nature COMMUNICATIONS

ARTICLE

Received 20 Oct 2015 | Accepted 22 Apr 2016 | Published 20 May 2016

DOI: 10.1038/ncomms11712 OPEN

Numerical approach for unstructured quantum key distribution

Patrick J. Coles[1], Eric M. Metodiev[1] & Norbert Lütkenhaus[1]

Quantum key distribution (QKD) allows for communication with security guaranteed by quantum theory. The main theoretical problem in QKD is to calculate the secret key rate for a given protocol. Analytical formulas are known for protocols with symmetries, since symmetry simplifies the analysis. However, experimental imperfections break symmetries, hence the effect of imperfections on key rates is difficult to estimate. Furthermore, it is an interesting question whether (intentionally) asymmetric protocols could outperform symmetric ones. Here we develop a robust numerical approach for calculating the key rate for arbitrary discrete-variable QKD protocols. Ultimately this will allow researchers to study 'unstructured' protocols, that is, those that lack symmetry. Our approach relies on transforming the key rate calculation to the dual optimization problem, which markedly reduces the number of parameters and hence the calculation time. We illustrate our method by investigating some unstructured protocols for which the key rate was previously unknown.

[1] Department of Physics and Astronomy, Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada N2L3G1. Correspondence and requests for materials should be addressed to P.J.C. (email: pcoles@uwaterloo.ca).

Quantum key distribution (QKD) will play an important role in quantum-safe cryptography, that is, cryptography that addresses the emerging threat of quantum computers[1]. Since its original proposal[2,3], QKD has developed significantly over the past three decades[4,5], both in theory and implementation. Indeed, QKD is now a commercial technology, with the prospect of global QKD networks on the horizon[6,7].

The main theoretical problem in QKD is to calculate how much secret key can be distributed by a given protocol. A crucial practical issue is that the QKD protocols that are easiest to implement with existing optical technology do not necessarily coincide with the protocols that are easiest to analyse theoretically[4]. Currently, calculating the secret key output of a protocol is typically extremely technical, and hence only performed by skilled experts. Furthermore, each new protocol idea requires a new calculation, tailored to that protocol. Ultimately, the technical nature of these calculations combined with the lack of universal tools limits the pace at which new QKD protocols can be discovered and analysed. Here we address this problem by developing a robust, user-friendly framework for calculating the secret key output, with the hope of bringing such calculations 'to the masses'.

The secret key output is typically quantified by the key rate, which refers to the number of bits of secret key established divided by the number of distributed quantum systems. Operationally, this corresponds to the question of how much privacy amplification Alice and Bob must apply to transform their raw key into the final secure key. Analytical simplifications of the key rate calculation can be made for some special protocols that have a high degree of symmetry[8]. Examples of such symmetric protocols, where the signal states have a group-theoretic structure, include the BB84 (ref. 3) and six-state protocols[9]. Indeed the key rate is known for these protocols. However, in practice, lack of symmetry is the rule rather than the exception. That is, even if experimentalists try to implement a symmetric protocol, experimental imperfections tend to break symmetries[10]. Furthermore, it is sometimes desirable due to optical hardware issues to implement asymmetric protocols, for example, as in ref. 11.

We refer to general QKD protocols involving signal states or measurement choices that lack symmetry as 'unstructured' protocols. Some recent work has made progress in bounding the key rate for special kinds of unstructured protocols, such as four-state protocols in refs 12,13 and qubit protocols in ref. 14. Still, there is no general method for computing tight bounds on the key rate for arbitrary unstructured protocols. Yet, these are the protocols that are most relevant to experimental implementations.

This motivates our present work, in which we develop an efficient, numerical approach to calculating key rates. Our ultimate aim is to develop a computer program, where Alice and Bob input a description of their protocol (for example, their signal states, measurement devices, sifting procedure and key map) and their experimental observations, and the computer outputs the key rate for their protocol. This program would allow for any protocol, including those that lack structure.

At the technical level, the key rate problem is an optimization problem, since one must minimize the well-known entropic formula for the key rate[15], over all states ρ_{AB} that satisfy Alice's and Bob's experimental data. The main challenge here is that this optimization problem is unreliable and inefficient. In this work, we give a novel insight that transforming to the dual problem (for example, see ref. 16) resolves these issues, hence paving the way for automated key rate calculations.

Specifically, the unreliable (or unphysical) aspect of the primal problem is that it is a minimization, hence the output will in general be an upper bound on the key rate. But one is typically more interested in reliable lower bounds, that is, physically achievable key rates. Transforming to the dual problem allows one to formulate the problem as a maximization, and hence approach the key rate from below. Therefore, every number outputted from our computer program represents an achievable asymptotic key rate, even if the computer did not reach the global maximum.

The inefficient aspect of the primal problem is that the number of parameters grows as $d_A^2 d_B^2$ for a state ρ_{AB} with $d_A = \dim(\mathcal{H}_A)$ and $d_B = \dim(\mathcal{H}_B)$. For example, if $d_A = d_B = 10$, the number of parameters that one would have to optimize over is 10,000. In contrast, in the dual problem, the number of parameters is equal to the number of experimental constraints that Alice and Bob choose to impose. For example, in the generalization of the BB84 protocol to arbitrary dimensions[17,18], Alice and Bob typically consider two constraints, their error rates in the two mutually-unbiased bases (MUBs). So, for this protocol, we have reduced the number of parameters to something that is constant in dimension. We, therefore, believe that our approach (of solving the dual problem) is ideally suited to efficiently calculate key rates in high dimensions.

We have written a MATLAB program to implement our key rate calculations. To illustrate the validity of our program, we show (Fig. 1) that it exactly reproduces the known theoretical dependence of the key rate on error rate, for both the BB84 and six-state protocols.

But ultimately the strength of our approach is its ability to handle unstructured protocols. We demonstrate this by investigating some unstructured protocols for which the key rates were not previously known. For example, we study a general class of protocols where Alice and Bob measure n MUBs, with $2 \leq n \leq d+1$, in dimension d. Also, we investigate the B92 protocol[19], which involves two signal states whose inner product is arbitrary. Our key rates are higher than known analytical lower bounds[20,21] for B92. Finally, we argue that our approach typically gives markedly higher key rates than those obtained from an analytical approach based on the entropic uncertainty relation[22,23].

We focus on asymptotic key rates in this work. Nevertheless, the optimization problem that we solve is also at the heart of

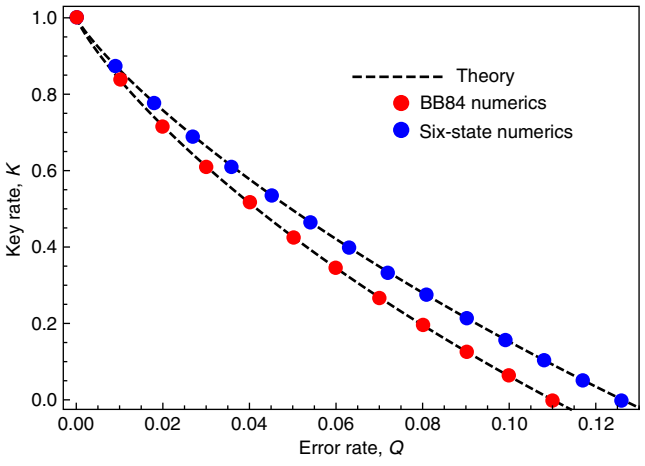

Figure 1 | Key rate for two well-known QKD protocols. Here we compare our numerics (from Theorem 1) with the theoretical curves. The results of our numerical optimization for the BB84 and six-state protocols are respectively shown as red and blue dots. The known theoretical curves for these protocols are also shown as black dashed lines. The dots should be viewed as reliable lower bounds on the key rate, but in this case they happen to be perfectly tight, coinciding with the theoretical curves.

finite-key analysis, for example, see refs 24,25. We, therefore, hope to extend our approach to the finite-key scenario in future efforts. We remark that finite-size effects generally reduce the key rate below its asymptotic value.

