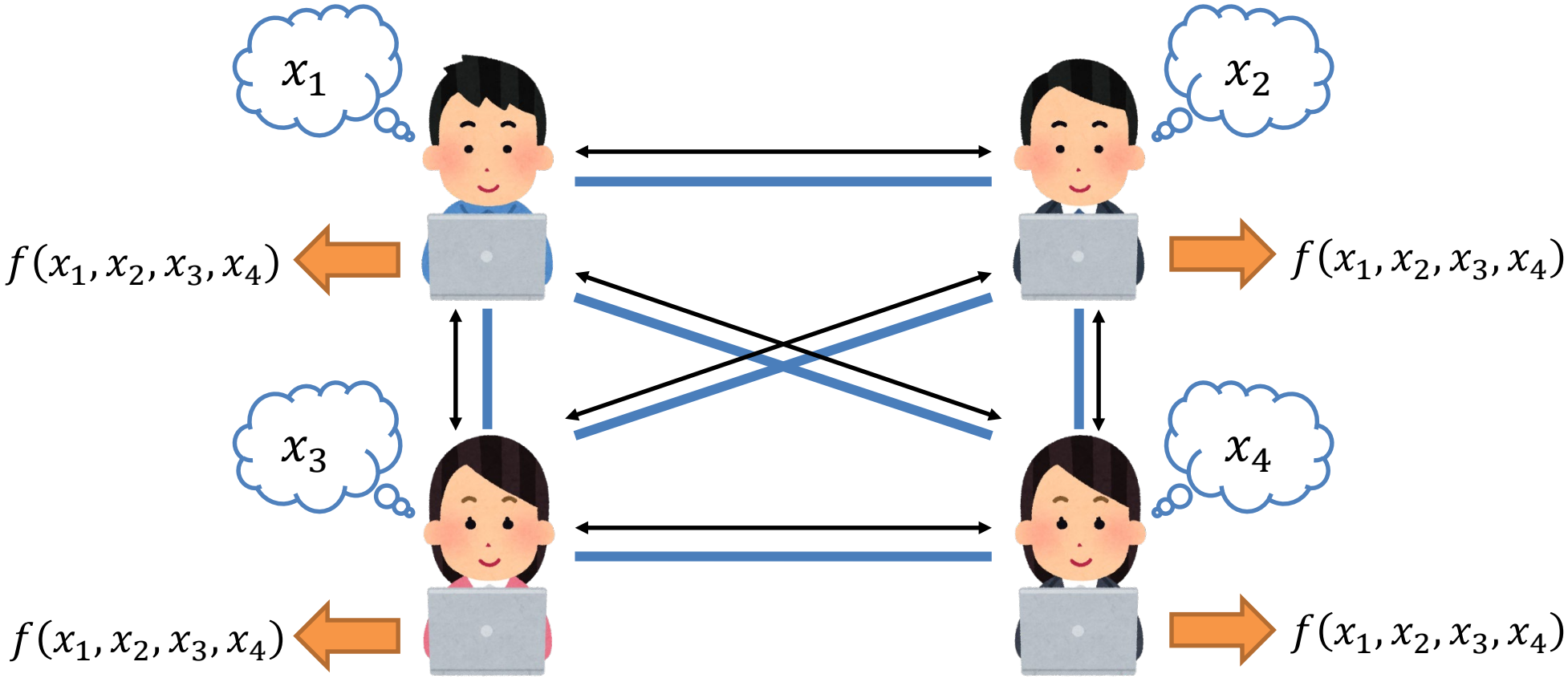
Recent Progress in Private Simultaneous Messages Protocols

Akinori Kawachi

Mie University

Including collaborations with Maki Yoshida (NICT) & Harumichi Nishimura (Nagoya Univ.)

Multi-Party Computation (MPC)



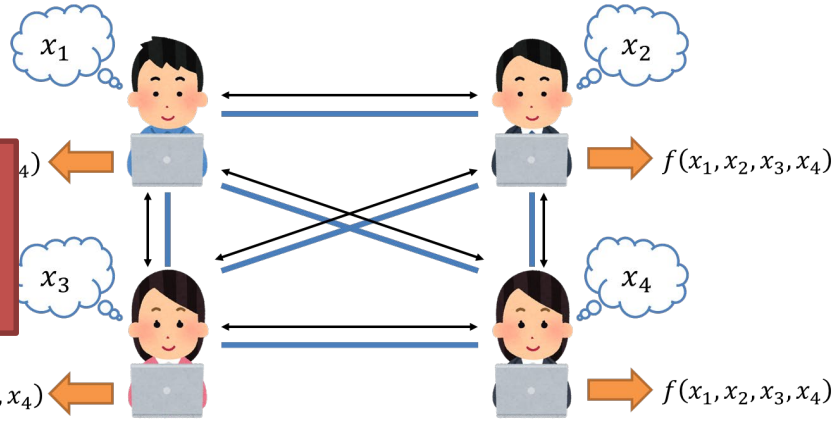
Goal

Jointly compute $f(x_1, x_2, x_3, x_4)$
with revealing nothing but $f(x_1, x_2, x_3, x_4)$

Multi-Party Computation (MPC) [Yao (1986)]

From party P_i's secret x_i, MPC can compute $y = f(x_1, \ldots, x_k)$
w/o revealing any information except for y!

Enables collaborations across many companies using private information!

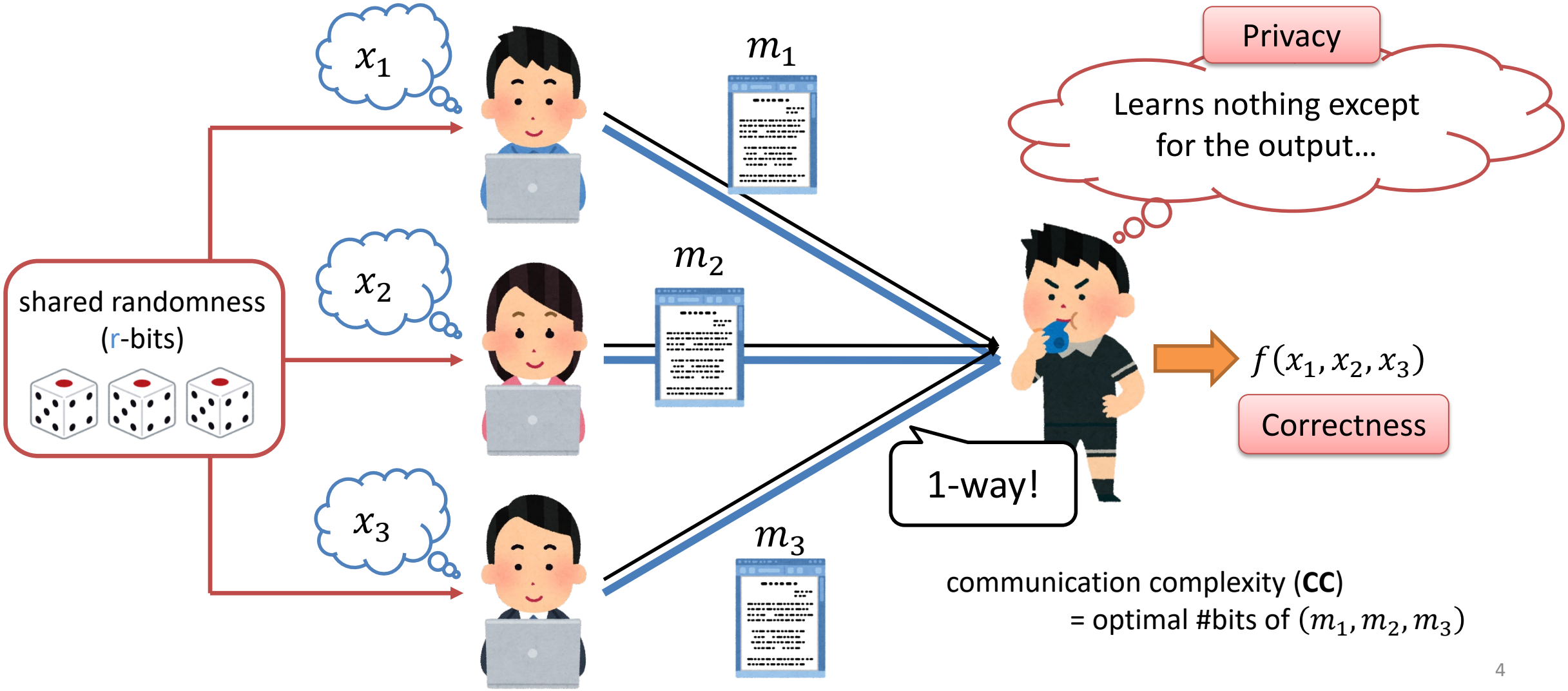


Necessary & sufficient communication resources (complexity), particularly, **effects of privacy requirement**?

Hard to analyze in complex models…
➔ **simpler communication patterns**!

Private Simultaneous Messages (PSM)

[Feige, Killian & Naor (1994)], [Ishai & Kushilevitz (1997)]



communication complexity (**CC**)
= optimal #bits of (m_1, m_2, m_3)

Information-Theoretically Perfect Privacy

Definition

k-party PSM protocol Π for $f: X_1 \times \cdots \times X_k \to \{0,1\}$ has **perfect privacy**

$$\Leftrightarrow \exists D_0 \exists D_1, \forall x_1, \ldots, \forall x_k : M(x_1, \ldots, x_k) \equiv D_{f(x_1,\ldots,x_k)}$$

D_0, D_1 = distributions over message space
$M(x_1, \ldots, x_k)$ = joint distribution of Π's message on inputs $x_1, \ldots, x_k$

Message distribution can be determined only by output $f(x_1, \ldots, x_k)$ w/o private inputs $x_1, \ldots, x_k$
= R learns nothing except for $f(x_1, \ldots, x_k)$.

Statistical version: $\Delta\left(M(x_1, \ldots, x_k), D_{f(x_1,\ldots,x_k)}\right) \leq \varepsilon$
Computational version: No poly-time adversary distinguish $M(x_1, \ldots, x_k)$ & $D_{f(x_1,\ldots,x_k)}$

Positive Results

Theorem [Feige, Kilian & Naor (1994)]

$\forall f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, $\exists$2-party PSM protocol of **CC** $\leq \boldsymbol{2^n + n + 1}$.

Improved to $\boldsymbol{O(2^{n/2})}$ by Beimel, Ishai, Kumaresan, & Kushilevitz (2014), but still **exponential**!

k-party PSM of **CC** $\leq \boldsymbol{O(k^3 2^{nk/2})}$ by Beimel, Kushilevitz & Nissim (2018)

Theorem [Ishai & Kushilevitz (1997)]

$\forall f: (\{0,1\}^n)^k \to \{0,1\} \in \mathrm{mod}_p \mathrm{L}$, $\exists k$-party PSM protocol of **CC** $\leq \mathbf{poly}(\boldsymbol{k}, \boldsymbol{n})$

Negative Results

Theorem [Beimel, Ishai, Kumaresan & Kushilevitz (2014)]

∀2-party PSM protocol for $f:\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ with **universal reconstruction** requires **CC** $\geq \boldsymbol{2^n}$.

universal reconstruction = referee does not depend on f

FKN protocol (1994) of CC $\leq 2^n + n + 1$ has universal reconstruction, and thus, it has (almost) optimal CC.

BIKK protocol (2014) of CC $\leq O\left(2^{n/2}\right)$ broke this barrier by non-universal reconstruction.

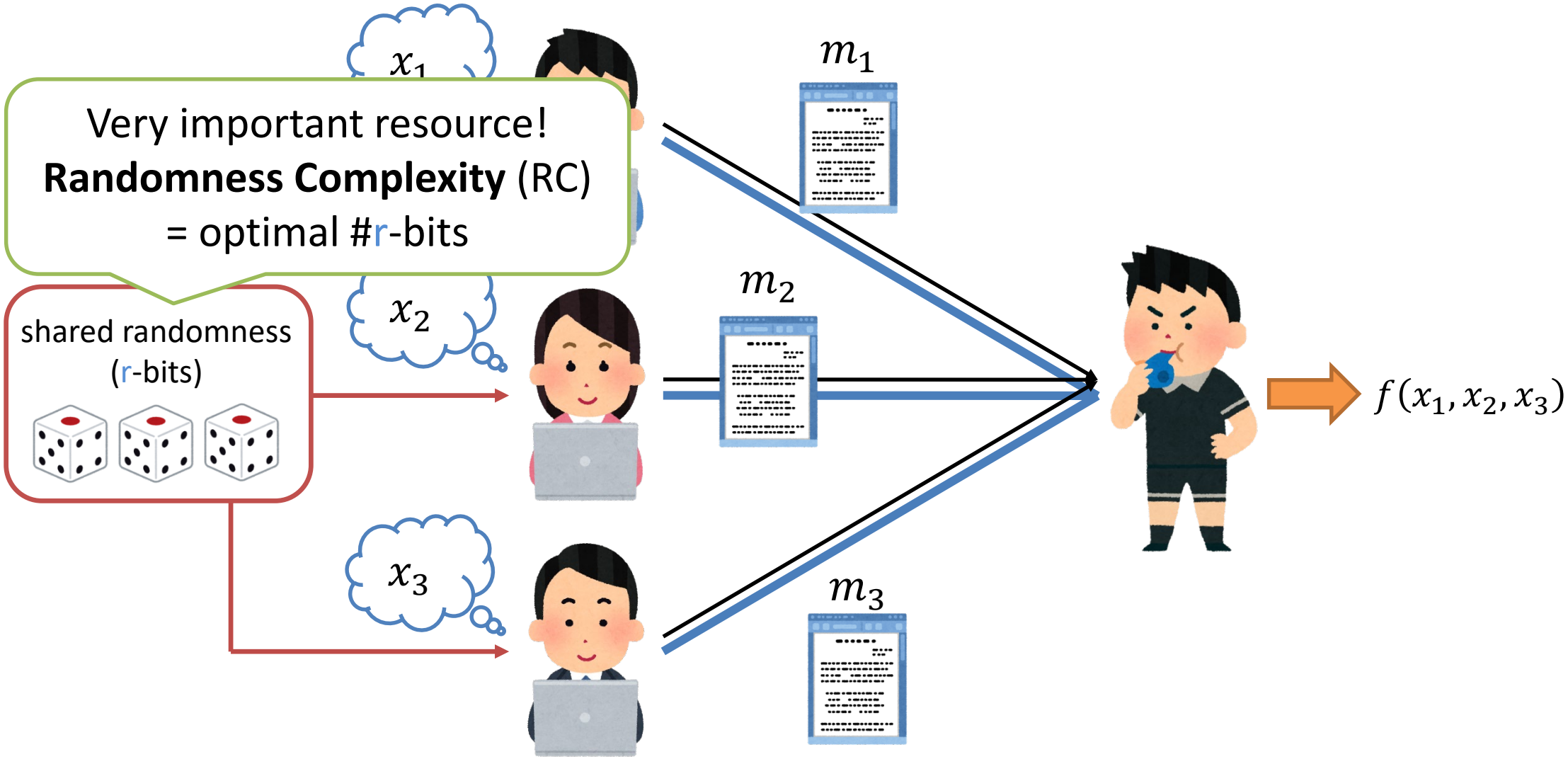
Theorem [Applebaum, Holenstein, Mishra & Shayevitz (2020)]

∀2-party PSM protocol has **CC** $\geq \boldsymbol{\left(3 - o(1)\right)n}$ for random $f:\{0,1\}^n \times \{0,1\}^n \to \{0,1\}$.

