# Unstructured QKD

Patrick J. Coles and Norbert Lütkenhaus
*Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, N2L3G1 Waterloo, Ontario, Canada*

*Introduction.*—Distribution of secret keys whose security is guaranteed by quantum theory was proposed in Ref. [1], and is known as quantum key distribution (QKD). Both the theory and implementation of QKD have developed dramatically over the past three decades; see, for example, Ref. [2]. The main theoretical problem in QKD is to calculate how much secret key can be distributed by a given protocol. This is the *key rate problem*, where key rate refers to the number of bits of secret key established divided by the number of distributed quantum systems.

Analytical formulas for the key rate are known for protocols that have a high degree of symmetry, such as the BB84 [3] and six-state protocols [4]. Theoretical treatments often exploit the group-theoretic structure (i.e., rotational symmetry) of the signal states in order to determine the optimal eavesdropping strategy [5]. However, experimental imperfections tend to break symmetries. Unfortunately this stifles the study of experimental imperfections. Since theoretical methods work best under symmetric conditions, the effects of imperfections on the key rate are difficult to quantify. A new approach for calculating key rates, that does not rely on symmetry, is needed to address the very important, practical issue of preparation and detection flaws.

Furthermore, it is an interesting question whether (intentionally) asymmetric QKD protocols could offer an advantage over their symmetric counterparts. For example, the three-state protocol from Ref. [6] lacks symmetry. We refer to general QKD protocols involving signal states or measurement choices that lack symmetry (either intentionally or unintentionally) as "unstructured" protocols. Before we can ask questions like, does this unstructured protocol outperform another protocol, we first need a method to calculate key rates for 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 Ref. [7, 8] and qubit protocols in Ref. [9]. Still, there is no general method for computing tight bounds on the key rate for arbitrary unstructured protocols.

*Our approach.*—This motivates our present work, in which we develop an efficient, numerical approach to calculating key rates. Our aim is fairly ambitious. We set out to develop a computer program, where Alice and Bob input a description of their measurement devices 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.

The key rate problem is an optimization problem, since one must minimize the well-known entropic formula for the key rate [10] over all states $\rho_{AB}$ that satisfy Alice's and Bob's experimental data. For two reasons, we find it advantageous to go to the dual problem. First, since the primal problem involves a minimization, the output will in general be an upper bound on the key rate. But one is typically more interested in reliable lower bounds, i.e., 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 key rate, even if the computer did not reach the global maximum.

Second, in many cases, transforming the problem dramatically reduces the number of parameters one must optimize over. For a state $\rho_{AB}$ with $d_A = \dim(\mathcal{H}_A)$ and $d_B = \dim(\mathcal{H}_B)$, the number of parameters is $d_A^2 d_B^2$. For example, if $d_A = d_B = 10$, the number of parameters that one would have to optimize over is 10000. In contrast, in the dual problem, the number of parameters is equal to the number of experimental constraints that Alice and Bob have. For example, in the generalization of the BB84 protocol to arbitrary dimensions [11, 12], Alice and Bob have 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.

*Illustrative examples.*—We have written a MATLAB program to implement our key rate calculations. To illustrate the validity of our program, we show in 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. Likewise, the inset of Fig. 1 shows perfect agreement between theory and our optimization for the generalization of BB84 to higher dimensions involving two MUBs.

But ultimately the strength of our approach is its ability to handle unstructured protocols. We demonstrate this by investigating an unstructured protocol for which the optimal key rates is, to our knowledge, unknown. Namely we consider BB84 but with an arbitrary angle between the two bases that Alice and Bob measure, see

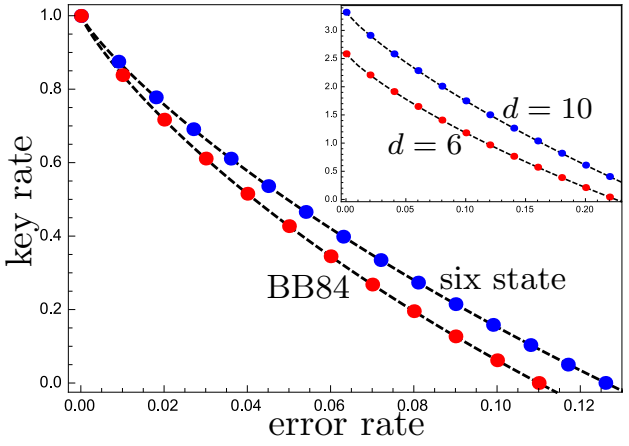


FIG. 1: The known theoretical curve for BB84 and the six-state protocol are shown as black dashed lines, while the results of our numerical optimization are shown as red (BB84) and blue (six state) dots. The dots should be viewed as reliable lower bounds on the key rate, but in this case they are perfectly tight, coinciding with the theoretical curves. (Inset) Higher dimensional analog of BB84, using two MUBs. This plot shows the theoretical key rate as dashed curves, while the results of our numerical optimization are shown as circular dots, for $d = 6$ (red) and $d = 10$ (blue) with $d_A = d_B = d$. Again, there is perfect agreement with the theory curves.

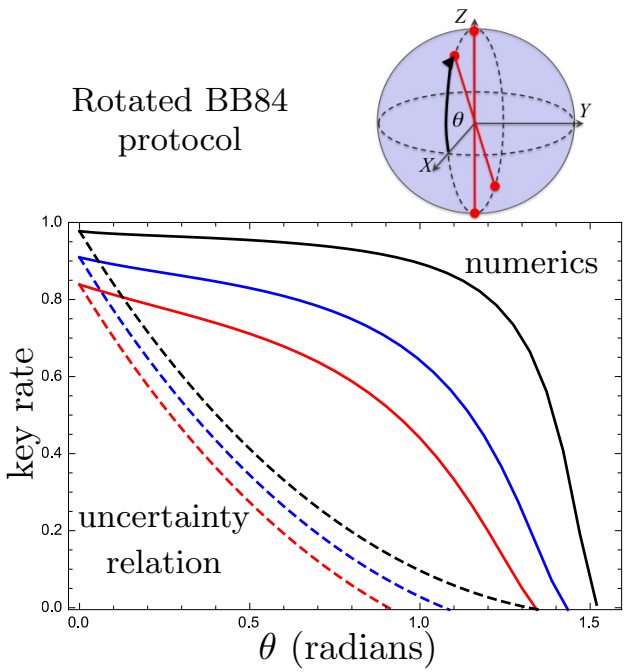


FIG. 2: Comparison of lower bounds on the key rate for the rotated version of BB84, where the $X$ basis is rotated by an angle $\theta$ away from the $x$-axis of the Bloch sphere, such that $\pi/2-\theta$ is the angle between the two bases used in the protocol. The solid curves are the key rates produced by our numerical optimization, while the dashed curves are the corresponding lower bounds obtained from the entropic uncertainty relation. These are shown for error rates of 0.1% (black), 0.5% (blue), and 1% (red). Clearly our numerics are dramatically outperforming the uncertainty relation in this case.

Fig. 2. In a sense, this is a toy model for the BB84 protocol with experimental imperfections associated with angular errors. The solid curves in Fig. 2 show the result of our numerical optimization, for three different error rates.

Let $\theta$ be the angle of rotation of the $X$ basis away from the $x$-axis of the Bloch sphere, see Fig. 2. Naturally, one would expect the key rate to go zero as $\theta \to \pi/2$, since the $X$ basis becomes identical to the $Z$ basis in this limit. But perhaps the most striking feature of the curves in Fig. 2 is *how slowly* these curves to zero as $\theta$ increases. In particular, for small values of $\theta$, our lower bounds on the key rate are fairly flat, with only a mild dependence on $\theta$. In this sense, the BB84 protocol is robust to errors associated with angle variation.

This is in sharp contrast to the lower bounds provided by the entropic uncertainty relation. Refs. [13, 14] discussed how the uncertainty relation can provide a lower bound on the key rate. For the rotated BB84 protocol, we plot these lower bounds as dashed curves in Fig. 2. These bounds have the opposite curvature from, and are much looser than, our numerical bounds. Hence the uncertainty relation paints a much more pessimistic picture of angular errors, as compared to our bounds.

*Technical statement.*—Let us now give a sketch of our main result [21]. Consider a general entanglement-based (EB) QKD protocol involving finite-dimensional quantum systems $A$ and $B$ that are respectively received by Alice and Bob. Let $Z_A$ ($Z_B$) denote the measurement that Alice (Bob) performs on system $A$ ($B$) in order to derive the key. Suppose they use one-way direct reconciliation for the classical post-processing, then the asymptotic key rate for collective attacks is given by the Devetak-Winter formula [10]. Actually, they must minimize this formula over all states $\rho_{AB}$ that are consistent with their experimental data. Our main result is a reformulation of this minimization problem as a maximization, as follows:

$$K \geqslant \left[\max_{\vec{\lambda}} f(\vec{\lambda}, \vec{\Gamma}, \vec{\gamma})\right] - H(Z_A|Z_B) \qquad (1)$$

where $H(Z_A|Z_B)$, the conditional entropy of $Z_A$ given $Z_B$, is known from Alice's and Bob's data. Generally speaking, Alice's and Bob's data can be written as the expectation values of a set $\vec{\Gamma} = \{\Gamma_i\}$ of Hermitian observables $\Gamma_i$, as follows:

$$\langle \Gamma_i \rangle = \mathrm{Tr}(\rho_{AB}\Gamma_i) = \gamma_i, \quad \text{for each } i. \qquad (2)$$

The function $f(\vec{\lambda}, \vec{\Gamma}, \vec{\gamma})$ in (1) depends on the observables $\vec{\Gamma}$ and their expectation values $\vec{\gamma} := \{\gamma_i\}$. It furthermore

depends on a set of Lagrange multipliers $\vec{\lambda} = \{\lambda_i\}$, which are arbitrary real numbers. The precise form of $f$ is given in the technical manuscript.

The cardinalities of the sets $\vec{\lambda}$ and $\vec{\Gamma}$ are the same. This means that the number of parameters $\lambda_i$ that one must optimize over, to solve (1), is equal to *the number of experimental constraints that Alice and Bob have*. This has the potential to be significantly less than the number of parameters in the primal problem, which directly minimizes the Devetak-Winter formula over all $\rho_{AB}$.

An additional benefit of this approach is that it allows us to systematically study the effect of experimental constraints on the key rate. That is, when Alice and Bob gradually use more of their experimental data they gradually produce tighter and tighter lower bounds on the key rate (see examples in [21]).

