npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Characterising the correlations of prepare-and-measure quantum networks

Yukun Wang[1], Ignatius William Primaatmaja[2], Emilien Lavie[1,2,3], Antonios Varvitsiotis[1] and Charles Ci Wen Lim[1,2]

Prepare-and-measure (P&M) quantum networks are the basic building blocks of quantum communication and cryptography. These networks crucially rely on non-orthogonal quantum encodings to distribute quantum correlations, thus enabling superior communication rates and information-theoretic security. Here, we present a computational toolbox that can efficiently characterise the set of input–output probability distributions for any discrete-variable P&M quantum network, assuming only the inner-product information of the quantum encodings. Our toolbox is thus highly versatile and can be used to analyse a wide range of quantum network protocols, including those that employ infinite-dimensional quantum code states. To demonstrate the feasibility and efficacy of our toolbox, we use it to solve open problems in multipartite quantum distributed computing and quantum cryptography. Taken together, these findings suggest that our method may have implications for quantum network information theory and the development of new quantum technologies.

npj Quantum Information (2019)5:17 ; https://doi.org/10.1038/s41534-019-0133-3

INTRODUCTION

Quantum correlations[1–3] (namely, entanglement, nonlocality, steering correlations, etc) are essential resources in quantum information processing. In short, they are the reason why we see such unique advantages in quantum communication, cryptography, computing, and imaging. The general observation is that the stronger these correlations are, the more powerful quantum information becomes. This is especially the case for quantum communication[4] and quantum cryptography,[5] where stronger entanglement means higher quantum fidelity and stronger information security. For this reason, the characterisation of quantum correlations is an integral step in many quantum information protocols and a central research topic in quantum information science.

In this work, we are interested in characterising the quantum correlations of prepare-and-measure (P&M) networks, which are the basic building blocks of quantum communication and quantum cryptography. The central goal of a P&M quantum network is to send some classical message z over a quantum network to a group of receivers (see Fig. 1). This message could be anything, e.g., a secret key, elements of a database, or a signed certificate—it depends on the function of the protocol. Quantum encoding is done by preparing a quantum signal in one of the n predefined pure states, $\{|\psi_z\rangle\}_{z=1}^{n}$ (determined by the input z), and decoding is accomplished by making a measurement (sampled from a finite set of decoding settings) on the output quantum signal. For a generic P&M quantum network with k spatially separated receivers, we write $p(a_1a_2\ldots a_k|x_1x_2\ldots x_k, z)$ to denote the probability of obtaining outcomes $a_1a_2\ldots a_k$ given decoding functions $x_1x_2\ldots x_k$ and message z. We use p to denote the entire list of input–output probability distributions.

Our broad goal is to reveal the fundamental limits of P&M quantum networks without restrictions on the network and local decoding strategies. In particular, we are interested in identifying the set of quantum-realisable correlations $\mathbf{p}$ (henceforth called the quantum set) using only the knowledge of the quantum encoding scheme $\{|\psi_z\rangle\}_z$. In fact, as we shall show later, it is enough to use the inner-product information of the encoding scheme (instead of the complete specification) to achieve tight characterisation of the quantum network. This type of approach is particularly useful for analysing the performance of quantum communication and quantum cryptography. For instance, one can use the quantum set to derive lower bounds on the quantum network's error probabilities.[6–8] These bounds essentially tell us what the encoding scheme could achieve in practice, be it for quantum cryptography, communication, or distributed computing purposes, as we shall demonstrate later.

Also, from the perspective of quantum information theory, this approach draws a direct connection between the distinguishability of quantum states and quantum correlations. More concretely, we first note that if the quantum encoding $\{|\psi_z\rangle\}_z$ is completely orthogonal, i.e., $\langle\psi_z|\psi_{z'}\rangle = \delta_{zz'}$, then $\mathbf{p}$ is generally *unconstrained*. That is, such encodings are classical states and hence can be arbitrarily copied—as such, there are no physical principles that could constrain the input–output probability distribution (except for the usual normalisation requirements). The interesting part comes when the encoding $\{|\psi_z\rangle\}_z$ is non-orthogonal. In this case, there are two unique consequences. First, it is generally impossible for every receiver to learn the same information about z. This is due to the fact that one cannot clone non-orthogonal states,[9] and consequently, there is a global trade-off between the amount of accessible information that each receiver can receive.[10,11] Second, no receiver can completely learn z even if he or she has received $\{|\psi_z\rangle\}_z$ with perfect fidelity. This is because non-orthogonal states are fundamentally indistinguishable: there is no measurement that can discriminate them with

[1]Department of Electrical and Computer Engineering, National University of Singapore, Singapore, Singapore; [2]Centre for Quantum Technologies, National University of Singapore, Singapore Centre for Quantum Technologies, National University of Singapore, Singapore, Singapore and [3]Télécom ParisTech, LTCI, Paris, France
Correspondence: Charles Ci Wen Lim (charles.lim@nus.edu.sg)

Received: 29 September 2018 Accepted: 23 January 2019
Published online: 08 February 2019

perfect reliability.[12] Consequently, probability assignments like $p(a = z|x) = 1$ are forbidden. Taken together, these imply that, contrary to orthogonal (classical) encodings, correlations emanating from quantum encodings have non-trivial constraints (e.g., see quantum broadcasting[13,14]).

