Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Exponential Advantage of Multipartite Entanglement over Quantum Communication with Applications to Bounded-Storage Cryptography

Ananya Chakraborty

ananyaphys.c@gmail.com

S. N. Bose National Centre for Basic Sciences

Manik Banik

S. N. Bose National Centre for Basic Sciences https://orcid.org/0000-0001-8036-790X

Ronald de Wolf

QuSoft, CWI and University of Amsterdam

Article

Keywords:

Posted Date: August 24th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10587821/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: There is **NO** Competing Interest.

Exponential Advantage of Multipartite Entanglement over Quantum Communication with Applications to Bounded-Storage Cryptography

Ananya Chakraborty[1*], Manik Banik[1] and Ronald de Wolf[2]

[1]S. N. Bose National Centre for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata, 700106, India.
[2]QuSoft, CWI and University of Amsterdam, Amsterdam, The Netherlands.

*Corresponding author(s). E-mail(s): ananyaphys.c@gmail.com;
Contributing authors: manik11ju@gmail.com; Ronald.de.Wolf@cwi.nl;

Abstract

We establish an exponential communication advantage enabled by multipartite quantum entanglement. Building on the bipartite Hidden Matching problem, we introduce a communication task involving multiple spatially separated senders and a single receiver. We show that a multipartite Greenberger–Horne–Zeilinger state shared among the senders and the receiver enables the task to be done using only logarithmically many bits of classical communication from each sender. In contrast, without preshared entanglement, any protocol achieving high success probability requires polynomial communication from at least one sender, even when *quantum* communication is allowed. Thus, classical communication assisted by multipartite entanglement can be exponentially more powerful than quantum communication without preshared entanglement. As a cryptographic application, we construct a seeded two-source randomness extractor and establish an exponential separation between entangled and unentangled quantum side-information. Specifically, compromising the extractor with two unentangled quantum states storing information about the two sources, respectively, requires polynomial-size memory, whereas exponentially smaller quantum memory suffices in the presence of a small amount of shared entanglement. Together, these findings illuminate the transformative, exponential advantages that multipartite entanglement imparts to both communication and cryptographic regimes.

Quantum entanglement, '*the characteristic trait of quantum mechanics*' [1], underlies some of the most profound phenomena in physics, including the Einstein-Podolsky-Rosen paradox, Schrödinger steering, and Bell nonlocality [2–6]. Beyond its foundational significance, entanglement is a key resource for quantum information processing, enabling communication, computation, and cryptographic tasks that are impossible or substantially less efficient within classical frameworks [7–15]. The communication advantages afforded by bipartite entanglement are now reasonably well understood [16]. By contrast, *multipartite* entanglement possesses a far richer structure, including genuinely multipartite forms that cannot be reduced to collections of bipartite correlations [17–19]. Despite remarkable experimental advances in generating and controlling multipartite entangled states [20–24], our understanding of how such states enhance distributed information-processing tasks remains comparatively limited. Communication complexity provides a natural framework for investigating this question. In communication complexity tasks, spatially separated parties seek to evaluate a global property of distributed inputs while exchanging as little communication as possible [25, 26]. Quantum resources can dramatically reduce communication costs and, in several notable instances, yield exponential advantages over classical protocols [27–30]. However, most known exponential separations are in bipartite settings [31–36], leaving open the question whether multipartite entanglement alone can provide comparable advantages in communication tasks.

Here, we address this question by introducing a multipartite one-way communication task wherein multiple spatially separated senders receive classical inputs and a single receiver must produce an output satisfying a prescribed global relation. We show that a Greenberger-Horne-Zeilinger (GHZ) state [37–39] shared among all the parties enables success using only $O(\log n)$ bits of *classical* communication from each sender. The protocol exploits the multipartite phase correlations of the GHZ state to encode the local inputs and recover the required global relation at the receiver. In contrast, any protocol achieving a high success probability without preshared entanglement requires polynomial communication from at least one sender. Remarkably, this lower bound continues to hold even when unrestricted *quantum* communication from the senders to the receiver is permitted. Consequently, classical communication assisted by multipartite entanglement is exponentially more powerful than unrestricted quantum communication without preshared entanglement. Our result establishes a multipartite analogue of the communication separation previously established in the bipartite setting [40], thereby identifying multipartite entanglement as a resource for exponential communication savings.

Beyond communication complexity, our results have implications for bounded-storage cryptography with quantum side-information [41]. The multipartite communication protocol developed here naturally gives rise to a seeded randomness extractor involving multiple independent weak sources (i.e., non-uniform but with some guaranteed min-entropy). The communication lower bound of our multipartite task translates directly into a lower bound on the quantum side-information required to compromise the resulting extractor. In particular, our construction shows that preshared entanglement exponentially enhances the power of quantum side-information: compromising the extractor requires polynomial-size unentangled quantum memory,

whereas exponentially smaller entangled quantum memory suffices. Consequently, our results establish an exponential separation between entangled and unentangled quantum side-information.

Results

I. Multiparty communication complexity

We now formally introduce the multipartite communication tasks underlying these results.

Multipartite Hidden Matching ($m\mathtt{HM}_n$). The task $m\mathtt{HM}_n$ involves m spatially separated senders $\{\text{Alice}_r\}_{r=1}^m$ and a receiver Bob. Each sender receives an input string: $\mathbf{x}^r \in \{0,1\}^n$ for Alice_r, where n is even. Bob receives a matching $\mathrm{M} = \{(i_\ell, j_\ell) : \ell = 1, \ldots, n/2\}$ from the set $\mathcal{M}_{n/2}$ of all perfect matchings on the set $[n] = \{1, \ldots, n\}$. We will assume throughout for simplicity that n is a power of 2.

The communication model is one-way: each Alice may send a message to Bob, but no communication is allowed among the Alices or from Bob to any of the Alices. Bob must output a triple $\big\langle i_\ell, j_\ell, \bigoplus_{r=1}^m (x^r_{i_\ell} \oplus x^r_{j_\ell}) \big\rangle$, for some edge $(i_\ell, j_\ell) \in \mathrm{M}$ (see Fig. 1). Thus, Bob reports one edge of the matching together with the parity, across all senders, of the corresponding endpoint bits.

For $m = 1$, this is the Hidden Matching problem introduced in [34]. Alice, when allowed to communicate qubits to Bob, encodes her input $\mathbf{x} = x_1 \ldots x_n$ into the $\log n$-qubit state

$$|\psi_{\mathbf{x}}\rangle = U_{\mathbf{x}} \left(\tfrac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle \right), \quad U_{\mathbf{x}} := \sum_{k=1}^{n} (-1)^{x_k} |k\rangle\langle k|, \tag{1}$$

and sends it to Bob. Given a perfect matching M, Bob performs the projective measurement $\mathfrak{M}_{\mathrm{M}} = \{\mathrm{P}^{i_\ell j_\ell} = |i_\ell\rangle\langle i_\ell| + |j_\ell\rangle\langle j_\ell| : (i_\ell, j_\ell) \in \mathrm{M}\}$, which projects onto a uniformly random edge $(i_\ell, j_\ell) \in \mathrm{M}$ with resulting state being $|\psi_{i_\ell j_\ell}\rangle = \frac{1}{\sqrt{2}}\big[(-1)^{x_{i_\ell}} |i_\ell\rangle + (-1)^{x_{j_\ell}} |j_\ell\rangle\big]$. Finally, Bob measures in the basis $\{(|i_\ell\rangle \pm |j_\ell\rangle)/\sqrt{2}\}$, which deterministically reveals the parity $x_i \oplus x_j$. Hence, the Hidden Matching relation $\mathtt{HM}_n$ is solved with perfect success using only $\log n$ qubits of communication.

Multipartite Boolean Hidden Matching ($m\mathtt{BHM}_n$). Notably, $m\mathtt{HM}_n$ is a relational communication problem: for each input $(\mathbf{x}, \mathrm{M})$, there is a valid output for each of the edges of M. We also consider a Boolean decision version of the task, denoted $m\mathtt{BHM}_n$, and defined as follows. A 1/4-matching M is a partial matching consisting of $n/4$ disjoint pairs from $[n]$. In addition to such an $\mathrm{M} \in \mathcal{M}_{n/4}$, Bob receives a string $\mathbf{w} \in \{0,1\}^{n/4}$ satisfying the promise $\mathbb{M}\big(\bigoplus_{r=1}^m \mathbf{x}^r\big) \oplus \mathbf{b}^{n/4} = \mathbf{w}$, where $\mathbb{M}$ is the $n/4 \times n$ incidence matrix of M, with one weight-2 row for each edge of M, and $\mathbf{b}^{n/4}$ is the length-$n/4$ all-b string. Equivalently, the promise ensures either $\mathbf{z} := \mathbb{M}\big(\bigoplus_{r=1}^m \mathbf{x}^r\big) = \mathbf{w}$ when $b = 0$, or $\mathbf{z} = \overline{\mathbf{w}}$ when $b = 1$. Bob's goal is to determine the value of the bit b, so this problem is now a partial Boolean function. The reason we are defining this with respect to a partial matching M rather than a perfect matching is that our main lower bound fails in the latter case, as will become evident in the discussion following Theorem 4 (see **Methods**).