Our proof of (1) relies on several technical tools. First is the notion of the duality of optimization, i.e., transforming the primal problem to its dual problem [15]. Second, we employ several entropic identities, from Refs. [16–18], in order to simplify the dual problem. Third, we use a recent, important result from Ref. [19] that solves a relative entropy optimization problem.

*Prepare-and-measure.*—On the one hand, we present our results in the entanglement-based (EB) scenario. However, we expect that many of the more interesting applications of our approach will be in the prepare-and-measure (PM) scenario. The source-replacement scheme discussed, e.g., in [5] can transform PM protocols into the EB framework, and we discuss in the technical manuscript [21] how this allows us to apply our approach to PM protocols.

*Outlook.*—In the future, we plan to use our method to systematically study the effect of experimental imperfections on key rates. Furthermore, we hope to investigate some interesting unstructured protocols for which the key rate is currently unknown. Just to give an example, we are interested in discrete-variable QKD protocols involving coherent states, i.e., where a small, discrete set of coherent states are the signal states and information may be encoded in the phase, e.g., as in Ref. [20].

We envision that our method could be a standard tool for researchers in the field. We hope to make our MATLAB code publicly available in the distant future. In the meantime, our main result is simple enough for anyone to use.


[1] S. Wiesner, ACM SIGACT News **15**, 78 (1983), ISSN 01635700.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Reviews of Modern Physics **81**, 1301 (2009), ISSN 0034-6861, URL `http://link.aps.org/doi/10.1103/RevModPhys.81.1301`.

[3] C. H. Bennett and G. Brassard, in *International Conference on Computers, Systems & Signal Processing, Bangalore, India* (1984), pp. 175–179.

[4] D. Bruss, Physical review letters **81**, 3018 (1998), ISSN 0031-9007, 0106126.

[5] A. Ferenczi and N. Lütkenhaus, Physical Review A **85**, 1 (2012), ISSN 10502947, 1112.3396.

[6] C. H. F. Fung and H. K. Lo, Physical Review A - Atomic, Molecular, and Optical Physics **74**, 1 (2006), ISSN 10502947, 0607056v3.

[7] O. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010), URL `http://link.aps.org/doi/10.1103/PhysRevA.82.032337`.

[8] E. Woodhead, Physical Review A **88**, 012331 (2013), ISSN 1050-2947, 1303.4821, URL `http://arxiv.org/abs/1303.4821$\delimiter"026E30F$nhttp://link.aps.org/doi/10.1103/PhysRevA.88.012331`.

[9] K. Tamaki, M. Curty, G. Kato, H.-k. Lo, and K. Azuma, Physical Review A **90**, 052314 (2014), ISSN 10941622, arXiv:1312.3514v2.

[10] I. Devetak and A. Winter, Proceedings of the Royal Society A **461**, 207 (2005), ISSN 1364-5021, 0306078, URL `http://arxiv.org/abs/quant-ph/0306078`.

[11] L. Sheridan and V. Scarani, Physical Review A - Atomic, Molecular, and Optical Physics **82**, 1 (2010), ISSN 10502947, 1003.5464.

[12] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, Physical Review A - Atomic, Molecular, and Optical Physics **88**, 1 (2013), ISSN 10502947, 1402.5810.

[13] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nature Physics **6**, 659 (2010), ISSN 1745-2473, URL `http://www.nature.com/doifinder/10.1038/nphys1734`.

[14] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature communications **3**, 634 (2012), ISSN 2041-1723, URL `http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3274703&tool=pmcentrez&rendertype=abstract`.

[15] S. Boyd and L. Vandenberghe, *Convex Optimization*, vol. 25 (2010), ISBN 9780521833783, 1111.6189v1, URL `https://web.stanford.edu/~boyd/cvxbook/bv_cvxbook.pdf`.

[16] K. Modi, T. Paterek, W. Son, V. Vedral, and M. Williamson, Physical Review Letters **104**, 1 (2010), ISSN 00319007, 0911.5417.

[17] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, Physical Review A **83**, 062338 (2011), ISSN 1050-2947, URL `http://link.aps.org/doi/10.1103/PhysRevA.83.062338`.

[18] P. J. Coles, Physical Review A **85**, 042103 (2012), ISSN 1050-2947, URL `http://link.aps.org/doi/10.1103/PhysRevA.85.042103`.

[19] M. Zorzi, F. Ticozzi, and A. Ferrante, IEEE Transactions on Information Theory **60**, 357 (2014), ISSN 00189448, 1301.6658.

[20] H. Lo and J. Preskill, Quantum Information and Computation **7**, 431 (2007), 0610203v2, URL `http://arxiv.org/abs/quant-ph/0610203`.

[21] See the attached technical manuscript for a detailed derivation and discussion of our results.

# Unstructured QKD

Patrick J. Coles and Norbert Lütkenhaus
*Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, N2L3G1 Waterloo, Ontario, Canada*

Quantum key distribution (QKD) allows for communication between distant parties with security guaranteed by quantum theory. The main theoretical problem in QKD is to calculate the secret key rate for a given physical protocol. Analytical formulas for the key rate are known for protocols that have a high degree of symmetry, such as the BB84 and six-state protocols. However, experimental imperfections tend to break symmetries. Since symmetry is exploited in theoretical treatments, the effect of experimental imperfections on key rates is difficult to estimate. Furthermore, it is an interesting question whether (intentionally) asymmetric protocols could offer an advantage over their symmetric counterparts.

In this work, we develop a robust numerical approach for calculating the key rate for arbitrary discrete-variable QKD protocols. Ultimately this approach will allow us to investigate the security of "unstructured" protocols, i.e., those that lack symmetry. Our approach relies on transforming the key rate calculation to the dual optimization problem, and analytically simplifying the dual problem using entropic identities. The resulting optimization problem can be solved efficiently, with significantly less parameters than the primal problem, and gives reliable lower bounds on the key rate. We illustrate our method by giving tight lower bounds for some unstructured protocols for which the key rate is unknown.

**Contents**



## I. INTRODUCTION

Secret keys are useful for a variety of tasks, such as encrypted communication and authentication. Distribution of secret keys whose security is guaranteed by quantum theory was proposed in Ref. [1], and is known as quantum key distribution (QKD). Both the theory and implementation of QKD have developed dramatically over the past three decades; see, for example, Ref. [2].

The main technical problem in QKD is to calculate how much secret key can be distributed by a given protocol. This is the *key rate problem*, where key rate refers to the number of bits of secret key established divided by the number of distributed quantum systems. Even if Alice and Bob have fully characterized their devices, they still may not know their key rate since the optimal eavesdropping attack for their protocol may be unknown.

In some special protocols that have a high degree of symmetry the optimal attack, and hence the key rate, is known [3]. Examples of such symmetric protocols, where the signal states have a group-theoretic structure, include the BB84 [4] and six-state protocols [5]. However, in some cases it is desirable to implement asymmetric protocols, e.g., the three-state protocol from Ref. [6]. In other cases, experimentalists may try to implement a symmetric protocol, but more often than not, experimental imperfections break symmetries. As a simple example of an asymmetric protocol where the optimal key rate is still under study, consider the usual BB84 protocol involving two orthonormal bases but where the Bloch-sphere angle between the two bases is arbitrary (instead of 90°).

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

Ref. [7, 8] and qubit protocols in Ref. [9]. Still, there is no general method for computing tight bounds on the key rate for arbitrary unstructured protocols. Yet, oftentimes 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 aim is fairly ambitious. We set out to develop a computer program, where Alice and Bob input a description of their measurement devices 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.

The key rate problem is an optimization problem, since one must minimize the well-known entropic formula for the key rate [10] over all states $\rho_{AB}$ that satisfy Alice's and Bob's experimental data. For two reasons, we find it advantageous to go to the dual problem. First, since the primal problem involves a minimization, the output will in general be an upper bound on the key rate. But one is typically more interested in reliable lower bounds, i.e., 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 key rate, even if the computer did not reach the global maximum.

Second, in many cases, transforming the problem dramatically reduces the number of parameters one must optimize over. For a state $\rho_{AB}$ with $d_A = \dim(\mathcal{H}_A)$ and $d_B = \dim(\mathcal{H}_B)$, the number of parameters is $d_A^2 d_B^2$. For example, if $d_A = d_B = 10$, the number of parameters that one would have to optimize over is 10000. In contrast, in the dual problem, the number of parameters is equal to the number of experimental constraints that Alice and Bob have. For example, in the generalization of the BB84 protocol to arbitrary dimensions [11, 12], Alice and Bob have two constraints, their error rates in the two mutually-unbiased bases. 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 (see 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 two unstructured protocols for which the key rates are (to our knowledge) unknown. First we consider BB84 with an arbitrary angle between the two bases. We show that the key rate is only very slightly reduced for small deviations in the angle (see Fig. 3), and in this sense, the protocol is robust to errors associated with the angle varying. Second, we consider a generalization of BB84 to higher dimensions that involves coarse-grained measurements (see Figs. 6 and 8). For both of these unstructured protocols, we compare results of our numerical optimization with lower bounds obtained using the entropic uncertainty relation (see Figs. 5 and 6). We find that our numerics dramatically outperform the uncertainty relation approach, giving much higher key rates. We even discuss a protocol for which the uncertainty relation gives a trivial bound on the key rate, while our numerics obtain positive key rates (see Fig. 8).

An additional benefit of our approach is that every number that the computer outputs is a reliable lower bound, and introducing more experimental constraints can only increase this lower bound. We demonstrate this with some simple examples (see Figs. 4 and 7) where, when Alice and Bob gradually use more of their experimental data they gradually produce tighter and tighter lower bounds on the key rate. Hence, our program allows us to systematically study the effect of experimental constraints on the key rate.

We focus on asymptotic key rates in this work. Nevertheless, the optimization problem that we solve is also at the heart of finite-key analysis, e.g., see Lemma 2 in Ref. [13]. We therefore hope to extend our approach to the finite-key scenario in future efforts.

In what follows we present our results in the entanglement-based (EB) scenario, and all of the examples that we use for illustration are EB protocols. However, we expect that many of the more interesting applications of our approach will be in the prepare-and-measure (PM) scenario. The source-replacement scheme discussed, e.g., in [3] can transform PM protocols into the EB framework, and we briefly remark in Sec. VI how this allows us to apply our approach to PM protocols.

For readability, we first state our main result in Sec. III, and we postpone its derivation to Sec. VII.

