ARTICLE OPEN

Check for updates

Efficient methods for one-shot quantum communication

Anurag Anshu[1]✉ and Rahul Jain[2,3]✉

We address the question of efficient implementation of quantum protocols, with small communication and entanglement, and short depth circuit for encoding or decoding. We introduce two methods for this; the first constructs a resource-efficient convex-split lemma and the second adapts the technique of classical correlated sampling in computer science literature. These lead to the following consequences in one-shot quantum information theory. First concerns the task of quantum decoupling, achieved in many previous works with the aid of a random or pseudo-random unitary. We show that given any choice of basis such as the computational basis, decoupling can be achieved by a unitary that takes basis vectors to basis vectors. Thus, the circuit acts in a 'classical' manner; furthermore our unitary performs addition and multiplication modulo a prime. As the second consequence, we construct near-optimal communication protocol for quantum channel coding that uses exponentially smaller entanglement than the previous near-optimal protocol.

npj Quantum Information (2022)8:97 ; https://doi.org/10.1038/s41534-022-00608-1

INTRODUCTION

It is hard to overstate the power of communication in today's society, which enjoys the benefits of technological advances due to telecommunication and the internet. These advances are a result of *reliable* and *efficient* classical communication protocols, which have been facilitated by decades of studies on data compression, error correction and physics of data transmission. As our technologies enter the quantum age, we have similarly started facing the question of how to make *quantum communication* reliable and efficient. Quantum communication is central to the important tasks of quantum key distribution[1,2], the transfer of quantum states[3] and the design of large scale quantum computers[4,5]. While the proposals and experimental implementations of quantum communication have made great strides in recent years[6,7], the range of communication is still limited to about a few hundred kilometers[7,8] in ground-based experiments. Some of the key challenges are the probabilistic nature (as well as decoherence) in optics-based models[8] and fast decoherence in matter-based models[8]. This strongly motivates the problem of finding quantum protocols that efficiently achieve certain tasks with small communication or fight noise to reliably communicate a given amount of message.

The efficiency of a quantum communication protocol is typically captured by two quantities: the number of qubits communicated and the amount of additional resource, such as quantum entanglement, needed in the protocol. Since the foundational works of Holevo, Schumacher and Westmoreland[9–11], great progress has been made in the understanding of optimal amount of communication and additional resources needed in a large family of quantum communication tasks. Well known results on quantum channel coding[10–16], quantum source coding[9], quantum state merging[17,18] and quantum state redistribution[19,20] have discovered a powerful collection of tools for quantum information processing. These tools have found applications in disciplines beyond quantum communication, such as quantum thermodynamics[21,22] and black hole physics[23,24]. One such tool that takes a central stage in our work is that of quantum decoupling.

Notably, aforementioned works in quantum information theory are set in the asymptotic and i.i.d. (independent and identically distributed) framework of Shannon[25], which allows the protocol to run over many independent instances of the input system. In practice, however, one typically does not have an access to such independent instances, limiting the scope of these results. The field of one-shot information theory addresses this problem, by constructing protocols that run on one instance of the input system. This leads to a generalization of the asymptotic and i.i.d. theory and brings information processing tasks to a more practical domain.

However, unlike the asymptotic and i.i.d. theory of quantum information, the understanding of optimal communication and additional resources is still lacking in one-shot quantum information theory. Even for the very basic task of entanglement-assisted quantum channel coding[14], state-of-the-art[26–28] one-shot protocols fail to simultaneously achieve optimal communication capacity and optimal amount of initial entanglement. The aim of this work is to introduce methods that make progress in this problem and exponentially improve upon the amount of initial entanglement needed in a family of one-shot protocols that achieve the best known communication for above tasks. In many cases, the resulting protocols have the additional property that either the encoding or the decoding operation is a quantum circuit of small depth.

In order to lay the groundwork for our results, we revisit the existing techniques of decoupling and more recent convex-split and position-based decoding. Decoupling (Fig. 1) refers to the process of applying some quantum operation on one of the two given systems (which share quantum correlation), so as to make the two systems independent of each other. More precisely, given a quantum state Ψ_{RC}, one adds registers T, T' in the quantum state $\sigma_{TT'}$, and applies a quantum operation U on registers CTT' such that

$$\mathrm{Tr}_{T'}(U^{\dagger}(\Psi_{RC}\otimes\sigma_{TT'})U)\approx\Psi_R\otimes\omega_C\otimes\sigma'_T.$$

That is, the registers R and C are approximately independent after register T' has been discarded. This idea has been applied in the

[1]School of Engineering and Applied Sciences, Harvard University, Cambridge, MA, USA. [2]Centre for Quantum Technologies and Department of Computer Science, National University of Singapore, Singapore, Singapore. [3]MajuLab, UMI 3654, Singapore, Singapore. ✉email: anuraganshu@fas.harvard.edu; rahul@comp.nus.edu.sg

