Concrete Functions in Private Simultaneous Quantum Messages

arXiv:2610.23090

Harumichi Nishimura (Nagoya U.)

Shenzhen-Nagoya Workshop on Quantum Science 2026
November 21, 2026

Well-motivated general question

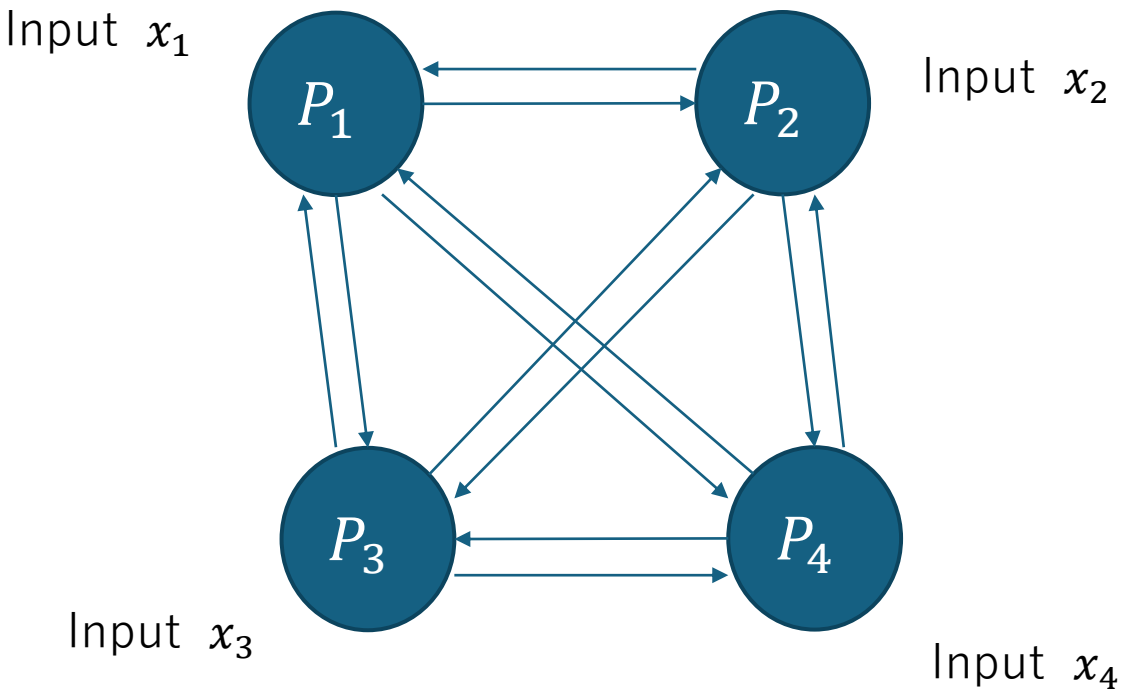
Q: Can we implement some tasks without revealing private data?

A: We can do them with several settings and conditions

- Zero-knowledge
- Multiparty computation

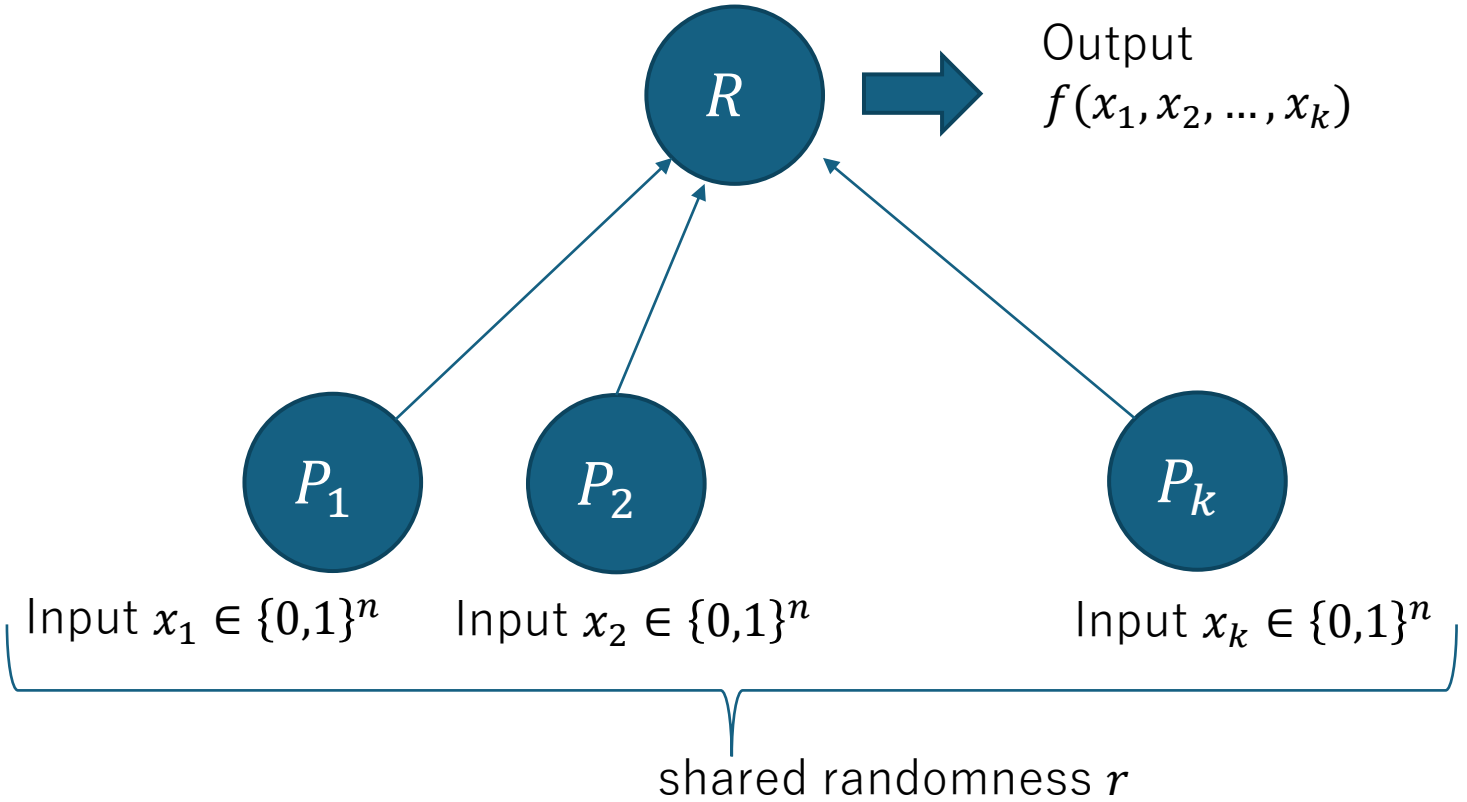
Multi-Party Computation (MPC)