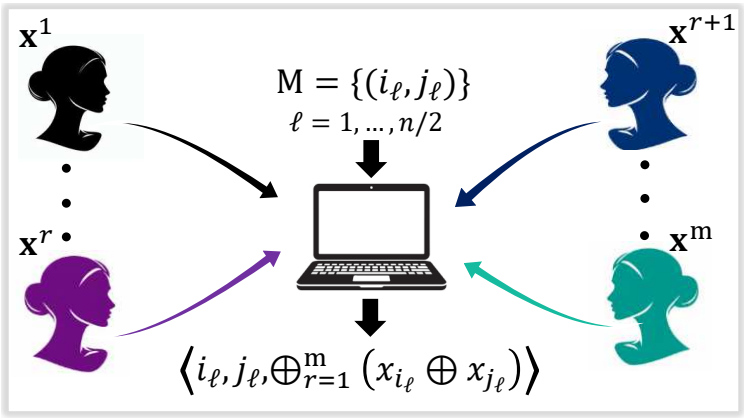


Figure 1 Multipartite Hidden Matching task ($m\mathtt{HM}_n$). It involves m spatially separated senders (Alices), where the rth Alice receives a string $\mathbf{x}^r \in \{0,1\}^n$. Bob receives a perfect matching $\mathrm{M} \in \mathcal{M}_{n/2}$ on $[n]$. His goal is to output a triple $\langle i_\ell, j_\ell, \bigoplus_{r=1}^m (x^r_{i_\ell} \oplus x^r_{j_\ell})\rangle$ for some edge $(i_\ell, j_\ell) \in \mathrm{M}$. The Boolean variant $m\mathtt{BHM}_n$ is a related decision problem defined in the text.

Within the Simultaneous Message Passing (SMP) framework [42], a natural hierarchy of one-way communication models emerges, distinguished by the communication resources and shared correlations available to the parties:

- *Classical communication without shared resources:* The Alices send classical messages to Bob, and no shared randomness or entanglement is available. The corresponding communication complexity (i.e., worst-case total number of bits sent, minimized over all protocols solving the task) for perfect, error-free protocols is denoted by $C^{\|}$.
- *Classical communication with global shared randomness:* All parties have access to a common random string. The corresponding complexity is denoted by $C^{\|,\mathrm{GSR}}$ for error-free protocols.
- *Classical communication assisted by bipartite entanglement:* Each Alice shares independent bipartite entanglement with Bob, yielding complexity $C^{\|,\{\mathrm{Ent}_{A_iB}\}_{i=1}^m}$. If, additionally, bipartite entanglement is shared between every pair of Alices, the complexity is denoted by $C^{\|,\{\mathrm{Ent}_{A_iB},\mathrm{Ent}_{A_iA_j}\}_{i,j=1}^m}$ for error-free protocols.
- *Classical communication assisted by genuine multipartite entanglement:* All parties share a genuine multipartite entangled state. The corresponding complexity is denoted $C^{\|,\mathrm{GEnt}}$ for perfect protocols.

"Error-free" above means that the protocol must produce a correct output with probability 1, for each possible input. We will also consider communication protocol that are allowed some error probability, at most 1/3 on every possible input, and we will add a subscript 1/3 below the C to indicate that.

Replacing the classical channels from the Alices to Bob by quantum channels gives rise to the corresponding quantum communication complexities $Q^{\|}$, $Q^{\|,\mathrm{GSR}}$, $Q^{\|,\{\mathrm{Ent}_{A_iB}\}_{i=1}^m}$, $Q^{\|,\{\mathrm{Ent}_{A_iB},\mathrm{Ent}_{A_iA_j}\}_{i,j=1}^m}$, and $Q^{\|,\mathrm{GEnt}}$, with a subscript 1/3 for their bounded-error versions.

We begin by presenting efficient classical communication protocol for $m\mathtt{HM}_n$ and $m\mathtt{BHM}_n$ when a multipartite GHZ state is shared among all the parties.

Theorem 1. *For every* $m \geq 1$, $C^{\|,\mathrm{GEnt}}(m\mathtt{HM}_n) \leq \log_2 n$ *and* $C^{\|,\mathrm{GEnt}}_{1/3}(m\mathtt{BHM}_n) \leq \log_2 n$.

Proof The m senders $\{\mathrm{Alice}_r\}_{r=1}^m$ and Bob share the $(m+1)$-partite n-dimensional GHZ state $|\mathcal{G}\rangle_{m+1} = \frac{1}{\sqrt{n}}\sum_{k=1}^n(\bigotimes_{r=1}^m|k\rangle_{A_r})|k\rangle_B$, where each party holds $\log_2 n$ qubits. Upon receiving $\mathbf{x}^r = x_1^r \ldots x_n^r$, Alice_r applies the unitary $U_{\mathbf{x}}^{(r)} = \sum_{k=1}^n(-1)^{x_k^r}|k\rangle\langle k|$ on her share of the GHZ state, thereby transforming the shared state into $|\mathcal{G}(\mathbf{x}^1,\ldots,\mathbf{x}^m)\rangle_{m+1} = \frac{1}{\sqrt{n}}\sum_{k=1}^n(-1)^{p_k}(\bigotimes_{r=1}^m|k\rangle_{A_r})|k\rangle_B$, where $p_k = \bigoplus_{r=1}^m x_k^r$. Each Alice then measures her subsystem in the Fourier basis $\mathbb{FB} \equiv \{|f_a\rangle := \frac{1}{\sqrt{n}}\sum_{k=1}^n\omega^{ka}|k\rangle\}_{a=1}^n$, $\omega := e^{2\pi i/n}$; and communicates the $\log_2 n$-bit outcome (o_r for the rth Alice) to Bob. Conditioned on the outcome tuple $\vec{o} = (o_1,\ldots,o_m)$, Bob's marginal state is

$$|\psi(\vec{o})\rangle_B = \frac{1}{\sqrt{n}}\sum_{k=1}^n(-1)^{p_k}\omega^{-k\eta}|k\rangle_B,\ \eta := \sum_{r=1}^m o_r. \tag{2}$$

Applying the unitary $U_B := \sum_{k=1}^n\omega^{k\eta}|k\rangle\langle k|$, Bob's state becomes

$$|\psi\rangle_B = \frac{1}{\sqrt{n}}\sum_{k=1}^n(-1)^{p_k}|k\rangle_B, \tag{3}$$

which is exactly the Hidden Matching encoding of the parity string $\mathbf{p} = (p_1,\ldots,p_n)$ [see Eq. (1)]. Bob then follows the same measurement procedure as in the bipartite protocol, obtaining $p_{i_\ell} \oplus p_{j_\ell} = \bigoplus_{r=1}^m(x_{i_\ell}^r \oplus x_{j_\ell}^r)$.

For the Boolean version $m\mathtt{BHM}_n$, Bob completes the 1/4-matching M to a perfect matching (adding $n/4$ edges in some arbitrary way), and measures the state (3) as before. With probability 1/2 the obtained edge (i_ℓ, j_ℓ) is in M. Bob computes $z_\ell = \bigoplus_{r=1}^m\big(x_{i_\ell}^r \oplus x_{j_\ell}^r\big)$ from the measurement outcome and compares it with w_ℓ. By the promise, $z_\ell = w_\ell$ iff $b = 0$, and $z_\ell \neq w_\ell$ iff $b = 1$. Hence, if indeed $(i_\ell, j_\ell) \in$ M, then Bob recovers b with certainty. If the obtained (i_ℓ, j_ℓ) was not in M then Bob outputs a random coin flip. His overall error probability is now $1/4 < 1/3$. □

Remark: A notable distinction between the bipartite and multipartite settings concerns information leakage. In the bipartite task, let's say with uniform input distribution, any successful protocol necessarily reveals partial information about Alice's input to Bob, namely the parity of the two input bits associated with the reported edge of the matching. By contrast, in multipartite protocol of Theorem 1, Bob learns only the global parity $\bigoplus_{r=1}^m\big(x_{i_\ell}^r \oplus x_{j_\ell}^r\big)$, while gaining no information about the input string of any individual sender, or even about the joint input strings of any $m-1$ of the senders. Thus, the protocol achieves perfect success while remaining completely oblivious to each sender's local input.

We now turn to communication lower bounds in the absence of preshared entanglement. By fixing the inputs for $m-1$ senders to the all-0 string 0^n, we immediately get a lower bound for the m-partite task from the bipartite task:

Lemma 1. *For every* $m \geq 1$, $C^{\|,\mathrm{GSR}}(m\mathtt{HM}_n) \geq C^{\|,\mathrm{GSR}}(\mathtt{HM}_n)$ *and* $C^{\|,\mathrm{GSR}}(m\mathtt{BHM}_n) \geq C^{\|,\mathrm{SR}}(\mathtt{BHM}_n)$*, and similarly for the bounded-error versions.*

Using the known lower bounds for the bipartite (i.e., $m = 1$) hidden matching problems [34, 43], Lemma 1 implies $C^{\|,\mathrm{GSR}}_{1/3}(m\mathtt{HM}_n) \geq \Omega(\sqrt{n})$ and $C^{\|,\mathrm{GSR}}_{1/3}(m\mathtt{BHM}_n) \geq \Omega(\sqrt{n})$ [35] for bounded-error protocols. We next strengthen these lower bounds by allowing unrestricted *quantum* communication while still forbidding preshared entanglement, namely in the communication model $Q^{\|,\mathrm{GSR}}$.