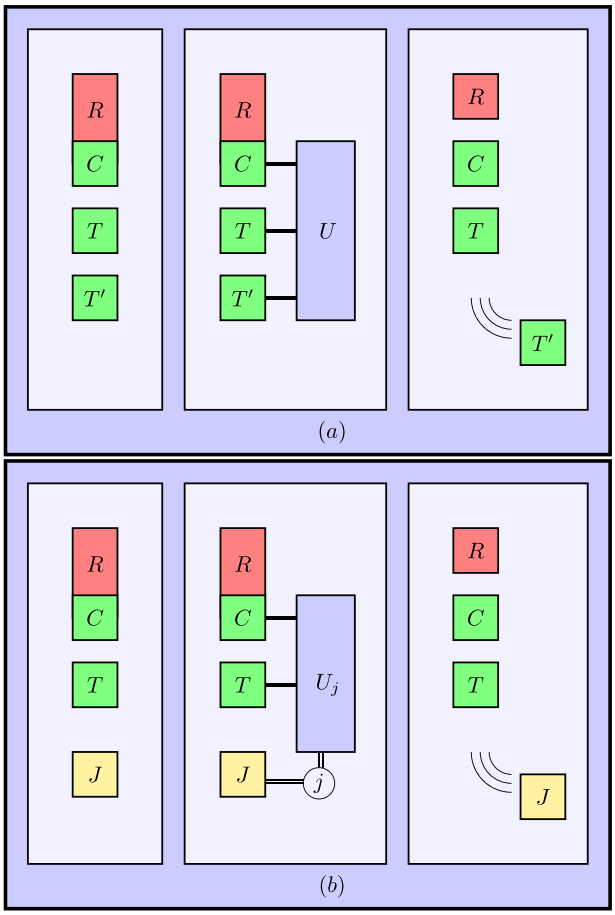

Fig. 1 Decoupling method. Process of removing the quantum correlation between two registers R and C, by means of quantum operations. The cost of performing a decoupling operation is characterized by the size of the register that must be discarded, in order to implement the operation. In Fig. **a**, the discarded register is T' and the operation performed on CTT' is a global unitary U. In Fig. **b**, the register J (that is eventually discarded) is maximally mixed to begin with and the operation performed is a controlled unitary. Thus, J can be viewed as a classical noise[61]. While the operation in Fig. **b** is a special kind of operation in Fig. **a**, the following equivalence holds due to the duality between teleportation[62] and superdense coding[63]. For every operation in Fig. **a** with $\log|T'|$ qubits that are discarded, there is an operation in Fig. **b** with $2\log|T'|$ bits of noise. Moreover, for every operation in Fig. **b** with $\log|J|$ bits of noise, there is an operation in Fig. **a** where $\frac{1}{2}\log|J|$ qubits that are discarded.

aforementioned tasks of quantum state merging[17,18,29–32], quantum state redistribution[19,20,33,34] and quantum channel coding[15,26,27,35], as well as randomness extraction[36–38]. The central approach in many of these works is to perform a random unitary operation[17,18] and then discard a part of the system. This technique has been expanded upon in various works such as refs. [39–42]. Due to the importance of decoupling technique and the limitation that random unitaries cannot be implemented with a quantum circuit of small size, there is a great interest in finding efficient circuits that achieve the same performance as a random unitary.

Existing methods to make decoupling efficient involve replacing random unitaries with unitary 2-designs[43–47] which can be simulated by Clifford circuits of small depth, random quantum circuits of small depth[48] and random unitaries diagonal in Pauli-X and Pauli-Z basis[49]. To elaborate, suppose we are given a quantum state Ψ_{RC} on two registers R and C, and we need to make C independent of R by acting on C. We must further ensure that the size of the discarded system, which is the cost of the decoupling operation (Fig. 1), is small enough, ruling out the operation that discards all of C. Note that the number of qubits of the discarded system translates to the quantum communication cost of a quantum protocol that employs decoupling. This motivates the question of minimizing the size of discarded system. The work[47] shows that a quantum circuit of size $\mathcal{O}(\log|C|\log\log|C|)$ and depth $\mathcal{O}(\log\log|C|)$ suffices for this purpose, achieving the same cost as that of a random unitary. A similar circuit size of $\mathcal{O}(\log|C|\log^2\log|C|)$ and depth $\mathcal{O}(\log^3\log|C|)$ is obtained in ref. [48], using elementary gates that mimic real world quantum processes. See Table 1 for a comparison of the methods.

Table 1. Parameters of various decoupling methods (Unitary 2-design[47], Random X and Z basis[49], Random gates[48], Convex-split[54], this work (Method A)).

Decoupling method	Circuit depth	Circuit size	Gate set
Unitary 2-design	O(log n)	O(n log n)	quantum
Random X and Z basis	O(log n)	O(n^2)	X or Z basis
Random gates	O($\log^3 n$)	O($n\log^2 n$)	quantum
Convex-split	O(n)	O(2^n)	classical
This work (Method A)	O(log n)	O(n log n)	classical

The parameter $n = \log|C|$ is the number of qubits in the register to be decoupled. Gate set column refers to the type of gates required in the decoupling circuit. The classical gates only act in one basis (Z basis, for example).

While the circuit size achieved by above results is impressive, the gates used in the circuit are highly quantum. More precisely, for a choice of preferred basis such as the computational basis, the gates convert any basis vector into a superposition over these vectors. Can the construction of a decoupling operation be further simplified, by only using the gates that are classical (taking basis vectors to basis vectors)? While being useful for practical implementation, such a construction would also lead to a surprising theoretical simplification: it would leave no conceptual difference between quantum decoupling and its classical counterpart of randomness extraction[50–52].

Random permutation is a canonical classical operation known to perform randomness extraction and also decouple classical-quantum systems[36–38]. In ref. [53] (see also ref. [40]) the authors used permutations to derive an analog of the decoupling theorem that however only removes quantum and not classical correlations between R and C. While the remaining classical correlation could also be removed by random permutations, the overall cost of decoupling would be larger than the cost of decoupling by a random unitary. This indicates that a decoupling method, which matches the random unitary decoupling in its cost, may involve operations that are not classical.

This is shown not to be true by the convex-split lemma[54], which expresses a relation of the following form

$$\Phi_{RCE} \approx \sum_i p_i \Phi_{RCE}^{(i)}, \tag{1}$$

showing how to view a given quantum state Φ_{RCE} as a convex combination of (more desirable) quantum states $\Phi_{RCE}^{(i)}$ in order to achieve an information-theoretic task. It implies decoupling (of the type in Fig. 1b) when the quantum state on the left hand side (that is, Φ_{RCE}) is a product state across R and CE. In particular, it was shown in ref. [54] that given Ψ_{RC}, if we add the quantum state $\sigma_{C_1}\otimes\ldots\sigma_{C_N}$ (for some large enough N) and randomly swap the register C with one of the registers $C_1,\ldots C_N$, then the register R becomes independent of all the other registers; leading to decoupling with the classical operation of permutation of

registers. Expressed mathematically in the form of Eq. (1), we would set $E = C_1C_2\ldots C_N$, $\Phi_{RCE} = \Psi_R \otimes \sigma_C \otimes \sigma_{C_1} \otimes \ldots \sigma_{C_N}$, $\Phi^{(i)}_{RCE} = \Psi_{RC_i} \otimes \sigma_C \otimes \sigma_{C_1} \otimes \ldots \sigma_{C_{i-1}} \otimes \sigma_{C_{i+1}} \otimes \ldots \sigma_{C_N}$ and $p_i = \frac{1}{N}$.