- Jointly computes $f(x_1, x_2, \ldots, x_k)$ with revealing nothing but $f(x_1, x_2, \ldots, x_k)$



Private simultaneous messages (PSM)

- Minimal model of multiparty computation [FKN94]
  - Non-interactive
  - Seems to be easy to analyze



[FKN94] U. Feige, J. Killian, M. Naor, Proc. 26th STOC (1994)

Previous work on PSM

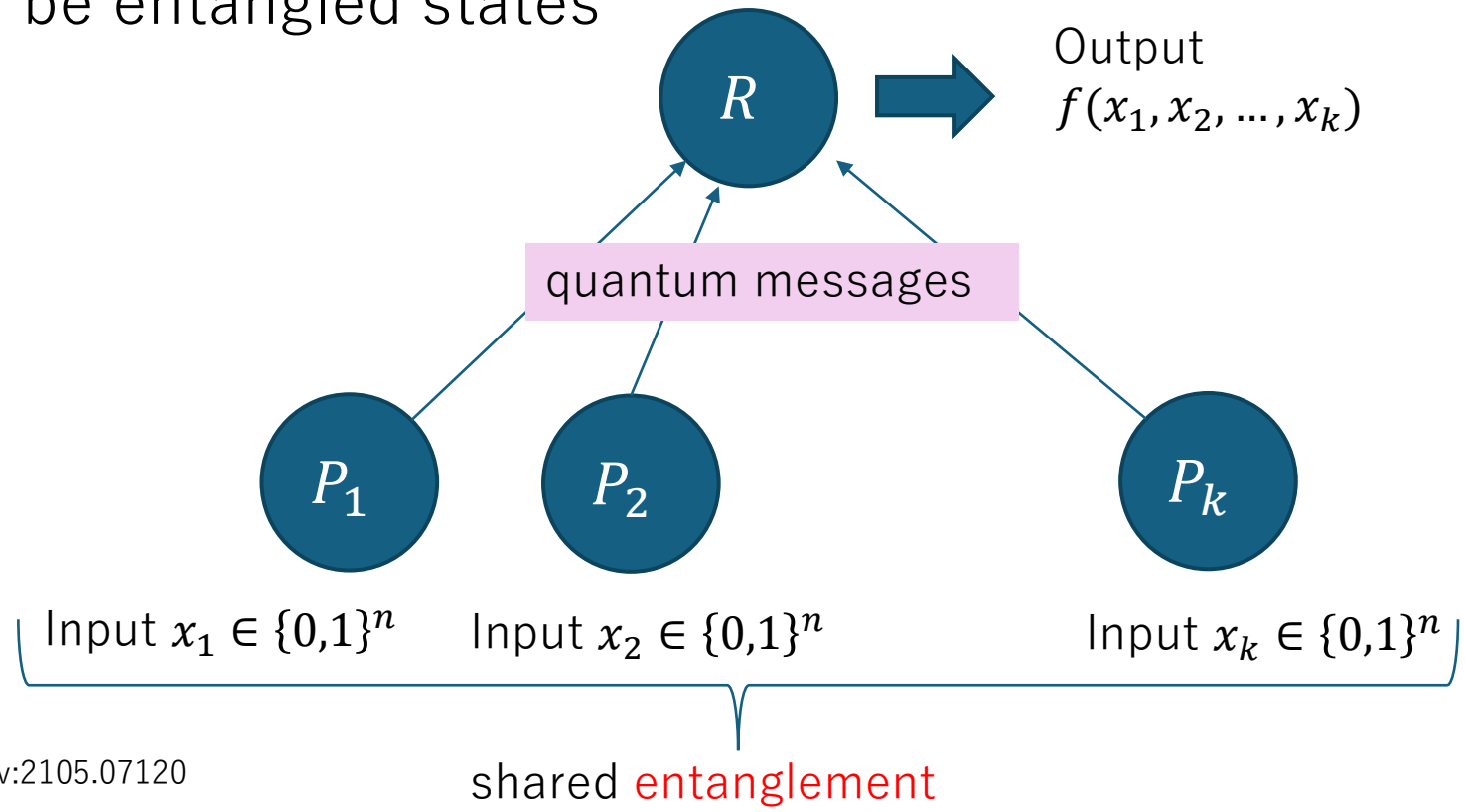
- Many works on communication complexity since [FKN94]
  - General: large gap even in the two-party case
    - Upper bound: exponential in the input-length
    - Lower bound: linear
  - Specific functions
    - (multiparty) AND [FKN94]
    - Functions with small branching programs [IK97]
    - Equality [NS23]
    - Majority [NS23]
    - …