RESULTS

To solve the above characterisation problem, we propose a general computational method that is able to approximate (from the outside) the quantum set of any P&M quantum network. The approximation is based on a hierarchy of semidefinite relaxations, which is a generalisation and novel application of earlier research in quantum nonlocality.[2,15–20] More specifically, we extend and generalise the hierarchy of semidefinite relaxations proposed in refs [19,20] to the case whereby the quantum state shared between the receivers is not fixed. A key feature of our method is that it is semi-device independent (SDI).[21–27] That is, the analysis provided is independent of how the network and measurements are implemented. The method only requires that the quantum encoding $\{|\psi_z\rangle\}_z$ is characterised in terms of its Gram matrix, i.e., $\langle\psi_z|\psi_{z'}\rangle = \lambda_{zz'}$, which in practice can be easily obtained by taking the inner products of the quantum code states (i.e., using their specifications).

The main advantage with this approach is that the dimension of the encoding system is no longer necessary in the analysis—using the inner-product information is enough to tightly characterise the quantum set. Indeed, the inner-product information is sufficient as it tells us how non-orthogonal the encoded states are and whether they are classical or not. As such, our approach is more practical than the standard SDI approach, which assumes the dimension of the quantum encoding system.[21–24] Notice that physical dimension is generally difficult to fix in practice as actual systems have multiple degrees of freedom. We remark that alternative SDI approaches based on bounded energy constraints[26] and the transmission of non-orthogonal binary states[27] have also been proposed. These have similar advantages as our approach, but present analyses using these approaches are so far limited to binary code states. It remains to be seen if these can be readily generalised to multiple code states, schemes that are often used in quantum technologies. In the following, we show that our method can be used to efficiently analyse any practical quantum communication protocol,[28] including those that use multiple infinite-dimensional code states.

To keep our presentation concise, we restrict the discussion to two-receiver P&M quantum networks (see Fig. 1); extension to larger networks is straightforward. Consider a P&M quantum task, where random code states are sent across a network to two independent receivers, called Alice and Bob, for measurement. For simplicity, we divide the task into two phases: a distribution phase and a measurement phase. In the first phase, a classical random source z is encoded into a quantum system $|\psi_z\rangle$ and distributed to Alice and Bob via an untrusted quantum network. For this type of transmission, it is useful to work in the purification picture, where state transformations are given by unitary evolutions.[29] That is, by working in a higher-dimensional Hilbert space, we may see the transmission as an isometric evolution that takes $|\psi_z\rangle$ to some pure output state $|\phi_z\rangle$, which is now shared between the receivers and the network environment (the purification system). The key advantage of this picture is that while the dimension and possibly other properties of $|\psi_z\rangle$ may change after the transmission, the inner-product information of $\{|\varphi_z\rangle\}_z$ remains the same: $\langle\phi_z|\phi_{z'}\rangle = \langle\psi_z|\psi_{z'}\rangle$. Importantly, this means that our initial knowledge about $\langle\psi_z|\psi_{z'}\rangle = \lambda_{zz'}$ is preserved in the transformed states.

In the measurement phase, Alice and Bob perform independent and random measurements on $|\phi_z\rangle$ to gain information about z. Since there are only two receivers here, we revert back to the usual convention and denote Alice's and Bob's measurements by x and y and their corresponding measurement outcomes by a and b, respectively. Then, using the quantum Born rule, we have that the probability of observing outcomes a, b given measurements x, y and $|\phi_z\rangle$ is

$$p(ab|xy,z) = \langle\phi_z|E_x^a E_y^b|\phi_z\rangle, \tag{1}$$

where $\{E_x^a\}$ and $\{E_y^b\}$ are projective measurements satisfying the following properties: (i) for any x, $E_x^a E_x^{a'} = 0$ for $a \neq a'$, (ii) $\sum_a E_x^a = \mathbb{I}$, (iii) $(E_x^a)^2 = E_x^a = (E_x^a)^\dagger$, and (iv) $[E_x^a, E_y^b] = 0$. We note that there is no loss of generality in assuming projective measurements here. Indeed, we can always lift any measurement to a projective one by working in a higher-dimensional Hilbert space; in our case this is possible since the dimension of the network is not fixed. The last property reflects the fact that Alice's and Bob's measurements are separable and hence the application of one has no effect on the outcome of the other.

Our characterisation problem is thus the following: Given an $n \times n$ Hermitian positive-semidefinite matrix λ, what is the corresponding quantum set $\mathbf{p}$? We denote this set by $\mathcal{Q}(\lambda)$. In principle, solving this problem would require optimising over all possible quantum states and measurements in Eq. (1) subject to the constraints $\langle\phi_z|\phi_{z'}\rangle = \lambda_{zz'}$. However, this task is computationally intractable: the dimension of the network is not fixed and thus could be infinite. To overcome this obstacle, we take inspiration from the characterisation techniques[16–20] developed in Bell nonlocality research,[2,15] which is a special case of our problem. Recall that in a Bell experiment, local random measurements are made on a fixed source $|\phi\rangle$ instead of a varying source $|\phi_z\rangle$. Notably, it was shown in refs [19,20] that the set of quantum probabilities derived from Bell experiments can be approximated via a hierarchy of membership tests. There, the basic idea is to bound the quantum set using a sequence of weaker (but tractable) characterisation tasks, which nevertheless still represent very well the original problem.