## II. SETUP OF THE PROBLEM

Consider a general entanglement-based (EB) QKD protocol involving finite-dimensional quantum systems $A$ and $B$ that are respectively received by Alice and Bob. Let $Z_A$ ($Z_B$) denote the measurement that Alice (Bob) performs on system $A$ ($B$) in order to derive the key. Suppose they use one-way direct reconciliation for the classical post-processing, then the asymptotic key rate for collective attacks is given by the Devetak-Winter formula [10]:

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

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

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

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

Here, $\rho_{ABE}$ is the tripartite density operator shared by Alice, Bob, and Eve. 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*.

Typically Alice's and Bob's shared density operator $\rho_{AB}$ 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 effectively constrain the form of $\rho_{AB}$. The measurements used for this purpose generally have a tensor product form:

$$\vec{\Gamma} = \{\Gamma_i\} = \{\Gamma_i^A \otimes \Gamma_i^B\} \tag{4}$$

and in general can be assumed to be bounded Hermitian operators.

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

$$\vec{\gamma} = \{\gamma_i\}, \quad \text{with } \gamma_i := \langle \Gamma_i \rangle = \text{Tr}(\rho_{AB}\Gamma_i) \tag{5}$$

and this gives a set of experimental constraints:

$$C = \{\text{Tr}(\rho_{AB}\Gamma_i) = \gamma_i\}. \tag{6}$$

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

$$\mathcal{C} = \{\rho_{AB} \in \mathcal{P}_{AB} : C \text{ holds}\} \tag{7}$$

where $\mathcal{P}_{AB}$ denotes the set of positive semi-definite 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 (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 as follows:

$$K = \min_{\rho_{AB} \in \mathcal{C}} [H(Z_A|E) - H(Z_A|Z_B)] \tag{8}$$

where Eve's system $E$ can be assumed to purify Alice and Bob's state $\rho_{AB}$ 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 semi-definite operator on $\mathcal{H}_{AB}$. We refer to (8) as the *primal problem*.

## III. MAIN RESULT

Our main result is a reformulation of the optimization problem in (8).

**Theorem 1:** The solution of the minimization problem in (8) is lower bounded by the following maximization problem:

$$K \geqslant \Theta - H(Z_A|Z_B) \tag{9}$$

where we define $\Theta := \widehat{\Theta}/\ln(2)$, with

$$\widehat{\Theta} := \max_{\vec{\lambda}} \left( -\left\| \sum_j Z_A^j R(\vec{\lambda}) Z_A^j \right\|_\infty - \vec{\lambda} \cdot \vec{\gamma} \right), \tag{10}$$

and

$$R(\vec{\lambda}) := \exp\left(-\mathbb{1} - \vec{\lambda} \cdot \vec{\Gamma}\right). \tag{11}$$

In (10), the optimization is over all vectors $\vec{\lambda} = \{\lambda_i\}$ with $|\vec{\lambda}| = |\vec{\Gamma}|$, where the $\lambda_i$ are arbitrary real numbers. Also, $\|M\|_\infty$ denotes the supremum norm of $M$, which is the maximum eigenvalue of $M$ in the case of where the argument $M$ is positive semi-definite, as in (10).

Notice that the cardinalities of the sets $\vec{\lambda}$ and $\vec{\Gamma}$ are the same. This means that the number of parameters $\lambda_i$ that one must optimize over, to solve (10), 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 (10) can be easily solved using MATLAB on a personal computer for a variety of interesting QKD protocols.

Before moving on, consider the following general remark about our optimization.

**Remark 1.** Adding in more constraints will never decrease the key rate obtained from our optimization. One can see this as follows. Suppose one has $n$ constraints, which leads to a value of $\widehat{\Theta} = \widehat{\Theta}_n$ obtained from optimizing (10). Now suppose one adds in an additional constraint $\langle \Gamma_{n+1} \rangle = \gamma_{n+1}$. For this new problem, the optimization in (10) runs over all values of $\lambda_{n+1}$, including the case where $\lambda_{n+1} = 0$. But the case where $\lambda_{n+1}$ vanishes corresponds to the previous problem, which had an optimal value of $\widehat{\Theta}_n$. So the optimal value of the new problem is lower bounded by $\widehat{\Theta}_n$.

## IV. REPRODUCING LITERATURE RESULTS

### A. Introduction

In this section we illustrate our numerical approach for lower bounding the key rate by considering some well-known protocols. In particular, we consider the BB84 protocol, the six-state protocol, and the generalized BB84 protocol involving two mutually-unbiased

bases (MUBs) in any dimension. In each case, the dependence of the key rate on error rate is known. As we show below, our numerical approach exactly reproduces these theoretical dependences, hence illustrating the tightness of our bounds.

### B. BB84 protocol

Consider an entanglement-based version of the BB84 protocol [4], where Alice and Bob each receive a qubit and measure either the $\sigma_Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ or $\sigma_X = |+\rangle\langle +| - |-\rangle\langle -|$ observables, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Let us suppose that Alice and Bob each use their $Z$ basis (the standard basis) in order to generate key.

Suppose that Alice and Bob observe that their error rates in the $X$ and $Z$ bases are identical and equal to $Q$, then it is known (see, e.g., [2]) that the key rate is given by

$$K = 1 - 2h(Q) \tag{12}$$

where $h(p) := -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy. The dependence of $K$ on $Q$ in Eq. (12) is plotted as the red solid curve in Fig. 1(A).

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

$$\begin{aligned} \text{Key-map POVM: } & Z_A = \{|0\rangle\langle 0|, |1\rangle\langle 1|\} && \text{(13a)}\\ \text{Constraints: } & \langle \mathbb{1}\rangle = 1 && \text{(13b)}\\ & \langle E_X\rangle = Q && \text{(13c)}\\ & \langle E_Z\rangle = Q && \text{(13d)} \end{aligned}$$

where the error operators are defined as

$$E_Z := |0\rangle\langle 0| \otimes |1\rangle\langle 1| + |1\rangle\langle 1| \otimes |0\rangle\langle 0| \tag{14}$$
$$E_X := |+\rangle\langle +| \otimes |-\rangle\langle -| + |-\rangle\langle -| \otimes |+\rangle\langle +|. \tag{15}$$

Equation (13) highlights the fact that, as far as the optimization in (10) is concerned, a QKD protocol is defined the POVM elements used for generating the key, and the experimental constraints used for "parameter estimation". Once these two things are specified, the protocol is defined and the key rate is determined.

Numerically solving the problem defined in (13), for several different values of $Q$, leads to the blue dots depicted in Fig. 1(A). Note that they agree perfectly with the theoretical curve, indicating that our lower bound is perfectly tight in this case.

### C. Six state protocol

Consider an entanglement-based version of the six-state protocol, where Alice and Bob each measure in one of three MUBs ($X$, $Y$, or $Z$) on their qubit. Suppose that Alice and Bob observe that their error rates in all

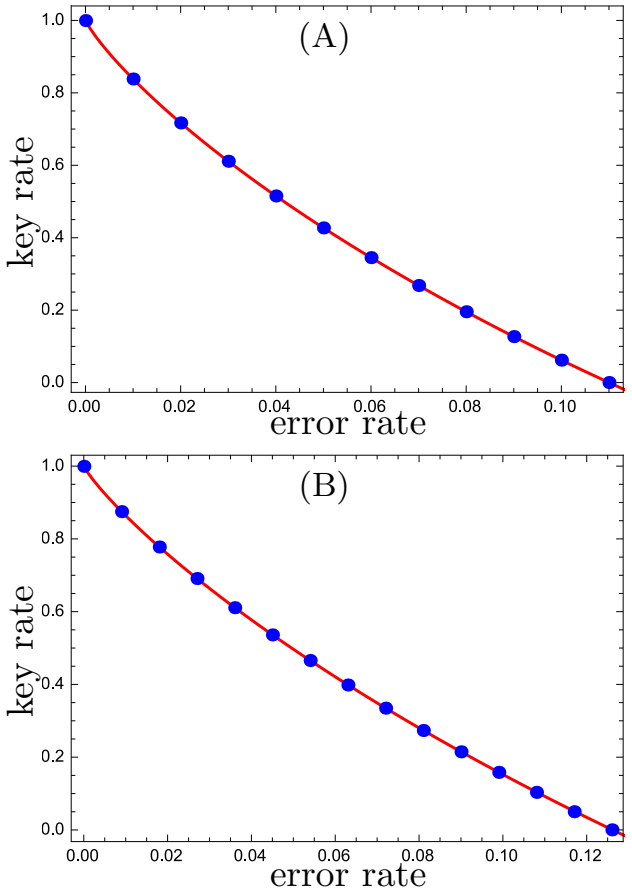


FIG. 1: (A) The known theoretical curve for BB84 is shown in red, while the results of our numerical optimization are shown as blue dots. The blue dots should be viewed as reliable lower bounds on the key rate, but in this case they happen to be perfectly tight, coinciding with the theoretical curve. (B) A similar plot is shown for the six-state protocol.

three MUBs are identical and equal to $Q$, then the key rate is given by [5]

$$K = 1 - h(Q) - Q + (1+Q) * h\left(\frac{1-3Q/2}{1-Q}\right) \tag{16}$$

This dependence of $K$ on $Q$ is plotted as the red solid curve in Fig. 1(B).

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

$$\begin{aligned} \text{Key-map POVM: } & Z_A = \{|0\rangle\langle 0|, |1\rangle\langle 1|\} && \text{(17a)}\\ \text{Constraints: } & \langle \mathbb{1}\rangle = 1 && \text{(17b)}\\ & \langle E_{XY}\rangle = Q && \text{(17c)}\\ & \langle E_Z\rangle = Q && \text{(17d)} \end{aligned}$$

where $E_Z$ is defined in (14) and $E_{XY} = (1/2)*(E_X + E_Y)$ quantifies the average error for $X$ and $Y$, with

$$E_Y := |y_+\rangle\langle y_+| \otimes |y_+\rangle\langle y_+| + |y_-\rangle\langle y_-| \otimes |y_-\rangle\langle y_-| \tag{18}$$

where $|y_\pm\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$.

Numerically solving the problem defined in (17), for several values of $Q$, leads to the blue dots in Fig. 1(B). Much like the BB84 case, they agree with the theoretical curve, hence our lower bound is perfectly tight for the six-state protocol.