In what follows, we first present our main result: a reformulation of the key rate optimization problem in such a way that it is easily computable. We then outline our general framework for treating a broad range of protocols. Finally, we illustrate our approach with various examples.

Results

Setup of the problem. Consider a general entanglement-based QKD protocol involving finite-dimensional quantum systems A and B that are respectively received by Alice and Bob. Note that prepare-and-measure QKD protocols can be recast as entanglement-based protocols, as discussed below. For simplicity of presentation, we consider protocols where Alice's raw key is derived from a measurement on her system, possibly after some post-selection corresponding to a public announcement with a binary outcome, 'pass' or 'fail'. However, our approach can easily be extended to more general protocols.

Let Z_A (Z_B) denote the measurement that Alice (Bob) performs on system A (B) to derive the raw key. Suppose they use one-way direct reconciliation for the classical post-processing and that their error correction is optimal (that is, leaks out the minimum number of bits), then the asymptotic key rate is given by the Devetak–Winter formula[15]:

$$K = H(Z_A|E) - H(Z_A|Z_B). \tag{1}$$

In equation (1), $H(X|Y) := H(\rho_{XY}) - H(\rho_Y)$ is the conditional von Neumann entropy, with $H(\sigma) := -\mathrm{Tr}\left(\sigma \log_2 \sigma\right)$, and

$$\rho_{Z_A Z_B} = \sum_{j,k} \mathrm{Tr}\left[\left(Z_A^j \otimes Z_B^k\right)\rho_{AB}\right] |j\rangle\langle j| \otimes |k\rangle\langle k|, \tag{2}$$

$$\rho_{Z_A E} = \sum_j |j\rangle\langle j| \otimes \mathrm{Tr}_A\left[\left(Z_A^j \otimes \mathbb{1}\right)\rho_{AE}\right]. \tag{3}$$

Here ρ_{ABE} is the tripartite density operator shared by Alice, Bob and Eve (and it may be the state after some post-selection procedure, see our general framework below). Also, $\{Z_A^j\}$ and $\{Z_B^k\}$ are the sets of positive operator valued measure (POVM) elements associated with Alice's and Bob's key-generating measurements. In what follows we refer to $\{Z_A^j\}$ as the key-map POVM.

In the previous paragraph and in what follows, we assume that the state shared by Alice, Bob and Eve has an i.i.d. (independent, identically distributed) structure, and hence it makes sense to discuss the state ρ_{ABE} associated with a single round of quantum communication. To avoid confusion, we emphasize that our approach is 'unstructured' in the sense of lacking structure for a given round of quantum communication, but we do impose the i.i.d. structure that relates one round to other rounds. This i.i.d. structure corresponds to Eve doing a so-called collective attack. However, the security of our derived asymptotic key rate also holds against the most general attacks (coherent attacks) if one imposes that the protocol involves a random permutation of the rounds (a symmetrization step) such that the de Finetti theorem[26,27] or the post-selection technique[28] applies.

Typically, Alice's and Bob's shared density operator ρ_{AB} is unknown to them. A standard part of QKD protocols is for Alice and Bob to gather data through local measurements, and in a procedure known as parameter estimation, they use this data to constrain the form of ρ_{AB}. The measurements used for this purpose can, in general, be described by bounded Hermitian operators Γ_i, with the set of such operators denoted by $\vec{\Gamma} = \{\Gamma_i\}$.

From their data, Alice and Bob determine the average value of each of these measurements:

$$\vec{\gamma} = \{\gamma_i\}, \quad \text{with } \gamma_i := \langle \Gamma_i \rangle = \mathrm{Tr}(\rho_{AB}\Gamma_i), \tag{4}$$

and this gives a set of experimental constraints:

$$C = \{\mathrm{Tr}(\rho_{AB}\Gamma_i) = \gamma_i\}. \tag{5}$$

We denote the set of density operators that are consistent with these constraints as:

$$\mathcal{C} = \{\rho_{AB} \in \mathcal{P}_{AB} : C \text{ holds}\} \tag{6}$$

where $\mathcal{P}_{AB}$ denotes the set of positive semidefinite operators on $\mathcal{H}_{AB}$, and an additional constraint $\langle \mathbb{1} \rangle = 1$ is assumed to be added to the set C to enforce normalization.

Because Alice and Bob typically do not perform full tomography on the state, $\mathcal{C}$ includes many density operators, and hence the term $H(Z_A|E)$ in equation (1) is unknown. To evaluate the key rate, Alice and Bob must consider the most pessimistic of scenarios where $H(Z_A|E)$ takes on its smallest possible value that is consistent with their data. This is a constrained optimization problem, given by

$$K = \min_{\rho_{AB} \in \mathcal{C}} [H(Z_A|E) - H(Z_A|Z_B)] \tag{7}$$

where Eve's system E can be assumed to purify ρ_{AB} since it gives Eve the most information. Here the number of parameters in the optimization is $(d_A d_B)^2$, corresponding to the number of parameters in a positive semidefinite operator on $\mathcal{H}_{AB}$. We refer to equation (7) as the primal problem.

Main result. Our main result is a reformulation of the optimization problem in equation (7).

Theorem 1: The solution of the minimization problem in equation (7) is lower bounded by the following maximization problem:

$$K \geq \frac{\Theta}{\ln 2} - H(Z_A|Z_B) \tag{8}$$

where

$$\Theta := \max_{\vec{\lambda}} \left(-\left\| \sum_j Z_A^j R\left(\vec{\lambda}\right) Z_A^j \right\| - \vec{\lambda} \cdot \vec{\gamma} \right), \tag{9}$$

and

$$R\left(\vec{\lambda}\right) := \exp\left(-\mathbb{1} - \vec{\lambda} \cdot \vec{\Gamma} \right). \tag{10}$$

In equation (9), the optimization is over all vectors $\vec{\lambda} = \{\lambda_j\}$, where the λ_i are arbitrary real numbers and the cardinality of $\vec{\lambda}$ is equal to that of $\vec{\Gamma}$. Also, $\|M\|$ denotes the supremum norm of M, which is the maximum eigenvalue of M when M is positive semidefinite, as in equation (9).

The proof of Theorem 1 is given in the Methods section. It relies on the duality of convex optimization problems, as well as some entropic identities that allow us to simplify the dual problem. Note that the term $H(Z_A|Z_B)$ in equation (8) is pulled outside of the optimization since Alice and Bob can compute it directly from their data.

The cardinalities of the sets $\vec{\lambda}$ and $\vec{\Gamma}$ are the same. This means that the number of parameters λ_i that one must optimize over, to solve equation (9), is equal to the number of experimental constraints that Alice and Bob have. (More precisely this is the number of independent constraints, since one can eliminate constraints that carry redundant information.) This has the potential to be significantly less than the number of parameters in the primal problem. Indeed, we demonstrate below that equation (9) can be easily solved using MATLAB on a personal computer for a variety of interesting QKD protocols.