Theorem 2. *For all $m \geq 2$ the bounded-error communication complexity $Q^{\|,\mathrm{GSR}}_{1/3}(m\mathtt{BHM}_n) = \Omega(\sqrt{n})$, in fact at least one sender has to send $\Omega(\sqrt{n})$ qubits.*

Due to space constraints, we defer the proof to the **Methods** section. For comparison, the bipartite Hidden Matching problem admits a one-way quantum protocol requiring only $O(\log n)$ qubits of communication from Alice to Bob [34]. In contrast, Theorem 2 shows that if we have two or more unentangled Alices, then at least one of them needs to send $\Omega(\sqrt{n})$ qubits. Combined with Theorem 1, this establishes an exponential separation between entanglement-assisted classical communication and unassisted quantum communication in our multiparty setting.

Shared entanglement (between sender and receiver). Consider the communication model $Q^{\|,\{\mathrm{Ent}_{A_iB}\}_{i=1}^m}$, where each Alice shares r EPR pairs with Bob. Let the shared state be $\Phi_{AB}^{\otimes r}$. Upon receiving input $\mathbf{x}$, Alice can apply a CPTP map $\mathcal{G}_{\mathbf{x}} : A \to \mathcal{R} \otimes A'$ where $\mathcal{R}$ is a q-qubit message register and A' is an auxiliary system retained by Alice. The global state becomes $\rho^{(\mathbf{x})}_{\mathcal{R}A'B} = (\mathcal{G}_{\mathbf{x}} \otimes I_B)(\Phi_{AB}^{\otimes r})$. Alice then sends the register $\mathcal{R}$ to Bob. Consequently, Bob receives the system $\mathcal{R}B$ in state $\rho^{(\mathbf{x})}_{\mathcal{R}B} = \mathrm{Tr}_{A'}\left[\rho^{(x)}_{\mathcal{R}A'B}\right]$, which acts on a $(q+r)$-qubit Hilbert space. Notably this protocol can be simulated without any prior entanglement. Indeed, Alice can locally prepare the mixed state $\rho^{(\mathbf{x})}_{\mathcal{R}B}$ and transmit the entire $(q+r)$-qubit system to Bob, who thereby receives exactly the same state as in the original protocol. Hence any protocol using q qubits of communication and r shared EPR pairs induces a protocol without preshared entanglement using $q + r$ qubits of communication. Applying Theorem 2, we obtain $q + r = \Omega(\sqrt{n})$. If the amount of prior entanglement is limited, i.e., $r \leq c\sqrt{n}$ for sufficiently small constant c, then the bound implies $q = \Omega(\sqrt{n})$. However, if the shared entanglement is large ($r \gg \sqrt{n}$), then the condition $q + r \geq \Omega(\sqrt{n})$ does not impose a meaningful constraint on q, since the bound may already be satisfied by r alone.

Shared entanglement (among senders). The above lower-bound argument does not extend to the communication model $Q^{\|,\mathrm{Ent}_{A_1\ldots A_m}}$, in which the senders share preshared entanglement. In this setting, the quantum messages received by Bob are no longer tensor-product states, and consequently the simulation argument used above no longer applies. Indeed, suppose the senders $\{\mathrm{Alice}_r\}_{r=1}^m$ initially share the m-partite GHZ state $|\mathcal{G}\rangle_m = \frac{1}{\sqrt{n}} \sum_{k=1}^n \bigotimes_{r=1}^m |k\rangle_{A_r}$, where each party holds $\log_2 n$ qubits (in contrast to the previous, Bob does not share part of this GHZ state). Upon receiving their respective inputs, Alice_r applies the phase encoding $U^{(r)}_{\mathbf{x}}$ to her subsystem and sends

it to Bob using only $O(\log n)$ qubits of communication. Bob then holds the state

$$|\psi\rangle_m = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} (-1)^{p_k} |k\rangle_A, \quad |k\rangle_A := \bigotimes_{r=1}^{m} |k\rangle_{A_r}, \tag{4}$$

which takes a form similar to the state in Eq. (1). Therefore, Bob can do measurement based on his input M and solve the relational Hidden Matching problem.

II. Application to Bounded-Storage Cryptography

The Hidden Matching problem induces a strong seeded randomness extractor, as observed in [35]. Randomness extractors are important tools in theoretical computer science [44] and cryptography [45–47]. Before discussing the explicit construction, we recall two definitions.

Definition 1 (Weak random source)**.** *A random variable* $\mathbf{x}$ *over the set* $\{0,1\}^n$ *is called a* k-min-entropy source*, or simply a* weak random source*, if its min-entropy satisfies* $H_\infty(\mathbf{x}) \geq k$*. Here the* min-entropy *of* $\mathbf{x}$ *is defined as* $H_\infty(\mathbf{x}) = -\log_2 \left(\max_{\mathbf{x}\in\{0,1\}^n} \Pr[\mathbf{x} = \mathbf{x}]\right)$*. Thus, if* $H_\infty(\mathbf{x}) = k$*, then no individual outcome of the random variable occurs with probability greater than* 2^{-k}*.*

Definition 2 (Strong Seeded Randomness Extractor)**.** *Let* $n, \ell, d, k \in \mathbb{N}$ *and let* $\varepsilon > 0$*. A function* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^\ell$ *is called a strong* (k, ε)-seeded randomness extractor *if, for every random variable* $\mathbf{x}$ *over* $\{0,1\}^n$ *satisfying* $H_\infty(\mathbf{x}) \geq k$*, and an independent random variable* $\mathbf{y}$ *that is uniform over a finite set* S *(of possible seeds), the distribution of* $(\mathbf{y}, \mathrm{Ext}(\mathbf{x}, \mathbf{y}))$ *is* ε*-close to the uniform distribution on* $S \times \{0,1\}^\ell$*, equivalently*

$$\mathbb{E}_{\mathbf{y}} \left\| \mathbb{E}_{\mathbf{x}} \left[\mathrm{Ext}(\mathbf{x}, \mathbf{y}) - U_\ell \right] \right\|_{tvd} \leq \varepsilon.$$

Here total variation distance (tvd) between probability distributions P *and* Q *is defined as* $\|P - Q\|_{\mathrm{tvd}} = \frac{1}{2} \sum_{r\in\{0,1\}^\ell} |P(r) - Q(r)|$*.*

We first explain the result of [35]. Let $\mathbf{x} \in \{0,1\}^n$ be a weak random source and let $\mathrm{M} \in \mathcal{M}_{n/4}$ denote a uniformly random 1/4-matching. The Hidden Matching extractor $\mathrm{Ext} : \{0,1\}^n \times \mathcal{M}_{n/4} \to \{0,1\}^{n/4}$ defined as $\mathbb{M}(\mathbf{x})$, where $\mathbb{M}$ is an $n/4 \times n$ matrix over $\mathbb{F}_2$, with one weight-2 row for each edge of the 1/4-matching M. It produces an $n/4$-bit output $\mathbf{z} = \mathrm{Ext}(\mathbf{x}, \mathrm{M})$ that remains statistically close to uniform even when the seed M is public. The security of the resulting extractor against classical memory-bounded adversaries is very similar to the communication lower bound of [35] for Boolean Hidden Matching, relying on the Fourier coefficients inequality of Kahn, Kalai, and Linial (KKL) [48]. If the source has min-entropy $H_\infty(\mathbf{x}) \geq n - \gamma\varepsilon\sqrt{n}$, then $\mathbf{z}$ is ε-close to uniform, implying security against classical bounded-storage adversaries with memory $s = \gamma\varepsilon\sqrt{n}$ [35] (note that we fixed the α of [35] to be 1/4 in this paper). In contrast, a *quantum* adversary storing the $\log(n)$-qubit state $|\psi_{\mathbf{x}}\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle$ can recover one of the Hidden Matching parities (which is one of the bits of $\mathbf{z}$) once the seed M is revealed, as explained after Eq. (1). It should be noted that this extractor Ext is not intended to optimize extraction parameters, as it incurs a significant loss of source

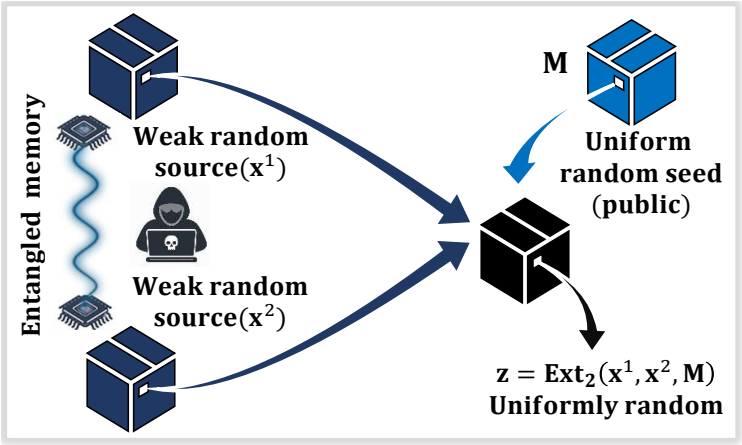


Figure 2 Multipartite Hidden Matching extractor. Two independent weak random sources $\mathbf{x}^1$ and $\mathbf{x}^2$, together with a uniformly random public seed M, are processed by the multipartite Hidden Matching extractor to produce an extracted key $\mathbf{z} = \mathrm{Ext}_2(\mathbf{x}^1, \mathbf{x}^2, \mathrm{M})$, that is statistically close to uniform. Adversaries with unentangled memory require polynomial-size quantum side-information to attack the protocol. In contrast, pre-shared entanglement enables an adversary to compromise the extractor using only $O(\log n)$ qubits of storage per source, establishing an exponential separation between entangled and unentangled quantum memory.

min-entropy and requires a long random seed M (much more efficient quantum-proof extractors are known, e.g. [49, 50]). Rather, its purpose is to establish a fundamental separation: a function that is a strong extractor against classical storage can completely fail in the presence of small quantum storage.