We remark that, in theory, one can get an improved bound on the key rate by splitting up the constraint $\langle E_{XY}\rangle = Q$ into the more fine-grained constraints $\langle E_X\rangle = Q$ and $\langle E_Y\rangle = Q$. However, our numerics show that this is not necessary, the coarse-grained constraint $\langle E_{XY}\rangle = Q$ is enough to produce a tight bound.

### D. Two MUBs in higher dimensions

A distinct advantage of our approach of solving (10) instead of the primal problem (8) is that we can easily perform the optimization in higher dimensions, where the number of parameters in (8) would be quite large.

To illustrate this, we consider a generalization of the BB84 to arbitrary dimension, where Alice and Bob measure generalized versions of the $X$ and $Z$ bases. This protocol has been implemented, e.g., in Ref. [12] using orbital angular momentum.

Taking $Z$ to be the standard basis $\{|j\rangle\}$, Alice's $X$ basis can be taken as the Fourier transform $\{F|j\rangle\}$, where

$$F = \sum_{j,k} \omega^{-jk} |j\rangle\langle k|$$

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 and equal to $Q$, then the key rate is given by [3, 11]

$$K = \log_2 d - 2h(Q) - 2Q\log_2(d-1) \tag{19}$$

This dependence of $K$ on $Q$ is plotted as the solid curves in Fig. 2, for the cases $d = 6, 8, 10$.

To reproduce this result using our numerics, we first note Fano's inequality:

$$H(Z_A|Z_B) \leqslant h(Q) + Q\log_2(d-1), \tag{20}$$

which, when applied to Eq. (9), gives

$$K \geqslant \Theta - [h(Q) + Q\log_2(d-1)]. \tag{21}$$

Then we solve for $\Theta$ numerically, specifying the problem as

$$\text{Key-map POVM: } Z_A = \{|0\rangle\langle 0|, |1\rangle\langle 1|, ..., |d-1\rangle\langle d-1|\} \tag{22a}$$

$$\text{Constraints: } \langle \mathbb{1}\rangle = 1 \tag{22b}$$

$$\langle E_X\rangle = Q \tag{22c}$$

$$\langle E_Z\rangle = Q \tag{22d}$$

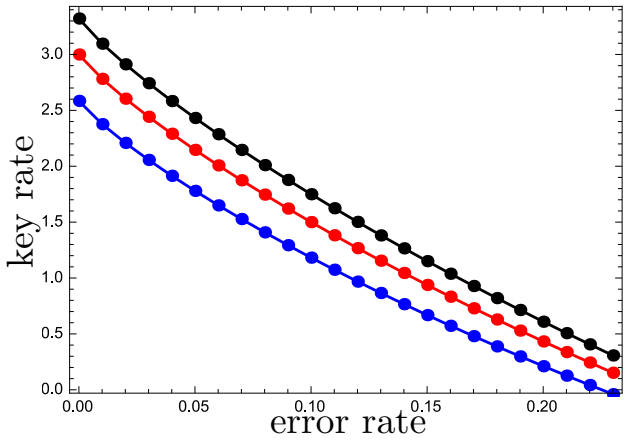


FIG. 2: Higher dimensional analog of BB84, using two MUBs. This plot shows the theoretical key rate as solid curves, and the result of our numerical optimization as circular dots, for $d_A = d_B = d$, with $d = 6$ (blue), $d = 8$ (red), and $d = 10$ (black). Again, the circular dots should be viewed as reliable lower bounds on the key rate, but in this case they happen to be perfectly tight.

Here, the generalized error operators can be written as $E_Z = \mathbb{1} - C_Z$ and $E_X = \mathbb{1} - C_X$, with

$$C_Z := \sum_{j=0}^{d-1} |j\rangle\langle j| \otimes |j\rangle\langle j| \tag{23}$$

$$C_X := \sum_{j=0}^{d-1} F|j\rangle\langle j|F^\dagger \otimes F^*|j\rangle\langle j|F^T \tag{24}$$

where $F^T$ is the transpose of $F$ in the standard basis.

Numerically solving for $\Theta$ with the above constraints gives the circular dots shown in Fig. 2. The figure shows the cases $d = 6, 8, 10$, and clearly there is perfect agreement with the theory. (Likewise, we have verified that we get perfect agreement for all $d$ in the range $2 \leqslant d \leqslant 10$, and naturally we suspect that the trend would continue for higher $d$.)

We again emphasize that the calculation of $\Theta$ 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 (8), where the number of parameters is $d^4$, which would be 10000 for $d = 10$.

## V. INVESTIGATING UNSTRUCTURED PROTOCOLS

### A. Introduction

We now move on to the task of using our numerical optimization for its intended purpose: studying unstructured protocols. We are encouraged by the fact that our bounds were tight for the structured protocols discussed above, and so there is reason to suspect that we will get strong bounds in the unstructured case.

### B. BB84 protocol with rotated basis

We first consider a variation on the BB84 protocol where Alice and Bob each measure either the $Z$ or $W$ basis, where the $W$ basis states are given by:

$$|W_{\pm}\rangle = e^{-i\sigma_Y \theta/2}|\pm\rangle$$

where $\sigma_Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$. In other words, the $W$ basis is rotated away from $X$ axis, towards the $Z$ axis, by an angle $\theta$. (See the inset of Fig. 3.) Let us refer to this as the *rotated BB84 protocol*.

Suppose that Alice and Bob observe that their error rates in both the $Z$ and $W$ bases are identical and equal to $Q$. We will show that is already enough to obtain a strong bound on the key rate. But we also find that they can obtain an even stronger bound if they use more of their measurement data. In particular, note that there can be correlations between Alice's $W$ basis and Bob's $Z$ basis. Such correlations are typically absent in the usual BB84, but they can play a role in the rotated protocol that we are considering.

Again, starting from the bound:

$$K \geqslant \Theta - h(Q), \tag{25}$$

we are motivated to solve for $\Theta$ via the following optimization problem:

$$\text{Key-map POVM: } Z_A = \{|0\rangle\langle 0|, |1\rangle\langle 1|\} \tag{26a}$$

$$\text{Constraints: } \langle \mathbb{1} \rangle = 1 \tag{26b}$$

$$\langle E_W \rangle = Q \tag{26c}$$

$$\langle E_Z \rangle = Q \tag{26d}$$

$$\langle C_{WZ} \rangle = Q + (1-2Q)\cos^2\left(\frac{\pi/2-\theta}{2}\right) \tag{26e}$$

Here, the $W$ error operator is

$$E_W := |W_+\rangle\langle W_+| \otimes |W_-\rangle\langle W_-| + |W_-\rangle\langle W_-| \otimes |W_+\rangle\langle W_+|$$

and the correlation between Alice's $W$ and Bob's $Z$ is quantified via the operator

$$C_{WZ} := |W_+\rangle\langle W_+| \otimes |0\rangle\langle 0| + |W_-\rangle\langle W_-| \otimes |1\rangle\langle 1|. \tag{27}$$

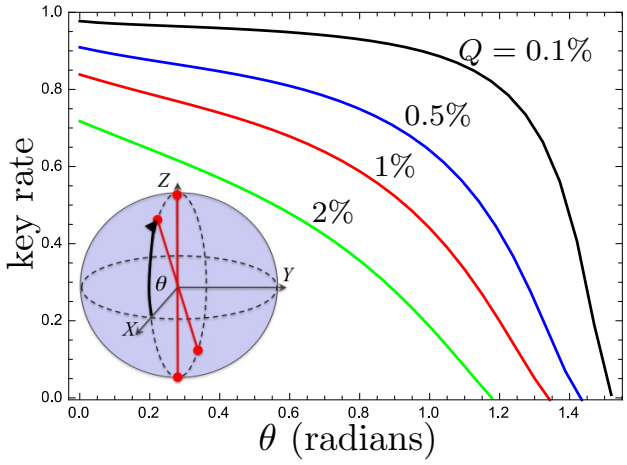


FIG. 3: Asymmetric version of BB84, involving orthonormal bases $W$ and $Z$, where the $W$ basis is rotated by an angle $\theta$ away from the $X$ axis of the Bloch sphere, such that $\pi/2 - \theta$ is the Bloch sphere angle between $W$ and $Z$. A schematic depiction of the Bloch sphere is shown in the lower-left corner. The plot shows (a lower bound on) the key rate as a function of $\theta$ as computed by our numerical optimization, for four different error rates: 0.1% (black), 0.5% (blue), 1% (red), and 2% (green).

The expression that appears in (26) for $\langle C_{WZ} \rangle$ corresponds to the value that one would obtain for a Werner state of the form $\rho_{AB} = (1-2Q)|\Phi_0\rangle\langle\Phi_0| + Q(\mathbb{1}/2)$, where $|\Phi_0\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ is the standard Bell state.

Solving the optimization problem defined in (26), for various values of $Q$ and $\theta$, leads to the curves shown in Fig. 3. Naturally, one would expect the key rate to go zero as $\theta \to \pi/2$, since the $W$ basis becomes identical to the $Z$ basis in this limit. But perhaps the most striking feature of the curves in Fig. 3 is *how slowly* these curves to zero as $\theta$ increases. In particular, for small values of $\theta$, our lower bounds on the key rate are fairly flat, with only a mild dependence on $\theta$.

One can think of this protocol as a toy model for experimental imperfections that occur when experimentalists attempt to implement the BB84 protocol, but have angular errors. Experimentally, it is not uncommon for $\theta$ to deviate away from zero by a few degrees. But note that Fig. 3 is plotted in radians. Hence, according to our results, a few degrees error would translate into a key rate that is very close to the value at $\theta = 0$.

Finally, in relation to Remark 1, we note the following. It is interesting to look at the hierarchy of lower bounds that we can obtain by gradually including more of the constraints in (26). This is shown in Fig. 4. Including only the constraints in (26b) and (26c) gives the red curve in Fig. 4. Adding in (26d) gives the blue curve, and further adding in (26e) gives the black curve. Hence, as noted in Remark 1, the bounds get tighter as one adds in more constraints, as one can clearly see in Fig. 4. It is

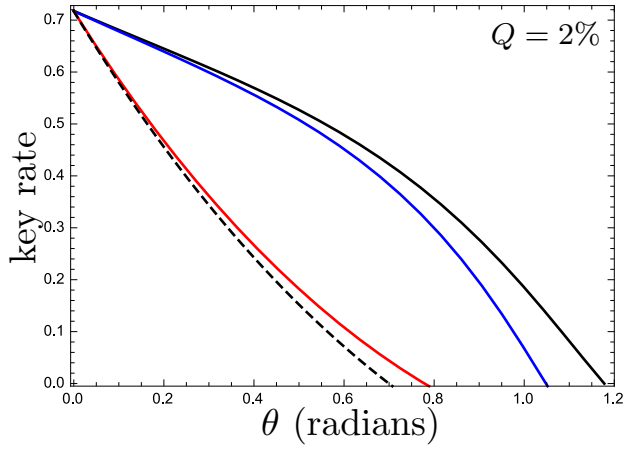


FIG. 4: A hierarchy of lower bounds on the key rate, for the rotated BB84 protocol, with $Q = 2\%$. The bounds obtained from our optimization become tighter as one adds in more constraints. Including only the constraints in (26b) and (26c) gives the red curve. Adding in (26d) gives the blue curve, and further adding in (26e) gives the black curve. All of these bounds lie above the black dashed line, which is the bound that one obtains from the entropic uncertainty relation.