Trivial protocol w/o privacy has CC $\leq 2n$.

Additional cost is inevitable for privacy!

Randomness Complexity



Positive Results

Explicit constructions of PSM protocols provide upper bounds of RC.
For example,

Theorem [Feige, Kilian & Naor (1994)]

$\forall f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, $\exists$2-party PSM protocol of **RC** $\leq \boldsymbol{2^n + n}$.

Negative Results

However, little work has been done for lower bounds of RC so far!

Theorem [Pillai, Prabhakaran, Prabhakaran & Sridhar (2019)]

$\forall$2-party PSM protocol for 2-bit input $\mathrm{AND}: \{0,1\} \times \{0,1\} \to \{0,1\}$ has $\mathbf{RC} \geq \mathbf{log\ 6}$.

This shows randomness optimality of k-party PSM protocols for k-bit AND [Feige, Killian, & Naor (1994)] when $k = 2$.

Randomness Bounds for PSM Protocols

Recent results for tight characterization of randomness complexity by communication complexity

Theorem [K & Yoshida (2021)]

λ := CC of PSM protocols for f, ρ := RC of PSM protocols for f

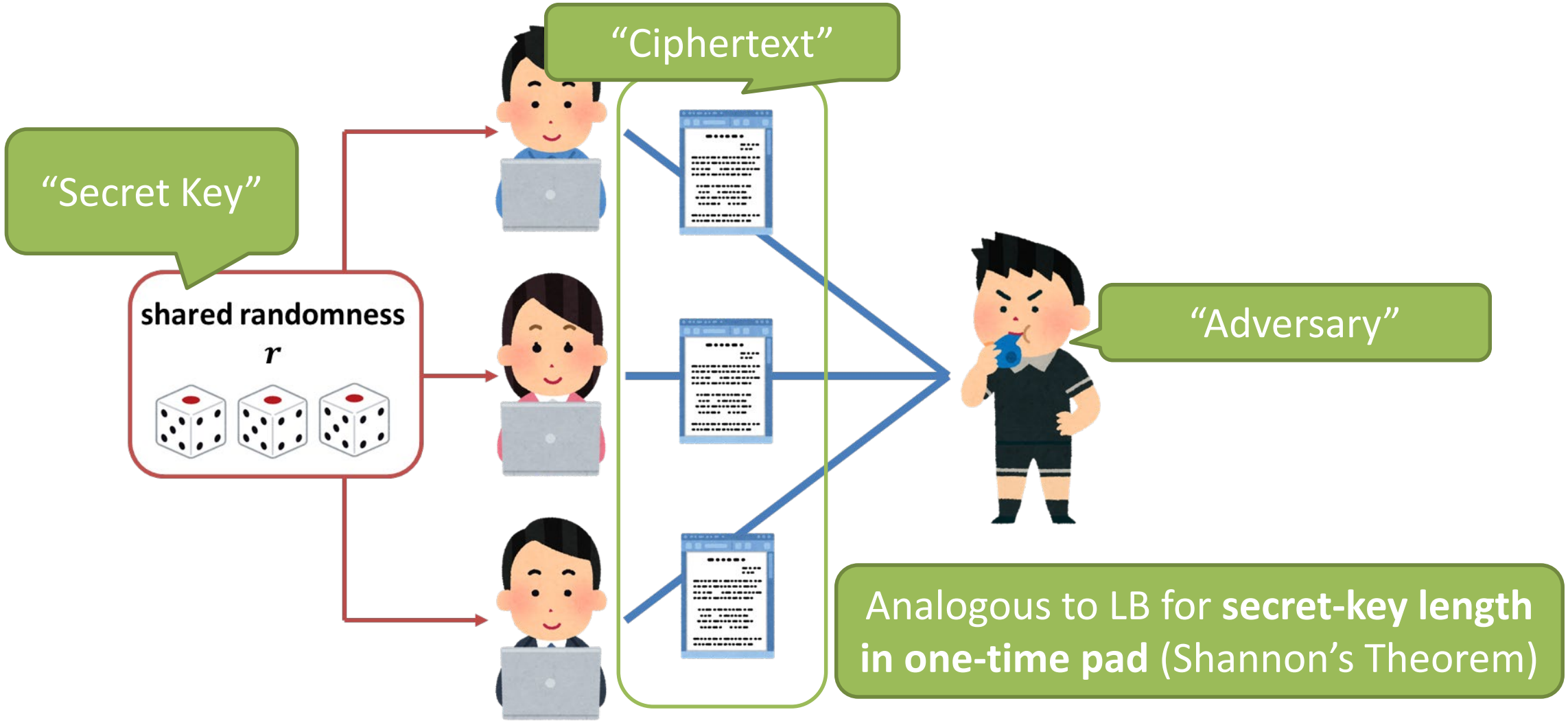
$$\boldsymbol{\lambda - 1 \leq \rho \leq \lambda}$$

Collorary [K & Yoshida (2021)]

$\forall$2-party PSM protocol for $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ with **universal reconstruction** has **RC** $\geq \boldsymbol{2^n - 1}$.

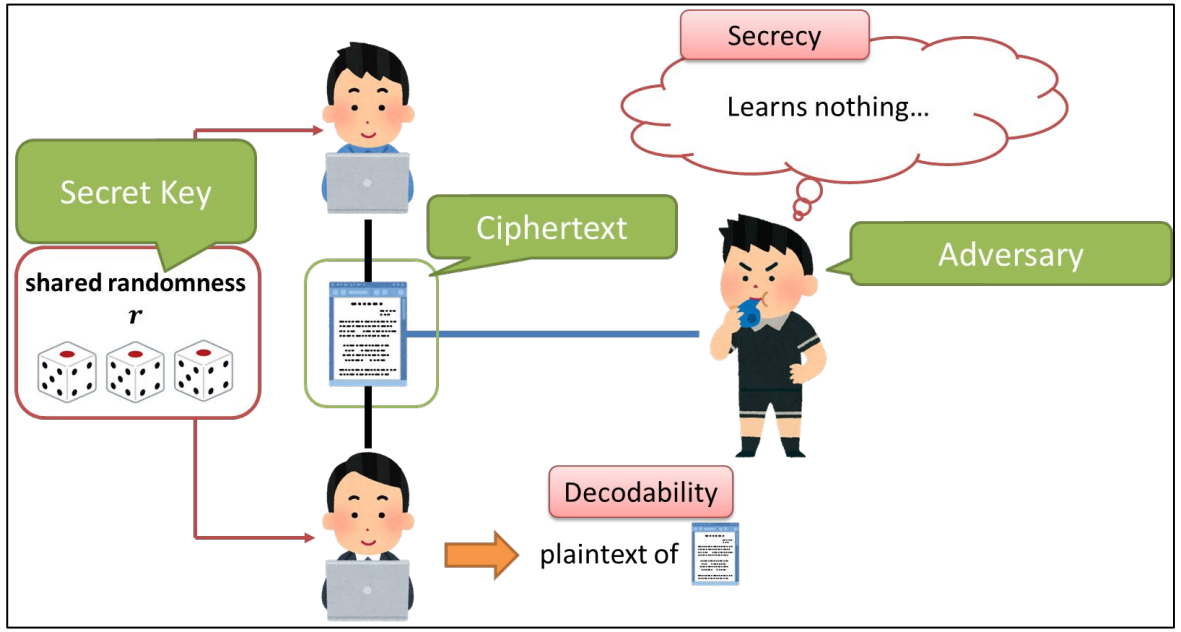
A. Kawachi & M. Yoshida: "Randomness Bounds for Private Simultaneous Messages and Conditional Disclosure of Secrets," IACR Cryptol. ePrint Arch. 2021: 1037 (2021)

Proof Idea: Randomness Lower Bounds $\rho \geq \lambda - 1$

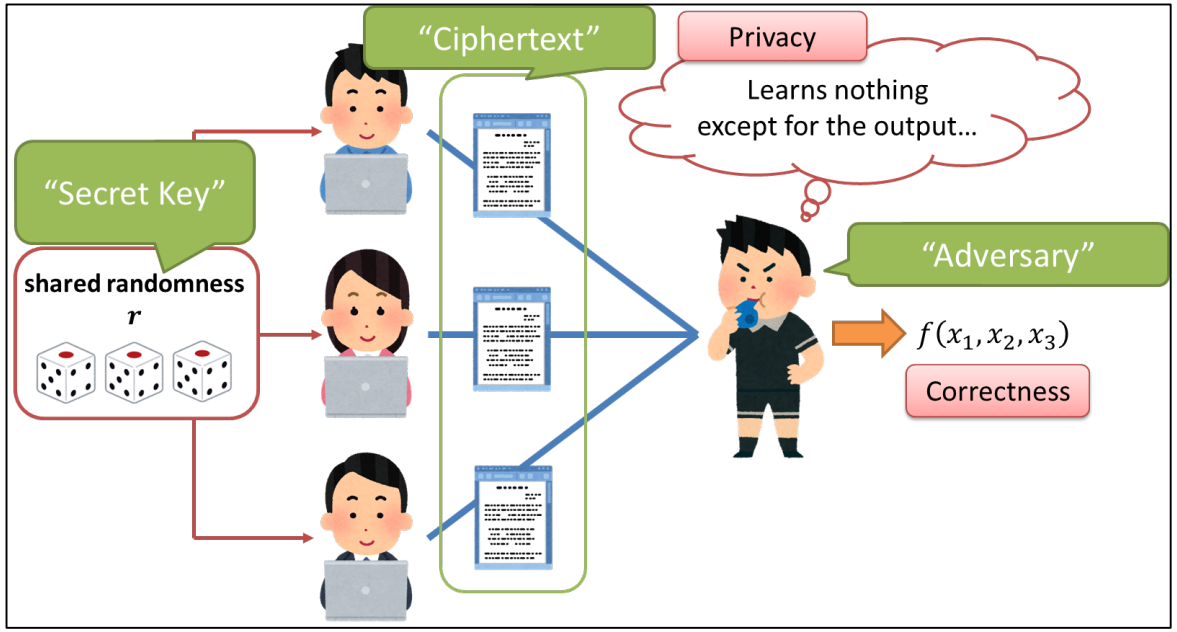


Proof Idea: Randomness Lower Bounds $\rho \geq \lambda - 1$

Encryption



PSM



Theorem (Shannon)

Encryption has perfect secrecy
➔ |secret key| ≥ |ciphertext|

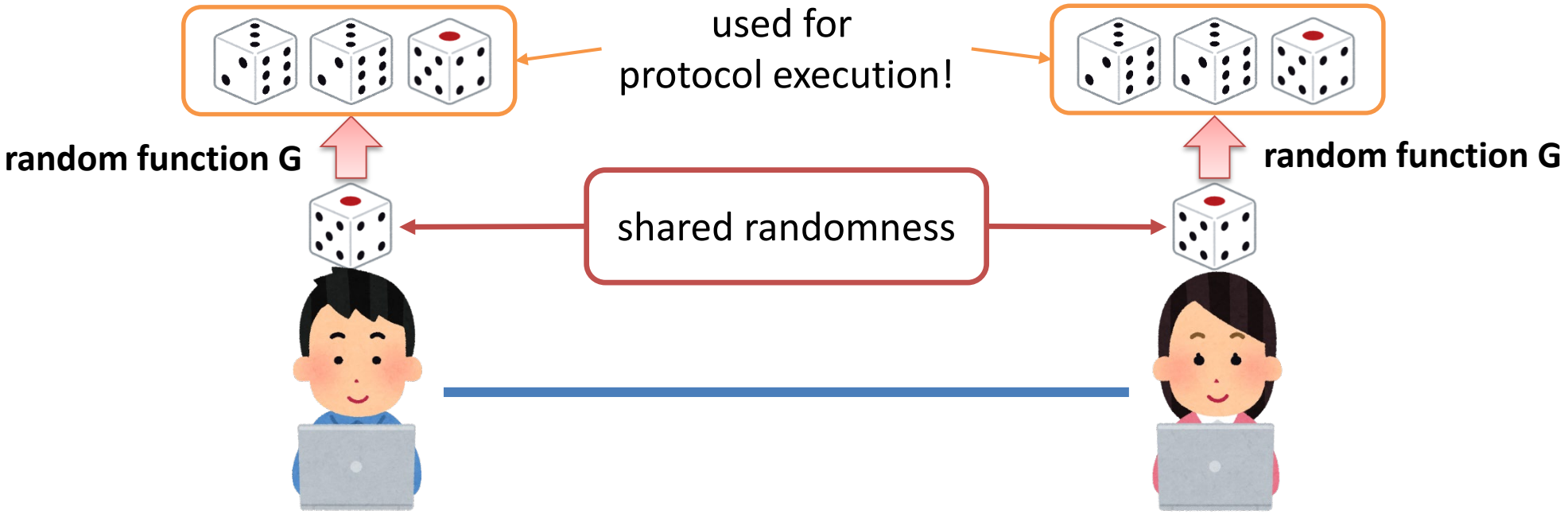
communication complexity

|secret key| is lower-bounded by λ in PSM!