We generalize this one-source construction to multiple independent weak sources by introducing a two-source Hidden Matching extractor: $\mathrm{Ext}_2 : \{0,1\}^n \times \{0,1\}^n \times \mathcal{M}_{n/4} \to \{0,1\}^{n/4}$ that combines the Hidden Matching parities of $\mathbf{x}^1$ and $\mathbf{x}^2$ as $\mathrm{Ext}_2(\mathbf{x}^1, \mathbf{x}^2, \mathrm{M}) = \mathbb{M}(\mathbf{x}^1 \oplus \mathbf{x}^2)$. This maps two independent n-bit sources ($\mathbf{x}^1$ and $\mathbf{x}^2$, each with a lower bound on their min-entropy) and a uniformly random seed (the 1/4-matching M) to an $n/4$-bit string that is intended to be close to uniform, see Fig. 2. Although multi-source randomness extractors have been studied extensively for decades [51–53], comparatively little is known about their security in the presence of entangled quantum side information [54].

In the case of extractors with classical side-information about the source(s), that side-information can be folded into the min-entropy condition. However, to deal with quantum side-information about the source(s) we need the following definition:

Definition 3 (Strong Seeded Two-Source Randomness Extractor with Quantum side-information)**.** *Let $n, \ell, d, k \in \mathbb{N}$ and let $\varepsilon > 0$. A function $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^\ell$ is called a strong (k, ε)*-seeded two-source randomness extractor *against quantum side-information map $(\mathbf{x}^1, \mathbf{x}^2) \mapsto \rho(\mathbf{x}^1, \mathbf{x}^2)$ if, for every pair of independent random variables $\mathbf{x}^1, \mathbf{x}^2$ over $\{0,1\}^n$ satisfying $H_\infty(\mathbf{x}^1) \geq k, H_\infty(\mathbf{x}^2) \geq k$, and an independent random variable $\mathbf{y}$ that is uniform over a finite set S (of possible seeds), the distribution of $(\mathbf{y}, \mathrm{Ext}(\mathbf{x}^1, \mathbf{x}^2, \mathbf{y}))$ is ε-close to the uniform distribution on*

$S \times \{0,1\}^\ell$ *even given* $\rho(\mathbf{x}^1, \mathbf{x}^2)$*, equivalently*

$$\mathbb{E}_{\mathbf{y}} \left\| \mathbb{E}_{\mathbf{x}^1,\mathbf{x}^2} \left[\rho(\mathbf{x}^1,\mathbf{x}^2) \otimes \mathrm{Ext}(\mathbf{x}^1,\mathbf{x}^2,\mathbf{y}) - \rho(\mathbf{x}^1,\mathbf{x}^2) \otimes U_\ell \right] \right\|_{tvd} \leq \varepsilon.$$

Here $\|\cdot\|_{tvd}$ *is the quantum generalization of total variation distance (=sum of singular values divided by 2).*

We show that this multipartite construction reveals a qualitatively new distinction between two unentangled and entangled *quantum* side-information:

Theorem 3. [Entangled vs Unentangled side-information] *Fix* $\varepsilon \in (0, 1/4)$*. The two-source Hidden Matching extractor* Ext_2 *exhibits an exponential separation between unentangled and entangled side-information:*

(1) there exists a positive constant K *such that if the side-information consists of two unentangled states of* $q = K\sqrt{\varepsilon n}$*-qubits each, one depending on* $\mathbf{x}^1$ *and one depending on* $\mathbf{x}^2$*, then* Ext_2 *is a strong* $(n - K\sqrt{\varepsilon n}, \varepsilon)$*-seeded two-source randomness extractor;*

(2) if the side-information may consist of two entangled states of $q = \log n$ *qubits, one depending on* $\mathbf{x}^1$ *and one depending on* $\mathbf{x}^2$*, then* Ext_2 *is not a strong* (n, ε)*-seeded two-source randomness extractor.*

Part (2) is easy: the entangled side-information can be

$$(U_{\mathbf{x}^1} \otimes U_{\mathbf{x}^2}) \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle|i\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i^1 \oplus x_i^2} |i\rangle|i\rangle,$$

and one bit of $\mathrm{Ext}_2(\mathbf{x}^1, \mathbf{x}^2, \mathrm{M})$ can be learned (with probability $1/2$, knowing when we succeed) by doing the usual M-dependent measurement. This one bit gives

$$\mathbb{E}_{\mathbf{y}} \left\| \mathbb{E}_{\mathbf{x}^1,\mathbf{x}^2} \left[\rho(\mathbf{x}^1,\mathbf{x}^2) \otimes \mathrm{Ext}(\mathbf{x}^1,\mathbf{x}^2,\mathbf{y}) - \rho(\mathbf{x}^1,\mathbf{x}^2) \otimes U_\ell \right] \right\|_{tvd} \geq 1/4.$$

Our analysis for unentangled quantum adversaries to establish part (1) is substantially more delicate than the security analysis against classical adversaries in [35], because the adversary now possesses quantum side-information about two independent weak sources rather than classical side-information. It relies on the hypercontractive inequality for matrix-valued functions developed by Ben-Aroya, Regev, and de Wolf [55], which generalizes the KKL inequality to the quantum setting. A complete proof is provided in **Methods**. The multipartite Hidden Matching extractor therefore establishes an exponential separation between entangled and unentangled quantum side-information, identifying entanglement as an important resource in multi-source bounded-storage cryptography. As in the one-source Hidden Matching extractor of [35], our two-source construction is intended as a proof-of-principle rather than an optimized extractor. Its primary significance is to demonstrate that security against unentangled quantum side-information does not necessarily extend to adversaries possessing even a modest amount of preshared entanglement.

Discussion

While the communication advantages of bipartite quantum resources have been extensively investigated, comparatively little has been known about the computational power of multipartite entanglement. We show that classical communication assisted multipartite entanglement can outperform unassisted quantum communication exponentially in a distributed computational task, establishing that preshared GHZ entanglement is not merely a substitute for quantum communication but can be a strictly stronger information-processing resource.

Beyond communication complexity, our work reveals a novel connection between multipartite communication protocols and bounded-storage cryptography. By extending the Hidden Matching extractor to multiple independent weak random sources, we establish an exponential separation between entangled and unentangled quantum side-information. Specifically, compromising the extractor requires polynomial-size unentangled quantum memory, whereas preshared entanglement reduces the required quantum memory exponentially.

More broadly, our work suggests that multipartite entanglement should be regarded as a computational resource whose power extends beyond the generation of nonlocal correlations. An important open question is to characterize the class of distributed computational tasks that admit exponential entanglement-assisted communication advantages and to determine which families of multipartite entangled states realize such advantages. Another natural direction is to investigate whether similar separations persist in interactive communication models, noisy communication settings, or networked quantum architectures. In particular, for $m \geq 3$, can we strengthen our polynomial lower bound on the required quantum communication when the Alices share pairwise entanglement, such as EPR pairs? (for $m = 2$, pairwise entanglement between the two Alices is just a GHZ state, which allows an efficient protocol)

Our cryptographic results likewise open several directions for future research. The multipartite Hidden Matching extractor presented here is intended as a proof-of-principle construction rather than an optimized extractor, raising the question of whether similar entanglement-induced separations can be achieved with randomness extractors possessing near-optimal parameters. More generally, it will be interesting to investigate similar qualitative distinction between entangled and unentangled quantum side-information for other cryptographic primitives, including privacy amplification, secret-key agreement, and secure multi-party computation. We expect that these connections between multipartite entanglement, communication complexity, and quantum cryptography will stimulate further developments in distributed quantum information processing and secure quantum networks.

Methods

Proof of Theorem 2 & Theorem 3

We begin by proving a more general theorem and then will argue that Theorems 2 and 3 follow as special cases. Consider the function $Z : \{0,1\}^n \times \{0,1\}^n \times \mathcal{M}_{n/4} \to \{0,1\}^{n/4}$ defined by $Z(\mathbf{x}^1, \mathbf{x}^2, \mathrm{M}) = \mathbb{M}(\mathbf{x}^1 \oplus \mathbf{x}^2)$, where $\mathbb{M}$ is an $n/4 \times n$ matrix over $\mathbb{F}_2$, with one weight-2 row for each edge of the 1/4-matching M. This maps two n-bit sources ($\mathbf{x}^1$ and $\mathbf{x}^2$) and a seed (the 1/4-matching M) to an $n/4$-bit string that is intended to be close to uniformly random. We sometimes write $Z_{\mathrm{M}}(\mathbf{x}^1, \mathbf{x^2})$ if M is fixed while $\mathbf{x}^1, \mathbf{x}^2$ are random. The analysis below roughly follows the proof of [35], with the hypercontractive inequality for matrix-valued functions of [55] replacing the standard hypercontractive inequality in order to deal with quantum storage instead of classical, but getting all the details to fit together is quite nontrivial.