Formulating constraints. For a given protocol, how does one decide which constraints to include in the set C? Consider the following remarks. First, adding in more constraints will never decrease the key rate obtained from our optimization. This follows since adding a new constraint gives an additional λ_i to maximize over, while setting this new λ_i to zero recovers the old problem. Second, coarse-graining constraints, that is, merging two constraints $\langle\Gamma_i\rangle=\gamma_i$ and $\langle\Gamma_j\rangle=\gamma_j$ into a single constraint $\langle\Gamma_i+\Gamma_j\rangle=\gamma_i+\gamma_j$, will never increase the key rate obtained from our optimization. This follows since merging two constraints means that two λ_i's are merged into a single λ_i, thus restricting the optimization. Hence, to obtain the highest key rates, one should input all of one's refined knowledge that is available into our optimization. On the other hand, coarse graining reduces the number of constraints and thus may help to simplify the optimization problem, possibly at the cost of a reduced key rate.

One's refined knowledge is captured as follows. In a general entanglement-based protocol, Alice measures a POVM (whose elements may be non-commuting, for example, if she randomly measures one of two MUBs), which we denote as $\Gamma_A=\{\Gamma_{A,i}\}$. Likewise Bob's corresponding POVM is $\Gamma_B=\{\Gamma_{B,i}\}$. Hence, through public discussion, Alice and Bob obtain knowledge of expectation values of the form

$$\mathrm{Tr}\left[\rho_{AB}\left(\Gamma_{A,i}\otimes\Gamma_{B,j}\right)\right]=\gamma_{ij},\quad \text{for each } i,j. \tag{11}$$

These constraints form the set C in equation (5). We remark that it is common in the QKD field to express correlations in terms of average error rates rather than in terms of the joint probability distribution in equation (11). This is an example of the coarse graining that we mentioned above. For simplicity of presentation, we will do this sort of coarse graining for some protocols that we investigate below, although equation (11) represents our general framework for constructing C.

Framework for prepare and measure. While our approach is stated in the entanglement-based scenario, let us note how it applies to prepare-and-measure protocols. Consider a prepare-and-measure protocol involving a set of N signal states $\{|\phi_j\rangle\}$, which Alice sends with probabilities $\{p_j\}$. It is well-known that prepare-and-measure protocols can be recast as entanglement-based protocols using the source-replacement scheme (see, for example, refs 4,8,29). Namely, one forms the entangled state:

$$|\psi_{AA'}\rangle=\sum_j\sqrt{p_j}|j\rangle|\phi_j\rangle. \tag{12}$$

One imagines that Alice keeps system A, while system A' is sent over an insecure quantum channel $\mathcal{E}$ to Bob, resulting in

$$\rho_{AB}=(\mathcal{I}\otimes\mathcal{E})(|\psi_{AA'}\rangle\langle\psi_{AA'}|). \tag{13}$$

The numerical optimization approach described above can then be applied to the state ρ_{AB} in equation (13). However, in addition to the constraints obtained from Alice's and Bob's measurement results, we must add in further constraints to account for the special form of ρ_{AB}. In particular, note that the partial trace over B gives

$$\rho_A=\sum_{j,k}\sqrt{p_jp_k}\langle\phi_k|\phi_j\rangle|j\rangle\langle k|. \tag{14}$$

The form of ρ_A, which is closely related to Gram matrix, depends on the inner products between the signal states, which (we assume) Alice knows. Suppose $\{\Omega_i\}$ is a set of tomographically complete observables on system A, then one can add in the calculated expectation values $\{\omega_i\}$ of these observables into the set of constraints. That is, add

$$\langle\Omega_i\otimes\mathbb{1}\rangle=\omega_i,\quad \text{for each } i \tag{15}$$

to the set C in equation (5). This will capture Alice's knowledge of her reduced density operator.

Framework for decoy states. In decoy-state QKD[30], which aims to combat photon-number splitting attacks, Alice prepares coherent states of various intensities and then randomizes their phases before sending them to Bob. Our framework can handle decoy states simply by allowing for additional signal states to be added to the set $\{|\phi_j\rangle\}$ in equation (12). For example, to treat decoy protocols with partial phase randomization[31], one can consider signal states that are bipartite (on the signal mode S and the reference mode R) of the form

$$\left|\phi_{jkl}\right\rangle=\left|\alpha_j e^{i(\theta_k+\phi_l)}\right\rangle_S\otimes\left|\alpha_j e^{i\theta_k}\right\rangle_R \tag{16}$$

where α_j is the amplitude of the coherent state associated with the jth intensity setting, θ_k is the kth phase used in phase randomization, and ϕ_l is the phase Alice uses to encode her information (for example, for generating key). Decoy protocols with complete phase randomization are also treatable in our framework, namely, by adding in a signal state for each photon-number basis state (up to a cutoff), and treating multi-photon signals as orthogonal states (so-called 'tagged states') since Eve can perfectly distinguish them.

Framework for MDI QKD. A special kind of prepare-and-measure protocol is measurement-device-independent (MDI) QKD[32]. In MDI QKD, Alice prepares states $\{|\phi_j\rangle\}$ with probabilities $\{p_j\}$ and sends them to Charlie, and Bob does the same procedure as Alice (Fig. 2). Charlie typically does a Bell-basis measurement, however the security proof does not assume this particular form of measurement. Charlie announces the outcome of his measurement, which we denote by the classical register M. Our framework for treating MDI QKD considers the tripartite state ρ_{ABM}, where A and B, respectively, are Alice's and Bob's systems in the source-replacement scheme, playing the same role as system A in equation (12) (see Supplementary Note 1 for elaboration). For our numerics, we impose the constraint that the marginal $\rho_{AB}=\rho_A\otimes\rho_B$ is fixed (since Eve cannot access A and B), with ρ_A and ρ_B given by the form in equation (14). We enforce this constraint using the same approach as used in

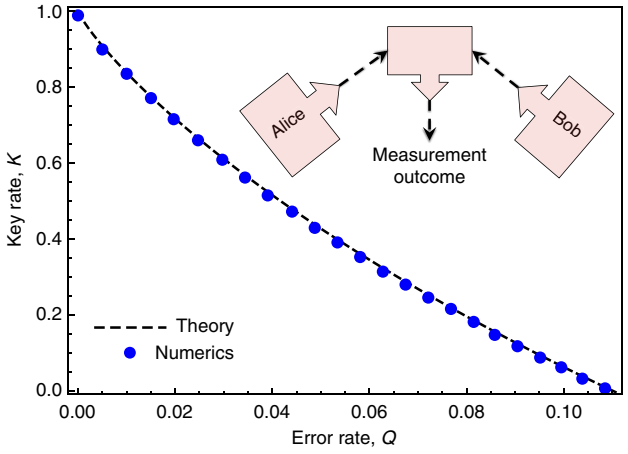

Figure 2 | Key rate for MDI QKD with the BB84 signal states. The inset shows the basic idea of MDI QKD: Alice and Bob each prepare a signal state and send it to an untrusted node, which performs an (untrusted) Bell-basis measurement and announces the outcome. Our numerics (circular dots) essentially reproduce the known theoretical dependence of the key rate on the error rate (dashed curve), which is the same expression as that given in (20). See Supplementary Note 1 for elaboration.

equation (15) to fix ρ_A for prepare-and-measure protocols. The only other constraints we impose are the usual correlation constraints, that is, a description of the joint probability distribution for the standard bases on A, B and M, of the form

$$\mathrm{Tr}[\rho_{ABM}(|j\rangle\langle j| \otimes |k\rangle\langle k| \otimes |m\rangle\langle m|)] = \gamma_{jkm}. \quad (17)$$

Framework for post-selection and announcements. In general, a QKD protocol may involve post-selection. As an example, if Alice sends photons to Bob over a lossy channel, then they may post-select on rounds in which Bob detects a photon. As noted above, for simplicity we consider protocols where the post-selection involves a binary announcement, and Alice and Bob keep (discard) rounds when 'pass' ('fail') is announced. Let $\mathcal{G}$ be the completely positive linear map corresponding to the post-selection. The action of $\mathcal{G}(\cdot)=G(\cdot)G^\dagger$ is given by a single Kraus operator G, corresponding to the 'pass' announcement.