Proof Idea: Randomness Upper Bounds $\rho \leq \lambda$

Randomness sparsification [Newman (1991)]

Common technique for saving randomness in communication protocols



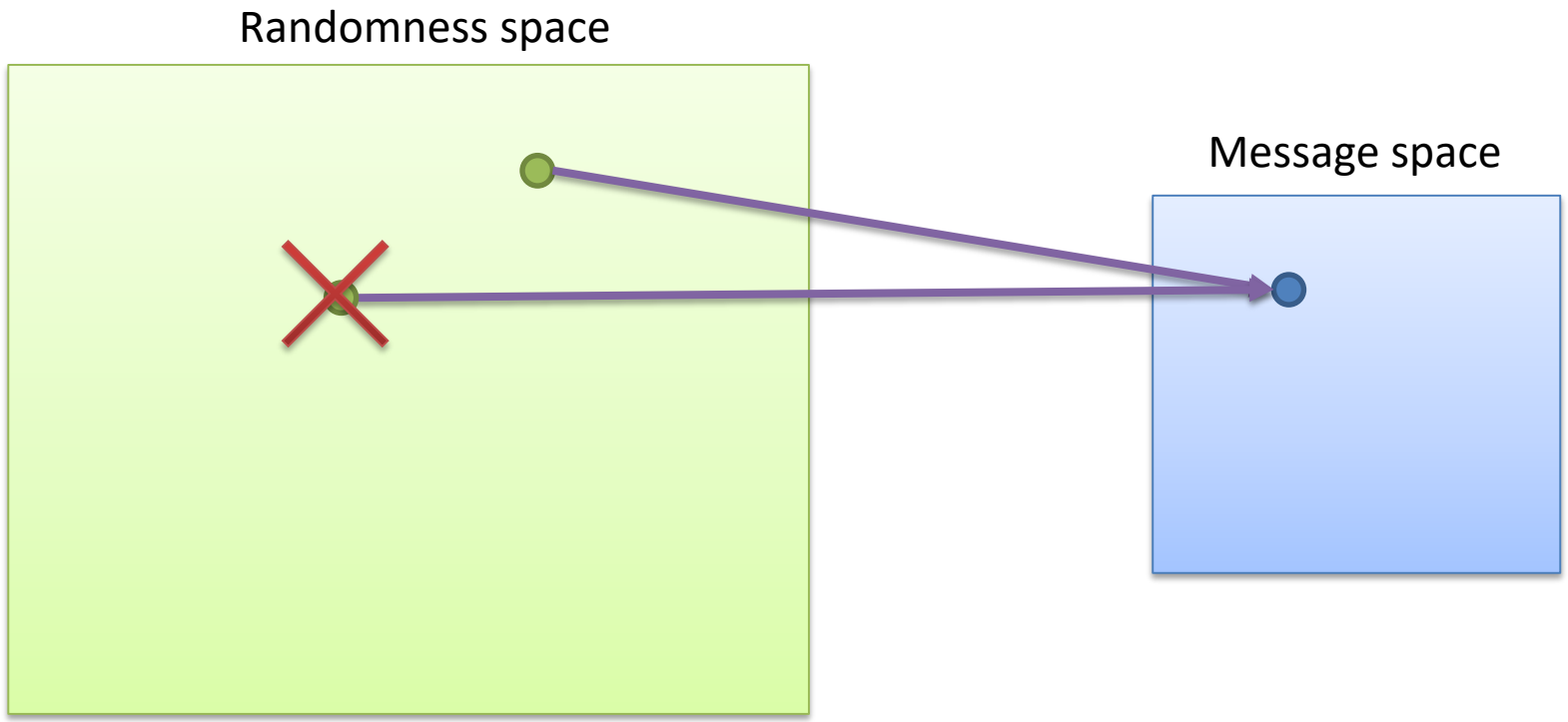
The converted protocol works well w.h.p. (w.r.t. G) with **additional error**!
(e.g., randomness sparsification for stat-private CDS [Applebaum & Vasudevan (2021)])

Problem: **NOT** applicable in our **perfect-privacy** setting!

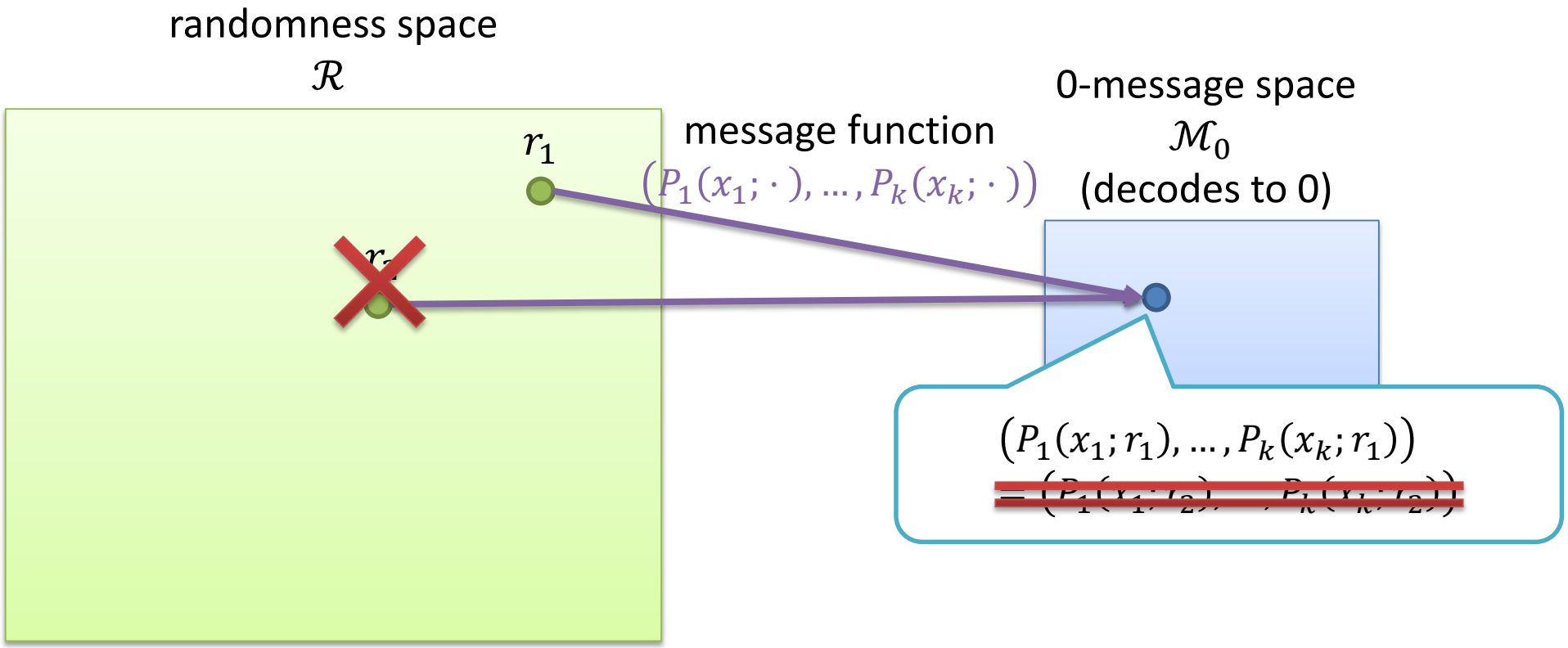
Proof Idea: Randomness Upper Bounds $\rho \leq \lambda$

Our new strategy: algorithmically convert the protocol as **preserving the perfect privacy**

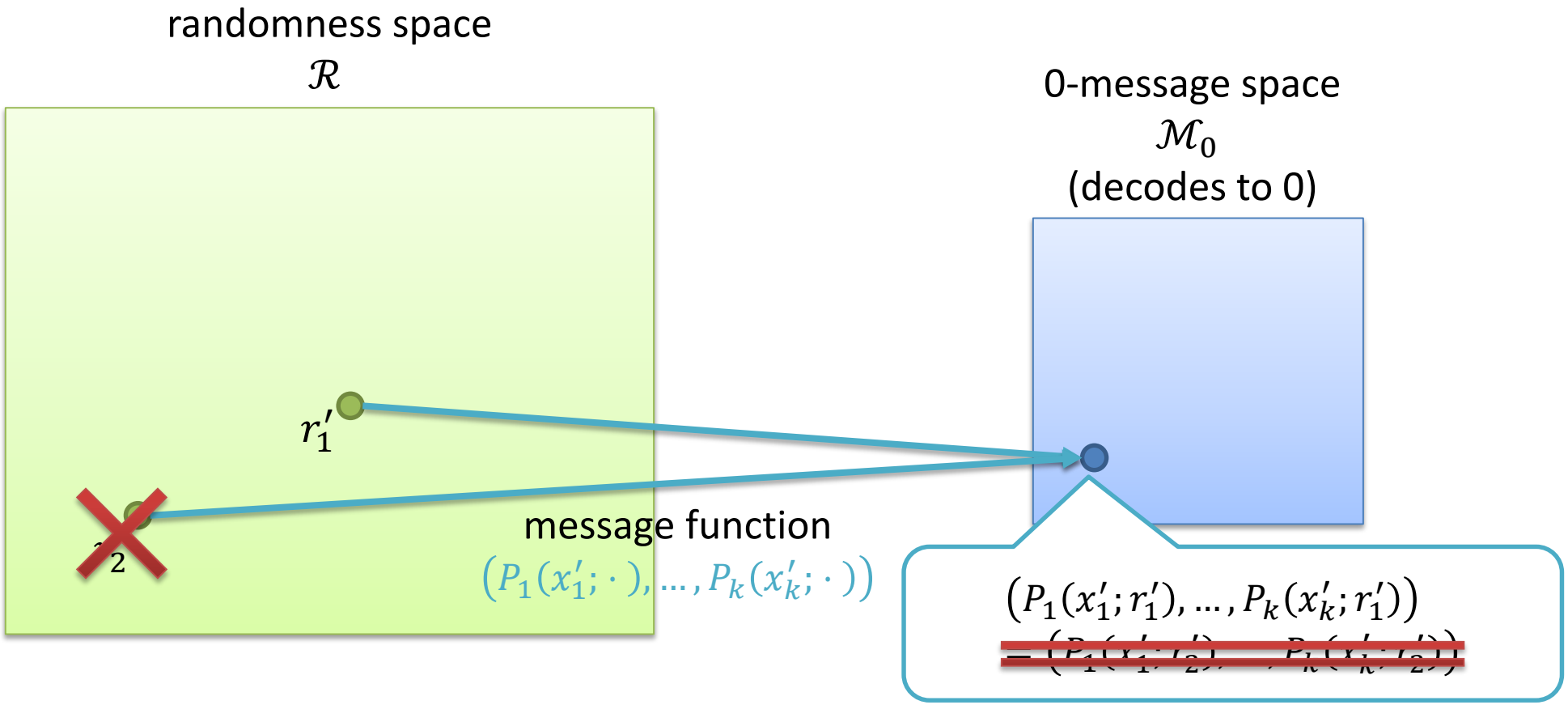
⇨ Find collisions in randomness space & delete one in preimage!

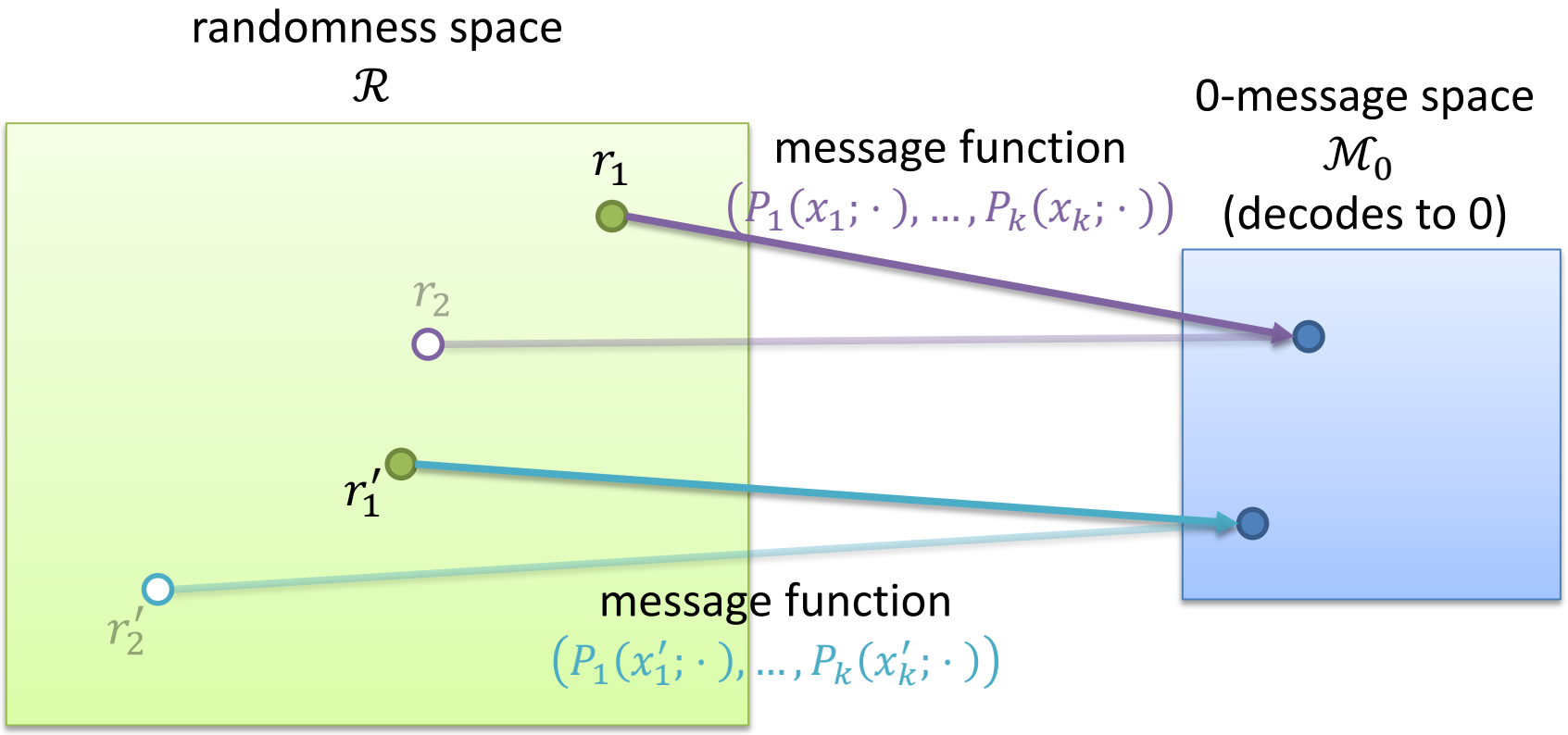


For private inputs $x_1, x_2, \ldots, x_k$ for which $f(x_1, x_2, \ldots, x_k) = 0$



