Finite-key security analysis for multilevel quantum key distribution

New Journal of Physics

CrossMark

PAPER

Finite-key security analysis for multilevel quantum key distribution

Kamil Brádler[1,2], **Mohammad Mirhosseini**[3], **Robert Fickler**[4], **Anne Broadbent**[1] and **Robert Boyd**[3,4]

1   Department of Mathematics and Statistics, University of Ottawa, Canada
2   Max Planck Centre for Extreme and Quantum Photonics, University of Ottawa, Canada
3   The Institute of Optics, University of Rochester, Rochester, NY 14627, USA
4   Department of Physics and Max Planck Centre for Extreme and Quantum Photonics, University of Ottawa, Ottawa, K1N 6N5, Canada

E-mail: kbradler@uottawa.ca

Abstract

We present a detailed security analysis of a d-dimensional quantum key distribution protocol based on two and three mutually unbiased bases (MUBs) both in an asymptotic and finite-key-length scenario. The finite secret key rates (in bits per detected photon) are calculated as a function of the length of the sifted key by (i) generalizing the uncertainly relation-based insight from BB84 to any d-level 2-MUB QKD protocol and (ii) by adopting recent advances in the second-order asymptotics for finite block length quantum coding (for both d-level 2- and 3-MUB QKD protocols). Since the finite and asymptotic secret key rates increase with d and the number of MUBs (together with the tolerable threshold) such QKD schemes could in principle offer an important advantage over BB84. We discuss the possibility of an experimental realization of the 3-MUB QKD protocol with the orbital angular momentum degrees of freedom of photons.

1. Introduction

It has been more than 30 years since the proposal of the first quantum key distribution (QKD) protocol—BB84 [1]. The ultimate goal of a QKD protocol is to establish a secure key between two parties for a further cryptographic use; in this context, quantum mechanics is a powerful ally of the legitimate parties. Therefore, it is advantageous to generate the key by distributing and measuring quantum states. Contrary to communication with classical signals, for quantum states there exists a fundamental trade-off between how much information a classical or quantum adversary can get and how much the quantum system is disturbed. For example, the most straightforward strategy of simply copying a quantum state does not work [2, 3]. A significant amount of effort has been invested in proving the security of BB84 and subsequent QKD protocols (starting with its proper definition [4, 5]) and experimental realization [6].

Most of the modern QKD schemes rely on two-level quantum systems (qubits) as quantum information carriers. This is especially easy to achieve using the photon polarization degree of freedom. The theoretical background as well as the experimental techniques are mature. However, quantum d-level states (qudits) have attracted much attention recently because they naturally offer higher quantum information transmission rates and together with continuous variables are promising candidates for next generation quantum information processing. In this approach, the information is encoded onto d distinct orthogonal states, for which in principle there is no upper limit on d. In the context of QKD, the d-level protocols not only offer a great potential to increase the transmitted key rate but they are also known to be more resilient to errors [7]. Experimentally, high-dimensional quantum states have been realized as discrete time-bins [8], positions [9] or angular momenta [10] in lab-scale proof-of-principle tests. They have also been successfully studied under real world environmental conditions where air turbulence or inter-modal coupling in fibers have to be taken into account [11, 12].

The experimental efforts for realization of multidimensional QKD has primarily relied on employing two mutually unbiased bases (MUBs). However, it is known that using only two MUBs for $d = 2$ does not realize the full potential of a qubit-based QKD. Instead, by using three MUBs we are rewarded by an increase in the