The key rate formula (1) should be applied to the post-selected state:

$$\tilde{\rho}_{AB} = \mathcal{G}(\rho_{AB})/p_{\mathrm{pass}} \quad (18)$$

where $p_{\mathrm{pass}}=\mathrm{Tr}(\mathcal{G}(\rho_{AB}))$ is the probability for passing the post-selection filter. We remark that since $\mathcal{G}$ is given by a single Kraus operator, it maps pure states to pure states, and hence taking Eve's system to purify the post-selected state $\tilde{\rho}_{AB}$ is equivalent to taking it to purify ρ_{AB}. Hence applying the key rate formula to $\tilde{\rho}_{AB}$ does not give Eve access to any more than she already has, and hence does not introduce any looseness into our bound. Future extension of our work to more general maps $\mathcal{G}$ will need to carefully account for how Eve's system is affected by $\mathcal{G}$, so as not to lose key rate from this proof technique.

The only issue is that Alice's and Bob's experimental constraints C in equation (5) are still in terms of state ρ_{AB}. To solve for the key rate, one must transform these constraints into constraints on $\tilde{\rho}_{AB}$. For the special case where $\mathcal{G}$ has an inverse $\mathcal{G}^{-1}$ that is also completely positive, one can simply insert the identity channel $\mathcal{I}=\mathcal{G}^{-1}\mathcal{G}$ into the expression $\mathrm{Tr}(\rho_{AB}\Gamma_i)=\mathrm{Tr}(\mathcal{G}^{-1}\mathcal{G}(\rho_{AB})\Gamma_i)$. Using cyclic permutation under the trace, we transform equation (5) into a set of constraints on $\tilde{\rho}_{AB}$,

$$\tilde{C} = \{\mathrm{Tr}(\tilde{\rho}_{AB}\tilde{\Gamma}_i) = \tilde{\gamma}_i\}. \quad (19)$$

where the $\tilde{\Gamma}_i = (\mathcal{G}^{-1})^\dagger(\Gamma_i)$ are Hermitian operators, with $(\mathcal{G}^{-1})^\dagger$ being the adjoint of $\mathcal{G}^{-1}$, and $\tilde{\gamma}_i=\gamma_i/p_{\mathrm{pass}}$. Note that p_{pass} is determined experimentally and hence the $\tilde{\gamma}_i$ are known to Alice and Bob. More generally, we provide a method for obtaining $\tilde{C}$ for arbitrary $\mathcal{G}$, as described in Supplementary Note 2.

We remark that public announcements can be treated with a simple extension of our post-selection framework. While our framework directly applies to announcements with only two outcomes corresponding to 'pass' or 'fail' (as discussed above), more general announcements can be treated by adding classical registers that store the announcement outcomes. Our treatment of MDI QKD is an example of this approach (Fig. 2 and Supplementary Note 1). Additional examples that could be treated in this way are protocols with two-way classical communication[33] such as advantage distillation.

Outline of examples. We now illustrate our numerical approach for lower bounding the key rate by considering some well-known protocols. First, we consider the BB84 and six-state protocols (Fig. 1), MDI QKD with BB84 states (Fig. 2), and the generalized BB84 protocol involving two MUBs in any dimension (Fig. 3). In each case, the dependence of the key rate on error rate is known, and we show that our numerical approach exactly reproduces these theoretical dependences. After considering these structured protocols, we move on to using our numerical optimization for its intended purpose: studying unstructured protocols. The fact that our bound is tight for the structured protocols mentioned above gives reason to suspect that we will get strong bounds in the unstructured case. We investigate below a protocol involving n MUBs, a protocol involving bases with arbitrary angle between them, and the B92 protocol.

BB84 example. Consider an entanglement-based version of the BB84 protocol[3], where Alice and Bob each receive a qubit and measure either in the $Z=\{|0\rangle, |1\rangle\}$ or $X=\{|+\rangle, |-\rangle\}$ basis, where $|\pm\rangle=(|0\rangle \pm |1\rangle)/\sqrt{2}$. For all protocols that we discuss, we assume perfect sifting efficiency, which can be accomplished asymptotically via asymmetric basis choice[34]. Let us suppose that Alice and Bob each use their Z basis to generate key. For simplicity, suppose they observe that their error rates in the Z and X bases are identical and equal to Q, then it is known (see, for example, ref. 4) that the key rate is given by

$$K = 1 - 2h(Q) \quad (20)$$

where $h(p) := -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy.

To reproduce this result using our numerics, we write the optimization problem as follows:

$$\text{Key-map POVM: } Z_A = \{|0\rangle\langle 0|, |1\rangle\langle 1|\} \quad (21)$$

$$\text{Constraints: } \langle \mathbb{1} \rangle = 1 \quad (22)$$

$$\langle E_X \rangle = Q \quad (23)$$

$$\langle E_Z \rangle = Q \quad (24)$$

where the error operators are defined as

$$E_Z := |0\rangle\langle 0| \otimes |1\rangle\langle 1| + |1\rangle\langle 1| \otimes |0\rangle\langle 0| \quad (25)$$

$$E_X := |+\rangle\langle +| \otimes |-\rangle\langle -| + |-\rangle\langle -| \otimes |+\rangle\langle +|. \quad (26)$$

Equations (21)–(24) highlight the fact that, as far as the optimization in equation (9) is concerned, a QKD protocol is defined by the POVM elements used for generating the key and the experimental constraints used for 'parameter estimation' (and also the post-selection map $\mathcal{G}$, but this is trivial for the ideal BB84 protocol). Once these things are specified, the protocol is

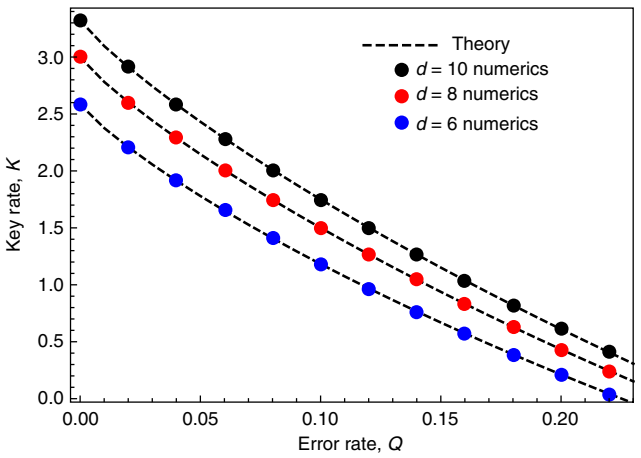

Figure 3 | Higher dimensional analog of BB84, using two MUBs. This plot shows the theoretical key rate as solid curves, and the result of our numerical optimization as circular dots, for $d_A=d_B=d$, with $d=6$ (blue), $d=8$ (red), and $d=10$ (black). Again, the dots should be viewed as reliable lower bounds, but in this case they are perfectly tight.

defined and the key rate is determined. Numerically solving the problem defined in equations (21)–(24) for several values of Q leads to the red dots in Fig. 1, which agree perfectly with the theory curve.

