**

Sample $x \leftarrow \{0,1\}^n$



$(v, v \oplus x)$

$(b, v \oplus b \cdot x)$

$$|h\rangle_{S_{ctl}} |v\rangle_{S_{msg}} \left(|0, v\rangle_R + (-1)^h \left|1, v \oplus x\right\rangle_R\right)$$

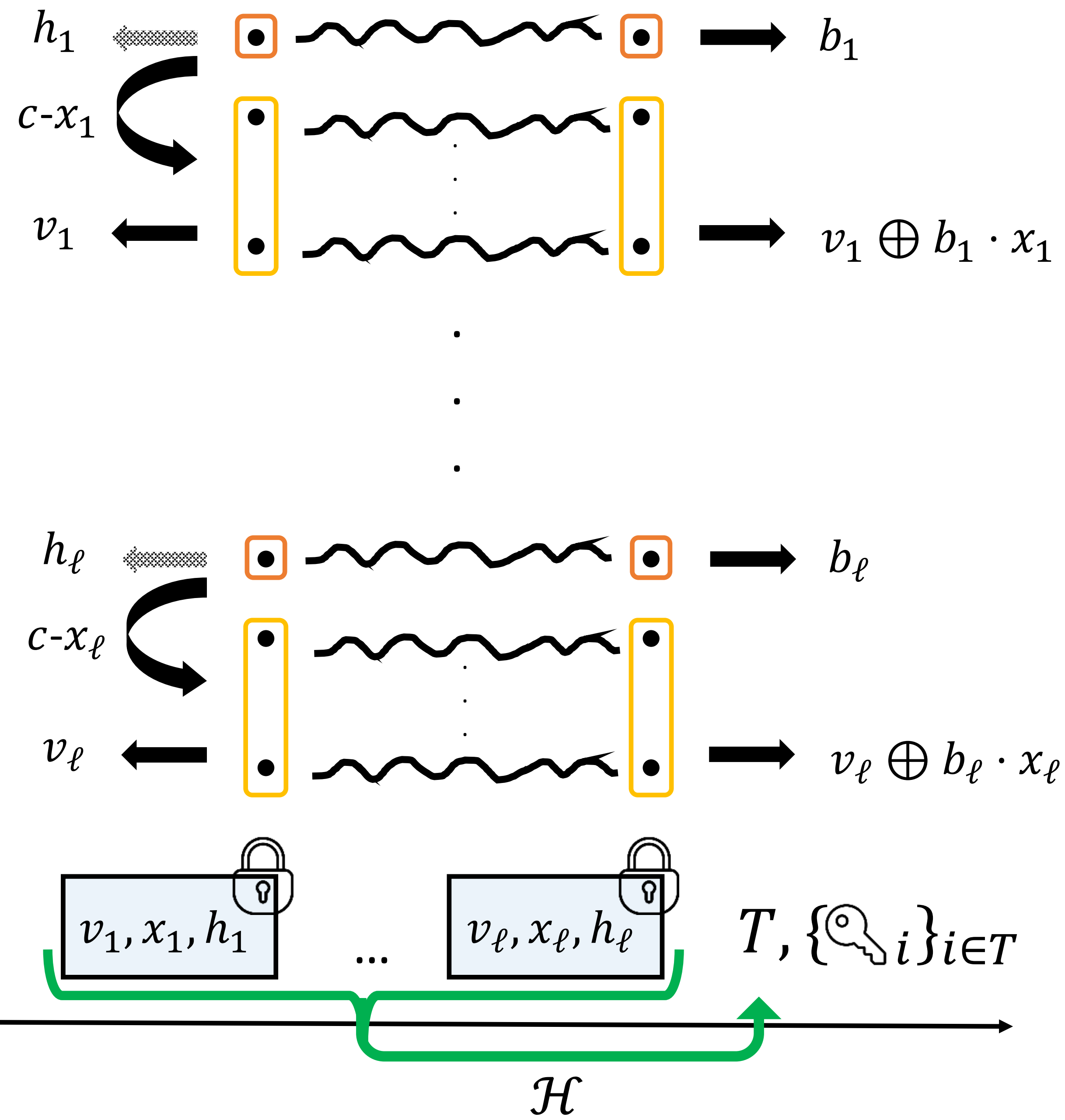
Given (v, x, h), Receiver can check that the Sender is being honest