maximum tolerable error rate in a QKD protocol known as the six-state protocol [13]. Considering this observation, it is expected that using more than two MUBs would provide enhancement in the security of the d-dimensional QKD protocols. It is well known that for d a prime number or the power of a prime, the maximum number of MUBs in a d-dimensional Hilbert space is $d + 1$ [14, 15]. For the non-prime dimensions, the number of MUBs is a major open problem. However, it is perhaps less well known that there always exists three MUBs for any d [16]. Motivated by this fact, we present a comprehensive security analysis for d-level QKD with two and three MUBs. Our main contribution in this paper is the calculation of the secret key rate upper bounds for discrete d-dimensional QKD protocols using two and three MUBs. We exemplify the key rate calculations on $d = 2$ to 7 but our approach can be immediately applied for any d. The secret key rates are calculated in both the asymptotic and finite key length scenario. In the asymptotic case, the 2-MUB rates reproduce the previously known results [6, 7, 17–25] but to our best knowledge the analytical results we obtain for 3-MUB rates and for any d are novel and the corresponding adversarial channels have not been studied before (only the $d = 2$ case reduces to the well studied six-state protocol [13]). The main reason to reproduce the already known results for the 2-MUB QKD protocol is the calculation method that may not be familiar to the practitioners of QKD. It can be summarized as '*ab initio*' since our starting point is the private classical capacity and the quantum capacity of a quantum channel [4] and we systematically derive the well-known expressions for the secret key rate. The main result of the asymptotic part of our analysis is the secret key rate calculation for the 3-MUB protocol and the derivation of the tolerable threshold for the error rate. We found that the threshold quite substantially increases accompanied by the increase of the secret key rate[5] as envisaged by the comparison of BB84 and the six-state protocol. Our results justify the overlapping numerical results presented in [26].

The second part of our analysis is the study of QKD in the non-asymptotic regime of a finite number of exchanged signals. We follow two different routes leading to excellent (achievable [27]) upper bounds on the secret key rates even for a relatively low number of signals. The first approach is the generalization of the uncertainty relation-based approach pioneered in [28] for two MUBs and $d = 2$. We generalize the key step spelled out in [29] for any d and using the large deviation estimate for the number of errors in the non-sacrificed part of the sifted key we derived the corresponding secret key rates. The intermediate step includes a numerical optimization over the ratio of dits in the secret key rates that are sacrificed for the parameter estimation purposes. As the number of sifted bits asymptotically increases the portion of sacrificed bits tends to zero [30] and the secret key rates approach the asymptotic ones derived previously. For another approach to the non-asymptotic regime see [31, 32].

The uncertainty-relation-based method is, however, not known to be applicable to the 3-MUB QKD protocol [28]. More precisely, it can be enforced even for three MUBs but our attempts lead to awfully suboptimal rates. Hence we adopt a different strategy. Using the recent advances in the second-order asymptotics for the quantum coding rates [33] we use the expansion of the relevant entropic quantity (the smooth min-entropy) in terms of the conditional entropy variance [33, 34] and expand the decoupling exponent of what is essentially a one-shot decoupling lemma [28]. The resulting rates are calculated both in the 2- and 3-MUB QKD scenario. In the latter, the resulting secret key rates are better for any d compared to the basic estimate first brought by Renner in [23] that is used as a template in almost all finite key studies. Since the 3-MUB QKD protocol for any d seems to be systematically studied for the first time here, it therefore establishes the best known secret key rates. The second-order asymptotic expansion also beats Renner's rates for the 2-MUB QKD protocol (for any d) but it is not as good as the uncertainty-relation-based estimates. This is the expected kind of behavior.

The remainder of the paper is structured as follows. In section 2 we introduce the minimal background material and notation for our approach to calculate the asymptotic secret key rates and collect several rudimentary facts about the Pauli group for qudits and mutually unbiased basis. We also recall the Choi-Jamiołkowski state-map correspondence. The asymptotic rates for 2- and 3-MUB QKD protocol are calculated in section 3. In section 4 we introduce the necessary entropic quantities that come out in the expressions for finite key length secret key rates and derive the previously discussed non-asymptotic secret key rates. In section 5 we describe one possible laboratory implementation of our results by considering photonic OAM based QKD schemes, which have become a promising candidate for real-life high-dimensional QKD applications. We show the spatial modes that would be required for three MUBs and describe possible next steps and open challenges. We, however, do not analyze the security of the studied QKD protocols by considering all realistic parameters such a platform offers. This would include taking into account the efficiency of photon sources and detectors together with the suboptimality of certain classical information algorithms used in the postprocessing step. The