Six state example. Now consider an entanglement-based version of the six-state protocol, where Alice and Bob each measure one of three MUBs (X, Y or Z) on their qubit. Suppose that Alice and Bob observe that their error rates in all three bases are identical, $\langle E_X\rangle = \langle E_Y\rangle = \langle E_Z\rangle = Q$, where

$$E_Y := |y_+\rangle\langle y_+| \otimes |y_+\rangle\langle y_+| + |y_-\rangle\langle y_-| \otimes |y_-\rangle\langle y_-|, \quad (27)$$

with $|y_\pm\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$. (Our definition of E_Y reflects the fact that the standard Bell state is correlated in Z and X but anti-correlated in Y.) To reproduce the known key rate[9,21], we write the optimization problem as:

$$\text{Key-map POVM: } Z_A = \{|0\rangle\langle 0|, |1\rangle\langle 1|\} \quad (28)$$

$$\text{Constraints: } \langle \mathbb{1}\rangle = 1 \quad (29)$$

$$\langle E_{XY}\rangle = Q \quad (30)$$

$$\langle E_Z\rangle = Q, \quad (31)$$

where $E_{XY} := (E_X + E_Y)/2$ quantifies the average error for X and Y. Note that the constraint $\langle E_{XY}\rangle = Q$ is obtained by coarse graining the individual error rates. In theory, one can get a stronger bound on the key rate by splitting up this constraint into $\langle E_X\rangle = Q$ and $\langle E_Y\rangle = Q$. However, our numerics show that this does not improve the key rate, and the constraints in equation (29)–(31) are enough to reproduce the theory curve. Indeed, numerically solving the problem in equation (28)–(31) leads to the blue dots in Fig. 1, which agree with the theory curve.

Two MUBs in higher dimensions example. A distinct advantage of our approach of solving equation (9) instead of the primal problem equation (7) is that we can easily perform the optimization in higher dimensions, where the number of parameters in equation (7) would be quite large. To illustrate this, we consider a generalization of BB84 to arbitrary dimension, where Alice and Bob measure generalized versions of the X and Z bases. This protocol has been implemented, for example, in ref. 18 using orbital angular momentum. Taking Z as the standard basis $\{|j\rangle\}$, Alice's X basis can be taken as the Fourier transform $\{F|j\rangle\}$, where

$$F = \sum_{j,k} \frac{\omega^{-jk}}{\sqrt{d}} |j\rangle\langle k| \quad (32)$$

is the Fourier matrix, with $\omega = e^{2\pi i/d}$, and for simplicity we choose Alice's and Bob's dimension to be equal: $d_A = d_B = d$. Bob's X basis is set to $\{F^*|j\rangle\}$, where F^* denotes the conjugate of F in the standard basis.

Suppose that Alice and Bob observe that their error rates in Z and X are identical. The theoretical key rates[8,17] for the cases $d = 6$, 8, 10 are shown as dashed curves in Fig. 3, while our numerics are shown as circular dots. Clearly there is perfect agreement with the theory.

For our numerics we employ the same constraints as used for BB84 in equation (21)–(24), but generalized to higher d. We again emphasize that the calculation of Θ here is very efficient and can easily handle higher dimension. This is because the number of parameters one is optimizing over is independent of dimension—equal to the number of constraints, which in this case is 3. This is in sharp contrast to the primal problem in equation (7), where the number of parameters is d^4, which would be 10,000 for $d = 10$.

***n* MUBs example**. A simple generalization of the above protocols is to consider a set of n MUBs in dimension d. For example, in prime power dimensions there exist explicit constructions for sets of n MUBs with $2 \leqslant n \leqslant d+1$ (ref. 35). Consisder a protocol where we fix the set of n MUBs, and in each round, Alice and Bob each measure their d dimensional system in one basis chosen from this set. For general n the symmetry group is not known for this protocol[8], so one can consider it an unstructured protocol. Indeed, only for the special cases $n = 2$ and $n = d+1$ do we have analytical formulas for the key rate[8]. Nevertheless it is straightforward to apply our numerics to this protocol for any n. Our results are shown in Fig. 4 for $d = 5$. To obtain these curves we only need three constraints, which are analogous to equation (29)–(31), but generalized such that $\langle E_{XY}\rangle$ is replaced by the average error rate in all $n-1$ bases, excluding the basis used for key generation (the Z basis).

Interestingly, Fig. 4 shows that just adding one basis, going from $n = 2$ to $n = 3$, gives a large jump in the key rate, whereas there are diminishing returns as one adds more bases. This can be seen in the inset of Fig. 4, which plots the error tolerance (that is, the value of Q for which the key rate goes to zero) as a function of n. We have seen similar behaviour for other d besides $d = 5$. After completion of this work, an analytical formula for $n = 3$ was discovered[36], and we have verified that it agrees perfectly with our numerics.

In Supplementary Note 3, we analytically prove the following.

Proposition 2: Our numerical results are perfectly tight for the protocols discussed in Figs 1,3 and 4. That is, for these protocols, our optimization exactly reproduces the primal optimization (equation (7)).

Note that this observation implies that key rate for protocols involving n MUBs (as in Fig. 4) is now known; namely it is given by our numerical optimization.

Arbitrary angle between bases example. While MUBs are a special case, our approach can handle arbitrary angles between the different measurements or signal states. For example, we consider a simple qubit protocol[37] where Alice and Bob each measure either the Z or W basis, where W is rotated by an angle θ away from the ideal X basis. This protocol provides the

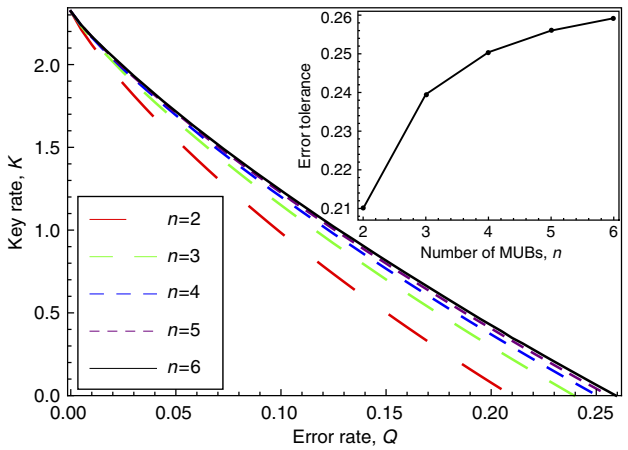

Figure 4 | Protocol where Alice and Bob each use *n* MUBs. The key rate is plotted for various $n \in \{2, 3, 4, 5, 6\}$ and for $d_A = d_B = 5$. This is an unstructured protocol, since for intermediate values of n the symmetry group and hence the key rate is unknown. However, our numerics provides the dependence of key rate on error rate for any n, as shown. The inset shows the error tolerance—the smallest error rate that makes the key rate vanish—as a function of n. Note that the largest jump in the error tolerance occurs from $n = 2$ to $n = 3$.

opportunity to compare our numerical approach to an analytical approach based on the entropic uncertainty principle, introduced in refs 22,23. This is the state-of-the-art method for lower bounding the key rate. So for comparison, Fig. 5 plots the bound obtained from the entropic uncertainty principle for bases Z and W.