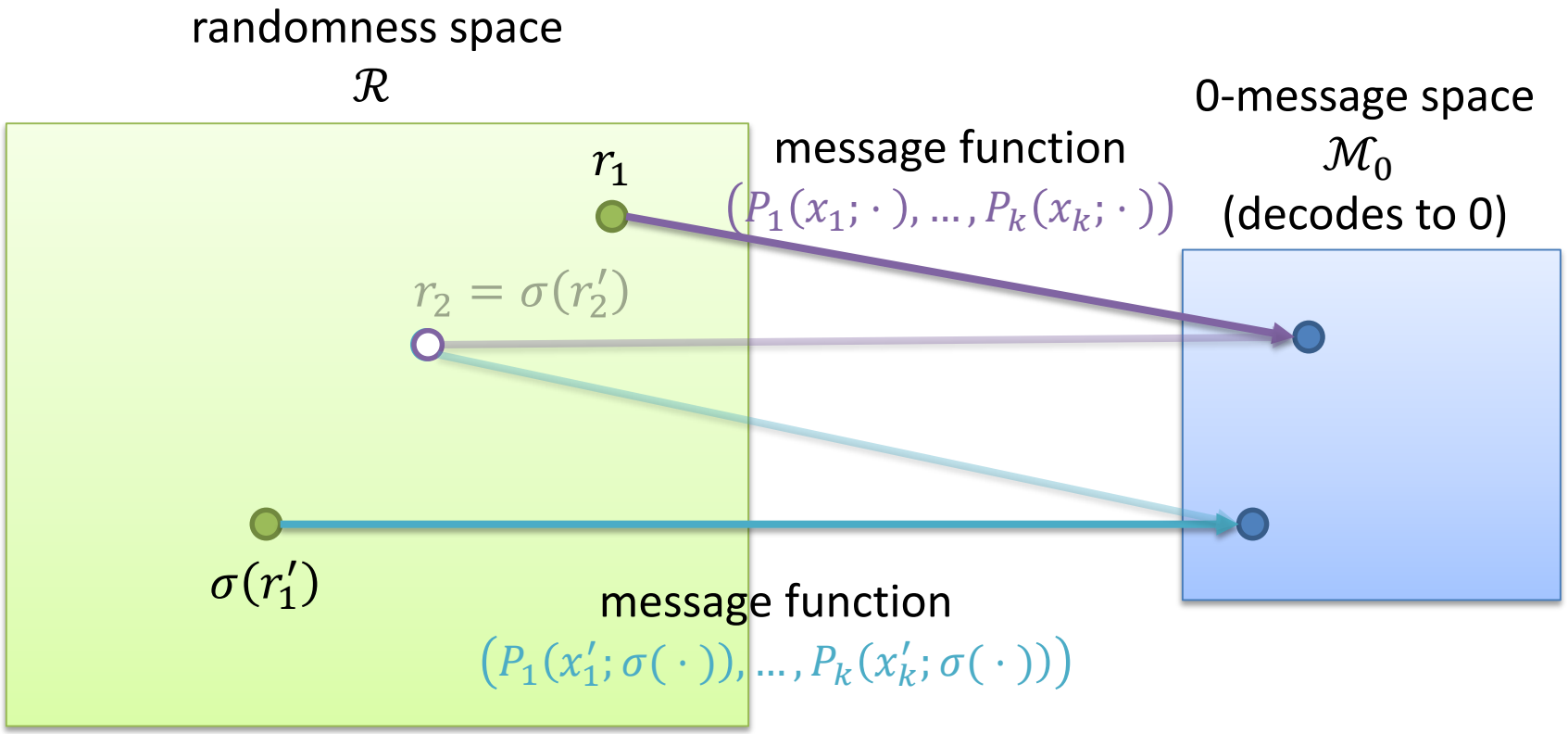
For another input $(x_1', x_2', \ldots, x_k')$ for which $f(x_1', x_2', \ldots, x_k') = 0$





Deleted elements are **inconsistent** in $(x_1, x_2, \dots, x_k)$ & $(x_1', x_2', \dots, x_k')$.

Permute $\mathcal{R}$ for $P_1(x_1';\cdot),\dots,P_k(x_k';\cdot)$ to coincide r_2' with r_2!



Deleted elements are **inconsistent** in $(x_1, x_2, \dots, x_k)$ & $(x_1', x_2', \dots, x_k')$.

Permute $\mathcal{R}$ for $P_1(x_1';\cdot),\dots,P_k(x_k';\cdot)$ to coincide r_2' with r_2!

⇒ By repeating deletions, get $|\mathcal{R}| \le |\mathcal{M}_0|$ (or $\rho \le |\mathcal{R}| \le \max\{|\mathcal{M}_0|, |\mathcal{M}_1|\} \le \lambda$)

Additional Remark

Our bounds are **exactly tight** for size of message/randomness space.

Theorem

$\mathcal{M}_b$:= b-message space of PSM protocols of optimal CC for f $(b \in \{0,1\})$,
$\mathcal{R}$:= randomness space of PSM protocols for f

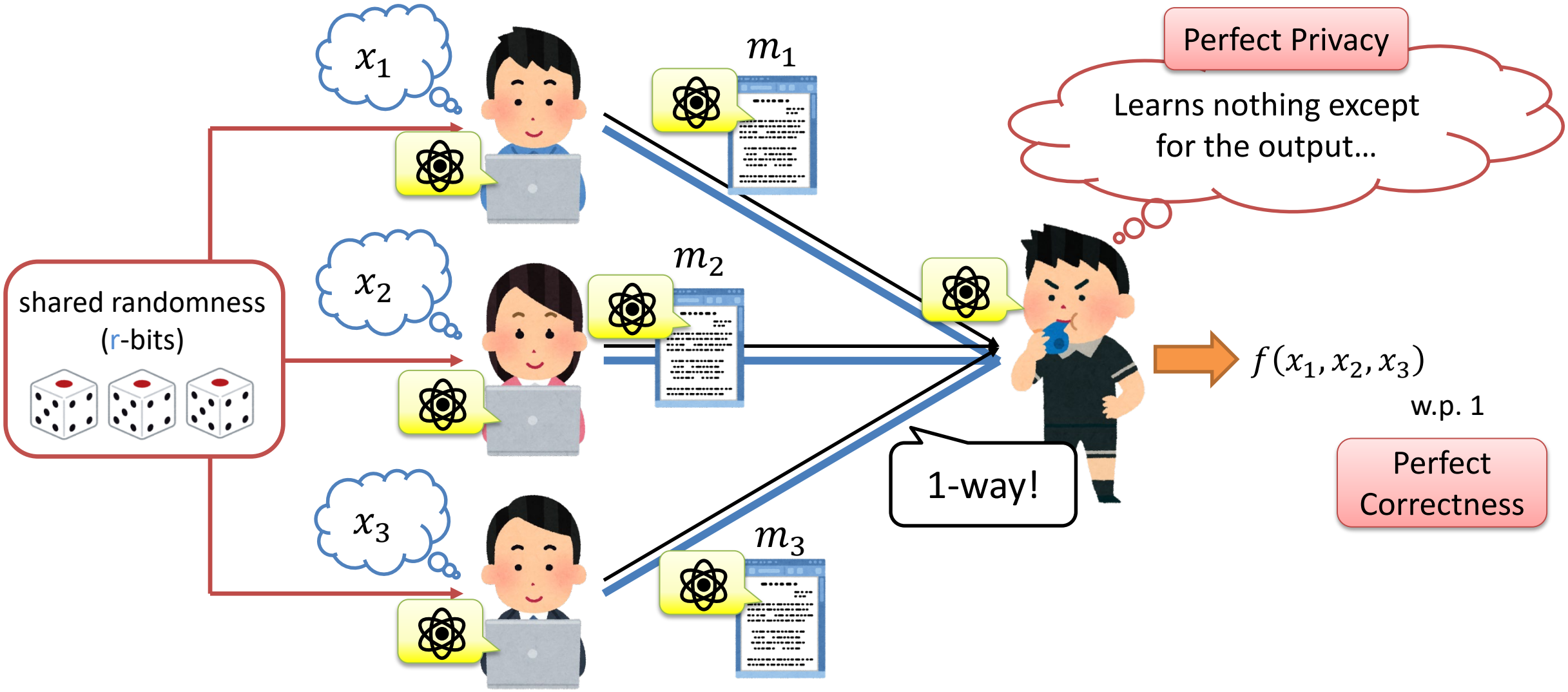
$$|\mathcal{R}| = \mathbf{max}\{|\mathcal{M}_0|, |\mathcal{M}_1|\}$$

Related Models with PSM

- Decomposable Randomized Encoding (DRE) [Applebaum, Ishai & Kushilevitz (2004)]
  - ➢ DRE ≈ PSM in which every party has 1-bit inputs.
    - DRE implies PSM.
  - ➢ DRE has extremely efficient encoding procedure (=parties).
- Ad-hoc PSM [Beimel, Gabizon, Ishai & Kushilevitz (2016)]
  - ➢ PSM in which a part of parties participate at actual execution.
- Non-interactive MPC (NIMPC)

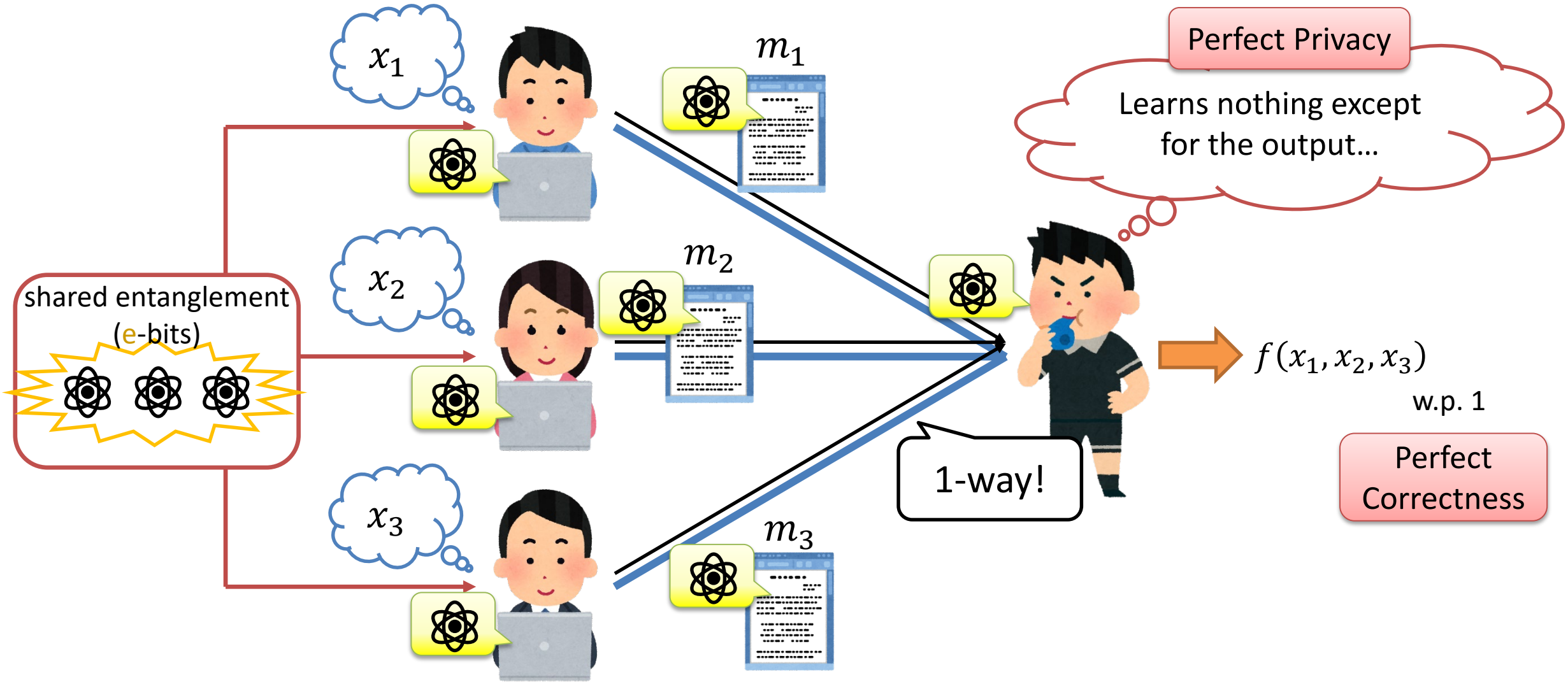
  [Beimel, Gabizon, Ishai, Kushilevitz, Meldgaard & Paskin-Cherniavsky (2014)]
  - ➢ Referee & some of parties may be corrupted by adversary.
  - ➢ PSM→NIMPC [Benhamouda, Krawczyk & Rabin (2017)], [Eriguchi, Ohara, Nuida & Yamada (2021)]
- Quantum versions of PSM
  - ➢ for quantum circuits (Q-DRE, Q-garbled circuits) [Brakerski & Yuen (2020)]
  - ➢ for Boolean functions (PSQM) [K & Nishimura (2021)]

Private Simultaneous **Quantum** Messages (PS**Q**M)



A. Kawachi & H. Nishimura: "Communication Complexity of Private Simultaneous Quantum Messages Protocols," IACR Cryptol. ePrint Arch. 2021: 636 (2021)

Private Simultaneous **Quantum** Messages (PS**Q**M)



A. Kawachi & H. Nishimura: "Communication Complexity of Private Simultaneous Quantum Messages Protocols," IACR Cryptol. ePrint Arch. 2021: 636 (2021)

Quantum Version of Privacy

Definition

k-party PS**Q**M protocol Π for $f: X_1 \times \cdots \times X_k \to \{0,1\}$ has **perfect privacy**

$$\Leftrightarrow \exists \rho_0 \exists \rho_1, \forall x_1, \dots, \forall x_k : M(x_1, \dots, x_k) = \rho_{f(x_1,\dots,x_k)}$$

ρ_0, ρ_1 = density operators over message space
$M(x_1, \dots, x_k)$ = joint quantum state of Π's message on inputs $x_1, \dots, x_k$

Message state can be determined only by output $f(x_1, \dots, x_k)$ w/o private inputs $x_1, \dots, x_k$
= R learns nothing except for $f(x_1, \dots, x_k)$.