Q: How does the complexity change in the **quantum** case?

[IK97] Y. Ishai, E. Kushilevitz, Proc. 5 th ISTCS (1997)
[NS23] K. Shinagawa, K. Nuida, Proc. 24th INDOCRYPT (2023)

Private simultaneous quantum messages (PSQM)

- PSQM [KN21]
  - Messages are quantum states
  - Shared resources may be entangled states



[KN21] A. Kawachi, H. Nishimura, Proc. 2nd ITC (2021); arXiv:2105.07120

Previous work on PSQM

- General
  - Non-trivial lower bound for the 2-party case with shared randomness (not with shared entanglement) [KN21]
  - Exponential quantum-classical gap for the 2-party case
    - Partial function [KN21]
    - Relation in the robust setting (with correctness & privacy errors) [KN21]
    - Partial function [GMOW26]
  - Relation to nonlocal quantum computation [ABMSV24]
  - Conversion from QSMP (no privacy) with low-T-depth to PSQM [GMPY26]

  …

[GMOW26] U. Girish, A. May, L. Orshansky, C. Waddell, Quantum (2026)
[ABMSV24] R. Allerstofer, H. Buhrman, A. May, F. Speelman, P. Verduyn Luel, Quantum (2024)
[GMPY26] U. Grish, A. May, N. Parham, H. Yuen, Proc. 58th STOC (2026)

Previous work on PSQM

- General
  - Non-trivial lower bound for the 2-party case with shared randomness (not with shared entanglement) [KN21]
  - Exponential quantum-classical gap for the 2-party case
    - Partial function [KN21]
    - Relation in the robust setting (with correctness & privacy errors) [KN21]
    - Partial function [GMOW26]
  - Relation to nonlocal quantum computation [ABMSV24]
  - Conversion from QSMP (no privacy) with low-T-depth to PSQM [GMPY26]

  …
- Specific functions
  - Equality for the 2-party case [KN21]
  - 2-bit AND [CP23,TN21]

[CP23] R. Christensen, P. Popovski, IEEE Quantum Eng. (2023)
[TN21] R. Takeda, H. Nishimura, QIT45 (2021)