In this work we will solely be interested in quantum tasks where decoupling is the same as constructing an appropriate convex-split, and hence we will use the two terms interchangeably. However, we highlight that the convex-split method is more general and can be used even in situations where no decoupling exists: such as in classical or classical-quantum communication tasks[28,55,56] and resource theoretic tasks[57–59].

Since the process of swapping two registers is a 'classical' operation (that is, it takes basis vectors to basis vectors), the convex-split lemma of ref. [54] gives a classical unitary for performing quantum decoupling. Unfortunately, the value of N can be as large as $\mathcal{O}(|C|)$, where $|C|$ is the dimension of the register C. Hence swapping the register C with a random register C_i requires a circuit of depth $\mathcal{O}(|C|)$, which is exponential in the number of qubits of register C. Even an alternate implementation of swap operation, by placing the registers on a three dimensional grid, would require $\mathcal{O}(|C|^{1/3})$ operations. Thus, it has so far been unknown if one can achieve quantum decoupling by efficient classical operations.

Recent works have shown several applications of the convex-split method in one-shot quantum information theory, along with the dual method of position-based decoding[28]. The methods have been used to obtain near-optimal communication for one-shot entanglement-assisted quantum channel coding[28], near-optimal communication for one-shot quantum state splitting[54] (with slight improvement of the additive $\log\log|C|$ factor over[31], for communicating the register C) and smallest known communication for one-shot quantum state redistribution[60]. As mentioned earlier, all these protocols use a large amount of entanglement. Other known protocols[14,26,27], for entanglement-assisted quantum channel coding and[33,34] for quantum state redistribution, that do not rely on these two methods use exponentially small entanglement, but their communication is not known to be near-optimal. This motivates the question of find a scheme that achieves the best of both of the lines of work.

RESULTS

We show how to achieve near-optimal communication and the size of initial entanglement at most constant factors away from the optimal, in all the aforementioned quantum communication tasks. We further show that, in several cases, the implementation of either the encoding or the decoding operation in the protocol can be made efficient. Our results are obtained by two methods that we outline below.

Method A: Efficient decoupling procedures

As mentioned earlier, the quantity of interest in a decoupling procedure is the number of bits or qubits that are discarded to achieve the decoupling. There are two models under which decoupling is performed, see Fig. 1. The first model involves adding a quantum state, applying a global unitary (without involving the register R) and then discarding some quantum system.

The second model also involves adding a quantum state followed by a unitary, but the system that is discarded is classical and the unitary acts in a classical-quantum manner[61]. The two models can be converted into each other by a Clifford circuit of depth 1 and the number of qubits/bits discarded are the same up to a factor of 2, due to the well known duality between teleportation[62] and superdense coding[63]. Additional quantum systems that are not discarded act as a catalyst for the decoupling process[31,54,57,58,64]. For example, the randomness used in the process of decoupling via unitary 2-design acts as a catalyst. In principle, this randomness can be fixed by standard derandomization arguments, but it leads to a loss in efficient implementation.

In this work, we consider the second model of decoupling. We construct two convex-split lemmas which immediately lead to efficient decoupling procedures for a quantum state Ψ_{RC} (recall the discussion following Eq. (1)). One of these lemmas solves the aforementioned problem of decoupling via an efficient classical operation.

- **Method** *A*. 1: A set of unitaries $\{V_\ell\}_{\ell=1}^{|C|^2}$ on a register C forms a 1-design if

$$\frac{1}{N}\sum_\ell V_\ell \rho_C V_\ell^\dagger = \frac{\mathsf{I}_C}{|C|}, \quad \forall \text{ quantum state } \rho_C.$$

  A canonical example of unitary 1-design is the set of the tensor products of Pauli-X and Z operators if the register C admits a qubit decomposition. Our first procedure shows how to achieve decoupling using a mixture of small number of $\approx \log|C| - \mathrm{H}_{\min}(C|R)_\psi$ unitaries from any 1-design. Here Ψ_{RC} is the quantum state on registers R and C and $\mathrm{H}_{\min}(C|R)$ is the conditional min-entropy. The additional randomness used to choose the unitaries is $4\log|C|$ bits. We highlight that this is in stark contrast with many of the previous constructions for decoupling, which required unitaries from a 2-design. Details appear in Supplementary Discussion. This method is related to the explicit schemes presented in refs. [65,66] for quantum encryption. These works show how to achieve decoupling with a mixture of Pauli operators chosen from an explicit set. But the size of the set can be large, and hence does not directly compare with our work. The classical-quantum version of this method previously appeared in the work[67].
- **Method** *A*. 2: The second decoupling procedure enlarges the Hilbert space $\mathcal{H}_C \otimes \mathcal{H}_C$ in a manner that the resulting Hilbert space $\mathcal{H}_G$ has prime dimension $|G| \le 2|C|^2$. This is possible due to Bertrand's postulate[68], which says that there is a prime between any natural number and its twice. It also introduces a register L of size $\sim N \stackrel{\text{def}}{=} \log|C| - \mathrm{H}_{\min}(C|R)_\psi$. A preferred basis on $\mathcal{H}_C$ (such as the computational basis in the qubit representation of the registers) is chosen, which gives a basis $\{|i\rangle_G\}_{i=0}^{|G|-1}$ on $\mathcal{H}_G$. Similarly, a preferred basis $\{|\ell\rangle\}_{\ell=1}^N$ is chosen on $\mathcal{H}_L$. Following this, a unitary operation $U = \sum_{\ell=1}^N U_\ell \otimes |\ell\rangle\langle\ell|_L$ is applied, where U_ℓ acts on two registers $G, G' \equiv G$ as

$$U_\ell|i\rangle_G|j\rangle_{G'} = |i + (j-i)\ell(\mathrm{mod}|G|)\rangle_G|j + (j-i)\ell(\mathrm{mod}|G|)\rangle_{G'}. \tag{2}$$

  Upon tracing out register L, register R becomes independent of GG'. Furthermore, the final state on registers GG' is maximally mixed and the register G' is returned in the original state. As can be seen, the unitaries U_ℓ are 'classical' as they take basis vectors to basis vectors and perform addition and multiplication modulo $|G|$. This makes the construction of U efficient, with circuit depth $\mathcal{O}(\log\log|C|)$ and size $\mathcal{O}(\log|C|\log\log|C|)$ due to well known results in modular arithmetic[69]. Details appear in Supplementary Discussion.