In this work, we show that a similar characterisation technique can also be devised for the general problem. More specifically, we give a general procedure for deriving (tractable) necessary conditions for any discrete-variable P&M quantum network. To start with, consider a quantum probability distribution $p(ab|xy,z) = \langle\phi_z|E_x^a E_y^b|\phi_z\rangle$, where $\langle\phi_z|\phi_{z'}\rangle = \lambda_{zz'}$, and with $\{E_x^a, E_y^b\}_{a,x,b,y}$ satisfying properties (i)–(iv). Let $\mathcal{S} = \{S_1, \ldots, S_m\}$ be a finite set of m operators, where each element is a linear combination of products of $\{E_x^a, E_y^b\}_{a,x,b,y}$. Then define G to be the $nm \times nm$ block matrix

$$G = \sum_{z,z'=1}^{n} G^{zz'} \otimes |e_z\rangle\langle e_{z'}|,$$

where $G^{zz'}_{(i,j)} = \langle\phi_z|S_i^\dagger S_j|\phi_{z'}\rangle$ for all $z, z' \in [n]$, $i, j \in [m]$. Here we denote by $\{|e_z\rangle\}_{z=1}^n$ the standard orthonormal basis of $\mathbb{C}^n$ and by $G^{zz'}_{(i,j)}$ the ij-entry of the matrix $G^{zz'}$. By construction, the matrix G is Hermitian and positive-semidefinite (PSD).[30] Furthermore, properties (i)–(iv) of the measurement operators and the inner-product constraints $\langle\phi_z|\phi_{z'}\rangle = \lambda_{zz'}$ translate to linear conditions on the entries of G. To see this, we note that if the set $\mathcal{S}$ contains operators $\{E_x^a\}_{a,x}$ and $\{E_y^b\}_{b,y}$, then it can be easily verified that G satisfies

$$\sum_b G^{zz}_{(a,x),(b,y)} = \sum_b p(ab|xy,z)$$

$$\sum_a G^{zz'}_{(a,x),(a,x)} = \lambda_{zz'}.$$

Therefore, for any discretely modulated P&M quantum network, it is always possible to define a PSD matrix that captures the original quantum model (1) in terms of constraints that are linear in its entries. Importantly, the existence of such a matrix provides

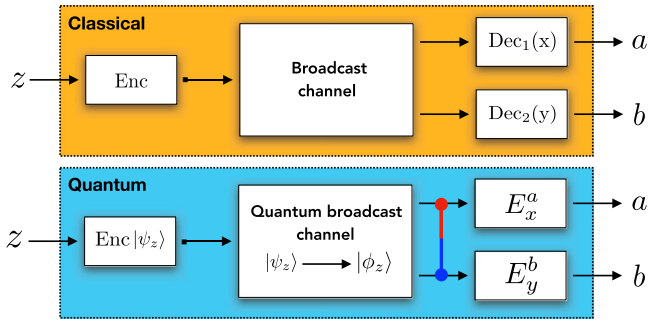

Fig. 1 Scenario and assumptions. The behaviour of a two-receiver prepare-and-measure (P&M) quantum network is generally described by $\mathbf{p} = [p(ab|xy, z)]$, which expresses the probability of z transiting to outcomes a, b given measurement inputs x, y. In the quantum setting, the set of conditional probabilities are given by $p(ab|xy, z) = \langle\phi_z|E_x^a E_y^b|\phi_z\rangle$, with the constraint that $\langle\phi_z|\phi_{z'}\rangle = \lambda_{zz'}$ is fixed. Our consideration hence assumes three conditions: (1) the set of code states are pure states, (2) the Gram matrix of these states is known, and (3) the receivers are independent of each other (they do not share any quantum resources, although classical randomness is allowed)

us with a powerful means to check if a given $\mathbf{p}$ is of quantum origin. More specifically, we can use semidefinite programming (SDP) techniques[31] to verify if $\mathbf{p}$ is in the set of compatible PSD matrices: if $\mathbf{p}$ is not a member, we conclude that it is not quantum realisable. However, successful membership does not necessarily mean $\mathbf{p}$ is of quantum origin. This is due to the fact that our characterisation method is a semidefinite relaxation[32] of the original problem and hence can only provide an outer-approximation of $\mathcal{Q}(\lambda)$.

However, by introducing additional linear constraints via a hierarchical procedure, it is possible to gain a tighter characterisation of $\mathcal{Q}(\lambda)$. In particular, we could use the hierarchy proposed in refs [19,20] to build a series of increasingly stringent membership tests, where the associated Gram matrix G grows bigger in each step and more constraints are generated. More precisely, we define a sequence of hierarchical sets $\mathcal{S}_1 = \{E_x^a, E_y^b\}$, $\mathcal{S}_2 = \mathcal{S}_1 \cup \{E_x^a E_{x'}^{a'}\} \cup \{E_y^b E_{y'}^{b'}\} \cup \{E_x^a E_y^b\}$, where $\mathcal{S}_k$ is defined inductively as the set of all operator sequences constructed from E_x^a, E_y^b satisfying $\mathcal{S}_k \subseteq \mathcal{S}_{k+1}$. This corresponds to a sequence of Gram matrices, G^1, G^2,… with increasing size and constraints. Since the Gram matrix G^k of a particular kth step is at least as informative as a smaller sized Gram matrix $G^{k'}$, we conclude that the approximated set $\mathcal{Q}(\lambda)_k$ is a subset of $\mathcal{Q}(\lambda)_{k'}$. Therefore, moving up the hierarchy gives a tighter approximation of the quantum set: $\mathcal{Q}(\lambda) \subseteq \mathcal{Q}(\lambda)_k \subseteq \mathcal{Q}(\lambda)_{k-1} \ldots$. In the online supplementary material, we prove that this hierarchy is in fact sufficient: it converges to the quantum set, $lim_{k\to\infty} \mathcal{Q}(\lambda)_k = \mathcal{Q}(\lambda)$. Nevertheless, in the applications below, we see that low-level approximations are already enough to achieve very tight bounds.