Our results

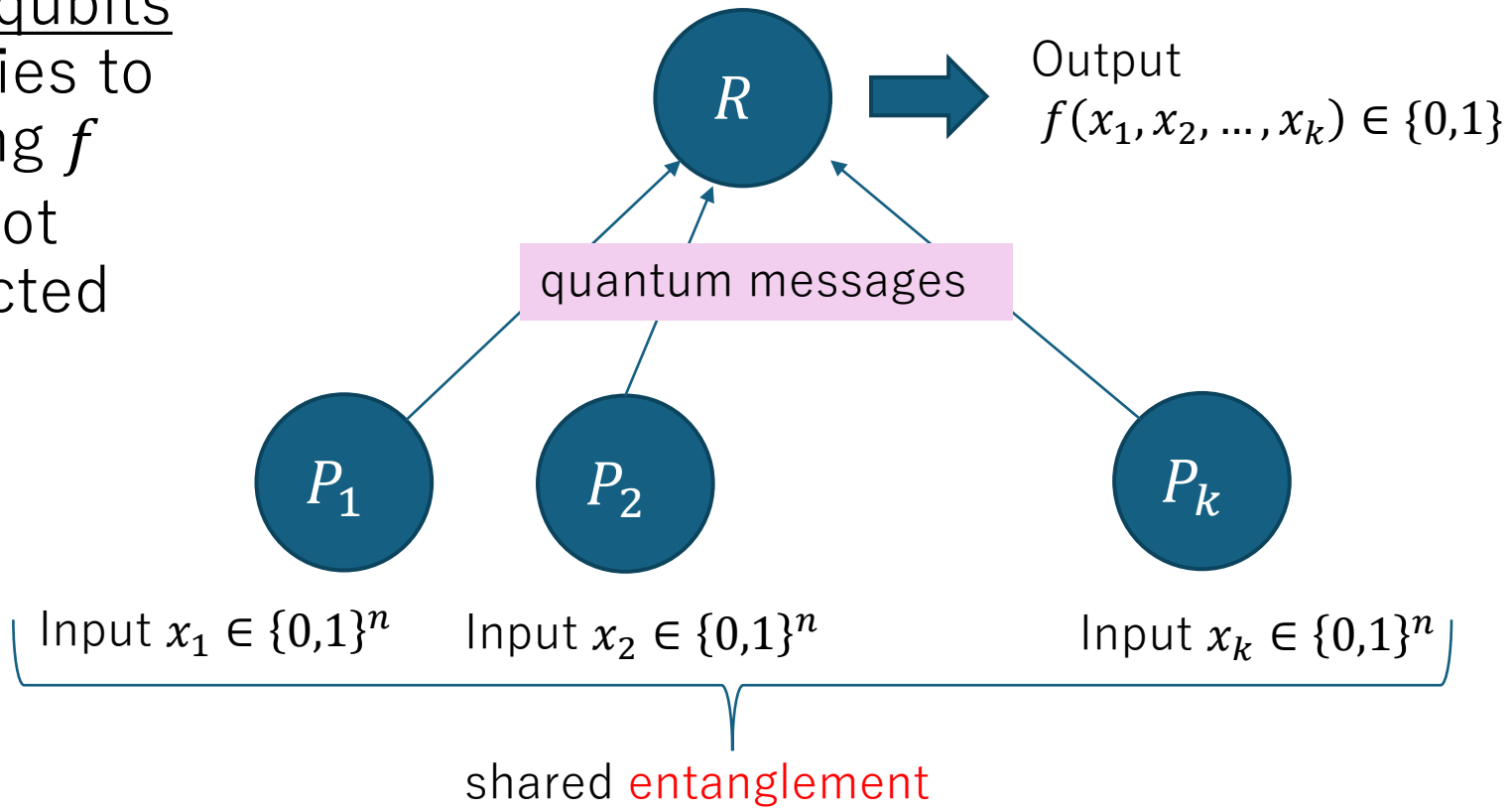
- Upper bounds of several concrete Boolean-valued functions
- Conditional lower bound of AND
- Microsoft Copilot & Chat GPT5.6Sol used

Function	Classical PSM	Entanglement-assisted PSQM
$\mathrm{EQ}_{k,n}$	$\geq kn$ bits	$\leq \frac{k}{2h_2(1/k)}\, n + O_k(\sqrt{n})$ qubits
MAJ_3	6 bits [21]	3 qubits
EQ_3	$3\log_2 3$ bits [21]	3 qubits
AND_3	$[6, 3\log_2 5]$ bits [7, 21]	$\leq 3\log_2 3$ qubits
AND_k $(k \geq 3)$	$\leq k \log_2 \ell_k$ bits [7]	$\leq k \log_2 p_k \leq k \log_2 k$ qubits

Table 1.1: Classical and entanglement-assisted quantum communication bounds for the functions studied in this paper. Here, ℓ_k is the smallest prime greater than k, while p_k is the smallest prime satisfying $k \leq 2(p_k - 1)$. The interval in the AND_3 row gives the currently known classical lower and upper bounds.