  In the other direction, our result shows that the reversible or quantum circuit complexity (such as depth or size) of integer multiplication modulo a prime is lower bounded by the reversible or quantum circuit complexity of the 'best' decoupling method. This holds since integer multiplication is the most expensive step in Eq. (2). We highlight that a super-linear lower bound on the circuit complexity of integer multiplication is an outstanding open question in the area of complexity theory[70,71]. The aforementioned connection to decoupling may suggest attacking this problem using an

entirely different avenue connected to decoupling[24]: scrambling of quantum information in black holes[72].

Method B: Exponential improvement in entanglement

A procedure, that realizes any classical distribution as a marginal of a uniform distribution in a larger space, has been used in the context of classical correlated sampling in several works[73–79]. A counterpart of this procedure for quantum states was considered in ref. [80]. Since this procedure makes the distribution uniform or 'flat' in its support, we will call it a *flattening* procedure. Let the eigendecomposition of σ_C be $\sigma_C = \sum_i p_i |i\rangle\langle i|_C$. Append a register E through the transformation

$$|i\rangle\langle i|_C \to |i\rangle\langle i|_C \otimes \left(\frac{1}{Kp_i}\sum_{j=1}^{Kp_i}|j\rangle\langle j|_E\right),$$

where K is a large enough real such that $\{Kp_i\}_i$ are all integers. The existence of such a K can be ensured, for example, by an arbitrarily small perturbation in $\{p_i\}_i$, so that they all are rationals. As a result, the quantum state σ_C transforms to

$$\sigma_C \to \frac{1}{K}\sum_{i,j:j\le Kp_i}|i\rangle\langle i|_C \otimes |j\rangle\langle j|_E, \tag{3}$$

which is uniform in a subspace. However, ref. [80] did not provide a unitary operation to realize the above extension of σ_C. We show that this extension can be constructed in a unitary manner using embezzling states[81]. If the basis $\{|i\rangle\}_i$ can be efficiently prepared from computational basis and the eigenvalues $\{p_i\}_i$ are easy to compute, then the flattening procedure is also computationally efficient. Details appear in Supplementary Discussion. The consequences of this method are as follows, with all the tasks appearing below summarized in Fig. 2.

- **Entanglement-assisted classical communication over quantum channel:** Consider a quantum channel $\mathcal{N}_{A\to B}$, over which we wish to communicate a message from the set $\{1, 2, \ldots 2^R\}$, with small error. The work[14] considered the asymptotic and i.i.d. setting for this task, involving the channel $\mathcal{N}_{A\to B}^{\otimes n}$ for large enough n. It was shown that the rate of communication $\frac{R}{n}$ converges to

$$\max_{|\Psi\rangle_{AA'}} \mathrm{I}(A' : B)_{\mathcal{N}_{A\to B}(\Psi_{AA'})},$$

where $\mathrm{I}(A' : B)$ is the quantum mutual information. The number of qubits of entanglement in the protocol from[14] was $\sim nS(\Psi_A)$ (the von-Neumann entropy) and the rate of communication was shown to be optimal. The work[27] obtained a one-shot version of their protocol, with $\log|A|$ qubits of pre-shared entanglement. Their communication was characterized by the *quantum hypothesis testing relative entropy* between the quantum state $\mathcal{N}_{A\to B}(\Psi_{AA'})$ and a separable state derived from $\Psi_{AA'}$, which may not be optimal. The work[28] introduced the position-based decoding method, showing how to achieve a communication characterized by the quantum hypothesis testing relative entropy between $\mathcal{N}_{A\to B}(\Psi_{AA'})$ and $\mathcal{N}_{A\to B}(\Psi_A)\otimes\Psi_{A'}$. The achievable communication is near-optimal, due to the converse given in ref. [82]. But the protocol in ref. [28] required $\mathcal{O}(|A|)$ qubits of entanglement. Using our flattening procedure on the quantum state $|\Psi\rangle_{AA'}$, we show how to achieve the same near-optimal communication with $\mathcal{O}(\log|A|)$ qubits of entanglement. If the flattening procedure is efficient, then the encoding by Alice is efficient as well.

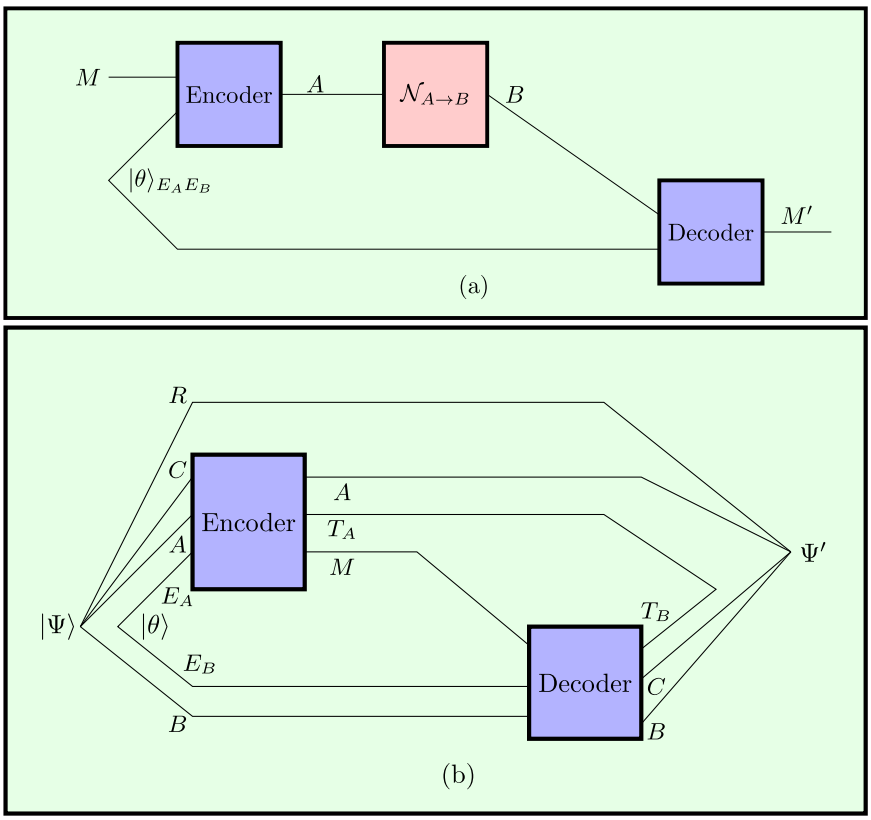

Fig. 2 Quantum communication tasks. Figure **a** depicts the task of entanglement-assisted quantum channel coding, where the register M holds a message $m \in \{1, 2, \ldots 2^R\}$. The goal is to maximize the value of R, while keeping the error in decoding small. Figure **b** shows the task of quantum state redistribution with entanglement assistance. The goal is to ensure that the register C is obtained by Bob using as less communication $\log|M|$ as possible and ensuring that $\Psi' \approx |\Psi\rangle\langle\Psi|$.