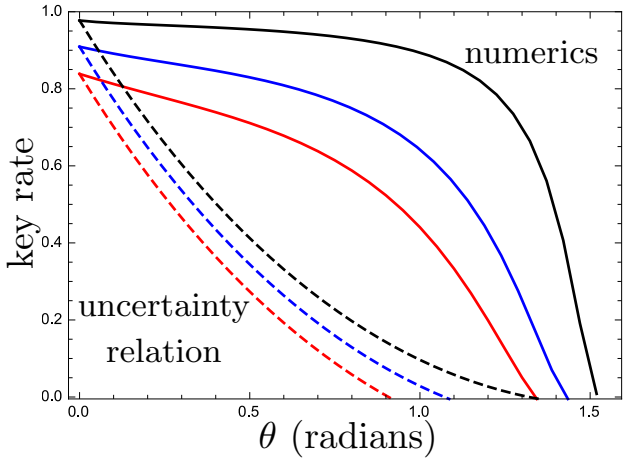


FIG. 5: Comparison of lower bounds on the key rate for the rotated version of BB84 described in Fig. 3. The entropic uncertainty relation provides a lower bound on the key rate, and is shown by the dashed curves in the plot, for error rates of 0.1% (black), 0.5% (blue), and 1% (red). The plot shows that these lower bounds are significantly less tight than the corresponding bounds obtained from our numerical optimization.

interesting to note that all of the bounds in this hierarchy lie above the dashed line in Fig 4, which is the bound that one can obtain from the entropic uncertainty relation. We discuss the uncertainty relation approach in the next subsection.

### C. Comparison with uncertainty relation approach

Consider the entropic uncertainty relation allowing for quantum memory [14, 15],

$$H(Z_A|E) + H(W_A|W_B) \geqslant \log_2(1/c) \tag{28}$$

where the complementarity factor for the POVMs $Z_A$ and $W_A$ is given by

$$c := \max_{j,k} \left\| \sqrt{Z_A^j} \sqrt{W_A^k} \right\|_\infty^2 \tag{29}$$

Inserting this formula into Eq. (1) gives

$$K \geqslant \log_2(1/c) - [H(W_A|W_B) + H(Z_A|Z_B)]\,. \tag{30}$$

Hence the entropic uncertainty relation allows us to lower bound the key rate. This approach for bounding the key rate was proposed in Refs. [14, 16].

Let us now compare the bound in (30) to the bounds that we obtain from our optimization. Consider again the rotated BB84 protocol. Here, the complementarity factor simplifies to:

$$c = \cos^2\left(\frac{\pi/2 - \theta}{2}\right). \tag{31}$$

Also, assuming an error rate of $Q$ for both the $Z$ and $W$ bases, we obtain

$$K \geqslant \log_2\left[1/\cos^2\left(\frac{\pi/2-\theta}{2}\right)\right] - 2h(Q). \tag{32}$$

Figure 5 shows the dependence of the bound provided by (32) for various error rates. It is interesting that the uncertainty relation bounds have a convex dependence on $\theta$. In contrast, our numerical bounds have a concave dependence on $\theta$. Furthermore, our bounds are much stronger, particularly for large $\theta$. It seems that the key rate is much more robust to small variations in $\theta$ than the uncertainty relation would suggest.

We remark that there are other methods [7–9] in the literature, besides the entropic uncertainty relation, that can be applied to the rotated BB84 protocol. For example, we have also compared our numerics to the bound in Ref. [8]. While the bound in Ref. [8] outperforms the entropic uncertainty relation in this case, our bound is still significantly tighter than that of Ref. [8].

### D. Protocols with binary measurements in dimension $d$

#### 1. *Binary $X$ measurement*

Let us consider another generalization of the BB84 protocol, where $d_A = d_B = d$, and Alice and Bob use their $Z$ bases to generate key (and for parameter estimation). However instead of using their $X$ bases for param-

eter estimation, they use a coarse-grained version of $X$. Namely, Alice and Bob respectively use the POVMs:

$$\widetilde{X}_A = \{\widetilde{X}_A^0, \widetilde{X}_A^1\} = \{|X_0\rangle\langle X_0|, \mathbb{1} - |X_0\rangle\langle X_0|\},$$
$$\widetilde{X}_B = \{\widetilde{X}_B^0, \widetilde{X}_B^1\} = \{|\overline{X}_0\rangle\langle \overline{X}_0|, \mathbb{1} - |\overline{X}_0\rangle\langle \overline{X}_0|\} \quad (33)$$

where $|X_0\rangle = F|0\rangle$ and $|\overline{X}_0\rangle = F^*|0\rangle$.

Suppose the error rate in the $Z$ basis is $Q$, then as discussed previously, Fano's inequality (20) implies

$$K \geqslant \Theta - [h(Q) + Q\log_2(d-1)]. \quad (34)$$

We compute $\Theta$ with the following optimization problem:

$$\text{Key-map POVM: } Z_A = \{|0\rangle\langle 0|, |1\rangle\langle 1|, ..., |d-1\rangle\langle d-1|\} \quad (35a)$$
$$\text{Constraints: } \langle \mathbb{1}\rangle = 1 \quad (35b)$$
$$\langle E_{\widetilde{X}}\rangle = \frac{2}{d} * Q \quad (35c)$$
$$\langle E_Z\rangle = Q \quad (35d)$$
$$\langle E_{\widetilde{X}_0}\rangle = (1-Q)/d \quad (35e)$$

Here, the $\widetilde{X}$ error operator is

$$E_{\widetilde{X}} := \widetilde{X}_A^0 \otimes \widetilde{X}_B^1 + \widetilde{X}_A^1 \otimes \widetilde{X}_B^0 \quad (36)$$

and we also find it helpful to introduce the operator

$$E_{\widetilde{X}_0} := \widetilde{X}_A^0 \otimes \widetilde{X}_B^0. \quad (37)$$

The correlations given by the constraints in (40) are consistent with those of a Werner state.

Solving the optimization problem defined in (40), for $d = 3, 4, 5$, leads to the solid curves shown in Fig. 6. Note that as the error rate $Q$ goes to zero, the key rates approach the value of $\log_2 d$, which is the same behavior as one sees in Eq. (19) for the fine-grained protocol. In this sense, we see that the effect of coarse-graining the parameter estimation observable is not too detrimental - so long as the error rate is low.

For comparison, we can obtain a bound using the entropic uncertainty relation. In this case

$$c = (d-1)/d$$

and from (30) we obtain the bound

$$K \geqslant \log_2\left(\frac{d}{d-1}\right) - [h(2Q/d) + h(Q) + Q\log_2(d-1)]. \quad (38)$$

The dashed lines in Fig. 6 correspond to the bounds provided by (38). Clearly the numerical approach gives much stronger bounds than the uncertainty relation in this case.

Analogous to Fig. 4, it is interesting to consider the heirarchy of lower bounds that we obtain by including more or less of the constraints in (40). This is depicted in Fig. 7. Including only the constraints in (40b) and (40c) gives the green curve in Fig. 7. Adding in (40d) gives the red curve, whereas instead adding in (40e) gives the blue curve. Including all four constraints gives the black curve.

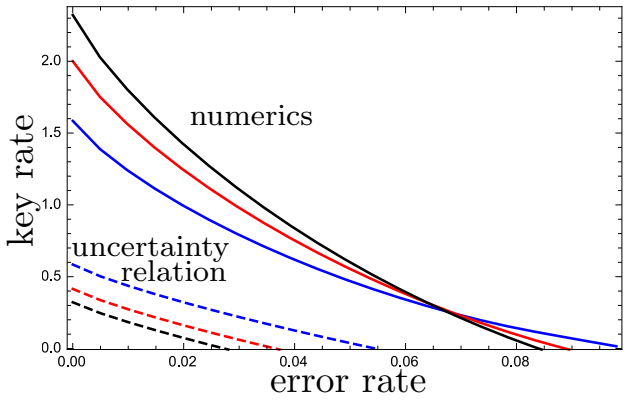


FIG. 6: Comparison of lower bounds on the key rate for the coarse-grained BB84, where $Z$ is fine-grained while $X$ is coarse, and the error rate refers to the $Z$ basis. The entropic uncertainty relation provides a lower bound on the key rate, and is shown by the dashed curves in the plot, for $d = 3$ (blue), $d = 4$ (red), and $d = 5$ (black). The plot shows that these lower bounds are significantly less tight than the corresponding bounds obtained from our numerical optimization, which are shown as solid curves.

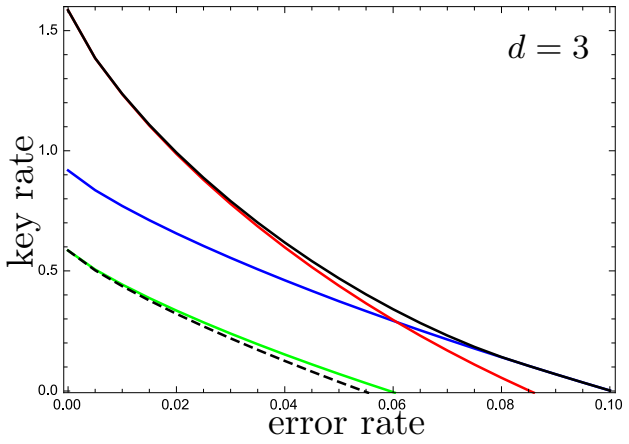


FIG. 7: A hierarchy of lower bounds on the key rate for the coarse-grained BB84 protocol defined by Eq. (40), with $d = 3$. Including only the constraints in (40b) and (40c) gives the green curve. Adding in (40d) gives the red curve, whereas instead adding in (40e) gives the blue curve. Including all four constraints gives the black curve. All of these bounds lie above the black dashed line, which is the bound (38) obtained from the entropic uncertainty relation.