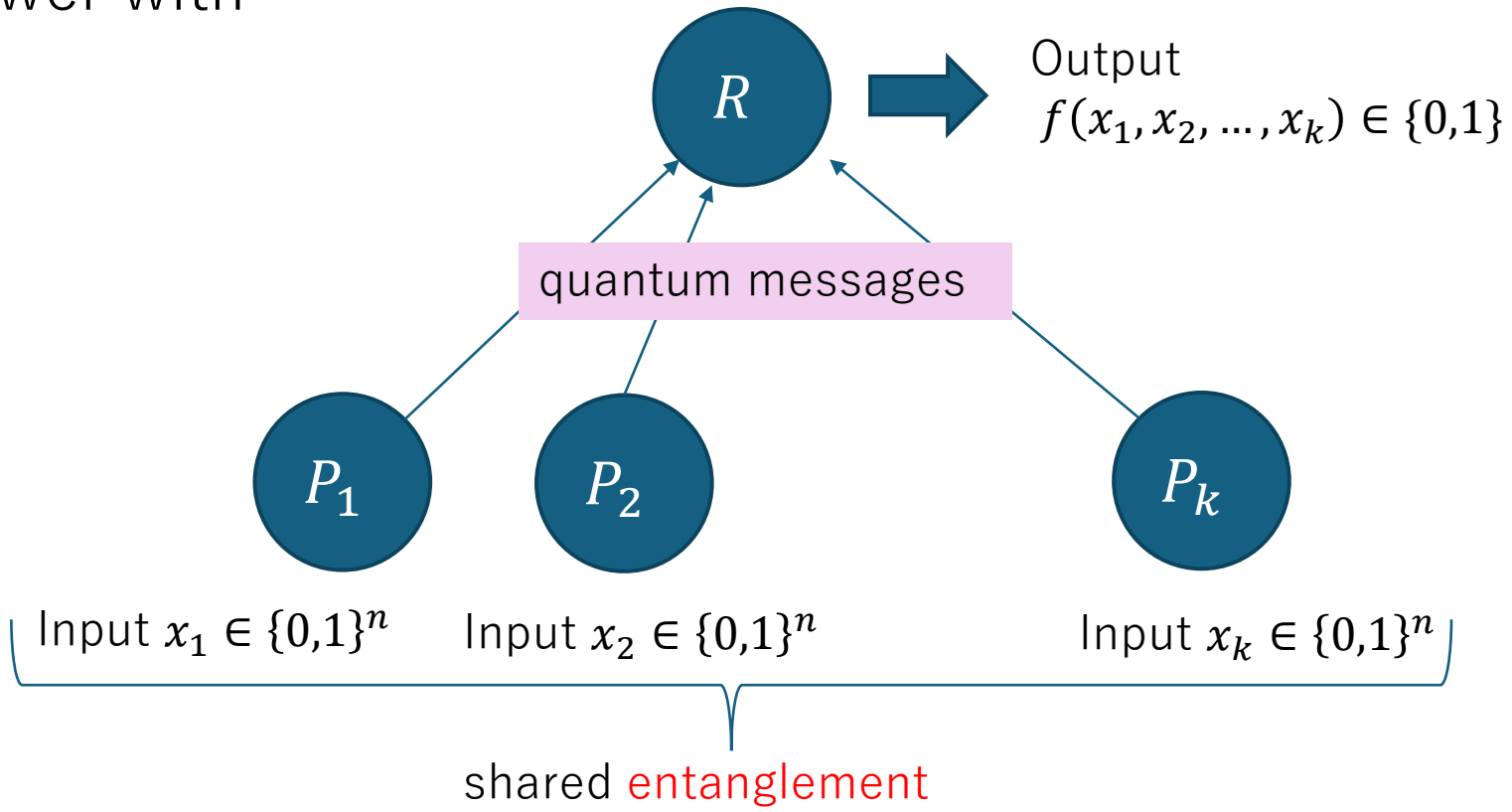
Formalization

- Cost
  - $Q^{PSQM,*}(f) :=$ <u>total communication of qubits</u> to be sent from the parties to the referee for computing f
  - Local operations are not computationally restricted