Communication Complexity in SMP

Randomness vs Entanglement

Simultaneous Message Passing
= PSM w/o privacy

- Some designated **relation** in 2-party S(**Q**)MP
  - Quantum (w/ r-bits): $\Omega((n/\log n)^{1/3})$
  - Classical (w/ e-bits): $O(\log n)$

[Gavinsky, Kempe, Regev & de Wolf (2009)]

Exponential Gap

- Equality function ($\mathrm{EQ}_n(x_1, x_2) = [x_1 = x_2]$) in 2-party S(**Q**)MP
  - Classical (w/ r-bits): $2n$
  - Quantum (w/ e-bits) n

[Horn et al. (2005)]

Factor-2 Gap

Best known gap for **total functions**!

Question 1

What about gaps of r-/e-bits in PS**Q**M protocols?

Gaps in Communication Complexity between Shared Randomness & Entanglement

Question 1

What about gaps of r-/e-bits in PS**Q**M protocols?

Theorem [K & Nishimura, 2021]

∃**total function** $f: (\{0,1\}^n)^k \to \{0,1\}$ s.t.

some PS**Q**M protocol w/ e-bits for f has $\boldsymbol{kn/2}$-bit messages
& any PS**Q**M protocol w/ r-bits for f requires $\geq \boldsymbol{kn}$-bit messages.

E-bits reduce message length by **half** for a **total function**
even under privacy-preserving setting!

Gaps in Communication Complexity between Shared Randomness & Entanglement

Question 1

What about gaps of r-/e-bits in PS**Q**M protocols?

Theorem [K & Nishimura, 2021]

∃partial function $f: (\{0,1\}^n)^2 \to \{0,1\}$ s.t.

some PSM protocol w/ e-bits for f has $\boldsymbol{O(\log n)}$-bit messages
& any PS**Q**M protocol w/ r-bits for f requires $\boldsymbol{\Omega(n)}$-bit messages.

E-bits reduce message length **exponentially** for a partial function even under privacy-preserving setting!

Communication Lower Bounds in PSM

Theorem [Applebaum, Holenstein, Mishra & Shayevitz (2020)]

∀2-party PSM protocol has **CC** $\geq \big(\mathbf{3} - \mathbf{o}(\mathbf{1})\big)\boldsymbol{n}$ for random $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$.

Trivial protocol w/o privacy has CC $\leq 2n$.
Additional cost is inevitable for privacy!

Question 2

What about lower bounds of PS**Q**M protocols?
Can break $(3 - o(1))n$ lower bound by quantum communication?

Communication Lower Bounds in PSQM

Question 2

What about lower bounds of PS**Q**M protocols?
Can break $(3 - o(1))n$ lower bound by **quantum communication?**

Theorem [K & Nishimura (2021)]

For $1 - o(1)$ fraction of functions $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$,
$\forall$PS**Q**M protocol w/ r-bits for f has **CC** $\geq \boldsymbol{(3 - o(1))n}$.

Privacy requires non-trivial communication cost
even for **Q**-messages!

Gaps in Communication Complexity between Shared Randomness & Entanglement

Theorem [K & Nishimura, 2021]

∃total function $f: (\{0,1\}^n)^k \to \{0,1\}$ s.t.

some PS**Q**M protocol w/ e-bits for f has $\boldsymbol{kn/2}$-bit messages
& any PS**Q**M protocol w/ r-bits for f requires $\geq \boldsymbol{kn}$-bit messages.

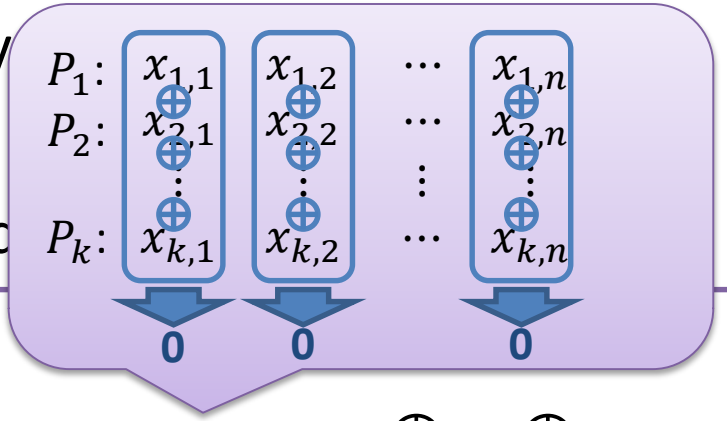
Proof Strategy

Consider Equality function $\mathrm{EQ}_n(x,y) = I[x=y]$ $(x,y \in \{0,1\}^n)$ for $k=2$

Theorem [Horn et al. (2005)]

EQ_n has 2-party S**Q**MP protocol w/ e-bits of message length = n.

This protocol does **NOT** satisfy privacy



Randomization of **Q**-messages encoded

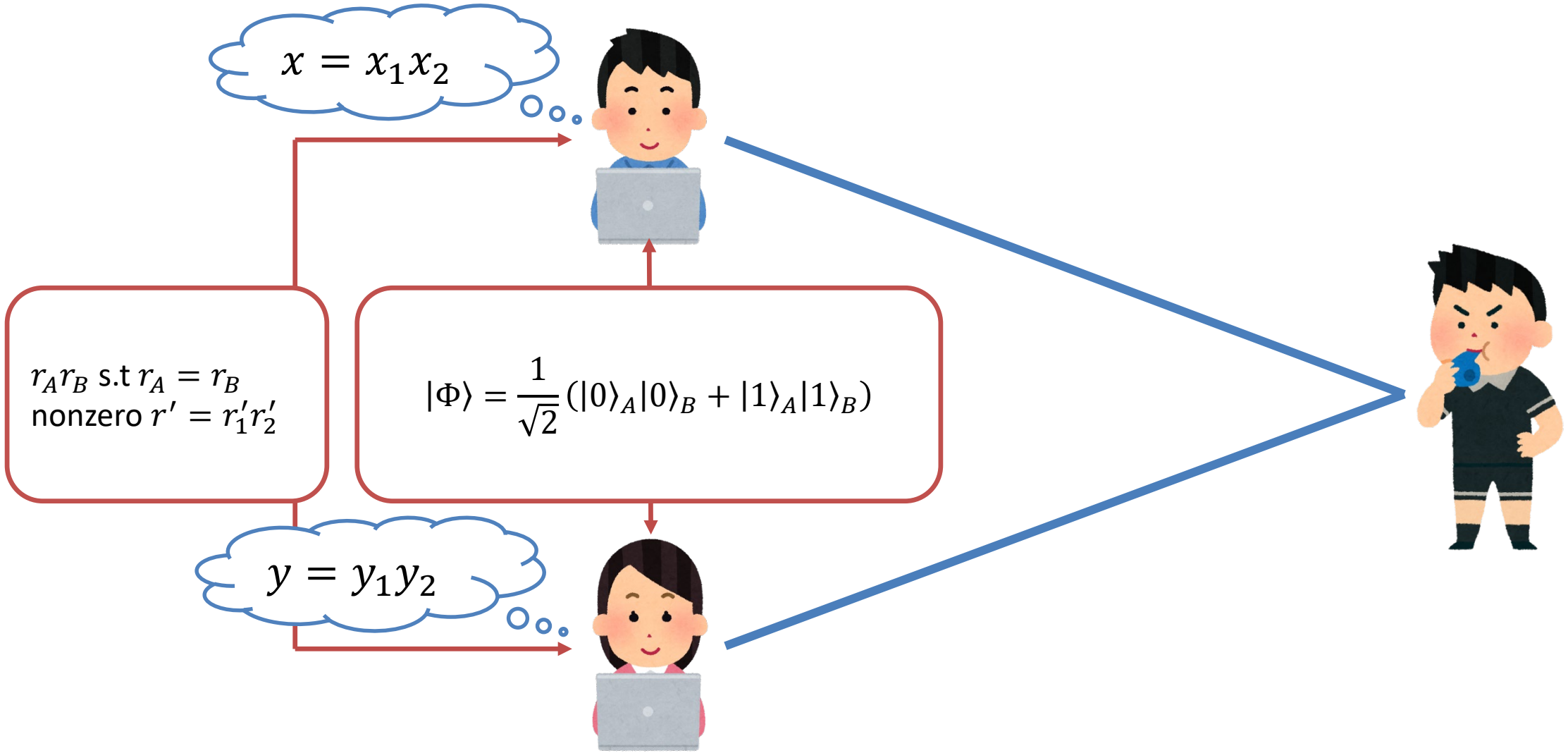
For k-party version, use the following generalization:

$$\mathrm{GEQ}_n(x_1, x_2, \ldots, x_k) = \begin{cases} 1 & x_{1,1} \oplus \cdots \oplus x_{k,1} = x_{1,2} \oplus \cdots \oplus x_{k,2} = \cdots = x_{1,n} \oplus \cdots \oplus x_{k,n} = 0 \\ 0 & \text{o. w.} \end{cases}$$

kn-bit lower bound (w/ r-bits) can be obtained by the argument of [Klauck (2007)] for one-way quantum communication.

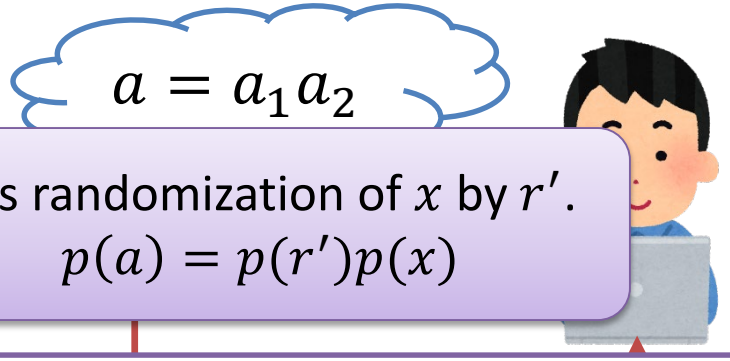
Protocol

Consider $\mathrm{GEQ}_2(x,y) = \begin{cases} 1 & x_1 \oplus y_1 = x_2 \oplus y_2 = 0 \ (\Leftrightarrow x = y) \\ 0 & \text{o. w.} \end{cases}$



Protocol

Consider $\mathrm{GEQ}_2(x, y) = \begin{cases} 1 & x_1 \oplus y_1 = x_2 \oplus y_2 = 0 \ (\Leftrightarrow x = y) \\ 0 & \text{o. w.} \end{cases}$



$a = a_1 a_2$

a is randomization of x by r'.
$p(a) = p(r')p(x)$

For $x_1, x_2 \in \mathbb{F}_2$,
$p(x_1 x_2) = x_1 + x_2 \alpha \bmod q(\alpha)$,
where $q(\alpha)$ is deg-2 irreducible poly.