APPLICATIONS

Our method can be applied to any quantum communication task that employs the P&M scheme. To illustrate this point, we provide two examples of application: (1) distributed quantum random access coding (QRAC)[33,34] and (2) quantum key distribution (QKD).[35,36]

In the first, we consider a distributed computing task where two random bits z_0z_1 are encoded into a quantum state $|\psi_{z_0z_1}\rangle$ and sent to Alice and Bob for selective decoding. For the decoding part, Alice and Bob are each given a random position bit and their goal is to guess the input bit that is associated with the position bit. For example, if Alice receives $x = 1$, she has to guess the value of z_1 via measurement on her share of $|\psi_{z_0z_1}\rangle$. This task can be

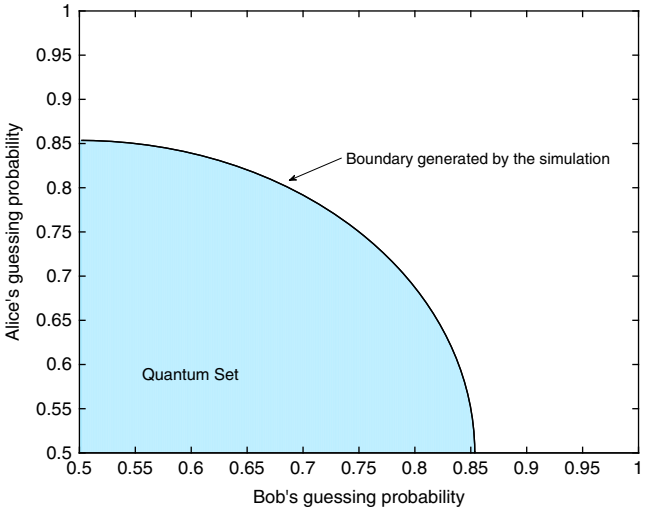

Fig. 2 Distributed two-receiver quantum random access coding (QRAC). The boundary is generated using the first level of the semidefinite programming (SDP) hierarchy. In principle, the boundary is not necessarily tight, for $\mathcal{Q}(\lambda)_1$ may contain correlations that are not of quantum origin. However, in our case we show that the derived boundary is tight: it is saturated by the optimal asymmetric qubit cloning machine. Suppose the quantum code states are given by the conjugate coding scheme: $|\psi_{00}\rangle = |+\rangle|0\rangle$,$|\psi_{10}\rangle = |+i\rangle|0\rangle$,$|\psi_{01}\rangle = |-i\rangle|0\rangle$, and $|\psi_{11}\rangle = |-\rangle|0\rangle$. The quantum network is assumed to be an asymmetric cloning channel U_f: $|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle$ and $|1\rangle|0\rangle \rightarrow \sqrt{1-f}|1\rangle|0\rangle + \sqrt{f}|0\rangle|1\rangle$, where $f \in [0, 1]$. For the decoding, we assume that Alice and Bob perform the optimal QRAC qubit measurements: $E_x^a = (\mathbb{I} + (-1)^a(\mathbb{X} + (-1)^{x+1}\mathbb{Y})/\sqrt{2})/2$, $E_y^b = (\mathbb{I} + (-1)^b(\mathbb{X} + (-1)^{y+1}\mathbb{Y})/\sqrt{2})/2$. Using these and setting the left subsystem as Alice's and the right subsystem as Bob's, we have that $p(a = z_x) = 1/2 + \sqrt{(1-f)/2}/2$ and $p(b = z_y) = 1/2 + \sqrt{f/2}/2$. These give $(2p(a = z_x) - 1)^2 + (2p(b = z_y) - 1)^2 = 1/2$, which is the quantum boundary predicted by the $\mathcal{Q}(\lambda)_1$ set

seen as a type of distributed quantum database, where network users can choose to learn any entry of the database; this includes the case whereby multiple users can choose to learn the same entry. To this end, we quantify the network's ability to distribute information by Alice's and Bob's guessing probabilities, which we denote by $p(a = z_x)$ and $p(b = z_y)$, respectively.

At this point, it is useful to recall that if $|\psi_{z_0z_1}\rangle$ is a two-level quantum system (i.e., a qubit), then the best encoding strategy (in the case of the standard two-party QRAC) is to use the so-called conjugate coding scheme:[37] $|\psi_{00}\rangle = |+\rangle$, $|\psi_{10}\rangle = |+i\rangle$, $|\psi_{01}\rangle = |-i\rangle$, and $|\psi_{11}\rangle = |-i\rangle$, where $|\pm\rangle$ and $|\pm i\rangle$ are the eigenstates of the Pauli operators $\mathbb{X}$ and $\mathbb{Y}$, respectively. This gives a guessing probability of $\left(1 + 1/\sqrt{2}\right)/2 \approx 0.853$,[33,34] which is optimal for qubit code states. Interestingly, using our method, we find that similar bounds can be established using only the Gram matrix information of the code states. In particular, we consider a set of code states $\{|\psi_{00}\rangle,|\psi_{11}\rangle,|\psi_{10}\rangle,|\psi_{01}\rangle\}$, whose Gram matrix is fixed to that of $\{|+\rangle,|-\rangle,|+i\rangle,|-i\rangle\}$, and ask what is Alice's optimal guessing probability given Bob's guessing probability is fixed. Our method predicts the following quantum boundary: $(2p(a = z_x) - 1)^2 + (2p(b = z_y) - 1)^2 \leq 1/2$, which is drawn in Fig. 2. The SDP for this optimisation is given in the supplementary material.