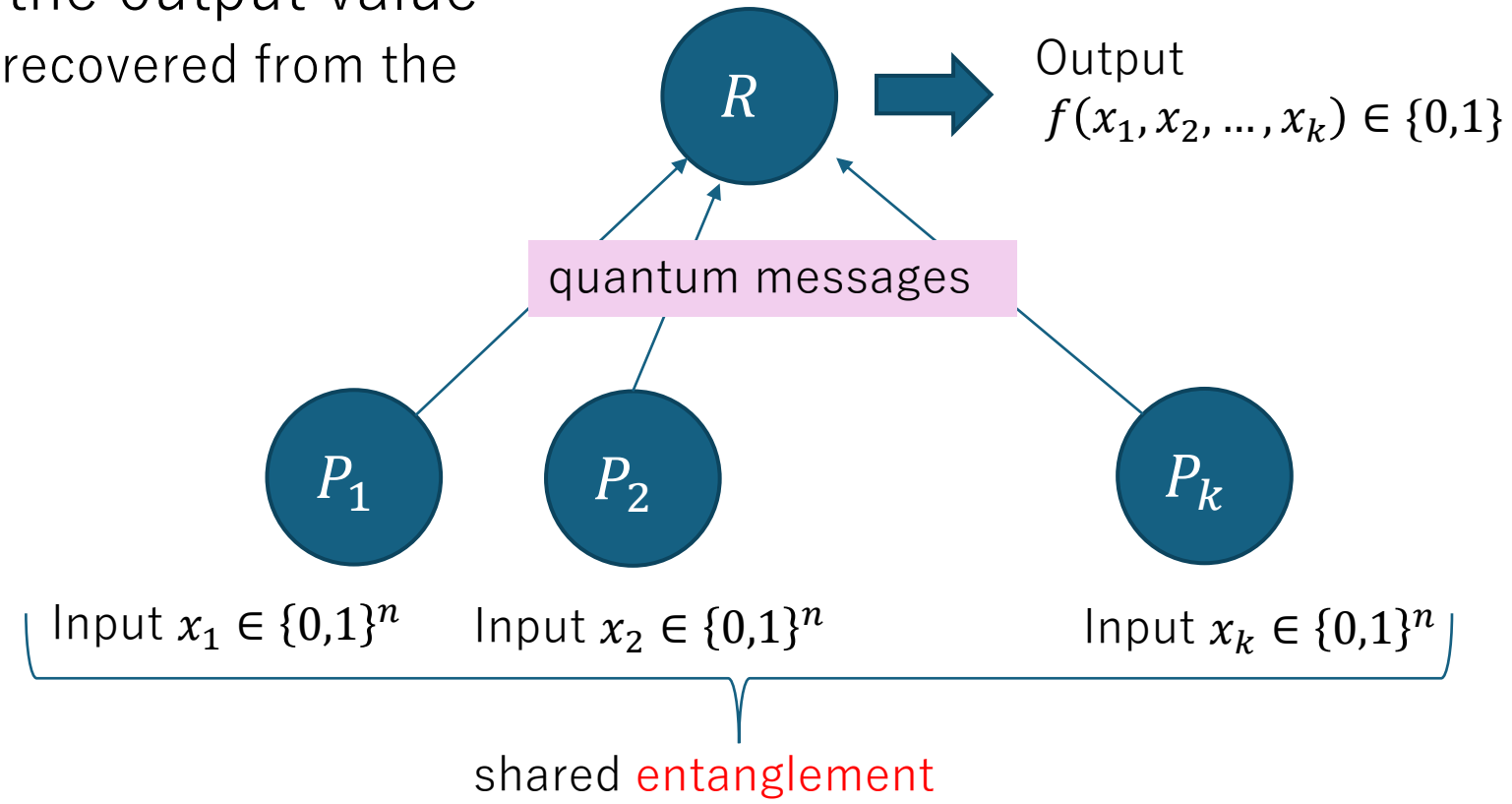
Formalization

- Correctness
  - Perfect correctness: the referee must output the correct answer with probability 1



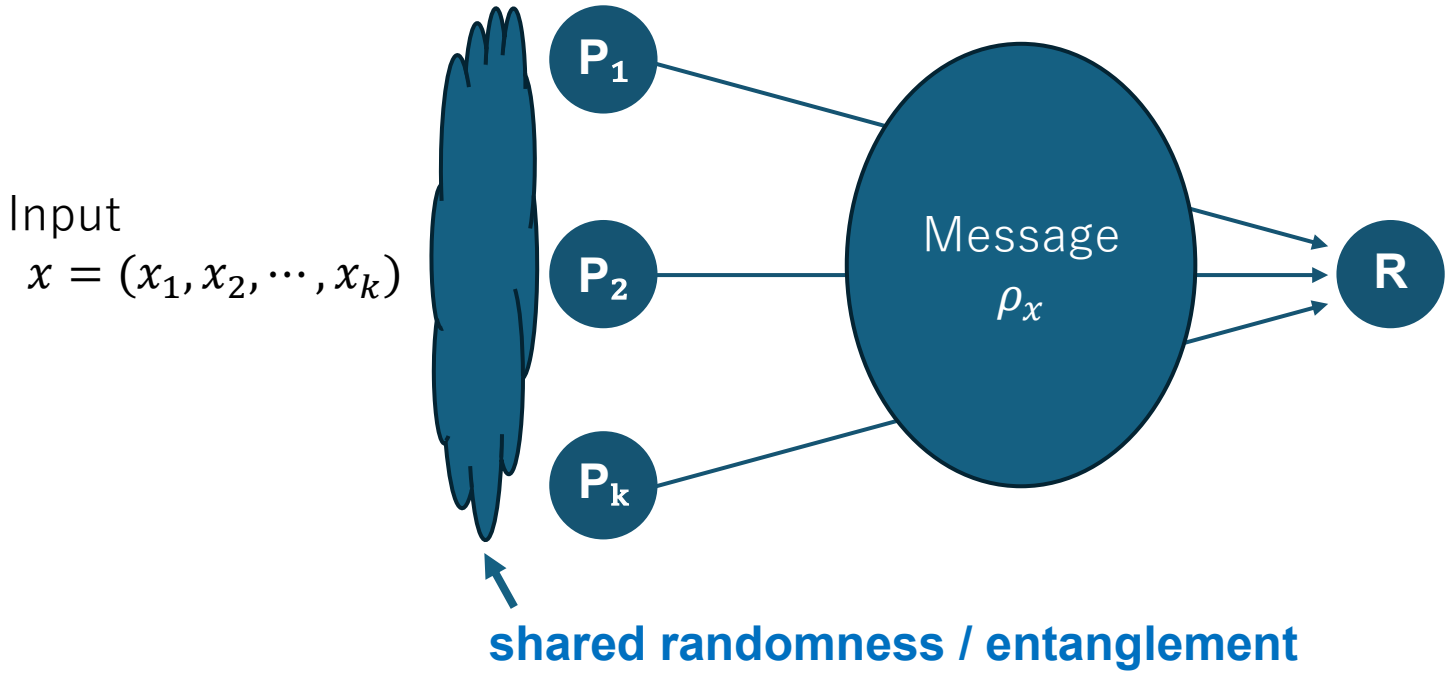
Formalization

- Privacy
  - Perfect privacy: the referee does not learn anything except the output value
    - The messages can be recovered from the output value