Details appear in Supplementary Discussion.

The work[28] also studied entanglement-assisted classical communication through various quantum networks, shown to be near optimal in ref. [83]. Our technique also exponentially improves upon the amount of entanglement in these protocols, while maintaining the achievable communication.

- **Quantum state splitting and quantum state redistribution:** The task of quantum state redistribution[19,20] considers a quantum state $|\Psi\rangle_{RABC}$, where the register R is inaccessible, registers A, C are with Alice and register B is with Bob. It is required that after communication from Alice to Bob, the register C should be held by Bob. Its special cases of quantum state splitting[29] and quantum state merging[17] are equivalent (up to reversal of the protocol) and quantum state splitting considers the case where register B is trivial. The work[31] obtained a one-shot protocol for quantum state splitting achieving near-optimal communication up to an additive factor of $\mathcal{O}(\log\log|C|)$. This was improved in ref. [54] through a near-optimal protocol with communication tight up to an additive factor of $\mathcal{O}(1)$. While the protocol in ref. [31] required $\mathcal{O}(\log|C|)$ qubits of pe-shared entanglement, the protocol in ref. [54] required much larger $\mathcal{O}(|C|)$ qubits. Here, we show how to improve the number of qubits of pre-shared entanglement to $\mathcal{O}(\log|C|)$, retaining the communication cost in ref. [54]. Again, we use the flattening procedure, efficiency of which ensures the efficiency of decoding operation by Bob.

  The work[60] gave a protocol for quantum state redistribution with smallest known quantum communication, improving upon the prior work[34]. But the number of qubits of pre-shared entanglement required was exponentially larger than that in ref. [34]. Similar to aforementioned results, here we give a protocol that has similar quantum communication to ref. [60] and similar number of qubits of entanglement to[34]. Details appear in Supplementary Discussion. We highlight that an upcoming work[84] uses our flattening procedure to further improve upon[60], and provides a connection between one-shot quantum state redistribution and quantum Markov chains.

DISCUSSION

Method *A*. 1 is reminiscent of the derandomizing unitaries constructed in ref. [85], which also uses unitary 1-design for quantum encryption. But there is a difference between our setting and that in ref. [85], since the number of unitaries that we use is dependent on the conditional min-entropy of the quantum state. On the other hand, the authors of ref. [85] only aim to decouple the maximally entangled state. We may also compare Method *A*. 1 with the unitaries in ref. [49], which shows how to perform decoupling with random unitaries diagonal in either X or Z bases. Our construction also yields a unitary diagonal in either X or Z bases, but it is explicit (that is, not a random unitary) and uses some additional catalytic randomness.

As mentioned earlier, the construction in Method *A*. 2 is efficient, with circuit depth $\mathcal{O}(\log\log|C|)$ and size $\mathcal{O}(\log|C|\log\log|C|)$. This already achieves the performance of circuits based on unitary 2-designs[47] (Table 1), by employing very simple operations of integer addition and multiplication. Thus, the method also improves upon the performance of ref. [48]. Furthermore, the integer addition and multiplication operations (Eq. (2)) are very similar to the pair-wise independent hash functions employed in randomness extraction against classical[50] and quantum side-information[36,37]. This provides a unified perspective on decoupling in the classical, classical-quantum and fully-quantum settings. The unitaries $\{U_\ell\}_\ell$, as defined in Eq. (2) have an interesting property that they act as a representation of the cyclic group, reflecting the property of permutation operations in the convex-split method.

In the language of resource theory of coherence, both the decoupling procedures in Method *A* belong to the class of Physically Incoherent Operations[86]. Thus, an immediate implication of our results is that quantum decoupling can be performed by incoherent unitaries. These decoupling procedures perform the same as decoupling via random unitary[37,39,42], when we consider the size of discarded system. None of these results (those in Method *A* and the decoupling via random unitary) are optimal due to the additional effort put in making the decoupled register C uniform. Indeed, it is known that the optimum cost of decoupling is characterized by the max-mutual information, rather than the conditional min-entropy[31,54,64]. Method *B* leads to a decoupling procedure achieving this, as it reduces the task to the case of uniform (or flat) marginal.

As shown in Eq. (3), the central idea behind Method *B* is to flatten a non-uniform quantum state, and use resource-efficient protocols for the flattened state. The work[31] used a different technique for flattening the eigenvalues of a quantum state. Their technique was to distribute the eigenvalues into bins $[2^{-i}: 2^{-i-1}]$ and run a protocol within each bin. While this method can be used for quantum state splitting (with a loss of communication of $\approx \log\log|C|$ required in transmitting the information about the bin), it is not clear how it can be used to construct a near-optimal entanglement-assisted protocol for quantum channel coding. In fact, the quantum channel coding protocol in ref. [27] also can be viewed in the light of this 'binning' technique. But, as mentioned, the one-shot optimality of their protocols is unknown. Our flattening method does not face this limitation and can be uniformly applied to all the quantum communication scenarios. It achieves near-optimal one-shot quantum communication for entanglement-assisted quantum channel coding. Further, our use of embezzling states in both quantum state splitting and entanglement-assisted quantum channel coding further highlights the duality between the two tasks[31,87].