Three remarks are in order here. First, we see that the boundary (obtained from $\mathcal{Q}(\lambda)_1$) gives the same upper bound as ref. [33] when one of the receivers is restricted to random guessing. This can be seen as the case in which one party receives $|\psi_{z_0z_1}\rangle$ with perfect

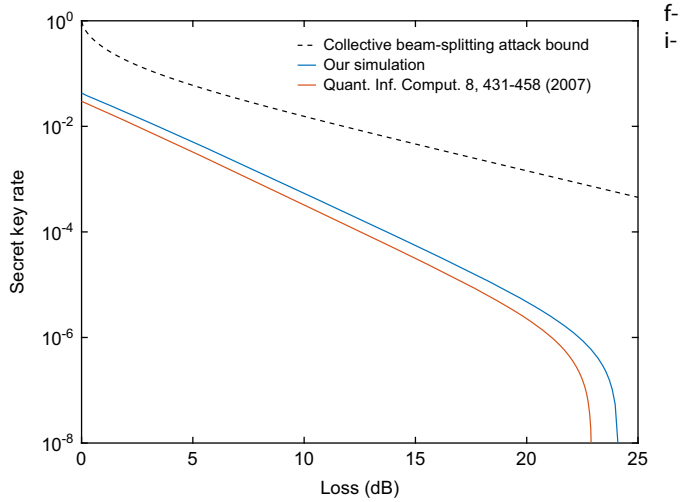

Fig. 3 Phase encoded coherent-state quantum key distribution (QKD). We compare our secret key rate against the one given in ref. [40]. For the key rate simulation, we assume a detector dark count rate of $p_{\mathrm{dc}} = 10^{-7}$ and an intrinsic optical error rate of 2%. For a given channel loss $1-\eta$, the probability of detecting a signal is $p_{\mathrm{det}} = 1-(1-p_{\mathrm{dc}})^2 \exp(-2\eta\mu)$ and the error probability is $\varepsilon = (p_{\mathrm{dc}} + (1-\exp(-2\mu\eta))0.02)/p_{\mathrm{det}}$. Using these, we maximise the expected secret key rate (2). More precisely, we perform two optimisations. First, for a given μ we maximise the phase error rate over $\mathcal{Q}(\lambda)_2$ subject to the above constraints. This gives us a lower bound on the achievable secret key rate. Then, we optimise the secret key rate over μ. This gives us an estimate of the optimal secret key rate. Comparing with the secret key rate of ref. [40] (red line), we see that our method predicts a higher secret key rate (blue line) for any loss point. For further comparison, we also plotted the collective beam-splitting attack bound with zero error[42] (the top curve: black dashed line), which serves as an upper bound on the achievable secret key rate; note that this bound is not tight and it assumes zero errors

delity and the other party receives a dummy state. Second, the boundary specifies a non-trivial trade-off function between Alice's and Bob's guessing probabilities, which is independent of their measurement strategies. This implies that the bound is absolute and cannot be improved upon with better measurement strategies, even if Alice and Bob are allowed to use shared randomness. Third, although our method can only provide an outer-approximation of the quantum set, it turns out that the first level of the hierarchy is already tight. More specifically, there is a concrete example, which saturates the boundary predicted by $\mathcal{Q}(\lambda)_1$; see Fig. 2 for more details. This example is given by the optimal asymmetric qubit cloning machine,[38] which optimally splits the qubit information between multiple parties (according to some predefined ratio); this is indeed a natural choice as the goal of the network is to preserve as much quantum information as possible for each party while splitting it.

In the second application, we prove the security of coherent-state QKD. Here, one of the receivers (Alice) is the eavesdropper (renamed to Eve) and her goal is to eavesdrop on the quantum channel connecting the transmitter and the other receiver (Bob). For concreteness, we first consider a phase encoded coherent-state QKD protocol,[39] which uses the encoding scheme $|\psi_{z_0z_1}\rangle : |\psi_{00}\rangle = |\sqrt{\mu}\rangle, |\psi_{10}\rangle = |-\sqrt{\mu}\rangle, |\psi_{01}\rangle = |i\sqrt{\mu}\rangle,$ and $|\psi_{11}\rangle = |-i\sqrt{\mu}\rangle$, where μ is the mean photon number of the coherent state. To maximise the sifting efficiency of the protocol, we use $\{|\sqrt{\mu}\rangle, |-\sqrt{\mu}\rangle\}$ for key generation and $\{|i\sqrt{\mu}\rangle, |-i\sqrt{\mu}\rangle\}$ for testing the security of the channel. Correspondingly on Bob's side, we have that he uses measurement $y = 0$ for key recovery and measurement $y = 1$ for estimating the channel noise; we write ε_0 and ε_1 to denote the error probabilities observed in the key basis and the test basis, respectively. In this case, the sifting rate of the protocol tends to 1 (in the limit of infinite keys) when the probability of choosing the key basis goes to 1.[35]