We apply our numerical approach with the constraints:

$$\text{Constraints: } \langle \mathbb{1} \rangle = 1 \tag{33}$$

$$\langle \sigma_W \otimes \sigma_W \rangle = 1 - 2Q \tag{34}$$

$$\langle \sigma_Z \otimes \sigma_Z \rangle = 1 - 2Q \tag{35}$$

$$\langle \sigma_Z \otimes \sigma_W \rangle = \langle \sin\theta \rangle (1 - 2Q) \tag{36}$$

$$\langle \sigma_W \otimes \sigma_Z \rangle = (\sin\theta)(1 - 2Q), \tag{37}$$

where σ_Z and σ_W are the Pauli operators associated with the Z and W bases. Figure 5 plots a hierarchy of lower bounds obtained from gradually adding in more of the constraints in equation (33)–(37). As the plot shows, we already beat the entropic uncertainty principle with only the first two constraints. Furthermore, adding in all these constraints gives a markedly higher bound, showing the uncertainty principle gives highly pessimistic key rates for this protocol. From an experimental perspective, Fig. 5 is reassuring, in that small variations in θ away from the ideal BB84 protocol ($\theta = 0$) have essentially no effect on the key rate. Figure 5 also highlights the fact that our approach allows us to systematically study the effect on the key rate of Alice and Bob using more or less of their data. In this example, we see that it is useful to keep data that one will usually discard in the sifting step of the protocol.

B92 example. Next we consider the B92 protocol[19], which is a simple, practical and unstructured protocol. It nicely illustrates our framework because it is inherently a prepare-and-measure protocol and it involves post-selection. In the protocol, Alice sends one of two non-orthogonal states $\{|\phi_0\rangle, |\phi_1\rangle\}$ to Bob. Since the Bloch-sphere angle θ between the two states is arbitrary, with $\langle\phi_0|\phi_1\rangle = \cos(\theta/2)$, the protocol is unstructured. Bob randomly (with equal probability) measures either in basis $B_0 = \{|\phi_0\rangle, |\overline{\phi_0}\rangle\}$ or basis $B_1 = \{|\phi_1\rangle, |\overline{\phi_1}\rangle\}$, where $\langle\phi_0|\overline{\phi_0}\rangle = \langle\phi_1|\overline{\phi_1}\rangle = 0$. If Bob gets outcome $|\overline{\phi_0}\rangle$ or $|\overline{\phi_1}\rangle$, then he publicly announces 'pass', and he assigns a bit value of 1 or 0, respectively, to his key. Otherwise, Bob announces 'fail' and they discard the round.

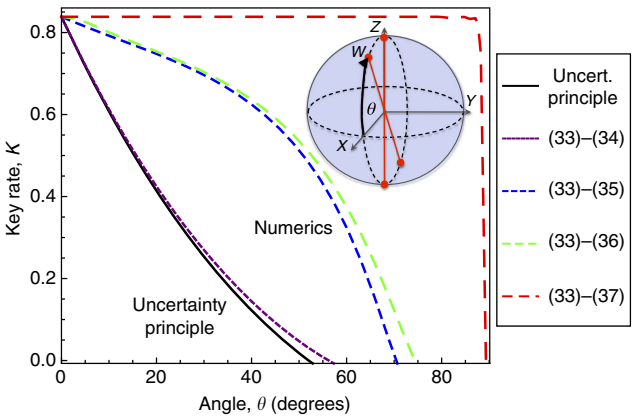

Figure 5 | Protocol where Alice and Bob each measure *Z* or *W*. Here Z is the standard basis and the W basis is rotated by an angle θ away from the X basis. The key rate versus θ is shown with the error rate set to $Q = 0.01$. Our numerics give a hierarchy of four lower bounds on the key rate, corresponding to adding in additional constraints from (33)-(37). All of our bounds are tighter than the bound obtained from the entropic uncertainty principle. The plot indicates that the uncertainty principle gives a dramatically pessimistic key rate, much lower than the true key rate of the protocol.

A detailed description of the constraints we employed for B92 can be found in Supplementary Note 4. Our numerical results are shown in Fig. 6. Figure 6 shows that the optimal angle for maximizing key rate depends on the depolarizing noise p, although small deviations $\pm 5°$ from the optimal angle do not affect the key rate much.

Our results give higher key rates for B92 than refs 20 and 21, which respectively predicted positive key rates for $p \leqslant 0.034$ and $p \leqslant 0.048$, while we predict it for $p \leqslant 0.053$. On the other hand, ref. 38 directly solved the primal problem equation (7) for B92 by brute-force numerics, and achieves positive key rate for $p \leqslant 0.065$. We have verified that the gap between our results and those of ref. 38 is due to the looseness of our usage of the Golden-Thompson inequality (equation (60) in the Methods section). However, ref. 38 only showed a plot for $p \geqslant 0.046$, noting that the numerical optimization for the primal problem did not converge for smaller p values. This highlights a benefit of going to the dual problem, in that we have no trouble with obtaining the full dependence on p.

Discussion

In conclusion, we address one of the main outstanding problems in QKD theory: how to calculate key rates for arbitrary protocols. Our main result is a numerical method for lower-bounding key rates that is both efficient and reliable. It is reliable in the sense that, by reformulating the problem as a maximization, every solution that one's computer outputs is an achievable key rate. It is efficient in the sense that we have reduced the number of parameters in the optimization problem from $d_A^2 d_B^2$ down to the number of experimental constraints, which in some cases is independent of dimension.

The motivation for our work is twofold. First, experimental imperfections tend to break symmetries, so theoretical techniques that exploit symmetries do not apply. Hence, there is no general method currently available for calculating the effect of imperfections on the key rate. Second, it is interesting to ask whether protocols that are intentionally designed to lack symmetry might outperform the well-known symmetric protocols. Such a question cannot be posed without a method for calculating key rates for unstructured protocols. Just to give an example where the key rate is currently unknown, we plan to apply our approach to protocols

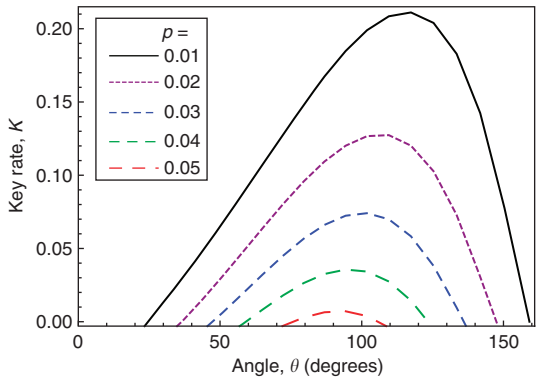

Figure 6 | The B92 protocol. The key rate (in bits per photon sent by Ailce) is plotted versus the Bloch-sphere angle between the two signal states. Curves are shown for various values of the depolarizing probability p.

where a small, discrete set of coherent states are the signal states and information is encoded in the phase[39].

We envision that our method could be a standard tool for QKD researchers. In future work we hope to extend our approach to the finite-key scenario. Indeed, the optimization problem we solve is closely related to one appearing in finite-key analysis[24].

Methods

Outline. Here we prove our main result, Theorem 1. Our proof relies on several technical tools. First is the notion of the duality of optimization, that is, transforming the primal problem to its dual problem. Second, we employ several entropic identities to simplify the dual problem. Third, we use a recent, important result from ref. 40 that solves a relative entropy optimization problem.

For readability, we prove Theorem 1 here for the special case where the key map POVM $Z_A=\{Z_A^j\}$ is a projective measurement, that is, where the Z_A^j are projectors (of arbitrary rank). We postpone the proof for arbitrary POVMs to Supplementary Note 5.