We end this section with some open questions. Our first question is if there exists an analog of Method *B* that does not require embezzling states to achieve near-optimal decoupling. An efficient scheme could lead to protocols with even smaller number of qubits of pre-shared entanglement in quantum communication tasks. Another important question is to see if the number of bits of additional randomness used in Method *A* can further be reduced. It is known that seed size in randomness extraction in the presence of quantum side information can be very small[88] (based on Trevisan's construction[52]). Since our construction treats classical side information and quantum side information in similar manner, we can hope to have similar results even in the case of quantum decoupling.

METHODS

Techniques for Method *A*

The proofs of results presented in Method *A* crucially rely on the following simple identity, which was first shown in ref. [54]. Below, $\mathrm{D}(.\|.)$ is the quantum relative entropy[89].

$$\mathrm{D}\left(\sum_i p_i\rho_i\|\theta\right) = \sum_i p_i(\mathrm{D}(\rho_i\|\theta) - \mathrm{D}(\rho_i\|\rho)).$$

This relation allows us to decompose the convex combination in Eq. (1) into individual components. In addition, the proof of the decoupling result in Method *A*. 1 also uses the notion of pairwise independent random variables to reduce the size of additional randomness, inspired by[55]. The proof of decoupling result in Method *A*. 2 is more subtle, as it requires us to find a collection of unitaries that form an appropriate representation of the cyclic group. Our construction, that is based on modular arithmetic, is inspired by explicit constructions of pairwise independent random variables[90,91].

Techniques for Method *B*

To implement the flattening procedure in Method *B*, we show the following relationships for quantum embezzlement. Let $\xi_D \stackrel{\text{def}}{=} \frac{1}{S}\sum_{j=1}^{n} \frac{1}{j} |j\rangle\langle j|_D$ be the marginal of the embezzling state from[81], for some integer n and S being the normalization factor. Let $\rho_E \stackrel{\text{def}}{=} \frac{1}{b}\sum_{e=1}^{b} |e\rangle\langle e|_E$ be uniform in a support of size b. We show the existence of a unitary U_b such that

$$\mathrm{D}_{\max}\left(U_b\left(\xi_D \otimes |1\rangle\langle 1|_E\right)U_b^{\dagger} \| \xi_D \otimes \rho_E\right) \leq \delta,$$

whenever $n > b^{\frac{1}{\delta}}$. Here $\mathrm{D}_{\max}(.\|.)$ is the quantum max-relative entropy[92,93]. Thus, it is possible to embezzle certain states with error guarantee in max-relative entropy, improving upon the earlier error guarantee in fidelity[81]. We crucially use this in our proofs, as small max-relative entropy allows us to bound other one-shot information theoretic terms.

DATA AVAILABILITY

The authors declare that the data supporting the findings of this study are available within the paper and its supplementary information files.

CODE AVAILABILITY

The authors declare that there are no custom codes in the manuscript. The mathematical algorithms are included within the paper and its supplementary information files.