Perfect correctness & privacy

- Perfect privacy
  - $\exists \xi_0, \xi_1 [\forall x \, [\rho_x = \xi_{f(x)}]]$
  - The whole received state depends only on the output value
- Perfect correctness
  - $\mathrm{supp}(\xi_0) \perp \mathrm{supp}(\xi_1)$
  - The output values are distinguishable with certainty



First result: multi-party equality

- Equality
  - $EQ_{k,n}(x_1, \cdots, x_k) = 1$ iff n-bit strings $x_1, \cdots, x_k$ are all the same
  - $k = 2$ [KN21]
    - Quantum: n qubits; Classical: $2n$ bits
  - Extension to multi-party
    - $GEQ_{k,n}(x_1, \cdots, x_k) = 1$ iff $x_1 \oplus \cdots \oplus x_k = 0^n$
    - Quantum: $\frac{kn}{2}$ qubits (n: even); Classical: kn bits

[Theorem 1] $Q^{PSQM,*}\left(EQ_{k,n}\right) \leq \frac{k}{2h_2\left(\frac{1}{k}\right)} n + O_k(\sqrt{n})$

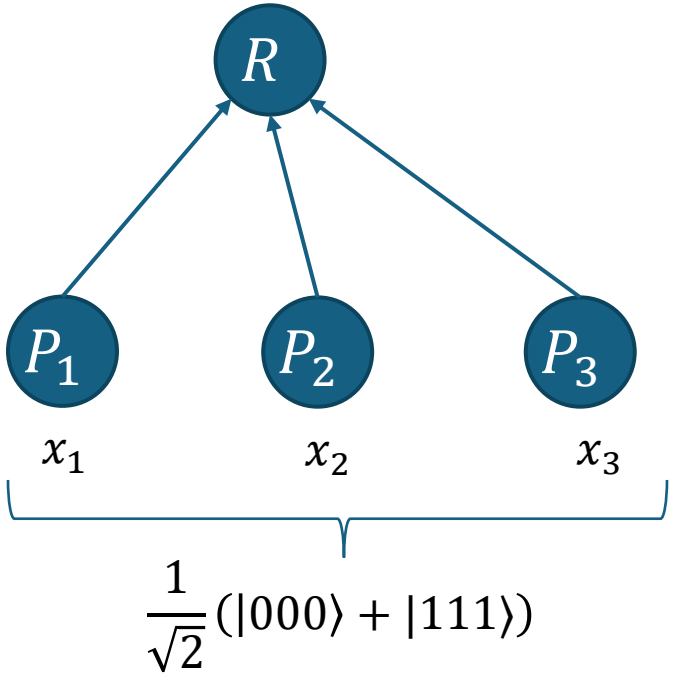
- $Q^{PSQM,*}\left(EQ_{3,n}\right) \leq (1.633\ldots)n + O(\sqrt{n})$ (cf. classical: $3n$ bits)
- Quantum advantage for $k \leq 9$
- Reduction to GEQ using additive combinatorics

Second result: 3-bit Majority

- 3-bit Majority
  - $MAJ_3(x_1, x_2, x_3) = 1$ iff at least two of 3 bits x_1, x_2, x_3 are 1
  - Classical: 6 bits [SN23]

[Theorem 2] $Q^{PSQM,*}(MAJ_3) = 3$

- 3-bit equality $EQ_{3,1}$ also has the cost of 3 qubits while the classical cost is $3\log_2 3$ bits [SN23]
- 80 functions of 256 3-bit Boolean functions also have the cost of 3 qubits
- Their protocols are implemented by local Paulis on the shared entanglement $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