In the supplementary information, we show that the expected secret key rate (per signal sent) is

$$R_{\mathrm{key}}^{\infty} \geq \max\{0, p_{\mathrm{det}}[1 - h_2(\varepsilon_0) - h_2(\varepsilon_{\mathrm{ph}})]\}, \tag{2}$$

where $\varepsilon_{\mathrm{ph}}$ is the so-called phase error rate of the key basis,[41] p_{det} is the probability of detection, and $h_2(\cdot)$ is the binary entropy function. The quantity of interest here is $\varepsilon_{\mathrm{ph}}$, which is maximised assuming fixed system parameters (e.g., μ, ε_0, and ε_1). Crucially, $\varepsilon_{\mathrm{ph}}$ is a linear function of the matrix G, which allows us to use SDP technique. (For the explicit expression of $\varepsilon_{\mathrm{ph}}$, we refer the interested reader to the supplementary information). Then, we use the second level of the hierarchy $\mathcal{S}_2$ and maximise $\varepsilon_{\mathrm{ph}}$ over the set of compatible probabilities in $\mathcal{Q}(\lambda)_2$. The outcome of the numerical optimisation is shown in Fig. 3 along with the simulation parameters. To benchmark our results against the best-known security analysis for the protocol, we also plot the security bound of ref. [40] using the same constraints. From the figure, it is evident that our secret key rates are always higher than the ones given by ref. [40]. Importantly, this shows that our method significantly improves the security and feasibility of practical QKD, despite making only a few assumptions about the implementation. For completeness, we note that refs [43,44] have also recently proposed a new security proof technique based on SDP (but using a completely different approach). In the case of the current protocol, their simulation outcomes are similar to ours, however, their method additionally requires that Bob's measurements are fully characterised and an optical squashing model exists for the measurements.[45]

To demonstrate the ability of our method to handle non-standard QKD protocols, we consider the security of a modified coherent-one-way (COW) QKD protocol,[46,47] which is based on the transmission of time encoded coherent states $\{|0\rangle|\alpha\rangle, |\alpha\rangle|0\rangle, |\alpha\rangle|\alpha\rangle\}$ with $\alpha = \sqrt{\mu}$. Here, the first two sequences of coherent states carry the secret bit (i.e., '0' $\rightarrow|0\rangle|\alpha\rangle$ and '1' $\rightarrow|\alpha\rangle|0\rangle$) and the last sequence is a test state used to estimate Eve's information about the secret bit. For Bob's measurements, we use the active switching measurement scheme proposed in ref. [48] instead of the original passive switching scheme.[46] In this setup, Bob employs an optical switch to send the incoming states either into the data line or the monitoring line: the former measures the arrival time of the incoming states, whereas the latter measures the coherence (the interference visibility) between two adjacent states. The advantage of this scheme is that it yields higher detection probabilities than the passive scheme. Another major modification is that only the coherence of the test sequence $|\alpha\rangle|\alpha\rangle$ is measured. More specifically, the variant protocol does not measure the coherence between adjacent encodings (e.g., in cases like $|0\rangle|\alpha\rangle;|\alpha\rangle|0\rangle$ or $|\alpha\rangle|\alpha\rangle;|\alpha\rangle|0\rangle$) like in the original protocol. This modification is largely motivated by earlier research, which showed that knowing the coherence information between adjacent encodings does not significantly improve the security of the protocol.[48] Importantly, in discarding these events, we have two benefits. First, the security analysis is greatly simplified, i.e., we only need to analyse a single encoding instead of a sequence of encodings, which can be unwieldy. Second, this opens up the possibility to explore scenarios whereby the mean photon number of the test sequence $|\alpha\rangle|\alpha\rangle$ is optimised. More concretely, we can now adjust the mean photon number of the test sequence to maximise the secret key rate. In the following, we will use $|\beta\rangle|\beta\rangle$ to represent the optimised test sequence.

Using the same approach as before (i.e., Eq. (2)), we compute the secret key rate of the variant protocol using a realistic error model that assumes an imperfect intensity modulator (on the