Theorem 4. *Let $0 \leq c \leq q \leq n$ be integers. Let $A, B \subseteq \{0,1\}^n$ each have size $\geq 2^{n-c}$. Let $f_1(\mathbf{x}^1)$ assign a q-qubit density matrix for each $\mathbf{x}^1 \in A$, and similarly let $f_2(\mathbf{x}^2)$ assign a q-qubit density matrix for each $\mathbf{x}^2 \in B$. Let $\mathbf{x}^1, \mathbf{x}^2$ be uniformly distributed over A, B respectively, and* M *be uniform over the set of all* 1/4*-matchings. Let*

$$\rho_{\mathrm{M}} = \mathbb{E}_{\mathbf{x}^1 \in A, \mathbf{x}^2 \in B} \left[f_1(\mathbf{x}^1) \otimes f_2(\mathbf{x}^2) \otimes |Z_{\mathrm{M}}(\mathbf{x}^1, \mathbf{x}^2)\rangle\langle Z_{\mathrm{M}}(\mathbf{x}^1, \mathbf{x}^2)| \right]$$

be the state of a party who has the quantum states $f_1(\mathbf{x}^1), f_2(\mathbf{x}^2)$ and the matching M *(but not $\mathbf{x}^1, \mathbf{x}^2$), alongside the value of the function Z_{M} (unknown to that party). Let $\Delta_{\mathrm{M}} = \mathbb{E}_{\mathbf{x}^1 \in A, \mathbf{x}^2 \in B} \left[f_1(\mathbf{x}^1) \otimes f_2(\mathbf{x}^2) \otimes \left(|Z_{\mathrm{M}}(\mathbf{x}^1, \mathbf{x}^2)\rangle\langle Z_{\mathrm{M}}(\mathbf{x}^1, \mathbf{x}^2)| - \frac{I}{2^{n/4}} \right) \right]$ be the difference between ρ_{M}, and the state where the last register is maximally mixed (i.e., uniform over $\{0,1\}^{n/4}$). Then*

$$\mathbb{E}_{\mathrm{M}}[\|\Delta_{\mathrm{M}}\|_{tvd}] \leq O(q^2/n).$$

Note that this theorem is false if M is a *perfect* matching even if $c = 0$ and $q = 1$: $f_1(\mathbf{x}^1)$ and $f_2(\mathbf{x}^2)$ could just be the parity of their respective inputs. The parity of those two bits equals the parity of the $n/2$ bits of $Z_{\mathrm{M}}(\mathbf{x}^1, \mathbf{x}^2)$ in the case where M is a perfect matching, so you would already break the uniformity property.

Proof We may assume without loss of generality that q is positive and even, and at most $\sqrt{n}$ (the conclusion is trivially true if $q > \sqrt{n}$). Define the functions f_1, f_2 to be 0 outside of A, B respectively. Fix a 1/4-matching M. For a function $f : \{0,1\}^n \to \mathcal{M}_d$, where $\mathcal{M}_d$ is the set of d-dimensional complex matrices, define its Fourier transform $\widehat{f} : \{0,1\}^n \to \mathcal{M}_d$ as

$$\widehat{f}(\mathbf{s}) = \frac{1}{2^n} \sum_{\mathbf{x} \in \{0,1\}^n} f(\mathbf{x})(-1)^{\mathbf{x} \cdot s}.$$

Note that the Fourier coefficient $\widehat{f}(\mathbf{s})$ is a d-dimensional matrix here, not a number as is more common in Fourier analysis. We have the Fourier decomposition $f(\mathbf{x}) = \sum_{\mathbf{s}} \widehat{f}(\mathbf{s})(-1)^{\mathbf{x} \cdot \mathbf{s}}$ for all $\mathbf{x} \in \{0,1\}^n$.

We will also use a slightly different decomposition for diagonal matrices to analyze the output of the function Z_{M}. Define $V : \{0,1\}^{n/4} \to \mathcal{M}_{2^{n/4}}$ as

$$V(\mathbf{u}) = \frac{1}{2^{n/4}} \sum_{\mathbf{w}\in\{0,1\}^{n/4}} (-1)^{\mathbf{u}\cdot\mathbf{w}} |\mathbf{w}\rangle\langle\mathbf{w}|.$$

Note that $V(0^{n/4})$ is the maximally mixed $n/4$-qubit state $I/2^{n/4}$, and for every $\mathbf{z} \in \{0,1\}^{n/4}$ we have the decomposition

$$|\mathbf{z}\rangle\langle\mathbf{z}| = \sum_{\mathbf{u}} V(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{z}}.$$

We now use the decompositions of the functions f_1, f_2, and $|Z_{\mathrm{M}}(\mathbf{x}^1,\mathbf{x}^2)\rangle\langle Z_{\mathrm{M}}(\mathbf{x}^1,\mathbf{x}^2)|$ to analyze ρ_{M}:

$$\begin{aligned}
\rho_{\mathrm{M}} &= \mathbb{E}_{\mathbf{x}^1\in A,\mathbf{x}^2\in B}\left[f_1(\mathbf{x}^1)\otimes f_2(\mathbf{x}^2)\otimes |Z_{\mathrm{M}}(\mathbf{x}^1,\mathbf{x}^2)\rangle\langle Z_{\mathrm{M}}(\mathbf{x}^1,\mathbf{x}^2)|\right] \\
&= \frac{2^{2n}}{|A|\cdot|B|}\mathbb{E}_{\mathbf{x}^1\in\{0,1\}^n,\mathbf{x}^2\in\{0,1\}^n}\left[f_1(\mathbf{x}^1)\otimes f_2(\mathbf{x}^2)\otimes |Z_{\mathrm{M}}(\mathbf{x}^1,\mathbf{x}^2)\rangle\langle Z_{\mathrm{M}}(\mathbf{x}^1,\mathbf{x}^2)|\right] \\
&= \frac{2^{2n}}{|A|\cdot|B|}\mathbb{E}_{\mathbf{x}^1\in\{0,1\}^n,\mathbf{x}^2\in\{0,1\}^n}\left[\sum_{\mathbf{s}\in\{0,1\}^n}\widehat{f_1}(\mathbf{s})(-1)^{\mathbf{s}\cdot\mathbf{x}^1}\otimes\sum_{\mathbf{t}\in\{0,1\}^n}\widehat{f_2}(\mathbf{t})(-1)^{\mathbf{t}\cdot\mathbf{x}^2}\right. \\
&\qquad\left.\otimes\sum_{\mathbf{u}\in\{0,1\}^{n/4}}V(\mathbf{u})(-1)^{u\cdot\mathbb{M}(\mathbf{x}^1\oplus\mathbf{x}^2)}\right] \\
&= \frac{2^{2n}}{|A|\cdot|B|}\sum_{\mathbf{s},\mathbf{t},\mathbf{u}}\widehat{f_1}(\mathbf{s})\otimes\widehat{f_2}(\mathbf{t})\otimes V(\mathbf{u})\cdot\mathbb{E}_{\mathbf{x^1}\in\{\mathbf{0},\mathbf{1}\}^{\mathbf{n}}}\left[(-\mathbf{1})^{\mathbf{x^1}\cdot(\mathbb{M}^{\mathbf{T}}\mathbf{u}\oplus\mathbf{s})}\right] \\
&\qquad\cdot\mathbb{E}_{x^2\in\{0,1\}^n}\left[(-1)^{x^2\cdot(\mathbb{M}^T u\oplus t)}\right] \\
&= \frac{2^{2n}}{|A|\cdot|B|}\sum_{\mathbf{u}\in\{0,1\}^{n/4}}\widehat{f_1}(\mathbb{M}^T\mathbf{u})\otimes\widehat{f_2}(\mathbb{M}^T\mathbf{u})\otimes V(\mathbf{u}),
\end{aligned}$$

where the last equality is because the $\mathbb{E}_{\mathbf{x}^1}$ acts like a delta-function on $\mathbb{M}^T\mathbf{u}$ and $\mathbf{s}$, and the $\mathbb{E}_{\mathbf{x}^2}$ acts like a delta-function on $\mathbb{M}^T\mathbf{u}$ and $\mathbf{t}$.

The difference Δ_{M} between the above ρ_{M} and the state where the last register is the maximally mixed state is

$$\Delta_{\mathrm{M}} = \frac{2^{2n}}{|A|\cdot|B|}\sum_{\mathbf{u}\in\{0,1\}^{n/4}\setminus\{0^{n/4}\}}\widehat{f_1}(\mathbb{M}^T\mathbf{u})\otimes\widehat{f_2}(\mathbb{M}^T\mathbf{u})\otimes V(\mathbf{u}),$$

because $V(0^{n/4})$ equals the maximally mixed state $I/2^{n/4}$ so $\mathbf{u} = 0^{n/4}$ drops out of the sum.