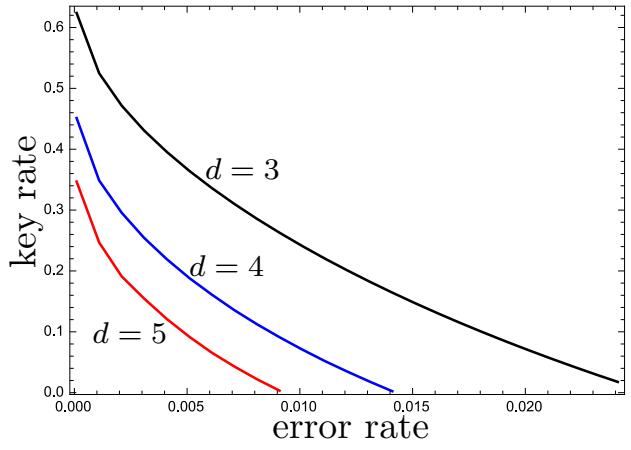


FIG. 8: Lower bounds on the key rate for the coarse-grained BB84, where both $Z$ and $X$ are coarse-grained, for $d = 3$ (black), $d = 4$ (blue), and $d = 5$ (red). The entropic uncertainty relation does not provide a non-trivial bound on the key rate in this case.

### 2. *Binary X and Z measurements*

Consider a slight modification of the previous protocol, where the key-generating measurement is also coarse-grained, and is given by:

$$\widetilde{Z} = \{\widetilde{Z}_0, \widetilde{Z}_1\} = \{|0\rangle\langle 0|, \mathbb{1} - |0\rangle\langle 0|\}$$

Suppose that Alice and Bob's error rates for the $\widetilde{Z}$ and $\widetilde{X}$ measurements are both $Q$, then

$$K \geqslant \Theta - h(Q), \tag{39}$$

and we consider the optimization problem:

$$\begin{aligned}
\text{Key-map POVM: } & Z_A = \{\widetilde{Z}_0, \widetilde{Z}_1\} && \text{(40a)}\\
\text{Constraints: } & \langle \mathbb{1} \rangle = 1 && \text{(40b)}\\
& \langle E_{\widetilde{X}} \rangle = Q && \text{(40c)}\\
& \langle E_{\widetilde{Z}} \rangle = Q && \text{(40d)}\\
& \langle E_{\widetilde{X}_0} \rangle = 1/d - Q/2 && \text{(40e)}
\end{aligned}$$

Here, the $\widetilde{Z}$ error operator is

$$E_{\widetilde{Z}} := \widetilde{Z}_0 \otimes \widetilde{Z}_1 + \widetilde{Z}_1 \otimes \widetilde{Z}_0 \tag{41}$$

Solving the optimization problem in (40), for $d = 3, 4, 5$, leads to the curves shown in Fig. 8. It is interesting that we obtain positive key rates for this protocol.

In contrast, the entropic uncertainty relation, in this case, leads to no non-trivial bounds on the key rate for $d \geqslant 3$, since we have $c \geqslant 1$ for the $\widetilde{X}$ and $\widetilde{Z}$ measurements. So this is an example where the uncertainty relation predicts no security, whereas our numerics predict distillable key.

## VI. PREPARE-AND-MEASURE SCENARIO

Our results stated above were for the EB scenario. However, we expect that many of the interesting applications of our approach will be for prepare-and-measure (PM) protocols. Let us briefly sketch how our approach can be used in the PM scenario.

Consider a PM protocol involving the set of $N$ signal states $\{|\phi_j\rangle\}$. It is well-known that PM protocols can be recast as EB protocols using the source-replacement scheme (see, e.g., [2, 3]). Namely, one forms the following entangled state:

$$|\psi\rangle_{AA'} = \sum_j \frac{1}{\sqrt{N}} |j\rangle|\phi_j\rangle. \tag{42}$$

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

$$\rho_{AB} = (\mathcal{I} \otimes \mathcal{E})(|\psi_{AA'}\rangle\langle\psi_{AA'}|). \tag{43}$$

The numerical optimization approach described above can then be applied to the state $\rho_{AB}$ in (43). However, in addition to the constraints obtained from the results of Alice's and Bob's measurements, we must add in some additional constraints, to account for the special form of $\rho_{AB}$ in (43). In particular, note that the partial trace over $B$ gives:

$$\rho_A = \sum_{j,k} \frac{1}{\sqrt{N}} \langle\phi_k|\phi_j\rangle |j\rangle\langle k|. \tag{44}$$

The form of $\rho_A$ 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 expectation values of these observables into the set of constraints. That is, add

$$\langle \Omega_i \rangle = \omega_i, \quad \text{for each } i \tag{45}$$

to the set $C$ in (6). This will capture Alice's knowledge of her reduced density operator.

## VII. TECHNICAL DERIVATION

Our proof of Theorem 1 relies on several technical tools. First is the notion of the duality of optimization, i.e., transforming the primal problem to its dual problem. Second, we employ several entropic identities in order to simplify the dual problem. Most of these entropic identities are from the literature (Refs. [15, 17, 18]), although our statement of coherence continuity (Lemma 3) may be novel. Third, we use a recent, important result from Ref. [19] that solves a relative entropy optimization problem.

### A. Primal problem

In what follows, for readability, we will first derive our main result for the special case where the key-generating POVM $Z_A = \{Z_A^j\}$ is a projective measurement, i.e., where the $Z_A^j$ are projectors (of arbitrary rank). Then we will extend the derivation to arbitrary POVMs in Sec. VII F.

Let us recall the primal problem discussed in Sec. II:

$$K = \min_{\rho_{AB}\in\mathcal{C}} [H(Z_A|E) - H(Z_A|Z_B)] \tag{46}$$

$$= \left[\min_{\rho_{AB}\in\mathcal{C}} H(Z_A|E)\right] - H(Z_A|Z_B) \tag{47}$$

Here we noted that the second term in (46), $H(Z_A|Z_B)$, will be determined experimentally and hence can be pulled out of the optimization. So we only need to optimize the first term.

Now we will show that this is a convex optimization problem.

**Lemma 2:** Let system $E$ purify $\rho_{AB}$. Then $H(Z_A|E)$ is a convex function of $\rho_{AB}$.

*Proof.* From Refs. [15, 18], we have the following relation between the conditional entropy and relative entropy:

$$H(Z_A|E) = D\left(\rho_{AB}||\sum_j Z_A^j \rho_{AB} Z_A^j\right) \tag{48}$$

where

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

Due to the joint convexity of the relative entropy, it follows that the right-hand side of (48) is a convex function of $\rho_{AB}$, hence proving the desired result. □

Due to Lemma 2 and the fact that the constraints in (6) are all linear functions of $\rho_{AB}$, Eq. (47) is a convex optimization problem.

### B. Coherence

Before transforming to the dual problem, let us make some remarks about the connection of our problem to a quantity known as coherence [20]. 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 $\rho$ is defined as [20]:

$$\Phi(\rho,\Pi) = D(\rho||\sum_j \Pi_j\rho\Pi_j) \tag{49}$$

Consider the following rescaled version of our primal problem,

$$\alpha = \min_{\rho_{AB}\in\mathcal{C}} H(Z_A|E) \tag{50}$$

Using an entropic identity from Refs. [15, 18], namely the one in (48), this can be rewritten as a coherence minimization problem:

$$\alpha = \min_{\rho_{AB}\in\mathcal{C}} \Phi(\rho_{AB}, Z_A). \tag{51}$$

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

Coherence has some nice properties. One property that we will make explicit use of is its *continuity* in the state $\rho$, which we prove in the following lemma.

**Lemma 3:** Let $\rho$ and $\sigma$ be two density operators on a Hilbert space of dimension $d$. Suppose they are close in trace distance $T(\tau,\tau') := (1/2)\mathrm{Tr}|\tau-\tau'|$, in particular, suppose $T(\rho,\sigma) \leqslant 1/e$. Then the coherence's of $\rho$ and $\sigma$ are nearly equal:

$$\begin{aligned}\Delta\Phi &:= |\Phi(\rho,\Pi) - \Phi(\sigma,\Pi)| \\ &\leqslant 2[T(\rho,\sigma)\log_2 d - T(\rho,\sigma)\log_2 T(\rho,\sigma)].\end{aligned} \tag{52}$$

*Proof.* The proof uses Fannes' inequality, which states that

$$|H(\rho) - H(\sigma)| \leqslant T(\rho,\sigma)\log_2 d - T(\rho,\sigma)\log_2 T(\rho,\sigma), \tag{53}$$

which holds so long as $T(\rho,\sigma) \leqslant 1/e$. Note that, because of the monotonicity of the trace distance under quantum channels, we also have $T(\rho_\Pi,\sigma_\Pi) \leqslant 1/e$, where $\rho_\Pi = \sum_j \Pi_j\rho\Pi_j$ and $\sigma_\Pi = \sum_j \Pi_j\sigma\Pi_j$. Hence (53) also holds for the states $\rho_\Pi$ and $\sigma_\Pi$.

Noting that $\log\rho_\Pi = \sum_j \Pi_j(\log\rho_\Pi)\Pi_j$, we have

$$H(\rho_\Pi) = -\mathrm{Tr}(\rho\log\rho_\Pi),$$

and hence we can rewrite the coherence as

$$\Phi(\rho,\Pi) = H(\rho_\Pi) - H(\rho).$$

This allows us to bound the coherence difference:

$$\Delta\Phi = |H(\rho_\Pi) - H(\sigma_\Pi) + H(\sigma) - H(\rho)| \tag{54}$$

$$\leqslant |H(\rho_\Pi) - H(\sigma_\Pi)| + |H(\sigma) - H(\rho)| \tag{55}$$

$$\leqslant T(\rho_\Pi,\sigma_\Pi)\log_2 d - T(\rho_\Pi,\sigma_\Pi)\log_2 T(\rho_\Pi,\sigma_\Pi) + T(\rho,\sigma)\log_2 d - T(\rho,\sigma)\log_2 T(\rho,\sigma) \tag{56}$$

$$\leqslant 2[T(\rho,\sigma)\log_2 d - T(\rho,\sigma)\log_2 T(\rho,\sigma)], \tag{57}$$

where the last line uses $T(\rho_\Pi,\sigma_\Pi) \leqslant T(\rho,\sigma)$, as well as the monotonicity of $(-x\log x)$ over the interval $x \in [0, 1/e]$. □

### C. Change of domain

We now wish to argue that the domain of our optimization problem can be restricted to positive definite matrices, i.e., states that are full rank. Our argument proceeds as follows.