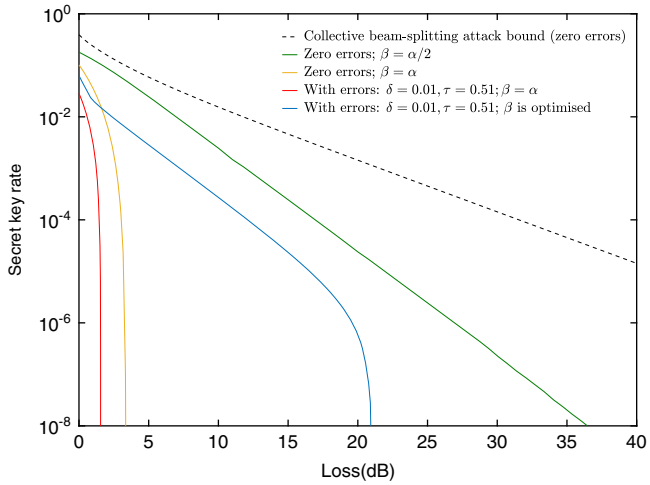

Fig. 4 Time encoded coherent-state quantum key distribution (QKD). For this simulation, we consider an error model that is based on imperfect intensity modulation and imperfect mixing of coherent states. On the transmitter's side, we assume that the intensity modulator used to perform the on-off keying has finite extinction ratio, i.e., states are prepared as $\left|\sqrt{1-\delta}a\right\rangle$ and $\left|\sqrt{\delta}a\right\rangle$ instead of $|a\rangle$ and $|0\rangle$. Here, we use $\delta = 0.01$. On the receiver side, we assume that the beam-splitter in the measurement scheme of ref. [48] has a ratio of 51/49 instead of the ideal 50/50. Using these component models and assuming that each detector has a dark count rate of $p_{\mathrm{dc}} = 10^{-7}$, we run the optimisation as per the previous QKD application and obtain four sets of data points using the original coherent-one-way (COW) QKD encoding and a new encoding strategy where the test sequence is optimised. For each of these, we compute the secret key rates with and without errors

transmitter side) and an imbalanced beam-splitter on the receiver side; see the description of Fig. 4 for more details. We first simulate the expected secret key rates of the protocol using the original COW QKD test sequence $|\beta = a\rangle|\beta = a\rangle$ with errors (red curve) and without errors (yellow curve). Both of these curves show that secret keys can only be distributed in the low loss regime (i.e., <4 dB loss; or equivalently 20 km of optical fibre length). Comparing with the collective beam-splitting attack curve[42] (black dashed curve), we observe that the original COW QKD encoding may be suboptimal. To investigate this possibility, we use the flexibility of our method and further optimise $|\beta\rangle|\beta\rangle$ over a discrete set of ratios β/a to search for the best test sequence for a given loss point. We find that the improvement is highly significant. In the case with zero errors, the optimal ratio is $\beta = a/2$ and the tolerable loss is extended to >35 dB, which spells a ≥30 dB improvement over the original COW QKD encoding. The secret key rates (green curve) are also significantly higher and are close to the collective beam-splitting attack bound (in the low loss regime). In the case with errors, we also see similar improvements. More concretely, the optimised variant protocol is now able to distribute secret keys up to about 21 dB loss with errors, which translates to a fibre distance of about 110 km. In conclusion, our findings strongly indicate that it is much more secure to vary the mean photon number of the test sequence.

DISCUSSION

Taken together, our findings thus provide a powerful method to analyse the quantum set of any discretely modulated P&M quantum network, independently of how the network and decoding measurements are implemented. From the perspective of quantum information theory, the toolbox can help to reveal the fundamental limits of quantum communication and to analyse the performance of any quantum coding scheme. On the application side, the toolbox can be used to analyse the performance of quantum network protocols and the security of quantum cryptography, as evidenced by the three examples given above. Concerning the latter, it would be interesting to investigate how the toolbox could be utilised to solve other open problems in quantum cryptography, e.g., the security of round-robin differential phase-shift QKD[49] or continuous variable QKD protocols with discrete modulations.[50] Another interesting direction would be to extend the method to multiple transmitters like in the case of measurement-device-independent quantum cryptography.[51–56] For instance, it would be interesting to see how our method can be used to analyse the security of phase-matching QKD,[56] which can break the fundamental distance limit of QKD using coherent states.

DATA AVAILABILITY

The data sets generated during the current study are available from the corresponding author upon request.

ACKNOWLEDGEMENTS

We acknowledge support from the National University of Singapore, the Centre for Quantum Technologies, the National Research Foundation, and the Asian Office of Aerospace Research and Development.

AUTHOR CONTRIBUTIONS

C.C.W.L. conceived the main idea of the method with inputs from all authors and supervised the project. Y.W., I.W.P, and E.L. performed the optimisation and simulations. C.C.W.L., A.V., and Y.W provided the technical derivations needed to prove the main results. The paper was written by all authors.

ADDITIONAL INFORMATION

Supplementary information accompanies the paper on the *npj Quantum Information* website (https://doi.org/10.1038/s41534-019-0133-3).

Competing interests: The authors declare no competing interests.

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

REFERENCES

1. Horodecki, R., Horodecki, P., Horodecki, M. & Horodecki, K. Quantum entanglement. *Rev. Mod. Phys.* **81**, 865–942 (2009).
2. Bell, J. S. On the Einstein-Podolsky-Rosen paradox. *Physics* **1**, 195–200 (1964).
3. Wiseman, H. M., Jones, S. J. & Doherty, A. C. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen Paradox. *Phys. Rev. Lett.* **98**, 140402 (2007).
4. Gisin, N. & Thew, R. Quantum communication. *Nat. Photonics* **1**, 165–171 (2007).
5. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
6. Yard, J., Hayden, P. & Devetak, I. Quantum broadcast channels. *IEEE Trans. Inf. Theory* **57**, 7147–7162 (2011).
7. Hirche, C. & Morgan, C. An improved rate region for the classical-quantum broadcast channel. *2015 IEEE Int. Symposium Inform Theory (ISIT)* https://doi.org/10.1109/ISIT.2015.7282963 (2015).
8. Savov, I. & Wilde, M. M. Classical codes for quantum broadcast channels. *IEEE Trans. Inf. Theory* **61**, 7017–7028 (2015).
9. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).
10. Fuchs, C. A. & Peres, A. Quantum-state disturbance versus information gain: uncertainty relations for quantum information. *Phys. Rev. A* **53**, 2038 (1996).
11. Horodecki, M., Horodecki, R., Sen (De), A. & Sen, U. Common origin of no-cloning and no-deleting principles - conservation of information. *Found. Phys.* **35**, 2041–2049 (2005).
12. Holevo, A. S. Statistical decision theory for quantum systems. *J. Multivar. Anal.* **3**, 337–394 (1973).
13. Barnum, H., Caves, C. M., Fuchs, C. A., Jozsa, R. & Schumacher, B. Noncommuting mixed states cannot be broadcast. *Phys. Rev. Lett.* **76**, 2818–2821 (1996).