$|1\rangle_A|1\rangle_B)$

$b = b_1 b_2$

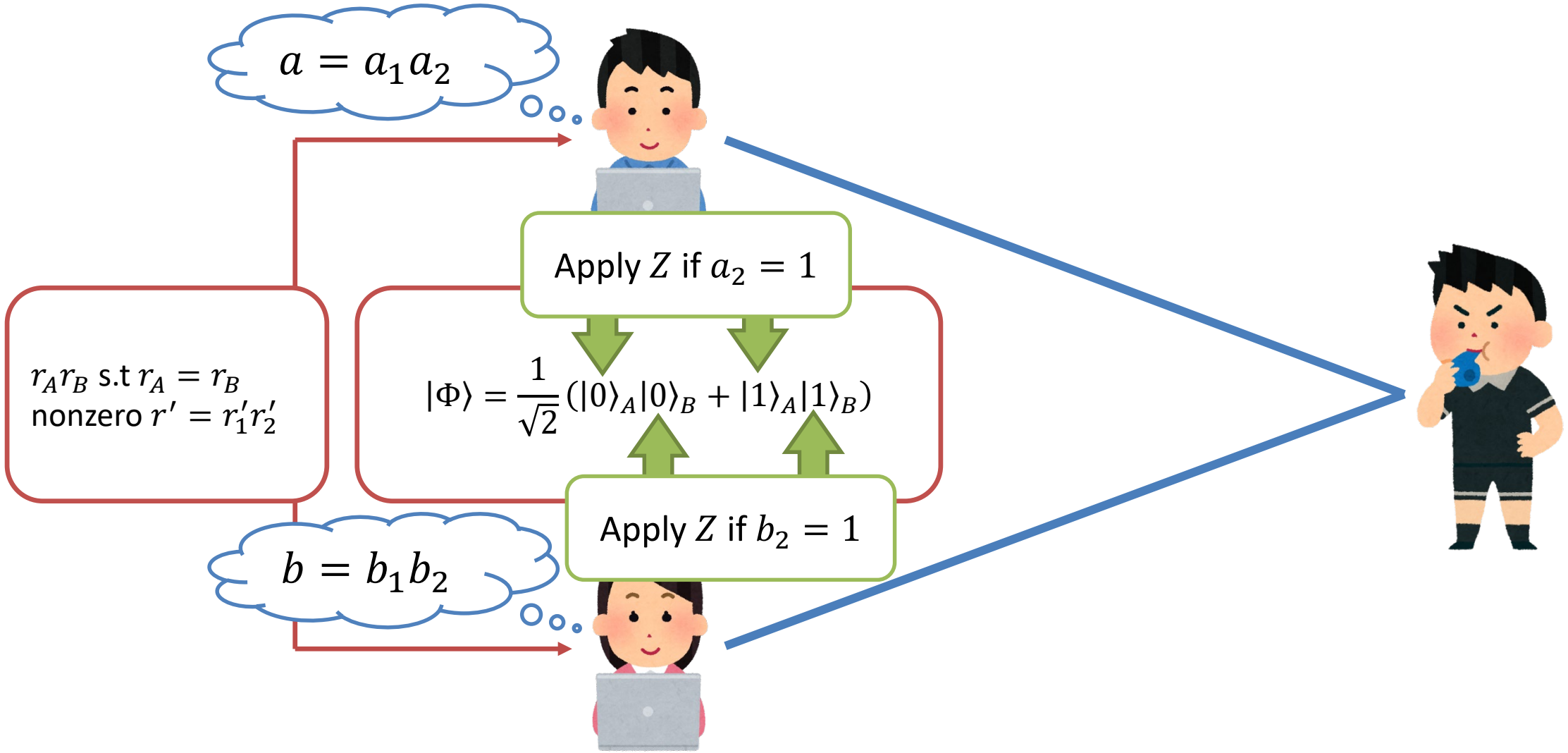
b is randomization of y by r'.
$p(b) = p(r')p(y)$

Note

$x = y \Leftrightarrow a = b$

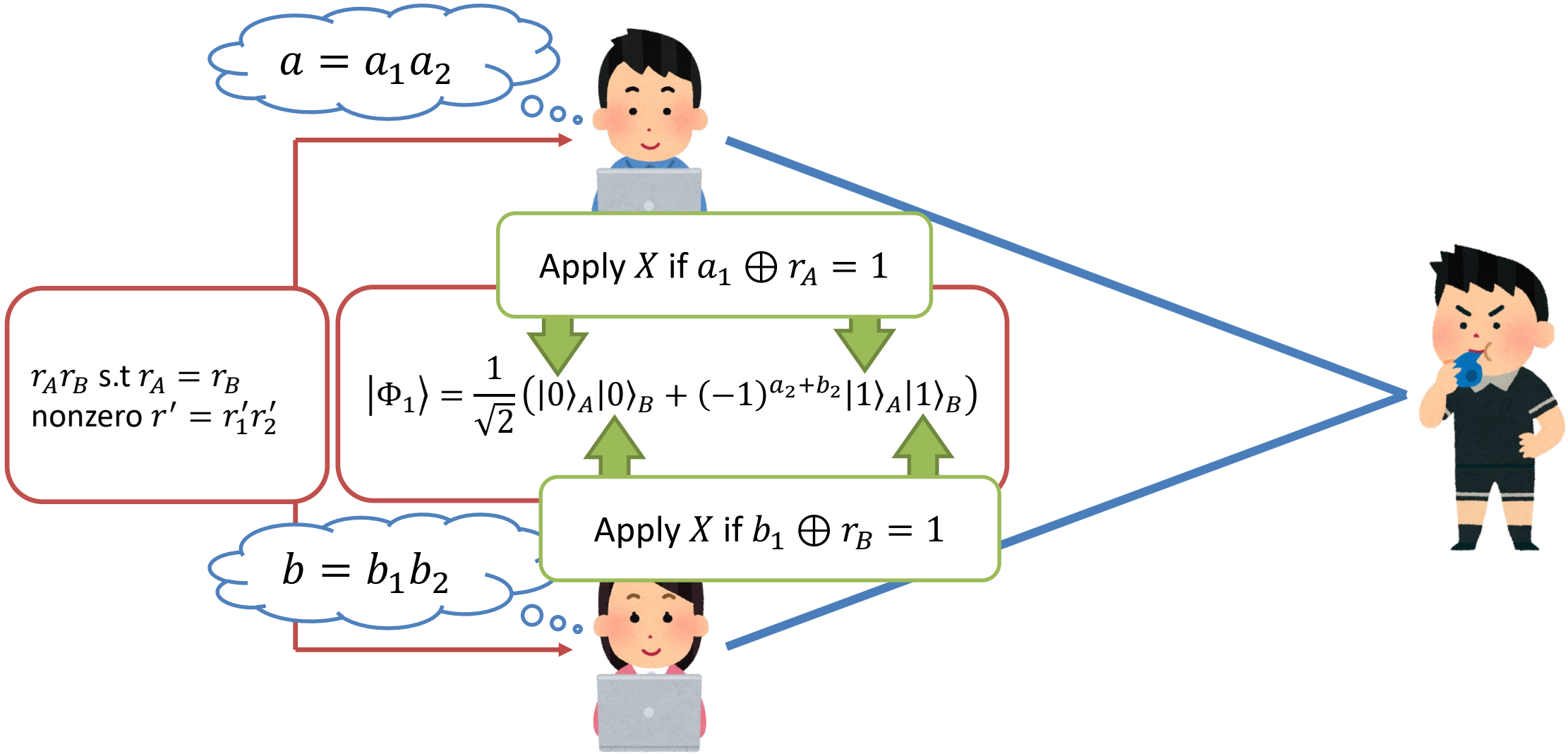
Protocol

Consider $\mathrm{GEQ}_2(x,y) = \begin{cases} 1 & x_1 \oplus y_1 = x_2 \oplus y_2 = 0 \ (\Leftrightarrow x = y) \\ 0 & \text{o. w.} \end{cases}$



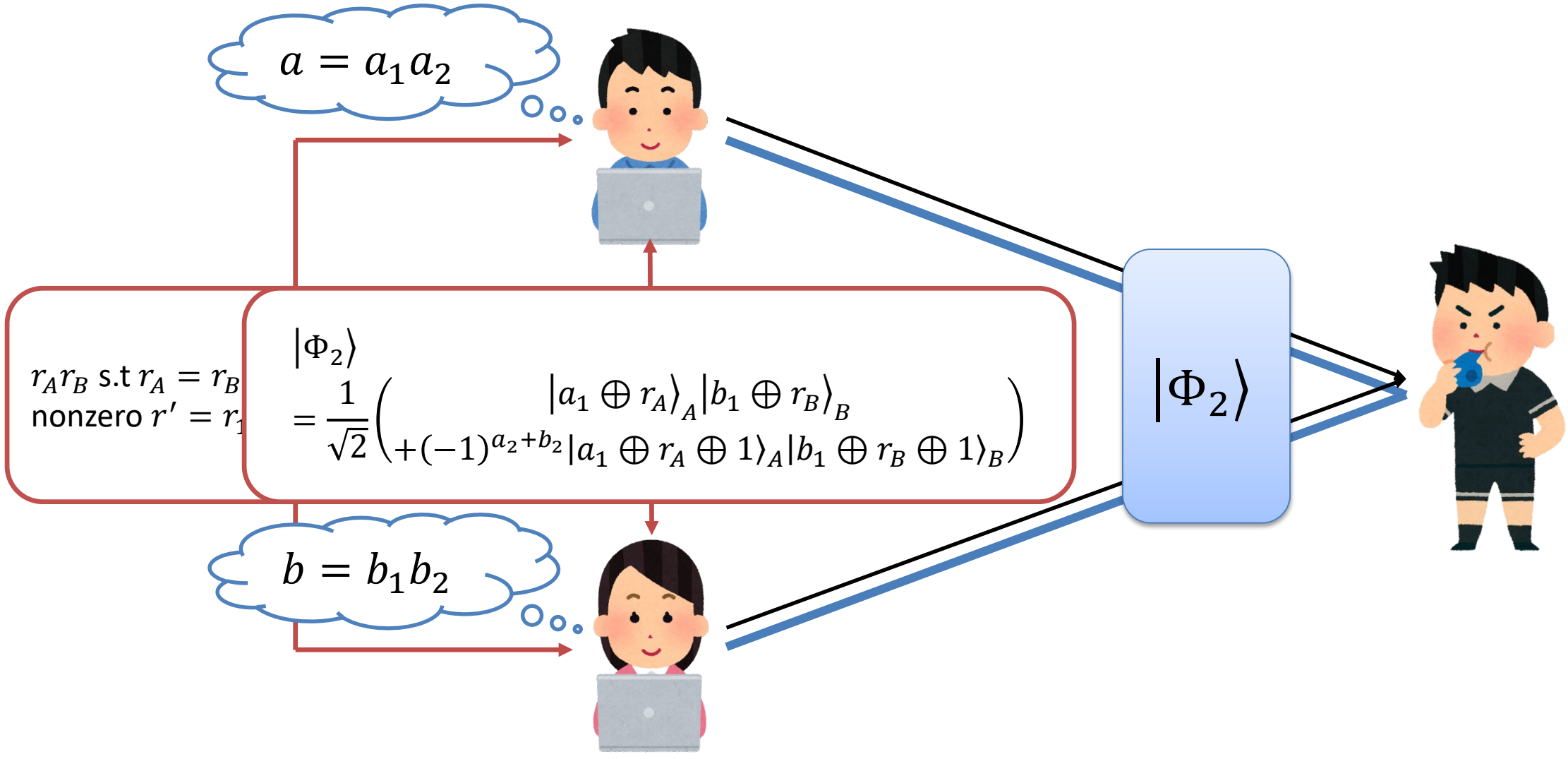
Protocol

Consider $\mathrm{GEQ}_2(x,y) = \begin{cases} 1 & x_1 \oplus y_1 = x_2 \oplus y_2 = 0 \ (\Leftrightarrow x = y) \\ 0 & \text{o.w.} \end{cases}$



Protocol

Consider $\mathrm{GEQ}_2(x,y) = \begin{cases} 1 & x_1 \oplus y_1 = x_2 \oplus y_2 = 0 \ (\Leftrightarrow x = y) \\ 0 & \text{o.w.} \end{cases}$



Protocol

Consider $\mathrm{GEQ}_2(x,y) = \begin{cases} 1 & x_1 \oplus y_1 = x_2 \oplus y_2 = 0 \ (\Leftrightarrow x = y) \\ 0 & \text{o} \end{cases}$

$a = a_1 a_2$

Measure in Bell basis:

$\{|\Phi_{00}\rangle = |00\rangle + |11\rangle, |\Phi_{10}\rangle = |10\rangle + |01\rangle,$
$|\Phi_{01}\rangle = |00\rangle - |11\rangle, |\Phi_{11}\rangle = |10\rangle - |01\rangle\}$

Output 1 iff Φ_{00} is measured.

$r_A r_B$ s.t $r_A = r_B$
nonzero $r' = r_1$

$$|\Phi_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} |a_1 \oplus r_A\rangle_A |b_1 \oplus r_B\rangle_B \\ +(-1)^{a_2+b_2}|a_1 \oplus r_A \oplus 1\rangle_A |b_1 \oplus r_B \oplus 1\rangle_B \end{pmatrix}$$

$|\Phi_2\rangle$

$b = b_1 b_2$

Correctness:

1. $x = y \Leftrightarrow a = b$
2. Φ_{00} is measured $\Leftrightarrow a_1 b_1 = r_A r_B \wedge a_2 = b_2$
3. $r_A = r_B$

Privacy:

randomization by affine transform with r & r'

Gaps in Communication Complexity between Shared Randomness & Entanglement

Theorem [K & Nishimura, 2021]

∃partial function $f: (\{0,1\}^n)^2 \to \{0,1\}$ s.t.

some PSM protocol w/ e-bits for f has $\boldsymbol{O(\log n)}$-bit messages
& any PS**Q**M protocol w/ r-bits for f requires $\boldsymbol{\Omega(n)}$-bit messages.

Proof Strategy

distributed
Deutsch-Jozsa problem
(partial function)

Consider $\mathrm{DJ}_n(x,y) = \begin{cases} 1 & x = y \\ 0 & \Delta(x,y) = n/2 \end{cases} \quad (x, y \in \{0,1\}^n).$

Theorem [Brassard et al. (1999)]

DJ_n has 2-party SMP protocol w/ e-bits of message length = $O(\log n)$.