Consider the following three problems, which we will show have the same optimal values.

$$\text{Problem 1: } a_1 = \min_{\rho\in\mathcal{S}_1} \Phi(\rho,\Pi) \tag{58}$$

$$\text{Problem 2: } a_2(\varepsilon) = \min_{\rho\in\mathcal{S}_2(\varepsilon)} \Phi(\rho,\Pi) \tag{59}$$

$$\text{Problem 3: } a_3 = \min_{\rho\in\mathcal{S}_3} \Phi(\rho,\Pi) \tag{60}$$

with

$$\begin{aligned}\mathcal{S}_1 &:= \{\rho\in\mathcal{H}_d : \rho\geqslant 0, \mathrm{Tr}(\rho\vec{\Gamma}) = \vec{\gamma}\}\\ \mathcal{S}_2(\varepsilon) &:= \{\rho\in\mathcal{H}_d : \rho\geqslant \varepsilon\mathbb{1}, \mathrm{Tr}(\rho\vec{\Gamma}) = (1-d\varepsilon)\vec{\gamma} + \varepsilon\mathrm{Tr}(\vec{\Gamma})\}\\ \mathcal{S}_3 &:= \{\rho\in\mathcal{H}_d : \rho> 0, \mathrm{Tr}(\rho\vec{\Gamma}) = \vec{\gamma}\}\end{aligned}$$

where $\mathcal{H}_d$ is the set of $d\times d$ Hermitian matrices, and for compactness we write the constraints involving $\vec{\Gamma} = \{\Gamma_i\}$ as a vector equation. Here we take $\varepsilon > 0$ to be a small positive number, $\varepsilon \ll 1$.

**Proposition 4:** For $\varepsilon \ll 1$,

$$a_2(\varepsilon) \approx a_1. \tag{61}$$

*Proof.* The proof relies on the continuity of coherence and the fact that there exists a bijection between the domains $\mathcal{S}_1$ and $\mathcal{S}_2(\varepsilon)$. Let us construct this bijection map. Let the map $\mathcal{M}_\varepsilon$ act on a state $\rho$ via

$$\mathcal{M}_\varepsilon(\rho) = (1-d\varepsilon)\rho + \varepsilon\mathbb{1}.$$

Note that if $\rho\in\mathcal{S}_1$, then $\mathcal{M}_\varepsilon(\rho)\in\mathcal{S}_2(\varepsilon)$. Now consider the inverse map $\mathcal{M}_\varepsilon^{-1}$, whose action is given by

$$\mathcal{M}_\varepsilon^{-1}(\rho) = (\rho - \varepsilon\mathbb{1})/(1-d\varepsilon).$$

Note that $\mathcal{M}_\varepsilon^{-1}(\mathcal{M}_\varepsilon(\rho)) = \rho$. Also, if $\rho\in\mathcal{S}_2(\varepsilon)$, then $\mathcal{M}_\varepsilon^{-1}(\rho)\in\mathcal{S}_1$. Hence the maps $\mathcal{M}_\varepsilon$ and $\mathcal{M}_\varepsilon^{-1}$ establish a one-to-one pairing, i.e., a bijection, between the states in $\mathcal{S}_1$ and the states in $\mathcal{S}_2(\varepsilon)$.

Next we argue that this bijection does not change the coherence much, due to continuity of coherence. First note that the states $\rho$ and $\mathcal{M}_\varepsilon(\rho)$ are close in trace distance: $T(\rho,\mathcal{M}_\varepsilon(\rho)) = d\varepsilon T(\rho,\mathbb{1}/d)\leqslant d\varepsilon$. From Eq. (52) we have that

$$|\Phi(\rho,\Pi) - \Phi(\mathcal{M}_\varepsilon(\rho),\Pi)| \leqslant -2d\varepsilon\log_2\varepsilon. \tag{62}$$

The right-hand side of (62) goes to zero as $\varepsilon\to 0$. Hence, the range of coherence values associated with $\mathcal{S}_1$ is equal to the range of coherence values associated with $\mathcal{S}_2(\varepsilon)$, in the limit of small $\varepsilon$, proving the desired result. □

Finally, we argue that Problem 3 is a special case of Problem 2. Note that the following two conditions are equivalent:

$$(\rho > 0) \leftrightarrow (\exists\varepsilon > 0 \text{ such that } \rho\geqslant\varepsilon\mathbb{1}) \tag{63}$$

As a consequence, we have that

$$\lim_{\varepsilon\to 0^+} S_2(\varepsilon) = \mathcal{S}_3. \tag{64}$$

Combining this with Eq. (61), we have

$$a_3 = \lim_{\varepsilon\to 0^+} a_2(\varepsilon) = a_1. \tag{65}$$

Because of this, we can change the domain of our optimization, from positive semi-definite matrices to positive definite matrices. That is,

$$\alpha = \min_{\rho_{AB}\in\mathcal{C}_+} \Phi(\rho_{AB}, Z_A) \tag{66}$$

where

$$\mathcal{C}_+ = \{\rho_{AB}\in\mathcal{H}_{d_Ad_B} : \rho_{AB} > 0, \mathrm{Tr}(\rho_{AB}\vec{\Gamma}) = \vec{\gamma}\}. \tag{67}$$

### D. Dual problem

Due to a pesky factor of ln(2), it is useful to rescale the primal problem as follows:

$$\widehat{\alpha} := \alpha\ln(2) = \min_{\rho_{AB}\in\mathcal{C}_+} \widehat{\Phi}(\rho_{AB}, Z_A) \tag{68}$$

where, henceforth, we generally use the notation $\widehat{M} := M\ln(2)$, for any quantity $M$.

The dual problem [21] of (68) is given by the following unconstrained optimization:

$$\widehat{\beta} = \max_{\vec{\lambda}} \min_{\rho_{AB}\in\mathcal{D}_+} \mathcal{L}(\rho_{AB},\vec{\lambda}) \tag{69}$$

where

$$\mathcal{D}_+ = \{\rho_{AB}\in\mathcal{H}_{d_Ad_B} : \rho_{AB} > 0\}.$$

Here the Lagrangian is given by

$$\mathcal{L}(\rho_{AB},\vec{\lambda}) := \widehat{\Phi}(\rho_{AB}, Z_A) + \sum_i \lambda_i[\mathrm{Tr}(\rho_{AB}\Gamma_i) - \gamma_i] \tag{70}$$

where the $\vec{\lambda} = \{\lambda_i\}$ are Lagrange multipliers.

In what follows, we will go through several steps in order to simplify the dual problem. The main technical tools that we employ are entropic identities and a result from Ref. [19] that solves a relative entropy optimization problem.

It helps to first state the following identity for the relative entropy, from Refs. [17, 18].

**Lemma 5:** Let $\Pi = \{\Pi_j\}$ be a set of orthogonal projectors that decompose the identity, $\sum_j\Pi_j = \mathbb{1}$. For some density operator $\tau$, the closest density operator that is block-diagonal with respect to the $\Pi$ projectors is $\sum_j\Pi_j\tau\Pi_j$, provided closeness is measured by the relative entropy. That is:

$$\min_{\omega\in\mathcal{D}} D\Big(\tau||\sum_j\Pi_j\omega\Pi_j\Big) = D\Big(\tau||\sum_j\Pi_j\tau\Pi_j\Big) \tag{71}$$

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

*Proof.* For any state $\omega$, one can show that

$$D\Big(\tau||\sum_j \Pi_j\omega\Pi_j\Big) = D\Big(\tau||\sum_j \Pi_j\tau\Pi_j\Big) + D\Big(\sum_j \Pi_j\tau\Pi_j||\sum_j \Pi_j\omega\Pi_j\Big) \tag{72}$$

Since the last term in (72) is non-negative, this implies that the left-hand side cannot be smaller than the first term on the right-hand side. □

Hence we have

$$\widehat{\Phi}(\rho_{AB}, Z_A) = \widehat{D}\Big(\rho_{AB}||\sum_j Z_A^j\rho_{AB}Z_A^j\Big) \tag{73}$$

$$= \min_{\sigma_{AB}\in\mathcal{D}} \widehat{D}\Big(\rho_{AB}||\sum_j Z_A^j\sigma_{AB}Z_A^j\Big). \tag{74}$$

Next, we interchange the two minimizations in (69)

$$\min_{\rho_{AB}\in\mathcal{D}_+}\min_{\sigma_{AB}\in\mathcal{D}} f(\rho_{AB},\sigma_{AB},\vec{\lambda}) = \min_{\sigma_{AB}\in\mathcal{D}}\min_{\rho_{AB}\in\mathcal{D}_+} f(\rho_{AB},\sigma_{AB},\vec{\lambda}) \tag{75}$$

where

$$f(\rho_{AB},\sigma_{AB},\vec{\lambda}) := \widehat{D}\Big(\rho_{AB}||\sum_j Z_A^j\sigma_{AB}Z_A^j\Big) + \sum_i \lambda_i(\langle\Gamma_i\rangle - \gamma_i). \tag{76}$$

Ref. [19] solved a relative entropy optimization problem, a special case of which is our problem:

$$\min_{\rho_{AB}\in\mathcal{D}_+} f(\rho_{AB},\sigma_{AB},\vec{\lambda}). \tag{77}$$

From [19], the unique solution of (77) is

$$\rho_{AB}^* = \exp\Big(Q(\vec{\lambda}) + \ln\Big(\sum_j Z_A^j\sigma_{AB}Z_A^j\Big)\Big) \tag{78}$$

where

$$Q(\vec{\lambda}) := -\mathbb{1} - \sum_i \lambda_i\Gamma_i.$$

Inserting, (78) into (76) gives the optimal value

$$f(\rho_{AB}^*,\sigma_{AB},\vec{\lambda}) = -\mathrm{Tr}(\rho_{AB}^*) - \sum_i \lambda_i\gamma_i. \tag{79}$$

In summary the dual problem becomes:

$$\beta = \max_{\vec{\lambda}} \eta(\vec{\lambda}) \tag{80}$$

with

$$\eta(\vec{\lambda}) := -\max_{\sigma_{AB}\in\mathcal{D}} \Big[\mathrm{Tr}(\rho_{AB}^*) + \vec{\lambda}\cdot\vec{\gamma}\Big]. \tag{81}$$