2. Delete

Sender

Receiver

Sample
$x_1, \ldots, x_\ell \leftarrow \{0,1\}^n$



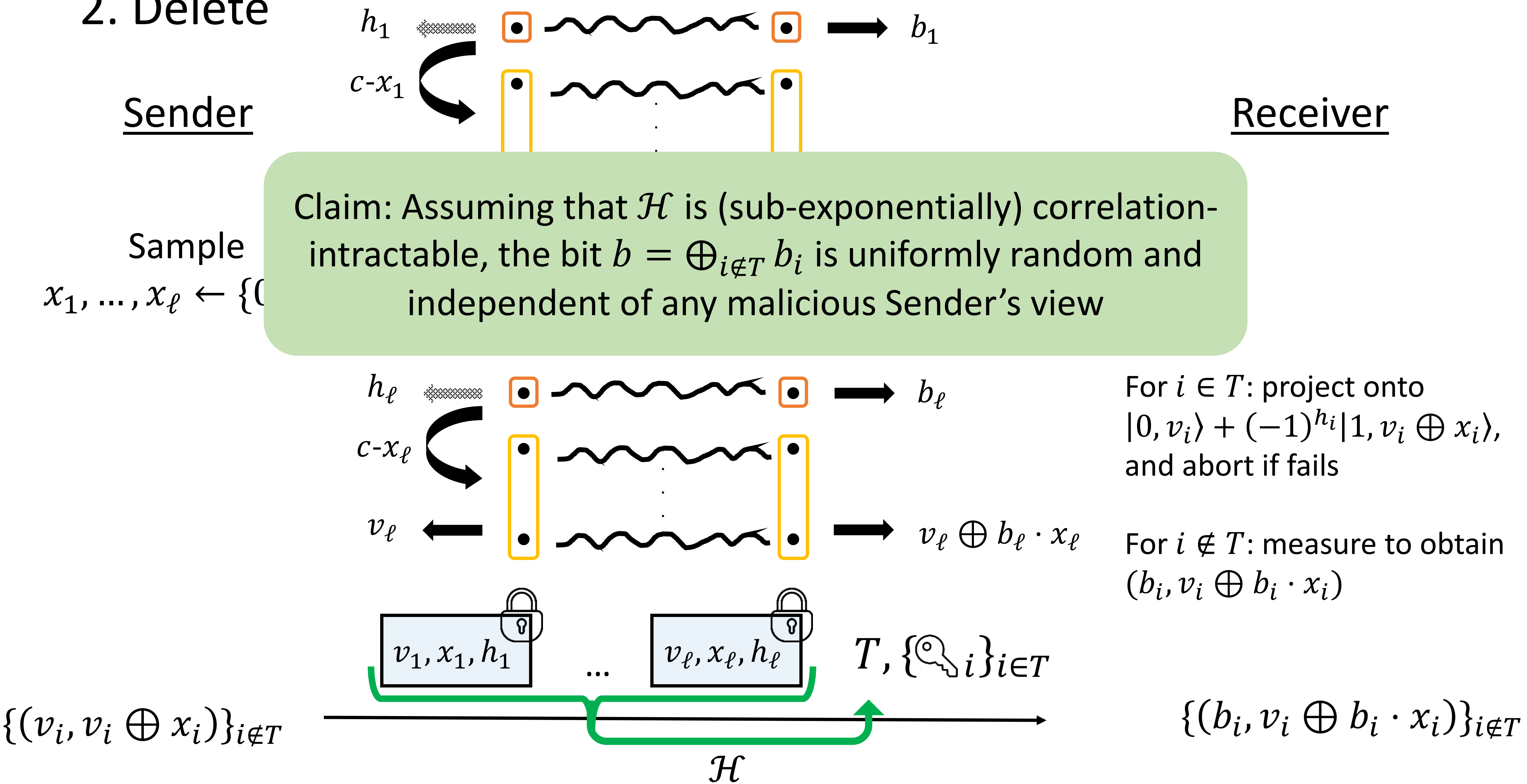
For $i \in T$: project onto $|0, v_i\rangle + (-1)^{h_i}|1, v_i \oplus x_i\rangle$, and abort if fails

For $i \notin T$: measure to obtain $(b_i, v_i \oplus b_i \cdot x_i)$

$\{(v_i, v_i \oplus x_i)\}_{i \notin T}$

$\{(b_i, v_i \oplus b_i \cdot x_i)\}_{i \notin T}$

2. Delete



Claim: Assuming that $\mathcal{H}$ is (sub-exponentially) correlation-intractable, the bit $b = \bigoplus_{i \notin T} b_i$ is uniformly random and independent of any malicious Sender's view

3. Combine

Guarantee: $b = \bigoplus_{i\in[k]} b_i$ is uniformly random from Sender's view

Sender

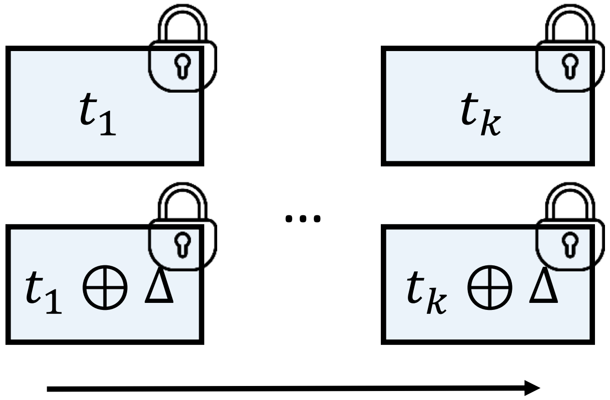
$\{(r_{i,0}, r_{i,1})\}_{i\in[k]}$

Receiver

$\{(b_i, r_{i,b_i})\}_{i\in[k]}$

🔑$_{i,b} = r_{i,b}$

Sample $t_1, \ldots, t_k \leftarrow \{0,1\}^n$
Sample $\Delta \leftarrow \{0,1\}^n$



Open $\{t_i \oplus b_i \cdot \Delta\}_{i\in[k]}$

$(r_0 = \bigoplus_{i\in[k]} t_i,\ \ r_1 = \bigoplus_{i\in[k]} t_i \oplus \Delta)$

$(b = \bigoplus_{i\in[k]} b_i,\ \ r_b = \bigoplus_{i\in[k]} t_i \oplus b \cdot \Delta)$

Conclusion

- Shared EPR pairs model
  - Natural model to study given current quantum internet proposals
  - One-message secure computation / secure teleportation
  - Two-round MPC from (the black-box use of) hash functions

- Concurrent work: [Colisson, Muguruza, Speelman 23] construct two-message chosen-input string OT from hash functions in the CRS model

- Open: Two-round MPC from hash functions in the CRS model