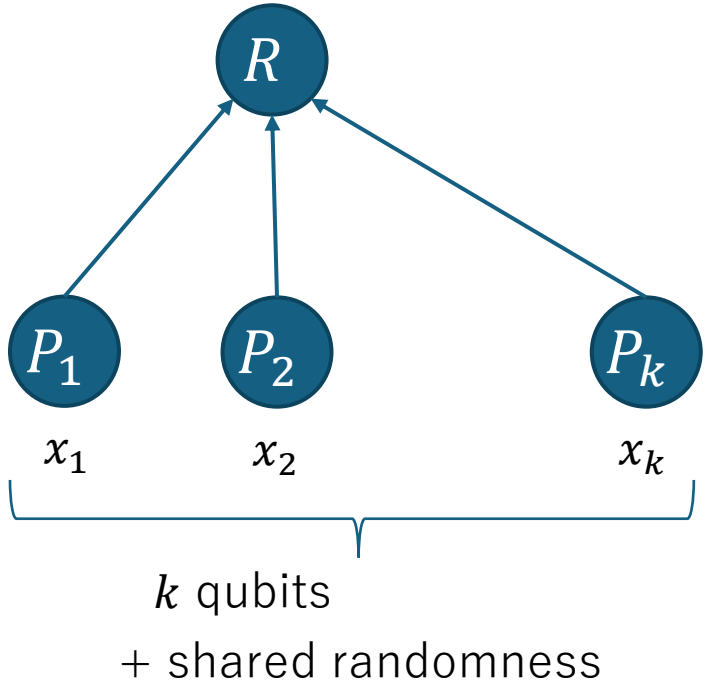


Third result: AND

- AND
  - $AND_k(x_1, \cdots, x_n) = 1$ iff $x_1 = \cdots = x_k = 1$
  - AND seems to be easier than MAJ
  - Classical case for $k = 3$: at least 6 bits [SN23]
  - $Q^{PSQM,*}(AND_2) = 2$ [CP23,TN21]

[Theorem 3] AND_k $(k \geq 3)$ cannot have the cost of k qubits in the one-qubit local unitary model:

- Shared entanglement is k qubits
- Local operation of each party is a one-qubit unitary depending on its own input and shared randomness
- Rank arguments on the state sent to the referee



Fourth result: upper bound for AND

- AND
  - $AND_k(x_1, \cdots, x_n) = 1$ iff $x_1 = \cdots = x_k = 1$
  - Classical case for $k = 3$: at least 6 bits [SN23]
  - $Q^{PSQM,*}(AND_2) = 2$ [CP23,TN21]

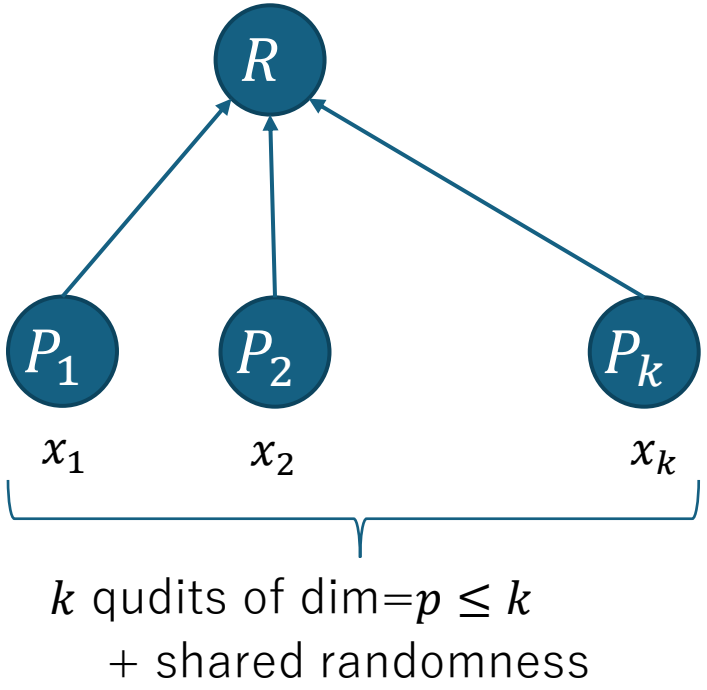
[Theorem 3] AND_k $(k \geq 3)$ cannot have the cost of k qubits in the one-qubit local unitary model:

[Theorem 4] $Q^{PSQM,*}(AND_k) \leq k \log_2 k$

- Better than the classical case [FKN94]
- Quantum advantage for $k = 3$

Cf: Classical case

- $O(k \log k)$ [FKN94]
- $\omega(k)$ [HW26,BCPP26]



[HW26] J. Holmgren, K. Wu, arXiv:2609.18020
[BCPP26] M. Ball, P. Crawford-Kahrl, V. Podolskii, M. Prior, arXiv:2610.21216

Summary & open problems

- Results
  - Upper bounds of several concrete Boolean-valued functions
  - Conditional lower bound of AND

Function	Classical PSM	Entanglement-assisted PSQM
$\mathrm{EQ}_{k,n}$	$\geq kn$ bits	$\leq \frac{k}{2h_2(1/k)}\, n + O_k(\sqrt{n})$ qubits
MAJ_3	6 bits [21]	3 qubits
EQ_3	$3\log_2 3$ bits [21]	3 qubits
AND_3	$[6, 3\log_2 5]$ bits [7, 21]	$\leq 3\log_2 3$ qubits
AND_k $(k \geq 3)$	$\leq k \log_2 \ell_k$ bits [7]	$\leq k \log_2 p_k \leq k \log_2 k$ qubits

Table 1.1: Classical and entanglement-assisted quantum communication bounds for the functions studied in this paper. Here, ℓ_k is the smallest prime greater than k, while p_k is the smallest prime satisfying $k \leq 2(p_k - 1)$. The interval in the AND_3 row gives the currently known classical lower and upper bounds.

- Open problems
  - Unconditional lower bound of AND
  - Better quantum advantage
  - Robust setting (Imperfect correctness & privacy)