For $p \geq 1$ define the normalized Schatten p-norm of a d-dimensional matrix W as $\|W\|_p = (\frac{1}{d}\operatorname{Tr}(|W|^p))^{1/p}$. One can show that these norms are monotone nondecreasing in p. Note that if W is an n-qubit density matrix, then $\|W\|_p^p \leq 2^{-n}$ for every p.

Using triangle inequality and the fact that $\|V(\mathbf{u})\|_1 = 2^{-n/4}$ for all $\mathbf{u} \in \{0,1\}^{n/4}$, we bound

$$\left\|\sum_{\mathbf{u}\in\{0,1\}^{n/4}\setminus\{0^{n/4}\}}\widehat{f_1}(\mathbb{M}^T\mathbf{u})\otimes\widehat{f_2}(\mathbb{M}^T\mathbf{u})\otimes V(\mathbf{u})\right\|_1$$

$$\leq 2^{-n/4} \sum_{k=1}^{n} \sum_{\mathbf{u}\in\{0,1\}^{n/4}:|\mathbb{M}^T\mathbf{u}|=k} \left\|\widehat{f_1}(\mathbb{M}^T u)\right\|_1 \cdot \left\|\widehat{f_2}(\mathbb{M}^T u)\right\|_1 .$$

This analysis of Δ_{M} so far is for a fixed 1/4-matching M. We now want to show that its norm is small when averaged uniformly over all 1/4-matchings M. We have the following probabilistic lemma from [35, Lemma 3.3] for all $\mathbf{v}$ of even Hamming weight:

$$\Pr_{\mathrm{M}}\left[\exists \mathbf{u} \in \{0,1\}^{n/4} \text{ s.t. } \mathbb{M}^T\mathbf{u} = \mathbf{v}\right] = \frac{\binom{n/4}{k/2}}{\binom{n}{k}} \leq (ek/2n)^{k/2},$$

where M is uniform over the set of all 1/4-matchings, and the last inequality uses the well-known bounds $\binom{n/4}{k/2} \leq (e(n/4)/(k/2))^{k/2} = (en/2k)^{k/2}$ and $\binom{n}{k} \geq (n/k)^k$. There is at most one $\mathbf{u}$ such that $\mathbb{M}^T\mathbf{u} = \mathbf{v}$. For $\mathbf{v}$ of odd Hamming weight, the probability is 0 because $\mathbb{M}^T\mathbf{u}$ always has twice the Hamming weight of $\mathbf{u}$, so its weight cannot be odd. This allows us to bound the expectation over uniform M:

$$\mathbb{E}_{\mathrm{M}}[\|\Delta_{\mathrm{M}}\|_1] \leq \frac{2^{2n}}{|A|\cdot|B|} 2^{-n/4} \sum_{k=1}^{2n/4} \sum_{\mathbf{v}\in\{0,1\}^n:|\mathbf{v}|=k} \Pr_{\mathrm{M}}\left[\exists \mathbf{u} \in \{0,1\}^{n/4} \text{ s.t. } \mathbb{M}^T\mathbf{u} = \mathbf{v}\right] \cdot \left\|\widehat{f_1}(\mathbf{v})\right\|_1 \cdot \left\|\widehat{f_2}(\mathbf{v})\right\|_1 , \tag{5}$$

We have the following "hypercontractive" inequality from [55, Theorem 1] to upper bound the Fourier coefficients of a function $f : \{0,1\}^n \to \mathcal{M}_d$: for every $p \in [1,2]$,

$$\sum_{\mathbf{v}\in\{0,1\}^n} (p-1)^{|\mathbf{v}|} \left\|\widehat{f}(\mathbf{v})\right\|_p^2 \leq \left(\frac{1}{2^n} \sum_{\mathbf{x}\in\{0,1\}^n} \|f(\mathbf{x})\|_p^p\right)^{2/p} \tag{6}$$

We will split the sum-over-k of Eq. (5) into the small and large k, upper bounding both parts separately.

The case of small k: $k \leq q$. We want to use Eq. (6) to bound the norms of the degree-k Fourier coefficients of the function f_1. Let $p = 1+\delta$ for $\delta \in [0,1]$ to be chosen later. Lower bound the left-hand side of (6) by restricting the sum to only the v's of weight k, and use $\left\|\widehat{f_1}(\mathbf{v})\right\|_1 \leq \left\|\widehat{f_1}(\mathbf{v})\right\|_p$. Upper bound the right-hand side using that $\|f_1(\mathbf{x})\|_p^p \leq 2^{-q}$ for all $\mathbf{x} \in A$ because $f_1(\mathbf{x})$ is a q-qubit density matrix, and $f_1(\mathbf{x}) = 0$ for $\mathbf{x} \notin A$. This gives the following bound on the degree-k coefficients of f_1:

$$\sum_{\mathbf{v}\in\{0,1\}^n:|\mathbf{v}|=k} \left\|\widehat{f_1}(\mathbf{v})\right\|_1^2 \leq \delta^{-k} \left(\frac{|A|}{2^{n+q}}\right)^{2/(1+\delta)}$$

Choosing $\delta = k/q$ (which is ≤ 1 because we assumed $k \leq q$ for this case), and using $2^n/|A| \leq 2^c$ and $c \leq q$ gives

$$\begin{aligned}
\frac{2^{2n}}{|A|^2} \sum_{\mathbf{v}\in\{0,1\}^n:|\mathbf{v}|=k} \left\|\widehat{f_1}(\mathbf{v})\right\|_1^2 &\leq \delta^{-k} 2^{-2q/(1+\delta)} \left(\frac{2^n}{|A|}\right)^{2\delta/(1+\delta)} \\
&\leq 2^{-2q/(1+\delta)} (4q/k)^k \\
&\leq 2^{-2q} 2^{2\delta q} (4q/k)^k \\
&= 2^{-2q} (16q/k)^k.
\end{aligned}$$

We have the analogous bound for the degree-k Fourier coefficients of f_2, with B instead of A.

Using Cauchy-Schwarz with these Fourier bounds for f_1 and f_2, we bound the part of the sum of (5) where $k \leq q$ by

$$\begin{aligned}
&\frac{2^{2n}}{|A|\cdot|B|}2^{-n/4}\sum_{k=1}^{q}\frac{\binom{n/4}{k/2}}{\binom{n}{k}}\sqrt{\sum_{\mathbf{v}\in\{0,1\}^n:|\mathbf{v}|=k}\left\|\widehat{f_1}(\mathbf{v})\right\|_1^2}\sqrt{\sum_{\mathbf{v}\in\{0,1\}^n:|\mathbf{v}|=k}\left\|\widehat{f_2}(\mathbf{v})\right\|_1^2}\\
&=2^{-n/4}\sum_{k=1}^{q}\frac{\binom{n/4}{k/2}}{\binom{n}{k}}\sqrt{\frac{2^{2n}}{|A|^2}\sum_{\mathbf{v}\in\{0,1\}^n:|\mathbf{v}|=k}\left\|\widehat{f_1}(\mathbf{v})\right\|_1^2}\sqrt{\frac{2^{2n}}{|B|^2}\sum_{\mathbf{v}\in\{0,1\}^n:|\mathbf{v}|=k}\left\|\widehat{f_2}(\mathbf{v})\right\|_1^2}\\
&\leq 2^{-2q-n/4}\sum_{\text{even }k=2}^{q}\frac{\binom{n/4}{k/2}}{\binom{n}{k}}(16q/k)^k\\
&\leq 2^{-2q-n/4}\sum_{\text{even }k=2}^{q}(ek/2n)^{k/2}(16q/k)^k\\
&\leq 2^{-2q-n/4}\sum_{\text{even }k=2}^{q}O(q/\sqrt{kn})^k\\
&\leq 2^{-2q-n/4}\,O(q^2/n),
\end{aligned}$$

where the last inequality is because the sum in the penultimate line is upper bounded by a geometric sum (by dropping the $\sqrt{k}$ from the denominator and assuming n is sufficiently large), which is dominated by the term with $k=2$.

The case of large k: $k > q$. Norm-monotonicity and Eq. (6) with $p=2$ implies

$$\sum_{v\in\{0,1\}^n}\left\|\widehat{f_1}(\mathbf{v})\right\|_1^2\leq\sum_{\mathbf{v}\in\{0,1\}^n}\left\|\widehat{f_1}(\mathbf{v})\right\|_2^2\leq\frac{1}{2^n}\sum_{\mathbf{x}\in\{0,1\}^n}\|f_1(x)\|_2^2\leq\frac{|A|}{2^{q+n}},$$

where the last inequality again uses that $\|f_1(\mathbf{x})\|_p^p \leq 2^{-q}$ for all $\mathbf{x}\in A$ because $f_1(\mathbf{x})$ is a q-qubit density matrix, and $f_1(\mathbf{x})=0$ for $\mathbf{x}\notin A$. We have a similar inequality for f_2.