14. Barnum, H., Barrett, J., Leifer, M. & Wilce, A. Generalized no-broadcasting theorem. *Phys. Rev. Lett.* **99**, 240501 (2007).
15. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–478 (2014).
16. Tsirel'son, B. S. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *J. Sov. Math.* **36**, 557–570 (1987).
17. Landau, L. J. Empirical two-point correlation functions. *Found. Phys.* **18**, 449–460 (1988).
18. Wehner, S. Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities. *Phys. Rev. A* **73**, 022110 (2006).
19. Navascués, M., Pironio, S. & Acín, A. Bounding the set of quantum correlations. *Phys. Rev. Lett.* **98**, 010401 (2007).
20. Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.* **10**, 073013 (2008).
21. Pawłowski, M. & Brunner, N. Semi-device-independent security of one-way quantum key distribution. *Phys. Rev. A* **84**, 010300(R) (2011).
22. Bowles, J., Quintino, M. T. & Brunner, N. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. *Phys. Rev. Lett.* **112**, 140407 (2014).
23. Lunghi, T. et al. Self-testing quantum random number generator. *Phys. Rev. Lett.* **114**, 150501 (2015).
24. Woodhead, E. & Pironio, S. Secrecy in prepare-and-measure Clauser-Horne-Shimony-Holt tests with a qubit bound. *Phys. Rev. Lett.* **115**, 150501 (2015).
25. Berta, M., Fawzi, O. & Scholz, V. B. Quantum bilinear optimization. *SIAM J. Optim.* **26**, 1529–1564 (2016).
26. Himbeeck, T. V., Woodhead, E., Cerf, N. J., García-Patrón, R. & Pironio, S. Semi-device-independent framework based on natural physical assumptions. *Quantum* **1**, 33 (2017).
27. Brask, J. B. et al. Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination. *Phys. Rev. Appl.* **7**, 054018 (2017).
28. Arrazola, J. M. & Lütkenhaus, N. Quantum communication with coherent states and linear optics. *Phys. Rev. A* **90**, 042335 (2014).
29. Wilde, M. M. *Quantum Information Theory*. (Cambridge Univ. Press, New York, 2013).
30. Horn, R. A. & Johnson, C. R. *Matrix Analysis: Characterizations and Properties CH.7*. (Cambridge Univ. Press, Cambridge, 2013).
31. Vandenberghe, L. & Boyd, S. Semidefinite programming. *SIAM Rev.* **38**, 49–95 (1996).
32. Burgdorf, S., Klep, I. & Povh, J. *Optimisation of Polynomials in Non-Commutative Variables*. (Springer, Switzerland, 2016).
33. Ambainis, A., Nayak, A., Ta-Shma, A. & Vazirani, U. Dense quantum coding and a lower bound for 1-way quantum automata. *Proceedings of the thirty-first annual ACM symposium on Theory of computing–STOC 99* (Atlanta, Georgia, USA, 1999).
34. Nayak, A. Optimal lower bounds for quantum automata and random access codes. *40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039)* 369 (1999).
35. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
36. Lo, H. K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **8**, 595–604 (2014).
37. Wiesner, S. Conjugate coding. *ACM SIGACT News* **15**, 78–88 (1983).
38. Cerf, N. J. Asymmetric quantum cloning in any dimension. *J. Mod. Opt.* **47**, 187 (2000).
39. Huttner, B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **51**, 1863–1869 (1995).
40. Lo, H. K. & Preskill, J. Security of quantum key distribution using weak coherent states with nonrandom phases. *Quant. Inf. Comput.* **8**, 431–458 (2007).
41. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
42. Branciard, C., Gisin, N., Lütkenhaus, N. & Scarani, V. Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography. *Quant. Inf. Comput.* **7**, 639–664 (2007).
43. Winick, A., Lütkenhaus, N. & Coles, P. J. Reliable numerical key rates for quantum key distribution. *Quantum* **2**, 77 (2018).
44. Coles, P. J., Metodiev, E. M. & Lütkenhaus, N. Numerical approach for unstructured quantum key distribution. *Nat. Commun.* **7**, 11712 (2016).
45. Beaudry, N. J., Moroder, T. & Lütkenhaus, N. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.* **101**, 093601 (2008).
46. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87**, 194108 (2005).
47. Korzh, B. et al. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat. Photonics* **9**, 163–168 (2015).
48. Moroder, T. et al. Security of distributed-phase-reference quantum key distribution. *Phys. Rev. Lett.* **109**, 260501 (2012).
49. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509**, 475–478 (2014).
50. Leverrier, A. & Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **102**, 180504 (2009).
51. Braunstein, S. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
52. Lo, H. K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
53. Tamaki, K., Lo, H. K., Fung, F. & Qi, B. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Phys. Rev. A.* **85**, 042307 (2012).
54. Ma, X. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A.* **86**, 062319 (2012).
55. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
56. Ma, X., Zheng, P. & Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X.* **8**, 031043 (2018).