---

[5] The secret key rate units are bits per channel where the channel is understood as a completely positive map whose exact form will be derived. Therefore our notion of a channel differs from its typical use in quantum optics experiments. A quantum channel is said to be realized in the QKD context whenever the photon is detected and used in the process of secret key extraction (not discarded). Knowing the number of realizations of the channel per second gives us the total number of secret bits per a unit of time, sometimes perhaps confusingly also called a rate.

experimental inefficiencies do not affect the secret key rate (measured by bits per channel) but rather the speed of how many secret bits one is able to collect per given time period.

2. Security of asymptotic QKD and preliminaries

The modern definition of security for a quantum key distribution protocol requires the final state ϱ_{ABE} to satisfy

$$\left\| \varrho_{ABE} - \frac{1}{|K|} \sum_{k \in K} |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B \otimes \tau_E \right\|_1 \leqslant \epsilon. \tag{1}$$

The indices A, B stand for the legitimate sender and receiver and E is an adversary (Eve). The condition says that after the protocols ends, the legitimate parties share classical correlations (in this case a classical key $\{ |k\rangle\langle k| \}_k$), where the knowledge of Eve can be made arbitrarily small—the quantum system in her possession is *decoupled* from the legitimate participants. The expression $\|M\|_1 \overset{\mathrm{df}}{=} \mathrm{Tr}\sqrt{MM^\dagger}$ denotes the trace norm. This approach was first rigorously introduced in a great generality in [4] and in the context of QKD also in [5]. The marginal state ϱ_B can be seen as an output of a noisy quantum channel $\mathcal{N}$ between a sender and a receiver. They do not know whether the noisy evolution is caused by decoherence of any kind or by an eavesdropper and mainly they must not care. As long as they know the channel and are able to use it asymptotically (sending a large number of quantum signals) one can often easily determine whether a secret key can be established. Here comes the idea of asymptotic QKD: with an ever increasing number of channel uses the parameter on the rhs of equation (1) is required to become arbitrarily small. For some channels this condition cannot ever be satisfied and in that case the asymptotic QKD is impossible. The normalized rate at which establishing classical correlation over a noisy quantum channel is in principle possible is called the *private classical capacity* of $\mathcal{N}$. Note that a secret key is a form of classical correlations [4]. If the private capacity is zero, equation (1) cannot be satisfied in the sense that Eve cannot be arbitrarily well decoupled from the state shared by the sender (A) to a receiver (B). The private classical capacity is given by

$$P(\mathcal{N}) \overset{\mathrm{df}}{=} \lim_{n \to \infty} \frac{1}{n} \sup_{\varrho_{XA^n}} P(\mathcal{N}^{\otimes n}, \varrho), \tag{2}$$

where

$$P(\mathcal{N}, \varrho) \overset{\mathrm{df}}{=} I(X; B)_\sigma - I(X; E)_\sigma \tag{3}$$

is the *private information*. The state $\sigma_{XBE} = \sum_x p_x |x\rangle\langle x| \otimes \sigma_{x,BE}$ is given by the action of a channel isometry $W_\mathcal{N} : A \mapsto BE$ on a classical-quantum input state $\varrho_{XA} = \sum_x p_x |x\rangle\langle x| \otimes \varrho_{x,A}$ and X denotes a classical random variable with a probability distribution P ($p_x \equiv \Pr(X = x)$). The quantity $I(A; B)$ is called the *quantum mutual information* defined as

$$I(A; B)_\sigma = H(A)_\sigma + H(B)_\sigma - H(AB)_\sigma, \tag{4}$$

where $H(A)_\sigma \overset{\mathrm{df}}{=} - \mathrm{Tr}[\sigma_A \log \sigma_A]$ is the von Neumann entropy[6] of a (possibly multipartite) state $\sigma_{AB\ldots Z}$. The private classical capacity in (2) is an unconstrained optimization problem whose tractable solution for a general channel $\mathcal{N}$ is not known at present and even the calculation of the *one-shot* private capacity ($n = 1$)