### E. Lower bound

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

$$\mathrm{Tr}(\exp(A+B)) \leqslant \mathrm{Tr}(\exp(A)\exp(B)). \tag{82}$$

Applying this inequality gives:

$$\begin{aligned}\mathrm{Tr}(\rho_{AB}^*) &\leqslant \mathrm{Tr}\Big(\exp(Q(\vec{\lambda}))\exp(\ln\sum_j Z_A^j\sigma_{AB}Z_A^j)\Big)\\ &= \mathrm{Tr}\Big(\exp(Q(\vec{\lambda}))\sum_j Z_A^j\sigma_{AB}Z_A^j\Big)\\ &= \mathrm{Tr}\Big(\sum_j Z_A^j\exp(Q(\vec{\lambda}))Z_A^j\sigma_{AB}\Big).\end{aligned} \tag{83}$$

Next, note that

$$\max_{\sigma_{AB}\in\mathcal{D}} \mathrm{Tr}\Big(\sum_j Z_A^j\exp(Q(\vec{\lambda}))Z_A^j\sigma_{AB}\Big) = \Big\|\sum_j Z_A^j\exp(Q(\vec{\lambda}))Z_A^j\Big\|_\infty. \tag{84}$$

Hence, we have

$$\widehat{\beta} \geqslant \max_{\vec{\lambda}}\left[-\Big\|\sum_j Z_A^j\exp(Q(\vec{\lambda}))Z_A^j\Big\|_\infty - \vec{\lambda}\cdot\vec{\gamma}\right]. \tag{85}$$

By weak duality [21], the dual problem gives a lower bound on the primal problem, i.e., $\widehat{\alpha} \geqslant \widehat{\beta}$. So we arrive at our final result:

$$\alpha \geqslant \frac{1}{\ln(2)}\max_{\vec{\lambda}}\left[-\Big\|\sum_j Z_A^j\exp(Q(\vec{\lambda}))Z_A^j\Big\|_\infty - \vec{\lambda}\cdot\vec{\gamma}\right], \tag{86}$$

where the right-hand side is denoted as $\Theta$ in Theorem 1.

### F. POVMs

The above result, derived for projective measurements, naturally extends to POVMs, as follows. First we note that the primal problem is convex.

**Lemma 6:** Let system $E$ purify $\rho_{AB}$. Then $H(Z_A|E)$ is a convex function of $\rho_{AB}$.

*Proof.* Let $\mathbb{Z}_\mathbb{A} = \{\mathbb{Z}_\mathbb{A}^j\}$ be a Naimark extension of Alice's POVM $Z_A = \{Z_A^j\}$, i.e., $\mathbb{Z}_\mathbb{A}$ is a projective measurement on an enlarged Hilbert space $\mathcal{H}_\mathbb{A}$, in which $\mathcal{H}_A$ is a subspace. Since the $Z_A$ and $\mathbb{Z}_\mathbb{A}$ measurements have the same statistics, we have $H(Z_A|E) = H(\mathbb{Z}_\mathbb{A}|E)$. Let $V : \mathcal{H}_A \to \mathcal{H}_\mathbb{A}$ be the isometry that embeds system $A$ into the Naimark extended system, $\mathbb{A}$, and let

$\tilde{\rho}_{\mathbb{A}B} = (V \otimes \mathbb{1})\rho_{AB}(V^\dagger \otimes \mathbb{1})$ denote the Naimark extended state. From Refs. [15, 18], we have:

$$H(\mathbb{Z}_{\mathbb{A}}|E) = D\bigg(\tilde{\rho}_{\mathbb{A}B}||\sum_j \mathbb{Z}^j_{\mathbb{A}}\tilde{\rho}_{\mathbb{A}B}\mathbb{Z}^j_{\mathbb{A}}\bigg) \tag{87}$$

Due to the joint convexity of the relative entropy, it follows that the right-hand side of (87) is a convex function of $\rho_{AB}$, proving the desired result. □

Next we rewrite the primal problem in terms of a coherence-like quantity. Consider some POVM $P = \{P_j\}$ with $P_j \geqslant 0$ for each $j$, and $\sum_j P_j = \mathbb{1}$. Let us first define a generalized notion of coherence as follows,

$$\Phi_G(\rho, P) := D(\rho||\sum_j P_j\rho P_j) \tag{88}$$

where we note that the second argument $\sum_j P_j\rho P_j$ is not necessarily normalized.

Suppose Alice's measurement is an arbitrary POVM, $Z_A = \{Z^j_A\}$. Then, from Ref. [15], we have:

$$H(Z_A|E) \geqslant \Phi_G(\rho_{AB}, Z_A) \tag{89}$$

where $E$ can be taken to purify $\rho_{AB}$. Hence we can define (or lower bound) the primal problem as

$$\alpha := \min_{\rho_{AB}\in\mathcal{C}} \Phi_G(\rho_{AB}, Z_A) \tag{90}$$

One can show that $\Phi_G(\rho, P)$ is continuous in $\rho$ using an argument similar to the one in Sec. VII B. Hence the domain of optimization can be restricted, as in (66), to positive definite matrices:

$$\alpha = \min_{\rho_{AB}\in\mathcal{C}_+} \Phi_G(\rho_{AB}, Z_A) \tag{91}$$

where $\mathcal{C}_+$ is defined in (67).

One can then transform to the dual problem, as described above. The only subtlety is that the analog of Eq. (74) can be written as an inequality:

$$\widehat{\Phi}_G(\rho_{AB}, Z_A) = \widehat{D}\bigg(\rho_{AB}||\sum_j Z^j_A\rho_{AB}Z^j_A\bigg) \tag{92}$$

$$\geqslant \min_{\sigma_{AB}\in\mathcal{D}} \widehat{D}\bigg(\rho_{AB}||\sum_j Z^j_A\sigma_{AB}Z^j_A\bigg). \tag{93}$$

The rest of the derivation proceeds as described in the previous subsection.

## VIII. CONCLUSIONS

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 power of our approach is perhaps demonstrated best by Fig. 5, which shows that our numerical method dramatically outperforms a commonly used analytical method for lower-bounding the key rate.

The practical motivation for our work is two-fold. First, experimental imperfections tend to break symmetries, which means that 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, we are interested in discrete-variable QKD protocols involving coherent states, i.e., where a small, discrete set of coherent states are the signal states and information may be encoded in the phase, e.g., as in Ref. [22]. Our aim is to apply our approach to protocols such as this, where the key rate is currently unknown.

We also 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 [13].

We envision that our method could be a standard tool for researchers in the field. We hope to make our MATLAB code publicly available in the distant future. In the meantime, the result in Theorem 1 is simple enough for anyone to use.


[1] S. Wiesner, ACM SIGACT News **15**, 78 (1983), ISSN 01635700.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Reviews of Modern Physics **81**, 1301 (2009), ISSN 0034-6861, URL `http://link.aps.org/doi/10.1103/RevModPhys.81.1301`.

[3] A. Ferenczi and N. Lütkenhaus, Physical Review A **85**, 1 (2012), ISSN 10502947, 1112.3396.

[4] C. H. Bennett and G. Brassard, in *International Conference on Computers, Systems & Signal Processing, Bangalore, India* (1984), pp. 175–179.

[5] D. Bruss, Physical review letters **81**, 3018 (1998), ISSN 0031-9007, 0106126.

[6] C. H. F. Fung and H. K. Lo, Physical Review A -

Atomic, Molecular, and Optical Physics **74**, 1 (2006), ISSN 10502947, 0607056v3.

[7] O. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010), URL http://link.aps.org/doi/10.1103/PhysRevA.82.032337.

[8] E. Woodhead, Physical Review A **88**, 012331 (2013), ISSN 1050-2947, 1303.4821, URL http://arxiv.org/abs/1303.4821$\delimiter"026E30F$nhttp://link.aps.org/doi/10.1103/PhysRevA.88.012331.

[9] K. Tamaki, M. Curty, G. Kato, H.-k. Lo, and K. Azuma, Physical Review A **90**, 052314 (2014), ISSN 10941622, arXiv:1312.3514v2.

[10] I. Devetak and A. Winter, Proceedings of the Royal Society A **461**, 207 (2005), ISSN 1364-5021, 0306078, URL http://arxiv.org/abs/quant-ph/0306078.

[11] L. Sheridan and V. Scarani, Physical Review A - Atomic, Molecular, and Optical Physics **82**, 1 (2010), ISSN 10502947, 1003.5464.

[12] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, Physical Review A - Atomic, Molecular, and Optical Physics **88**, 1 (2013), ISSN 10502947, 1402.5810.

[13] V. Scarani and R. Renner, Physical Review Letters **100**, 1 (2008), ISSN 00319007, 0708.0709.

[14] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nature Physics **6**, 659 (2010), ISSN 1745-2473, URL http://www.nature.com/doifinder/10.1038/nphys1734.

[15] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, Physical Review A **83**, 062338 (2011), ISSN 1050-2947, URL http://link.aps.org/doi/10.1103/PhysRevA.83.062338.

[16] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature communications **3**, 634 (2012), ISSN 2041-1723, URL http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3274703&tool=pmcentrez&rendertype=abstract.

[17] K. Modi, T. Paterek, W. Son, V. Vedral, and M. Williamson, Physical Review Letters **104**, 1 (2010), ISSN 00319007, 0911.5417.

[18] P. J. Coles, Physical Review A **85**, 042103 (2012), ISSN 1050-2947, URL http://link.aps.org/doi/10.1103/PhysRevA.85.042103.

[19] M. Zorzi, F. Ticozzi, and A. Ferrante, IEEE Transactions on Information Theory **60**, 357 (2014), ISSN 00189448, 1301.6658.

[20] T. Baumgratz, M. Cramer, and M. B. Plenio, pp. 1–10 (2013), 1311.0275, URL http://arxiv.org/abs/1311.0275.

[21] S. Boyd and L. Vandenberghe, *Convex Optimization*, vol. 25 (2010), ISBN 9780521833783, 1111.6189v1, URL https://web.stanford.edu/~boyd/cvxbook/bv_cvxbook.pdf.

[22] H. Lo and J. Preskill, Quantum Information and Computation **7**, 431 (2007), 0610203v2, URL http://arxiv.org/abs/quant-ph/0610203.