Define $g(k)=\binom{n/4}{k/2}/\binom{n}{k}$. [35] show that g is monotone nonincreasing for $k\in\{q,\ldots,n/2\}$. Together with Cauchy-Schwarz, this allows us to upper bound the part of the sum of (5) with $k>q$ by

$$\begin{aligned}
&\leq\frac{2^{2n}}{|A|\cdot|B|}2^{-n/4}g(q)\sqrt{\sum_{\mathbf{v}\in\{0,1\}^n}\left\|\widehat{f_1}(\mathbf{v})\right\|_1^2}\sqrt{\sum_{\mathbf{v}\in\{0,1\}^n}\left\|\widehat{f_2}(\mathbf{v})\right\|_1^2}\\
&\leq\frac{2^n}{\sqrt{|A|\cdot|B|}}2^{-q-n/4}g(q)\\
&\leq\frac{2^n}{\sqrt{|A|\cdot|B|}}2^{-q-n/4}(eq/2n)^{q/2}\\
&\leq 2^{c-q-n/4}(eq/2n)^{q/2}\\
&\leq 2^{-2q-n/4}\cdot q^2/n,
\end{aligned}$$

where the last inequality uses $c\leq q$ and $eq/2n\leq 2^{-1/4}$ for sufficiently large n (recall that we assumed $q\leq\sqrt{n}$). This concludes the upper bound for the large-k case.

The trace-norm (=sum of singular values, which is twice the total-variation distance) of an m-qubit matrix is 2^m times its Schatten 1-norm, hence combining the upper bounds for

the small and the large k, we have

$$\mathbb{E}_{\mathrm{M}}[\|\Delta_{\mathrm{M}}\|_{tr}] = 2^{2q+n/4}\mathbb{E}_{\mathrm{M}}[\|\Delta_{\mathrm{M}}\|_1] \leq O(q^2/n).$$

This completes the proof. □

The two main lower bound claims in our paper now follow as immediate corollaries:

Proof of Theorem 2: It suffices to prove the theorem for $m = 2$, since for $m \geq 3$ we can fix the inputs for $m-1$ senders to the all-0 string 0^n to reduce to the $m = 2$ case. Assume without loss of generality that the message lengths from the two Alices are equal to the same q.

By choosing $A = B = \{0,1\}^n$ (so $c = 0$), ε a small constant, $q = C\sqrt{n}$ for small constant C, we obtain a lower bound of $q = \Omega(\sqrt{n})$ for the bounded-error quantum communication complexity of the two-Alice version of Boolean Hidden matching, because a protocol that learns b (with success probability $\geq 2/3$) from $f_1(\mathbf{x}^1), f_2(\mathbf{x}^2), \mathrm{M}$ would be able to (with large probability) distinguish $Z_{\mathrm{M}}(\mathbf{x}^1, \mathbf{x}^2)$ from uniformly random, violating Theorem 4. Here the two Alices (and Bob) are allowed to share classical randomness but not entanglement. Shared randomness is not dealt with by Theorem 4 itself, but it is easy to see that shared randomness between the two Alices and/or Bob cannot improve their success probability under a fixed input distribution, since one can always fix the "best" shared random string w.r.t. that input distribution.

Proof of part (1) of Theorem 3: By choosing $c \leq q = C\sqrt{\varepsilon n}$ for sufficiently small constant C, we also obtain the proof that $Z(\mathbf{x}^1, \mathbf{x}^2, \mathrm{M})$ is an ε-secure strong seeded two-source extractor against two unentangled quantum adversaries who store $q = O(\sqrt{\varepsilon n})$ qubits about $\mathbf{x}^1$ and $\mathbf{x}^2$, respectively, assuming $\mathbf{x}^1, \mathbf{x}^2$ have min-entropy at least $n - c = n - O(\sqrt{\varepsilon n})$. Our Theorem 4 only handles the special case where the distributions of $\mathbf{x}^1, \mathbf{x}^2$ are so-called flat sets (uniform over sets A, B of size $\geq 2^{n-c}$, respectively), but Chor and Goldreich [56] showed that every distribution of min-entropy $\geq n - c$ is a convex combination of such flat sets, so our proof extends immediately to the general case.

References

[1] Schrödinger, E.: Discussion of Probability Relations between Separated Systems. Math. Proc. Camb. Philos. Soc. **31**(4), 555–563 (1935) https://doi.org/10.1017/s0305004100013554

[2] Einstein, A., Podolsky, B., Rosen, N.: Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? Phys. Rev. **47**, 777–780 (1935) https://doi.org/10.1103/PhysRev.47.777

[3] Bohr, N.: Can Quantum-Mechanical Description of Physical Reality be Considered Complete? Phys. Rev. **48**, 696–702 (1935) https://doi.org/10.1103/PhysRev.48.696

[4] Schrödinger, E.: Probability relations between separated systems. Math. Proc. Camb. Philos. Soc. **32**(3), 446–452 (1936) https://doi.org/10.1017/s0305004100019137

[5] Bell, J.S.: On the Einstein Podolsky Rosen paradox. Physics Physique Fizika **1**, 195–200 (1964) https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195

[6] Bell, J.S.: On the Problem of Hidden Variables in Quantum Mechanics. Rev. Mod. Phys. **38**, 447–452 (1966) https://doi.org/10.1103/RevModPhys.38.447

[7] Bennett, C.H., Bernstein, E., Brassard, G., Vazirani, U.V.: Strengths and Weaknesses of Quantum Computing. SIAM J. Comput. **26**(5), 1510–1523 (1997) https://doi.org/10.1137/S0097539796300933

[8] Steane, A.: Quantum computing. Rep. Prog. Phys. **61**(2), 117–173 (1998) https://doi.org/10.1088/0034-4885/61/2/002

[9] Bennett, C.H., DiVincenzo, D.P.: Quantum information and computation. Nature **404**(6775), 247–255 (2000) https://doi.org/10.1038/35005001

[10] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**, 145–195 (2002) https://doi.org/10.1103/RevModPhys.74.145

[11] Gisin, N., Thew, R.: Quantum communication. Nature Photonics **1**(3), 165–171 (2007) https://doi.org/10.1038/nphoton.2007.22

[12] Horodecki, R., Horodecki, P., Horodecki, M., Horodecki, K.: Quantum entanglement. Rev. Mod. Phys. **81**, 865–942 (2009) https://doi.org/10.1103/RevModPhys.81.865

[13] Buhrman, H., Cleve, R., Massar, S., de Wolf, R.: Nonlocality and communication complexity. Rev. Mod. Phys. **82**, 665–698 (2010) https://doi.org/10.1103/RevModPhys.82.665

[14] Childs, A.M., Dam, W.: Quantum algorithms for algebraic problems. Rev. Mod. Phys. **82**, 1–52 (2010) https://doi.org/10.1103/RevModPhys.82.1

[15] Huang, H.-Y., Choi, S., McClean, J.R., Preskill, J.: Vast World of Quantum Advantage. Phys. Rev. X **16**, 030501 (2026) https://doi.org/10.1103/tn89-g1xz

[16] Wilde, M.M.: Quantum Information Theory, 2nd edn. Cambridge University Press, Cambridge (2017). https://doi.org/10.1017/9781316809976 . https://doi.org/10.1017/9781316809976

[17] Svetlichny, G.: Distinguishing three-body from two-body nonseparability by a Bell-type inequality. Phys. Rev. D **35**, 3066–3069 (1987) https://doi.org/10.1103/PhysRevD.35.3066

[18] Bouwmeester, D., Pan, J.-W., Daniell, M., Weinfurter, H., Zeilinger, A.: Observation of Three-Photon Greenberger-Horne-Zeilinger Entanglement. Phys. Rev. Lett. **82**, 1345–1349 (1999) https://doi.org/10.1103/PhysRevLett.82.1345

[19] Dür, W., Vidal, G., Cirac, J.I.: Three qubits can be entangled in two inequivalent ways. Phys. Rev. A **62**, 062314 (2000) https://doi.org/10.1103/PhysRevA.62.062314

[20] Riedel, M.F., Böhi, P., Li, Y., Hänsch, T.W., Sinatra, A., Treutlein, P.: Atom-chip-based generation of entanglement for quantum metrology. Nature **464**(7292), 1170–1173 (2010) https://doi.org/10.1038/nature08988

[21] Wang, X.-L., Chen, L., Li, W., Huang, H.-L., Liu, C., Chen, C., Luo, Y.-H., Su, Z.-E., Chen, D., Guo, H., *et al.*: 18-Qubit Entanglement with Six Photons' Three Degrees of Freedom. Physical Review Letters **120**(26), 260502 (2018) https://doi.org/10.1103/PhysRevLett.120.260502

[22] Figgatt, C., Ostrander, A., Linke, N.M., Landsman, K.A., Zhu, D., Maslov, D., Monroe, C.: Parallel entangling operations on a universal ion-trap quantum computer. Nature **572**(7769), 368–372 (2019) https://doi.org/10.1038/s41586-019-1427-5

[23] Omran, A., Levine, H., Keesling, A., Semeghini, G., Wang, T.T., Ebadi, S., Bernien, H., Greiner, M., *et al.*: Generation and Manipulation of Schrödinger Cat States in Rydberg Atom Arrays. Science **365**(6453), 570–574 (2019) https://doi.org/10.1126/science.aax9743