$$P^{(1)}(\mathcal{N}) \overset{\mathrm{df}}{=} \sup_{\varrho_{XA}} P(\mathcal{N}, \varrho) \tag{5}$$

is not straightforward since ϱ_A admits a mixed state decomposition $\varrho_A = \sum_x p_x \varrho_{x,A}$.

Another fundamental quantity, seemingly unrelated to QKD, is called the *quantum channel capacity* [4]

$$Q(\mathcal{N}) \overset{\mathrm{df}}{=} \lim_{n \to \infty} \frac{1}{n} \sup_{\varrho_{A^n}} Q(\mathcal{N}^{\otimes n}, \varrho), \tag{6}$$

where

$$Q(\mathcal{N}, \varrho) \overset{\mathrm{df}}{=} H(B)_\vartheta - H(E)_\vartheta \tag{7}$$

is the *coherent information*. The isometry now acts on ϱ_A that (crucially) can be limited to a convex sum of rank-one states $\omega_{x,A}$ as $W_\mathcal{N} : \sum_x p_x |\omega_x\rangle\langle\omega_x|_A \mapsto \vartheta_{BE}$. The quantum capacity follows from a stronger condition than equation (1)—that the main goal is to successfully transmit a quantum state from a sender to a receiver who happens to be decoupled from the environment E (completely controlled by an adversary). Quantum channel capacity (6) is also intractable for a general channel $\mathcal{N}$ but the one-shot quantity (also called the optimized coherent information)

---

[6] Log is the logarithm base two and ln denotes the natural logarithm throughout the paper.

$$Q^{(1)}(\mathcal{N}) \overset{\mathrm{df}}{=} \sup_{\varrho_A} Q(\mathcal{N}, \varrho) \tag{8}$$

is fairly easy to evaluate (often not analytically but the numerics will do the job).

The decoupling mechanism is naturally useful for secret key generation. This is because the quantum capacity can crucially be interpreted as the one-way entanglement distillation rate which itself is a lower bound on the one-way secret key rate [4]. Once the parties share maximally entangled states, they can be used to teleport any type of information, in particular a secret key, at the same rate the pairs were distilled. Hence the quantum capacity is a channel secret key rate lower bound. Formally, it can be shown in the following way [4] (see also [35]). From equation (5) and the definition of the mutual information we write

$$P^{(1)}(\mathcal{N}) = \sup_{\varrho_{XA}} [I(X; B)_\sigma - I(X; E)_\sigma], \tag{9a}$$

$$= \sup_{\varrho_{XA}} [H(B)_\sigma - H(BX)_\sigma - H(E)_\sigma + H(EX)_\sigma], \tag{9b}$$

$$= \sup_{\varrho_{XA}} \left[H(B)_\sigma - H(E)_\sigma - \sum_x p_x (H(B)_{\sigma_x} - H(E)_{\sigma_x}) \right], \tag{9c}$$

$$= \sup_{\varrho_A} [H(B)_\sigma - H(E)_\sigma] - \inf_{\varrho_{XA}} \sum_x p_x (H(B)_{\sigma_x} - H(E)_{\sigma_x}), \tag{9d}$$

$$= Q^{(1)}(\mathcal{N}) - \inf_{p_x, \varrho_{x,A}} \sum_x p_x Q(\mathcal{N}, \varrho_x). \tag{9e}$$