The primal problem. First we rewrite equation (7) as:

$$K=\left[\min_{\rho_{AB}\in\mathcal{C}} H(Z_A|E)\right]-H(Z_A|Z_B), \tag{38}$$

noting that the second term in equation (38), $H(Z_A|Z_B)$, will be determined experimentally and hence can be pulled out of the optimization. We remark that, simply for illustration purposes we used Fano's inequality to upper-bound $H(Z_A|Z_B)$ in our figures; however, in practice $H(Z_A|Z_B)$ would be directly calculated from the data.

Since we only need to optimize the first term, we redefine the primal problem as

$$\alpha:=\min_{\rho_{AB}\in\mathcal{C}} H(Z_A|E), \tag{39}$$

and note that we can take E to be a purifying system of ρ_{AB}, since that gives Eve the most information. Next we use a result for tripartite pure states $\rho_{ABE}=|\psi\rangle\langle\psi|_{ABE}$ from refs 41,42 that relates the conditional entropy to the relative entropy:

$$H(Z_A|E)=D\left(\rho_{AB}\middle\|\sum_j Z_A^j\rho_{AB}Z_A^j\right) \tag{40}$$

where the relative entropy is defined by

$$D(\sigma\|\tau):=\mathrm{Tr}\left(\sigma\log_2\sigma\right)-\mathrm{Tr}\left(\sigma\log_2\tau\right). \tag{41}$$

We remark that the joint convexity of the relative entropy implies that the right-hand side of equation (40) is a convex function of ρ_{AB}. (See ref. 43 for an alternative proof of convexity.) Because of this, and the fact that the constraints in equation (5) are linear functions of ρ_{AB}, equation (39) is a convex optimization problem[16].

It is interesting to point out the connection to coherence[44]. For some set of orthogonal projectors $\Pi=\{\Pi^j\}$ that decompose the identity, $\sum_j\Pi^j=\mathbb{1}$, the coherence (sometimes called relative entropy of coherence) of state ρ is defined as[44]:

$$\Phi(\rho,\Pi)=D\left(\rho\middle\|\sum_j\Pi^j\rho\Pi^j\right). \tag{42}$$

Rewriting the primal problem in terms of coherence gives

$$\alpha=\min_{\rho_{AB}\in\mathcal{C}}\Phi(\rho_{AB},Z_A). \tag{43}$$

Hence, we make the connection that calculating the secret key rate is related to optimizing the coherence.

This observation is important since the coherence is a continuous function of ρ (Supplementary Note 6). This allows us to argue in Supplementary Note 6 that our optimization problem satisfies the strong duality criterion[16], which means that the solution of the dual problem is precisely equal to that of primal problem.

The dual problem. Now we transform to the dual problem. Due to a pesky factor of ln(2), it is useful to rescale the primal problem as follows:

$$\hat{\alpha}:=\alpha\ln(2)=\min_{\rho_{AB}\in\mathcal{C}}\hat{\Phi}(\rho_{AB},Z_A) \tag{44}$$

where, henceforth, we generally use the notation $\hat{M}:=M\ln(2)$, for any quantity M. The dual problem[16] of equation (44) is given by the following unconstrained optimization:

$$\hat{\beta}=\max_{\vec{\lambda}}\min_{\rho_{AB}\in\mathcal{C}}\mathcal{L}\left(\rho_{AB},\vec{\lambda}\right) \tag{45}$$

where $\mathcal{P}$ is the set of positive semidefinite operators:

$$\mathcal{P}=\{\rho_{AB}\in\mathcal{H}_{d_Ad_B}:\rho_{AB}\geqslant 0\}. \tag{46}$$

Here the Lagrangian is given by

$$\mathcal{L}\left(\rho_{AB},\vec{\lambda}\right):=\hat{\Phi}(\rho_{AB},Z_A)+\sum_i\lambda_i[\mathrm{Tr}(\rho_{AB}\Gamma_i)-\gamma_i], \tag{47}$$

where the $\vec{\lambda}=\{\lambda_i\}$ are Lagrange multipliers. Strong duality implies that

$$\hat{\beta}=\hat{\alpha}. \tag{48}$$

In what follows, we go through several steps to simplify the dual problem. It helps to first state the following lemma from refs 42,45.

Lemma 3: For any ρ and $\Pi=\{\Pi^j\}$, the coherence can be rewritten as

$$\Phi(\rho,\Pi)=\min_{\omega\in\mathcal{D}}D\left(\rho\middle\|\sum_j\Pi^j\omega\Pi^j\right) \tag{49}$$

where $\mathcal{D}$ is the set of density operators.

Hence, we have

$$\hat{\Phi}(\rho_{AB},Z_A)=\min_{\sigma_{AB}\in\mathcal{D}}\hat{D}(\rho_{AB}\|\mathcal{Z}_A(\sigma_{AB})), \tag{50}$$

where we define the quantum channel $\mathcal{Z}_A$ whose action on an operator O is given by

$$\mathcal{Z}_A(O):=\sum_j Z_A^jOZ_A^j. \tag{51}$$

Next, we interchange the two minimizations in (45)

$$\min_{\rho_{AB}\in\mathcal{P}}\min_{\sigma_{AB}\in\mathcal{D}}f\left(\rho_{AB},\sigma_{AB},\vec{\lambda}\right)=\min_{\sigma_{AB}\in\mathcal{D}}\min_{\rho_{AB}\in\mathcal{P}}f\left(\rho_{AB},\sigma_{AB},\vec{\lambda}\right) \tag{52}$$

where

$$f\left(\rho_{AB},\sigma_{AB},\vec{\lambda}\right):=\hat{D}(\rho_{AB}\|\mathcal{Z}_A(\sigma_{AB}))+\sum_i\lambda_i(\langle\Gamma_i\rangle-\gamma_i). \tag{53}$$

Ref. 40 solved a relative entropy optimization problem, a special case of which is our problem:

$$\min_{\rho_{AB}\in\mathcal{P}}f\left(\rho_{AB},\sigma_{AB},\vec{\lambda}\right). \tag{54}$$

From ref. 40, the unique solution of equation (54) is

$$\rho_{AB}^*=\exp\left(-\mathbb{1}-\vec{\lambda}\cdot\vec{\Gamma}+\ln(\mathcal{Z}_{\mathbb{A}}(\sigma_{\mathbb{AB}}))\right). \tag{55}$$

Inserting equation (55) into equation (53) gives the optimal value:

$$f\left(\rho_{AB}^*,\sigma_{AB},\vec{\lambda}\right)=-\mathrm{Tr}(\rho_{AB}^*)-\sum_i\lambda_i\gamma_i. \tag{56}$$

In summary, the dual problem becomes

$$\hat{\beta}=\max_{\vec{\lambda}}\eta\left(\vec{\lambda}\right), \tag{57}$$

with

$$\eta\left(\vec{\lambda}\right):=-\max_{\sigma_{AB}\in\mathcal{D}}\left[\mathrm{Tr}(\rho_{AB}^*)+\vec{\lambda}\cdot\vec{\gamma}\right]. \tag{58}$$