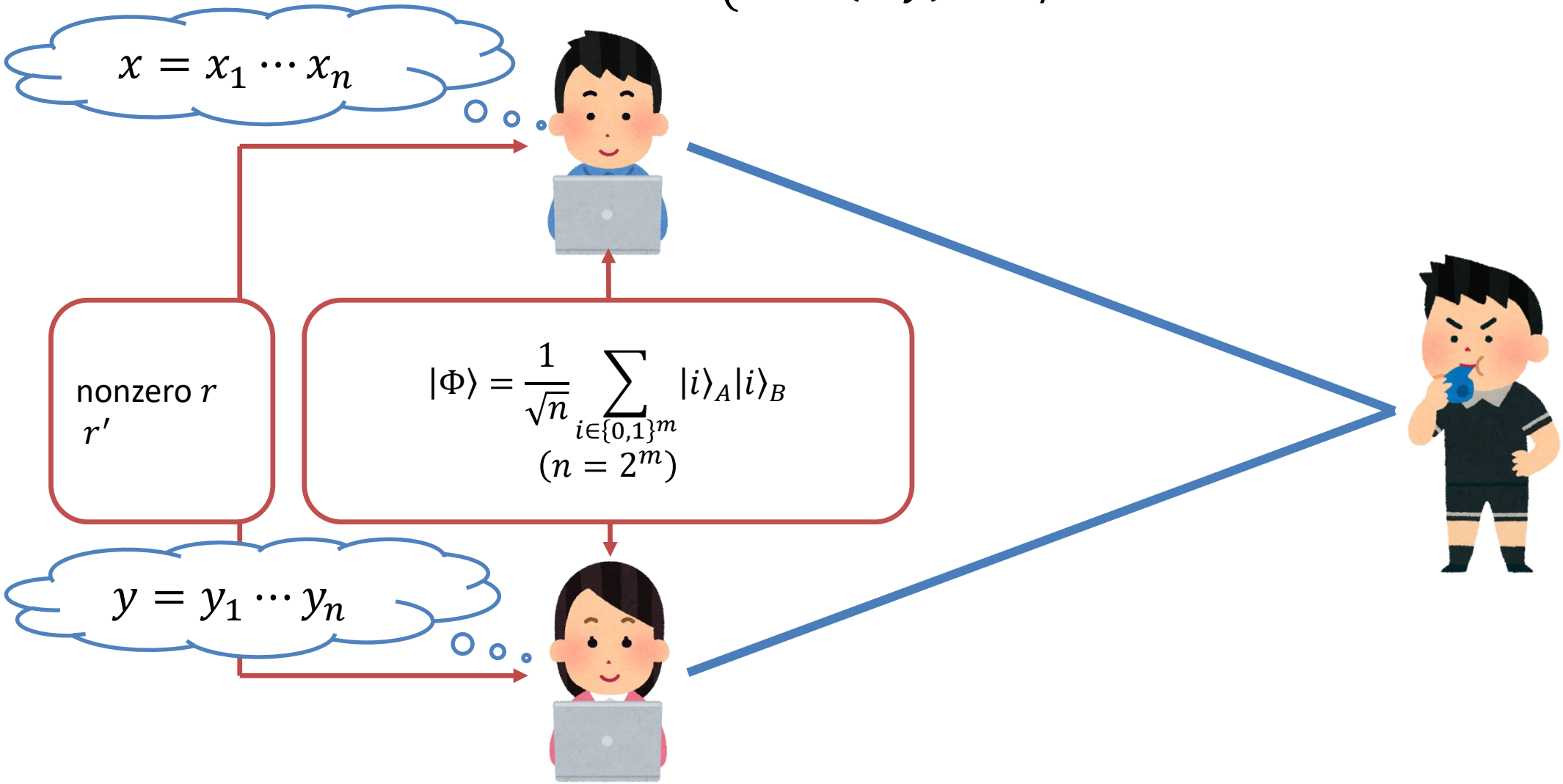
This protocol does **NOT** satisfy privacy condition…

Randomize **Q**-messages by random affine transform over $\mathbb{F}_2^n$

$\Omega(n)$-bit lower bound (w/ r-bits) can be obtained
by generalizing the argument of [de Wolf (2001)] for **partial functions**.

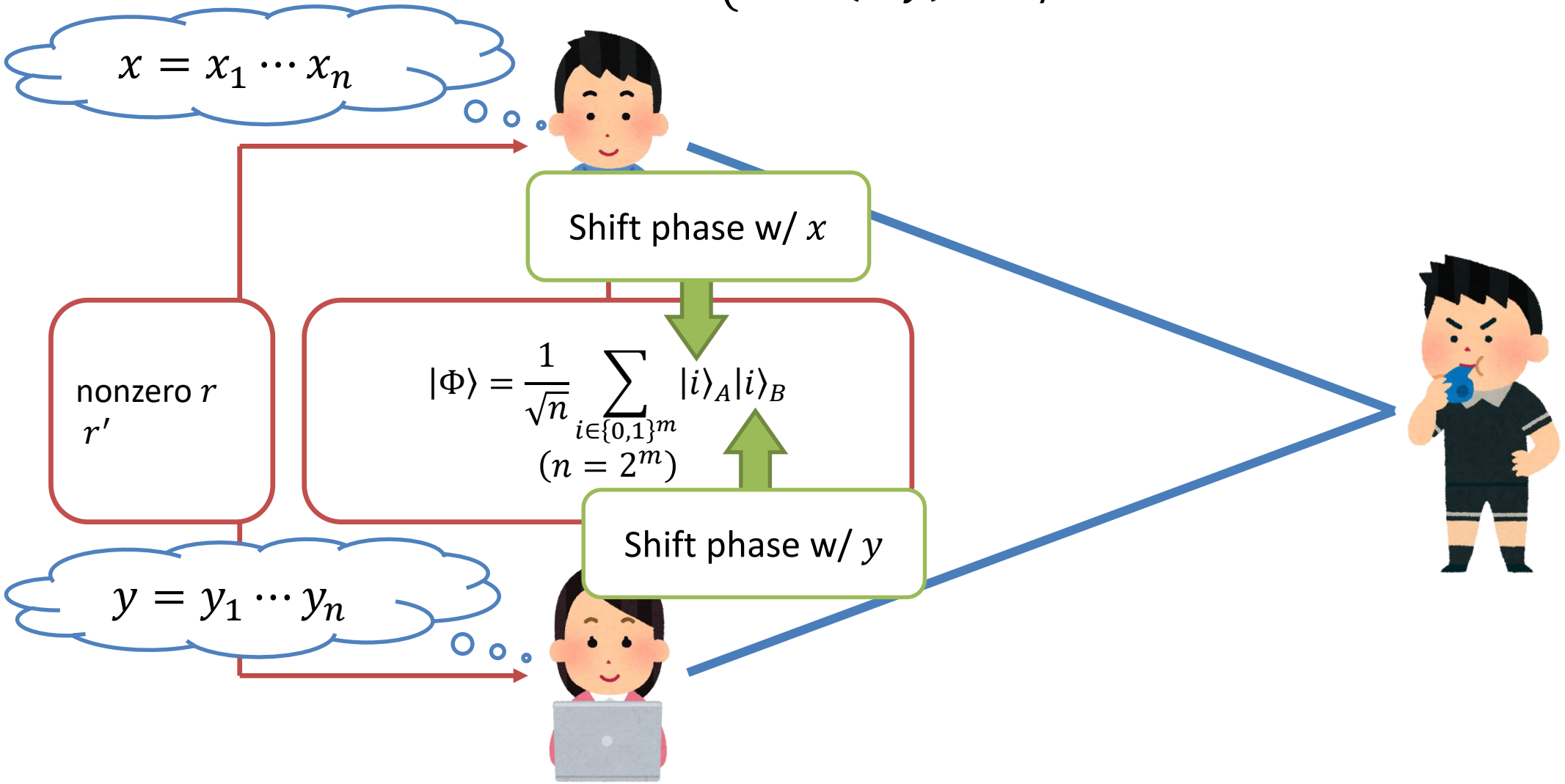
Protocol

Consider $\mathrm{DJ}_n(x,y) = \begin{cases} 1 & x = y \\ 0 & \Delta(x,y) = n/2 \end{cases} \quad (x, y \in \{0,1\}^n).$



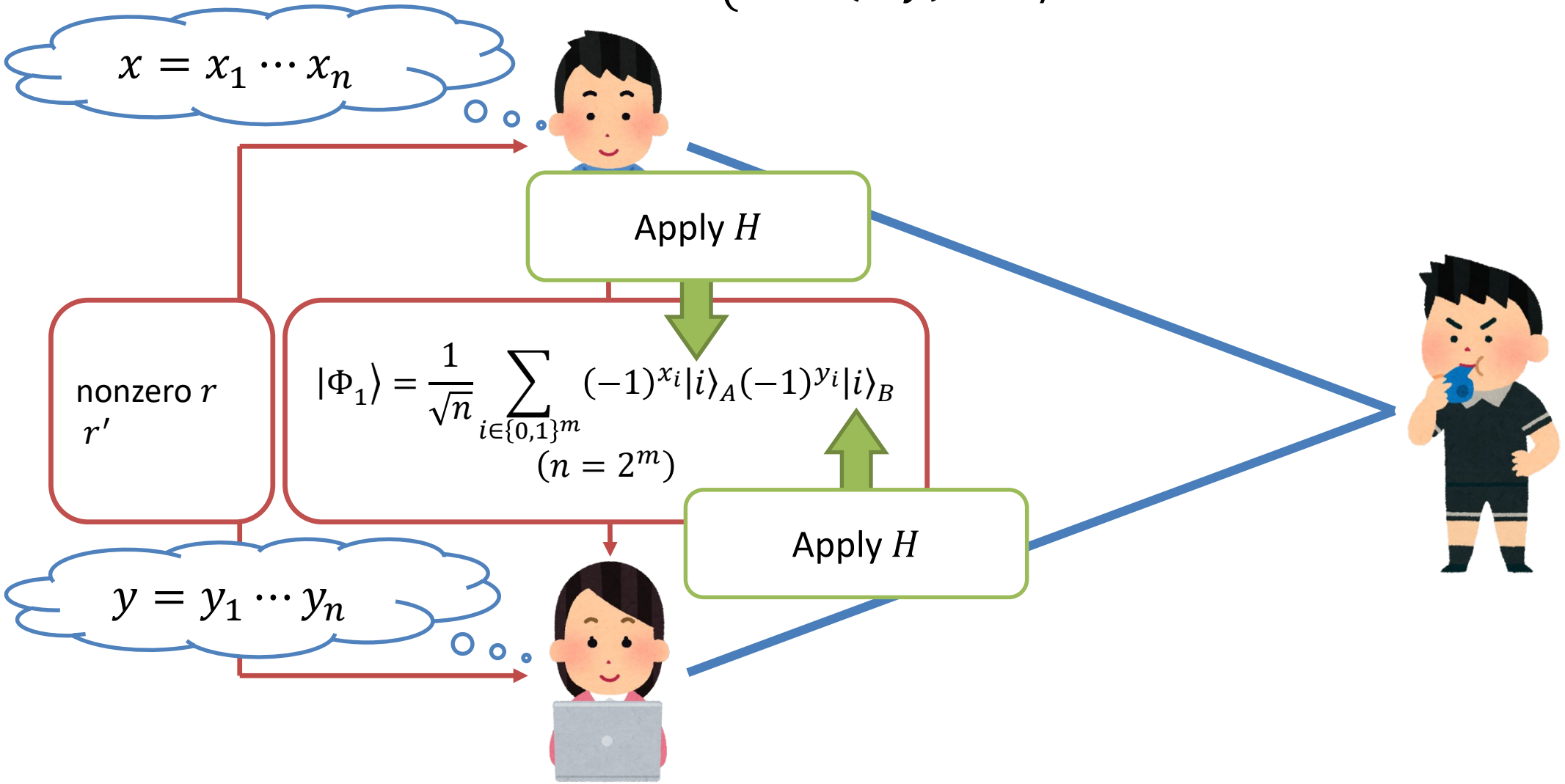
Protocol

Consider $\mathrm{DJ}_n(x,y) = \begin{cases} 1 & x = y \\ 0 & \Delta(x,y) = n/2 \end{cases} \quad (x, y \in \{0,1\}^n).$



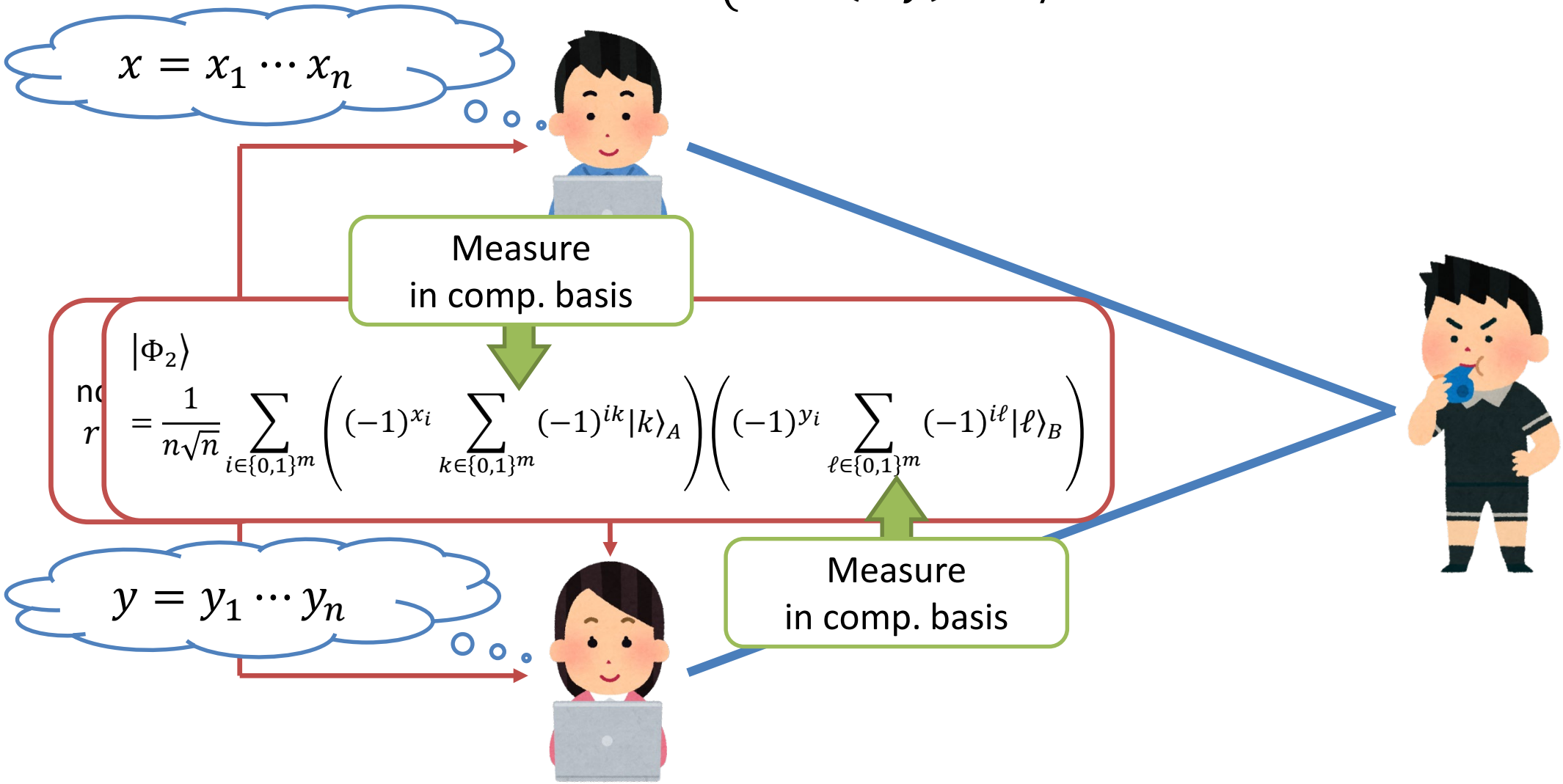
Protocol

Consider $\mathrm{DJ}_n(x,y) = \begin{cases} 1 & x = y \\ 0 & \Delta(x,y) = n/2 \end{cases} \quad (x, y \in \{0,1\}^n).$