Received: 28 May 2019; Accepted: 21 July 2022;
Published online: 20 August 2022

REFERENCES

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Theor. Comp. Sci.* **560**, 7–11 (2014).
2. Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
3. Cirac, J. I., Zoller, P., Kimble, H. J. & Mabuchi, H. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Phys. Rev. Lett.* **78**, 3221–3224 (1997).
4. Brown, K. R., Kim, J. & Monroe, C. Co-designing a scalable quantum computer with trapped atomic ions. *npj Quant. Inf.* https://doi.org/10.1038/npjqi.2016.34 (2016).
5. Monroe, C. et al. Large-scale modular quantum-computer architecture with atomic memory and photonic interconnects. *Phys. Rev. A* **89**, 022317 (2014).
6. Azuma, K., Tamaki, K. & Lo, H.-K. All-photonic quantum repeaters. *Nat. Comm.* **6**, 6787 (2015).
7. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
8. Pirandola, S. & Braunstein, S. L. Physics: Unite to build a quantum internet. *Nature* **532**, 169–171 (2016).
9. Schumacher, B. Quantum coding. *Phys. Rev. A.* **51**, 2738–2747 (1995).
10. Schumacher, B. & Westmoreland, M. D. Sending classical information via noisy quantum channels. *Phys. Rev. A* **56**, 131–138 (1997).
11. Holevo, A. S. The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory* **44**, 269–273 (1998).
12. Lloyd, S. Capacity of the noisy quantum channel. *Phys. Rev. A* **55**, 1613–1622 (1997).
13. Shor, P. *The Quantum Channel Capacity and Coherent Information* (IEEE, 2002).
14. Bennett, C. H., Shor, P. W., Smolin, J. A. & Thapliyal, A. V. Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem. *IEEE Trans. Inf. Theory* **48**, 2637–2655 (2002).
15. Devetak, I. The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Inf. Theory* **51**, 44–55 (2005).
16. Hayden, P., Horodecki, M., Winter, A. & Yard, J. A decoupling approach to the quantum capacity. *Open Sys. Inf. Dyn.* **15**, 7–19 (2008).
17. Horodecki, M., Oppenheim, J. & Winter, A. Partial quantum information. *Nature* **436**, 673–676 (2005).
18. Horodecki, M., Oppenheim, J. & Winter, A. Quantum state merging and negative information. *Comm. Math. Phys* **269**, 107–136 (2007).
19. Devetak, I. & Yard, J. Exact cost of redistributing multipartite quantum states. *Phys. Rev. Lett*. https://doi.org/10.48550/arXiv.quant-ph/0612050 (2008).
20. Yard, J. T. & Devetak, I. Optimal quantum source coding with quantum side information at the encoder and decoder. *IEEE Trans. Inf. Theory* **55**, 5339–5351 (2009).
21. Linden, N., Popescu, S., Short, A. J. & Winter, A. Quantum mechanical evolution towards thermal equilibrium. *Phys. Rev. E* **79**, 061103 (2009).
22. Rio, L. d., Aberg, J., Renner, R., Dahlsten, O. & Vedral, V. The thermodynamic meaning of negative entropy. *Nature* https://doi.org/10.48550/arXiv.1009.1630 (2011).
23. Page, D. N. Average entropy of a subsystem. *Phys. Rev. Lett.* **71**, 1291–1294 (1993).
24. Hayden, P. & Preskill, J. Black holes as mirrors: quantum information in random subsystems. *Jour. High Ener. Phys.* **2007**, 120 (2007).
25. Shannon, C. E. A mathematical theory of communication. *The Bell Sys. Tech. Jour.* **27**, 379–423 (1948).
26. Datta, N. & Hsieh, M. H. One-shot entanglement-assisted quantum and classical communication. *IEEE Trans. Inf. Theory* **59**, 1929–1939 (2013).
27. Datta, N., Tomamichel, M. & Wilde, M. M. On the second-order asymptotics for entanglement-assisted communication. *Quant. Inf. Proc.* **15**, 2569–2591 (2016).
28. Anshu, A., Jain, R. & Warsi, N. A. Building blocks for communication over noisy quantum networks. *IEEE Trans. Inf. Theory* **65**, 1287–1306 (2019).
29. Abeyesinghe, A., Devetak, I., Hayden, P. & Winter, A. The mother of all protocols: restructuring quantum information's family tree. *Proc. Roy. Soc. A* **465**, 2537–2563 (2009).
30. Berta, M. Single-shot quantum state merging. *arXiv* http://arxiv.org/abs/0912.4495 (2009).
31. Berta, M., Christandl, M. & Renner, R. The Quantum Reverse Shannon Theorem based on one-shot information theory. *Comm. Math. Phys.* **306**, 579–615 (2011).
32. Hirche, C. & Morgan, C. *2014 IEEE International Symposium on Information Theory* (IEEE, 2014).
33. Datta, N., Hsieh, M.-H. & Oppenheim, J. An upper bound on the second order asymptotic expansion for the quantum communication cost of state redistribution. *Jour. Math. Phys.* **57**, 052203 (2016).
34. Berta, M., Christandl, M. & Touchette, D. Smooth entropy bounds on one-shot quantum state redistribution. *IEEE Trans. Inf. Theory* **62**, 1425–1439 (2016).
35. Dupuis, F., Hayden, P. & Li, K. A father protocol for quantum broadcast channels. *IEEE Trans. Inf. Theory* **56**, 2946–2956 (2010).
36. Renner, R. Security of quantum key distribution. *arXiv* https://doi.org/10.22331/q-2021-12-07-602 (2005).
37. Berta, M. Quantum side information: uncertainty relations, extractors, channel simulations. *arXiv* https://doi.org/10.48550/arXiv.1310.4581 (2005).
38. Berta, M., Fawzi, O. & Wehner, S. Quantum to classical randomness extractors. *IEEE Trans. Inf. Theory* **60**, 1168–1192 (2014).
39. Dupuis, F. The decoupling approach to quantum information theory. *arXiv* http://arxiv.org/abs/1410.0664 (2010).
40. Szehr, O. Decoupling theorems. *arXiv* https://doi.org/10.48550/arXiv.1207.3927 (2011).
41. Szehr, O., Dupuis, F., Tomamichel, M. & Renner, R. Decoupling with unitary approximate two-designs. *New Jour. Phys.* **15**, 053022 (2013).
42. Dupuis, F., Berta, M., Wullschleger, J. & Renner, R. One-shot decoupling. *Comm. Math. Phys.* https://doi.org/10.48550/arXiv.1501.04592 (2014).
43. Dankert, C., Cleve, R., Emerson, J. & Livine, E. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A* **80**, 012304 (2009).
44. DiVincenzo, D. P., Leung, D. W. & Terhal, B. M. Quantum data hiding. *IEEE Trans. Inf. Theory* **48**, 580–598 (2002).
45. Chau, H. F. Unconditionally secure key distribution in higher dimensions by depolarization. *IEEE Trans. Inf. Theory* **51**, 1451–1468 (2005).
46. Low, R. A. Pseudo-randomness and learning in quantum computation. *arXiv* https://arxiv.org/abs/1006.5227 (2010).
47. Cleve, R., Leung, D., Liu, L. & Wang, C. Near-linear constructions of exact unitary 2-designs. *Quantum Infor. Comput.* https://doi.org/10.48550/arXiv.1501.04592 (2016).
48. Brown, W. & Fawzi, O. Decoupling with random quantum circuits. *Comm. Math. Phys.* https://doi.org/10.48550/arXiv.1307.0632 (2015).
49. Nakata, Y., Hirche, C., Morgan, C. & Winter, A. Decoupling with random diagonal unitaries. *Quantum* **1**, 18 (2017).
50. Nisan, N. & Zuckerman, D. Randomness is linear in space. *Journal of Computer and System Sciences* **52**, 43–52 (1996).
51. Radhakrishnan, J. & Ta-Shma, A. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM Journal on Discrete Mathematics* **13**, 2–24 (2000).
52. Trevisan, L. Extractors and pseudorandom generators. *J. ACM* **48**, 860–879 (2001).
53. Dupuis, F., Szehr, O. & Tomamichel, M. A decoupling approach to classical data transmission over quantum channels. *IEEE Trans. Inf. Theory* **60**, 1562–1572 (2014).
54. Anshu, A., Devabathini, V. K. & Jain, R. Quantum communication using coherent rejection sampling. *Phys. Rev. Lett.* **119**, 120506 (2017).