A lower bound. We can obtain a simple lower bound on $\eta(\vec{\lambda})$ as follows. The Golden–Thompson inequality states that

$$\mathrm{Tr}(exp(A+B))\leq\mathrm{Tr}(\exp(A)\exp(B)). \tag{59}$$

Applying this inequality gives:

$$\mathrm{Tr}(\rho_{AB}^*)\leq\mathrm{Tr}\left(R\left(\vec{\lambda}\right)\exp(\ln\mathcal{Z}_A(\sigma_{AB}))\right) \tag{60}$$

$$=\mathrm{Tr}\left(R\left(\vec{\lambda}\right)\mathcal{Z}_A(\sigma_{AB})\right) \tag{61}$$

$$=\mathrm{Tr}\left(\mathcal{Z}_A\left(R\left(\vec{\lambda}\right)\right)\sigma_{AB}\right), \tag{62}$$

where $R(\vec{\lambda})=\exp(-\mathbb{1}-\vec{\lambda}\cdot\vec{\Gamma})$ was defined in equation (10). Next, note that

$$\max_{\sigma_{AB}\in\mathcal{D}}\mathrm{Tr}\left(\mathcal{Z}_A\left(R\left(\vec{\lambda}\right)\right)\sigma_{AB}\right)=\left\|\mathcal{Z}_A\left(R\left(\vec{\lambda}\right)\right)\right\|. \tag{63}$$

Hence, we arrive at our final result

$$\hat{\beta}\geq\max_{\vec{\lambda}}\left[-\left\|\mathcal{Z}_A\left(R\left(\vec{\lambda}\right)\right)\right\|-\vec{\lambda}\cdot\vec{\gamma}\right], \tag{64}$$

where the right-hand side is denoted as Θ in Theorem 1.

Data availability. The authors declare that the data supporting the findings in this study are available within the article.

References

1. Campagna, M. *et al. Quantum Safe Cryptography and Security* (European Telecommunications Standards Institute, 2015).
2. Wiesner, S. Conjugate coding. *ACM SIGACT News* **15,** 78–88 (1983).
3. Bennett, C. H. & Brassard, G. in *International Conference on Computers, Systems & Signal Processing* 175–179 (Bangalore, India, 1984).
4. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
5. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8,** 595–604 (2014).
6. Sasaki, M. *et al.* Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19,** 10387–10409 (2011).
7. Wang, S. *et al.* Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **22,** 329–342 (2014).
8. Ferenczi, A. & Lütkenhaus, N. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A* **85,** 052310 (2012).
9. Bruss, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **81,** 3018–3021 (1998).
10. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.* **4,** 325–360 (2004).
11. Fung, C.-H. F. & Lo, H.-K. Security proof of a three-state quantum-key-distribution protocol without rotational symmetry. *Phys. Rev. A* **74,** 042342 (2006).
12. Maroy, O., Lydersen, L. & Skaar, J. Security of quantum key distribution with arbitrary individual imperfections. *Phys. Rev. A* **82,** 032337 (2010).
13. Woodhead, E. Quantum cloning bound and application to quantum key distribution. *Phys. Rev. A* **88,** 012331 (2013).
14. Tamaki, K., Curty, M., Kato, G., Lo, H.-K. & Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A* **90,** 052314 (2014).
15. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A* **461,** 207–235 (2005).
16. Boyd, S. & Vandenberghe, L. *Convex Optimization* (Cambridge University Press, 2004).
17. Sheridan, L. & Scarani, V. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A* **82,** 030301 (2010).
18. Mafu, M. *et al.* Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Phys. Rev. A* **88,** 032305 (2013).
19. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68,** 3121–3124 (1992).
20. Tamaki, K. & Lütkenhaus, N. Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. *Phys. Rev. A* **69,** 032316 (2004).
21. Renner, R., Gisin, N. & Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **72,** 012332 (2005).
22. Berta, M., Christandl, M., Colbeck, R., Renes, J. M. & Renner, R. The uncertainty principle in the presence of quantum memory. *Nat. Phys.* **6,** 659–662 (2010).
23. Tomamichel, M., Ci, C., Lim, W., Gisin, N. & Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3,** 634 (2012).
24. Scarani, V. & Renner, R. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **100,** 200501 (2008).
25. Sano, Y., Matsumoto, R. & Uyematsu, T. Secure key rate of the BB84 protocol using finite sample bits. *J. Phys. A* **43,** 2677–2681 (2010).
26. Renner, R. *Security of Quantum Key Distribution* (PhD Thesis, ETH Zurich, 2005).
27. Renner, R. Symmetry of large physical systems implies independence of subsystems. *Nat. Phys.* **3,** 645–649 (2007).
28. Christandl, M., König, R. & Renner, R. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.* **102,** 020504 (2009).
29. Bennett, C., Brassard, G. & Mermin, N. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68,** 557–559 (1992).
30. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
31. Cao, Z., Zhang, Z., Lo, H.-K. & Ma, X. Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New J. Phys.* **17,** 053014 (2015).
32. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).
33. Gottesman, D. & Lo, H. K. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theory* **49,** 457–475 (2003).
34. Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18,** 133–165 (2004).
35. Bandyopadhyay, S., Boykin, P. O., Roychowdhury, V. & Vatan, F. A new proof for the existence of mutually unbiased bases. *Algorithmica* **34,** 512–528 (2001).
36. Bradler, K., Mirhosseini, M., Fickler, R., Broadbent, A. & Boyd, R. Finite-key security analysis for multilevel quantum key distribution. Preprint at http://arxiv.org/abs/1512.05447 (2015).
37. Matsumoto, R. & Watanabe, S. Narrow basis angle doubles secret key in the BB84 protocol. *J. Phys. A* **43,** 145302 (2010).
38. Matsumoto, R. in *Proceedings of IEEE International Symposium on Information Theory,* 351-353 (2013).
39. Lo, H. & Preskill, J. Security of quantum key distribution using weak coherent states with nonrandom phases. *Quant. Inf. Comput.* **7,** 431–458 (2007).
40. Zorzi, M., Ticozzi, F. & Ferrante, A. Minimum relative entropy for quantum estimation: Feasibility and general solution. *IEEE Trans. Inf. Theory* **60,** 357–367 (2014).
41. Coles, P. J., Yu, L., Gheorghiu, V. & Griffiths, R. B. Information-theoretic treatment of tripartite systems and quantum channels. *Phys. Rev. A* **83,** 062338 (2011).
42. Coles, P. J. Unification of different views of decoherence and discord. *Phys. Rev. A* **85,** 042103 (2012).
43. Watanabe, S., Matsumoto, R. & Uyematsu, T. Tomography increases key rates of quantum-key-distribution protocols. *Phys. Rev. A* **78,** 042316 (2008).
44. Baumgratz, T., Cramer, M. & Plenio, M. B. Quantifying coherence. *Phys. Rev. Lett.* **113,** 140401 (2014).
45. Modi, K., Paterek, T., Son, W., Vedral, V. & Williamson, M. Unified view of quantum and classical correlations. *Phys. Rev. Lett.* **104,** 080501 (2010).

Acknowledgements

We thank Jie Lin, Adam Winick, and Bailey Gu for technical help with the numerics and for obtaining the data in Fig. 2. We thank Yanbao Zhang and Saikat Guha for helpful discussions. We acknowledge support from Industry Canada, Sandia National Laboratories, Office of Naval Research (ONR), NSERC Discovery Grant, and Ontario Research Fund (ORF).

Author contributions

P.J.C. obtained the conceptional main results. E.M.M. contributed the approach to incorporate post-selection and announcements. N.L. conceived and supervised the project. P.J.C. wrote the manuscript with input from E.M.M. and N.L.

Additional information

Supplementary Information accompanies this paper at http://www.nature.com/naturecommunications

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: Coles, P. J. *et al.* Numerical approach for unstructured quantum key distribution. *Nat. Commun.* 7:11712 doi: 10.1038/ncomms11712 (2016).