[24] Mooney, G.J., White, G.A.L., Hill, C.D., Hollenberg, L.C.L.: Generation and verification of 27-qubit Greenberger-Horne-Zeilinger states in a superconducting quantum computer. J. Phys. Commun. **5**(9), 095004 (2021) https://doi.org/10.1088/2399-6528/ac1df7

[25] Yao, A.C.-C.: Some Complexity Questions Related to Distributive Computing (Preliminary Report). In: Proceedings of the 11th Annual ACM Symposium on Theory of Computing (STOC), pp. 209–213. ACM Press, Atlanta, GA, USA (1979). https://doi.org/10.1145/800135.804414

[26] Kushilevitz, E., Nisan, N.: Communication Complexity. Cambridge University Press, Cambridge, UK (1997). https://doi.org/10.1017/CBO9780511574948

[27] Yao, A.C.-C.: Quantum Circuit Complexity. In: Proceedings of the 34th Annual Symposium on Foundations of Computer Science (FOCS), pp. 352–360. IEEE Computer Society, Palo Alto, CA, USA (1993). https://doi.org/10.1109/SFCS.1993.366852

[28] Cleve, R., Buhrman, H.: Substituting quantum entanglement for communication. Phys. Rev. A **56**, 1201–1204 (1997) https://doi.org/10.1103/PhysRevA.56.1201

[29] de Wolf, R.: Quantum Communication and Complexity. Theoretical Computer Science **287**(1), 337–353 (2002) https://doi.org/10.1016/S0304-3975(02)00377-8

[30] Brassard, G.: Quantum Communication Complexity. Found. Phys. **33**(11), 1593–1616 (2003) https://doi.org/10.1023/a:1026009100467

[31] Buhrman, H., Cleve, R., Wigderson, A.: Quantum vs. Classical Communication and Computation. In: Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC), pp. 63–68. ACM Press, Dallas, TX, USA (1998). https://doi.org/10.1145/276698.276713

[32] Raz, R.: Exponential Separation of Quantum and Classical Communication Complexity. In: Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC), pp. 358–367. ACM, Atlanta, GA, USA (1999). https://doi.org/10.1145/301250.301343

[33] Buhrman, H., Cleve, R., Watrous, J., de Wolf, R.: Quantum Fingerprinting. Phys. Rev. Lett. **87**, 167902 (2001) https://doi.org/10.1103/PhysRevLett.87.167902

[34] Bar-Yossef, Z., Jayram, T.S., Kerenidis, I.: Exponential Separation of Quantum and Classical One-Way Communication Complexity. In: Proceedings of the 36th Annual ACM Symposium on Theory of Computing (STOC), pp. 128–137. ACM, Chicago, IL, USA (2004). https://doi.org/10.1145/1007352.1007379

[35] Gavinsky, D., Kempe, J., Kerenidis, I., Raz, R., de Wolf, R.: Exponential Separations for One-Way Quantum Communication Complexity, with Applications to Cryptography. In: Proceedings of the 39th Annual ACM Symposium on Theory of Computing (STOC), pp. 516–525. ACM, San Diego, CA, USA (2007). https://doi.org/10.1145/1250790.1250866 . Preprint available at arXiv:quant-ph/0611209

[36] Kumar, N., Kerenidis, I., Diamanti, E.: Experimental demonstration of quantum advantage for one-way communication complexity surpassing best-known classical protocol. Nat. Commun. **10**(1), 4152 (2019) https://doi.org/10.1038/s41467-019-12139-z

[37] Greenberger, D.M., Horne, M.A., Shimony, A., Zeilinger, A.: Bell's theorem without inequalities. Am. J. Phys. **58**(12), 1131–1143 (1990) https://doi.org/10.1119/1.16243

[38] Mermin, N.D.: Quantum mysteries revisited. Am. J. Phys. **58**(8), 731–734 (1990) https://doi.org/10.1119/1.16503

[39] Pan, J.-W., Bouwmeester, D., Daniell, M., Weinfurter, H., Zeilinger, A.: Experimental test of quantum nonlocality in three-photon Greenberger–Horne–Zeilinger entanglement. Nature **403**(6769), 515–519 (2000) https://doi.org/10.1038/35000514

[40] Gavinsky, D., Kempe, J., Regev, O., de Wolf, R.: Bounded-Error Quantum State Identification and Exponential Separations in Communication Complexity. In: Proceedings of the 38th Annual ACM Symposium on Theory of Computing

(STOC), pp. 594–603. ACM, Seattle, WA, USA (2006). https://doi.org/10.1145/1132516.1132602

[41] Damgård, I.B., Fehr, S., Salvail, L., Schaffner, C.: Cryptography In the Bounded Quantum-Storage Model. In: 46th Ann. IEEE Symp. Found. Comput. Sc., pp. 449–458. IEEE, 2005. https://doi.org/10.1109/sfcs.2005.30 . http://dx.doi.org/10.1109/SFCS.2005.30

[42] Babai, L., Kimmel, P.G.: Randomized Simultaneous Messages: Solution of a Problem of Yao in Communication Complexity. In: Proceedings of the 12th Annual IEEE Conference on Computational Complexity (CCC), pp. 239–246. IEEE Computer Society, Ulm, Germany (1997). https://doi.org/10.1109/CCC.1997.612319

[43] Buhrman, H., Regev, O., Scarpa, G., de Wolf, R.: Near-Optimal and Explicit Bell Inequality Violations. Theory Comput. **8**(1), 623–645 (2012) https://doi.org/10.4086/toc.2012.v008a027

[44] Shaltiel, R.: Recent Developments in Explicit Constructions of Extractors. In: Păun, G., Rozenberg, G., Salomaa, A. (eds.) Current Trends in Theoretical Computer Science: The Challenge of the New Century vol. 1, pp. 189–228. World Scientific, Singapore (2004). https://doi.org/10.1142/9789812562494_0013 . Expanded version of the survey published in *Bulletin of the EATCS*, **77**, 67–95 (2002)

[45] Bennett, C.H., Brassard, G., Robert, J.-M.: Privacy Amplification by Public Discussion. SIAM J. Comput. **17**(2), 210–229 (1988) https://doi.org/10.1137/0217014

[46] Impagliazzo, R., Levin, L.A., Luby, M.: Pseudo-Random Generation from One-Way Functions. In: Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC), pp. 12–24. ACM Press, Seattle, WA, USA (1989). https://doi.org/10.1145/73007.73009

[47] König, R., Maurer, U., Renner, R.: On the Power of Quantum Memory. IEEE Tran. Inf. Theory **51**(7), 2391–2401 (2005) https://doi.org/10.1109/tit.2005.850087

[48] Kahn, J., Kalai, G., Linial, N.: The Influence of Variables on Boolean Functions. In: Proceedings of the 29th Annual Symposium on Foundations of Computer Science (FOCS), pp. 68–80. IEEE Computer Society, White Plains, NY, USA (1988). https://doi.org/10.1109/SFCS.1988.21923

[49] De, A., Portmann, C., Vidick, T., Renner, R.: Trevisan's Extractor in the Presence of Quantum Side Information. SIAM J. Comput. **41**(4), 915–940 (2012) https://doi.org/10.1137/100813683

[50] Ben-Aroya, A., Ta-Shma, A.: Better short-seed quantum-proof extractors. Theor.

Comput. Sci. **419**, 17–25 (2012) https://doi.org/10.1016/j.tcs.2011.11.036

[51] Barak, B., Impagliazzo, R., Wigderson, A.: Extracting Randomness Using Few Independent Sources. SIAM J. Comput. **36**(4), 1095–1118 (2006) https://doi.org/10.1137/s0097539705447141

[52] Barak, B., Rao, A., Shaltiel, R., Wigderson, A.: 2-source dispersers for $n^{o(1)}$ entropy, and Ramsey graphs beating the Frankl-Wilson construction. Ann. Math. **176**(3), 1483–1544 (2012) https://doi.org/10.4007/annals.2012.176.3.3

[53] Chattopadhyay, E., Zuckerman, D.: Explicit two-source extractors and resilient functions. Ann. Math. **189**(3), 653–705 (2019) https://doi.org/10.4007/annals.2019.189.3.1

[54] Kasher, R., Kempe, J.: Two-Source Extractors Secure Against Quantum Adversaries. Theory Comput. **8**(1), 461–486 (2012) https://doi.org/10.4086/toc.2012.v008a021

[55] Ben-Aroya, A., Regev, O., de Wolf, R.: A Hypercontractive Inequality for Matrix-Valued Functions with Applications to Quantum Computing and LDCs. In: Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 477–486. IEEE, Philadelphia, PA, USA (2008). https://doi.org/10.1109/FOCS.2008.45

[56] Chor, B., Goldreich, O.: Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity. SIAM J. Comput. **17**(2), 230–261 (1988) https://doi.org/10.1137/0217015

Acknowledgement

MB acknowledges the financial support through the National Quantum Mission (NQM) of the Department of Science and Technology, Government of India. RdW is partially supported by the Dutch Research Council (NWO) through Gravitation-grant Quantum Software Consortium, 024.003.037.

Author contributions

All the authors contributed extensively to develop the idea, proving the results, and preparing the manuscript.

Competing interests

The authors declare no competing interests.

AI statement

All the ideas and writing are human. ChatGPT 5.6 pro was used for a sanity-check on the near-final manuscript, revealing some small errors in the writing that we corrected.