55. Anshu, A., Jain, R. & Warsi, N. A. *Convex-Split and Hypothesis Testing Approach to One-Shot Quantum Measurement Compression and Randomness Extraction* (IEEE, 2019).
56. Anshu, A., Garg, A., Harrow, A. W. & Yao, P. Expected communication cost of distributed quantum tasks. *IEEE Trans. Inf. Theory* **64**, 7395–7423 (2018).
57. Anshu, A., Hsieh, M.-H. & Jain, R. Quantifying resources in general resource theory with catalysts. *Phys. Rev. Lett.* **121**, 190504 (2018).
58. Berta, M. & Majenz, C. Disentanglement cost of quantum states. *Phys. Rev. Lett.* **121**, 190503 (2018).
59. Liu, Z.-W. & Winter, A. Resource theories of quantum channels and the universal role of resource erasure. *arXiv* https://arxiv.org/abs/1904.04201 (2019).
60. Anshu, A., Jain, R. & Warsi, N. A. A one-shot achievability result for quantum state redistribution. *IEEE Trans. Inf. Theory* **64**, 1425–1435 (2018).
61. Groisman, B., Popescu, S. & Winter, A. Quantum, classical, and total amount of correlations in a quantum state. *Phys. Rev. A* **72**, 032317 (2005).
62. Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
63. Bennett, C. H. & Wiesner, S. J. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.* **69**, 2881–2884 (1992).
64. Majenz, C., Berta, M., Dupuis, F., Renner, R. & Christandl, M. Catalytic decoupling of quantum information. *Phys. Rev. Lett.* **118**, 080503 (2017).
65. Ambainis, A. & Smith, A. in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques* (eds Jansen, K. et al.) 249–260 (Springer Berlin Heidelberg, Heidelberg, 2004).
66. Desrosiers, S. P. & Dupuis, F. Quantum entropic security and approximate quantum encryption. *IEEE Trans. Inf. Theory* **56**, 3455–3464 (2010).
67. Hayashi, M. Quantum wiretap channel with non-uniform random number and its exponent and equivocation rate of leaked information. *IEEE Trans. Inf. Theory* **61**, 5595–5622 (2015).
68. Tchebychev, P. Mémoire sur les nombres premiers. *J. Math. Pures Appl.* **1**, 366–390 (1852).
69. McLaughlin, P. B. New frameworks for montgomery's modular multiplication method. *Math. Comput.* **73**, 899–906 (2004).
70. Schönhage, A. & Strassen, V. Schnelle multiplikation großer zahlen. *Computing* **7**, 281–292 (1971).
71. Furer, M. Faster integer multiplication. *SIAM J. Comput.* **39**, 979–1005 (2009).
72. Lashkari, N., Stanford, D., Hastings, M., Osborne, T. & Hayden, P. Towards the fast scrambling conjecture. *Jour. High. Ener. Phys.* **2013**, 22 (2013).
73. Broder, A.O. *Proc. Compression and Complexity of Sequences 1997, SEQUENCES '97* (IEEE Computer Society, Washington, DC, 1997).
74. Charikar, M. S. *Similarity EstimationTechniques From Rounding Algorithms* (ACM, 2002).
75. Kleinberg, J. & Tardos, E. Approximation algorithms for classification problems with pairwise relationships: metric labeling and markov random fields. *J. ACM* **49**, 616–639 (2002).
76. Holenstein, T. *Parallel Repetition: Simplifications and the No-Signaling Case* (ACM, 2007).
77. Barak, B. et al. *Rounding Parallel Repetitions of Unique Games* (IEEE Computer Society, 2008).
78. Braverman, M. & Rao, A. *Information Equals Amortized Communication* (IEEE Computer Society, 2011).
79. Anshu, A., Jain, R. & Warsi, N. A unified approach to source and message compression. *arXiv* https://arxiv.org/abs/1707.03619 (2017).
80. Anshu, A., Jain, R., Mukhopadhyay, P., Shayeghi, A. & Yao, P. New one-shot quantum protocols with application to communication complexity. *IEEE Trans. Inf. Theory* **62**, 7566–7577 (2016).
81. van Dam, W. & Hayden, P. Universal entanglement transformations without communication. *Phys. Rev. A* **67**, 060302 (2003).
82. Matthews, W. & Wehner, S. Finite blocklength converse bounds for quantum channels. *IEEE Trans. Inf. Theory* **60**, 7317–7329 (2014).
83. Anshu, A., Jain, R. & Warsi, N. A. On the near-optimality of one-shot classical communication over quantum channels. *Jour. Math. Phys.* **60**, 012204 (2019).
84. Anshu, A., Hadiashar, S. B., Jain, R., Nayak, A. & Touchette, D. One-shot quantum state redistribution and quantum markov chains. *arXiv* https://arxiv.org/abs/2104.08753 (2021).
85. Ambainis, A. & Smith, A. D. Small pseudo-random families of matrices: derandomizing approximate quantum encryption. *arXiv* https://doi.org/10.48550/arXiv.quant-ph/0404075 (2004).
86. Streltsov, A., Adesso, G. & Plenio, M. B. Colloquium: Quantum coherence as a resource. *Rev. Mod. Phys.* **89**, 041003 (2017).
87. Bennett, C. H., Devetak, I., Harrow, A. W., Shor, P. W. & Winter, A. The quantum reverse shannon theorem and resource tradeoffs for simulating quantum channels. *IEEE Trans. Inf. Theory* **60**, 2926–2959 (2014).
88. De, A., Portmann, C., Vidick, T. & Renner, R. Trevisan's extractor in the presence of quantum side information. *SIAM J. Comput.* **41**, 915–940 (2012).
89. Umegaki, H. Conditional expectation in an operator algebra, i. *Tohoku Math. J.* **6**, 177–181 (1954).
90. Lovett, S. *Pairwise Independent Hash Functions and Applications*. http://cseweb.ucsd.edu/slovett/teaching/SP15-CSE190/ (2015).
91. Kopparty, S., Cheung, Y. K. & Nikolov, A. *K-Wise Independent Hashing and Applications*. http://sites.math.rutgers.edu/sk1233/courses/topics-S13/lec5.pdf (2013).
92. Datta, N. Min- and max- relative entropies and a new entanglement monotone. *IEEE Trans. Inf. Theory* **55**, 2816–2826 (2009).
93. Jain, R., Radhakrishnan, J. & Sen, P. A property of quantum relative entropy with an application to privacy in quantum communication. *J. ACM* **56**, 1–33 (2009).

ACKNOWLEDGEMENTS

Part of this work was completed when A.A. was at the Centre for Quantum Technologies, National University of Singapore, Singapore, where A.A.'s research was supported by the Singapore Ministry of Education through the Tier 3 Grant MOE2012-T3-1-009. A.A. is supported through the NSF award QCIS-FF: Quantum Computing & Information Science Faculty Fellow at Harvard University (NSF 2013303). R.J.'s research is supported by the National Research Foundation, Singapore, also through the grant NRF2021-QEP2-02-P05, and the Ministry of Education, Singapore under the Research Centres of Excellence programme. R.J. is also supported by the "VAJRA Faculty Scheme" of the Science and Engineering Board (SERB), Department of Science and Technology (DST), Government of India.

AUTHOR CONTRIBUTIONS

All the authors contributed equally. A.A. and R.J. are co-authors.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-022-00608-1.

Correspondence and requests for materials should be addressed to Anurag Anshu or Rahul Jain.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.