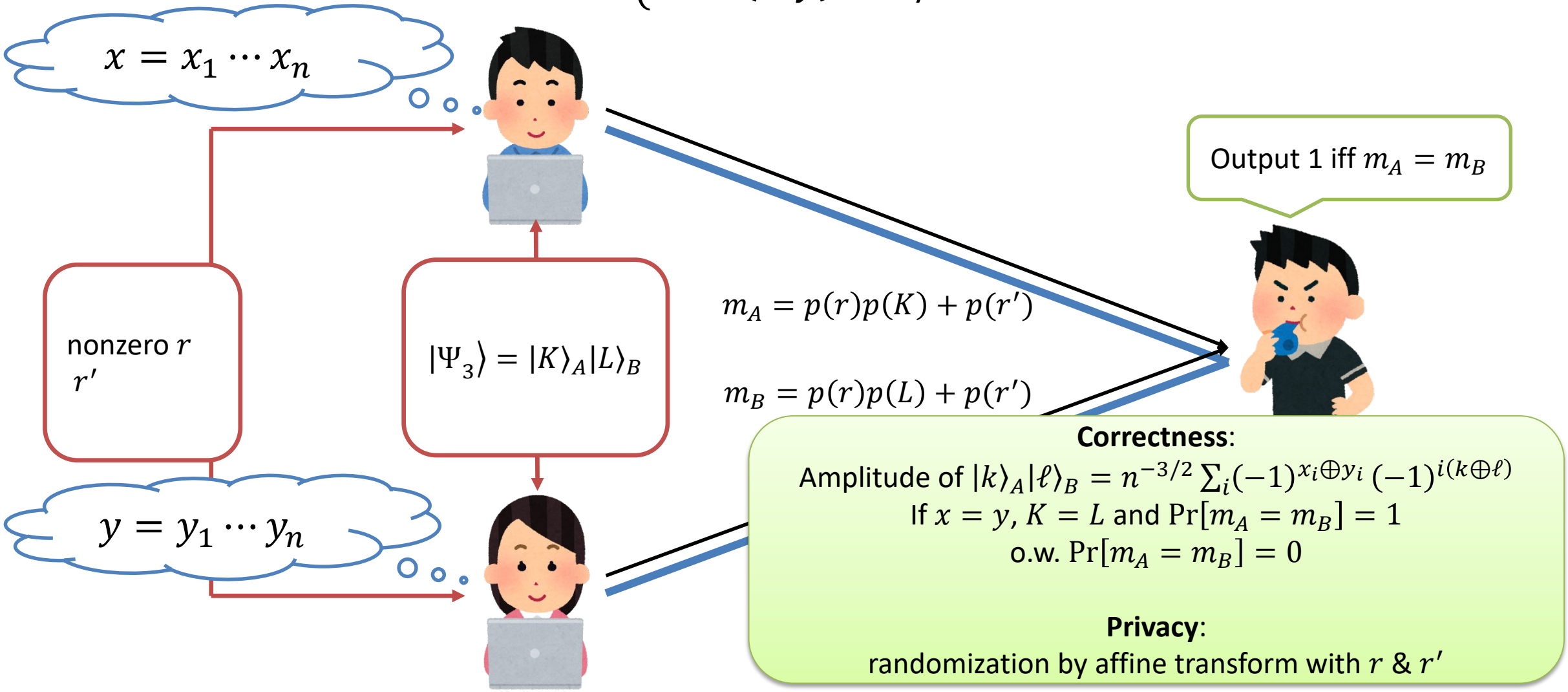
Protocol

Consider $\mathrm{DJ}_n(x,y) = \begin{cases} 1 & x = y \\ 0 & \Delta(x,y) = n/2 \end{cases} \quad (x, y \in \{0,1\}^n).$



Protocol

Consider $\mathrm{DJ}_n(x,y) = \begin{cases} 1 & x = y \\ 0 & \Delta(x,y) = n/2 \end{cases} \quad (x, y \in \{0,1\}^n).$



Communication Lower Bounds in PSQM

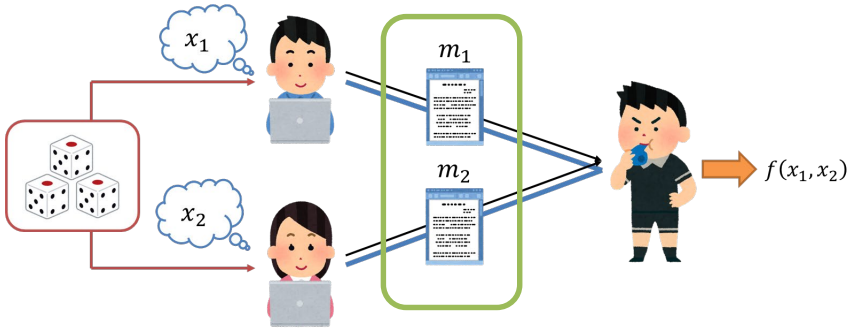
Theorem [K & Nishimura (2021)]

For $1 - o(1)$ fraction of functions $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$,
∀PS**Q**M protocol w/ r-bits for f has **CC** $\geq \boldsymbol{\left(3 - o(1)\right)n}$.

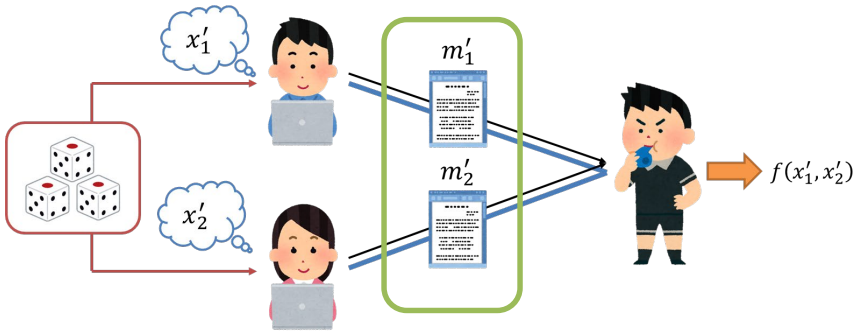
Proof Strategy (Classical lower bounds)

Run PSM twice independently!

1st message
$\boldsymbol{m} \in M$



2nd message
$\boldsymbol{m'} \in M$



Event $P^{(=)} \equiv [m = m'] \equiv$ 1st & 2nd messages collide.

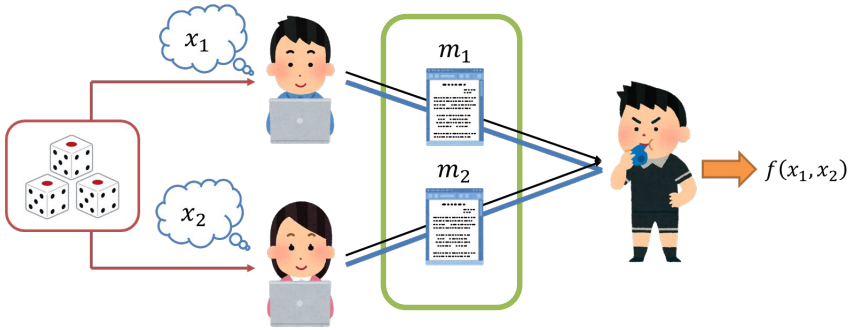
Fact

Collision prob. $\geq 1/|$message domain$|$

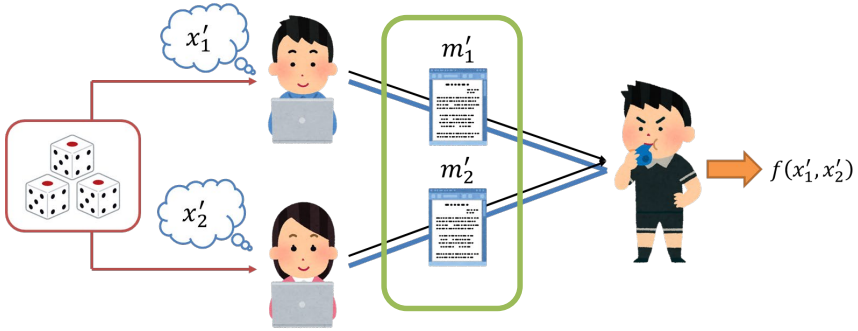
Proof Strategy (Classical lower bounds)

Run PSM twice independently!

1st message
$\boldsymbol{m} \in M$



2nd message
$\boldsymbol{m}' \in M$



Event $P^{(=)} \equiv [m = m'] \equiv$ 1st & 2nd messages collide.

Fact

message length

$$\Pr\left[P^{(=)}\right] \geq 1/|M|, \text{ i.e., } \log|M| \geq \log\left(\frac{1}{\Pr\left[P^{(=)}\right]}\right)$$

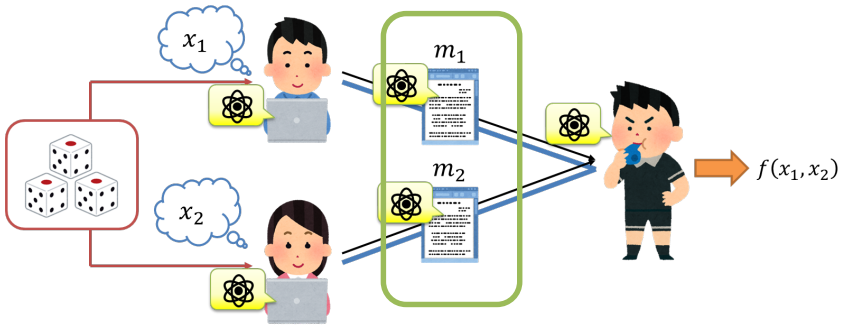
UB of $\Pr\left[P^{(=)}\right]$ ➔ LB of message length!

Proof Strategy (Quantum lower bounds)

Run PS**Q**M twice independently!

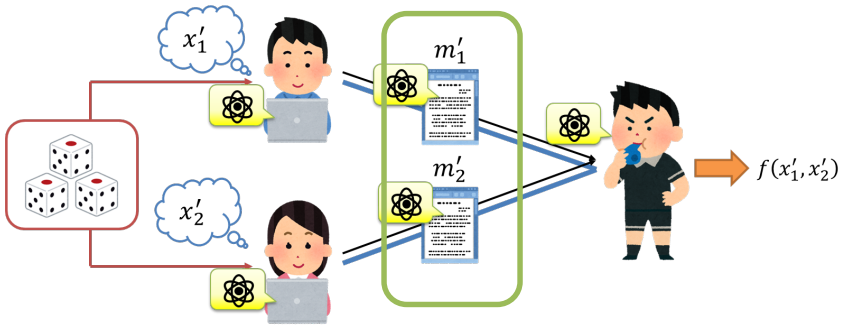
1st message

$\rho_m \in \mathcal{H}_M$



2nd message

$\rho_{m'} \in \mathcal{H}_M$



Event $P^{(=)} \equiv [\rho_m = \rho_{m'}] \equiv$ 1st & 2nd messages collide.

$\Pr[P^{(=)}] \geq 1/\dim \mathcal{H}_M$ does **NOT** hold!

Infinite states can live in finite-dimensional $\mathcal{H}_M$…

Proof Strategy (Quantum lower bounds)

"collision measure" for **Q**-messages ??

The **purity** $\mathrm{tr}(\rho_m^2)$ of **Q**-message ρ_m = "how pure ρ_m is"

= "**how much two ρ_m collide**"

Fact

Q-message length

$$\mathrm{tr}(\rho_m^2) \geq 1/\dim \mathcal{H}_M, \text{ i.e., } \log(\dim \mathcal{H}_M) \geq \log(\mathrm{tr}(\rho_m^2)^{-1})$$

UB of $\mathrm{tr}(\rho_m^2)$ ➔ LB of **Q**-message length!

Classical LB — Collision probability: $\Pr[m = m']$ → Combinatorial analysis of probability

Quantum LB — Purity: $\mathrm{tr}(\rho_m^2)$ → Combinatorial analysis of **trace** w/ quantum barriers

Open Problems

- Exponential gap of CC in PSM w/ IT privacy
  - UB: $2^{n/2}$ for all functions [Beimel et al. (2014)]
  - LB: $(3 - o(1))n$ for almost all functions [Applebaum et al. (2020)]
    - cf. DRE has $\Omega(n^2/\log n)$ LB for Element Distinctness [Ball, Holmgren, Ishai, Liu & Malkin (2020)]
- Computational power of PSM w/ IT privacy
  - mod_p-L functions have poly CC w/ IT privacy [Ishai & Kushilevitz (1997)]
    - P functions have poly CC w/ comp. privacy [Feige, Kushilevitz & Naor (1994)]
- Limitations of entanglement in PSQM
  - $(3 - o(1))n$ LB in PSQM protocols w/ r-bits [K & Nishimura (2021)]
  - Can break this LB w/ e-bits, or not?