Equation (9c) follows from

$$H(BX)_\sigma = H\left(\sum_x p_x |x\rangle\langle x| \otimes \sigma_{x,B} \right) = H(X)_P + \sum_x p_x H(B)_{\sigma_x}$$

and similarly for the $H(EX)_\sigma$. The first two summands in equation (9d) can be optimized over ϱ_A instead of ϱ_{XA} since we trace over the classical variable X. The von Neumann entropy $H(X)_P$ over a classical probability distribution P is simply the Shannon entropy $S(\{p_x\}) \overset{\mathrm{df}}{=} -\sum_x p_x \log p_x$. In the end we arrived at [4]

$$Q^{(1)}(\mathcal{N}) \leqslant P^{(1)}(\mathcal{N}) \tag{10}$$

and thus the lhs turns out to be a useful lower bound in the QKD scenario as claimed. The equality is achieved for $\varrho_{x,A} = |\omega_x\rangle\langle\omega_x|_A$ in which case $H(B)_{x,\vartheta} = H(E)_{x,\vartheta}$ for all x and so $Q(\mathcal{N}, \varrho_x) = 0$.

The usual starting point for an asymptotic analysis of a QKD's secret key rate r is the following formula [5][7]

$$r_n \overset{\mathrm{df}}{=} \frac{1}{n} \min_{\sigma_{AB} \in \Gamma} [H(X^n|E^n)_\sigma - H(X^n|Y^n)_\sigma], \tag{11}$$

where $\sigma_{A^n B^n E^n}$ is a pure tripartite state shared by all parties, σ_{XYE} is a classical-quantum state obtained by measuring $\sigma_{A^n B^n E^n}$ (so X, Y are classical variables also called a raw key) and n is the block size. The marginal state $\sigma_{A^n B^n}$ over which is being optimized is essentially a Choi state introduced on p 6. The set Γ are all Choi states compatible with the channel estimation step in the protocol and we will see it in action in equations (23c). Finally, the expression in equation (11)

$$H(A|B)_\varrho \overset{\mathrm{df}}{=} H(AB)_\varrho - H(B)_\varrho \tag{12}$$

is the quantum conditional entropy. We can quickly see the equivalence between equation (11) and $P^{(1)}(\mathcal{N}) = \sup_{\varrho_{XA}} [H(X|E)_\sigma - H(X|B)_\sigma]$ from equation (9b). We get rid of the supremum by realizing that in all mainstream QKD protocols, the input states (or private codes) ϱ_A are pure states (or mixtures thereof) leaving us with the classical-quantum input state of the form $\varrho_{XA} = \sum_x p_x |x\rangle\langle x| \otimes |\omega_x\rangle\langle\omega_x|_A$. The maximum is achieved for ϱ_A maximally mixed and so from equation (9e) we get $P^{(1)}(\mathcal{N}) = Q^{(1)}(\mathcal{N})$, see below (10)[8]. In the second step, we realize that in all QKD protocols, Bob applies a POVM on the received quantum state generating a classical variable Y and so equation (11) for $n = 1$ has been recovered

$$Q^{(1)}(\mathcal{N}) = r_1,$$

where σ_{AB} from the rhs represents $\mathcal{N}$ on the lhs via the Choi–Jamiołkowski isomorphism (see p 6). There is also a missing sup for r_1 (or r_n in general) as opposed to $Q^{(1)}(\mathcal{N})$ and this a subtle point. From the quantum capacity standpoint, the channel $\mathcal{N}$ is given and the maximization is over all possible input states ϱ_A (quantum codes). In the QKD scenario (specifically in its entanglement version) the parties try to share maximally entangled states

---

[7] The actual expression for the key rate can be applied under very general circumstances, see [5], corollary 6.5.2.

[8] Note that we are not *a priori* assuming anything. If a new QKD protocol is invented, the fact that the one-shot private capacity is maximized for a maximally mixed state must be proved.

and the most reasonable strategy is obviously to start the distribution with maximally entangled states (quantum codes)[9]. The fact that they may become disrupted due to decoherence or an eavesdropper implies that the channel will be different. As we will see later, such a disrupted code *is* a channel representation (the Choi matrix).

Pauli group for qudits and MUBs

It is instructive to investigate the case of two complementary bases (MUBs) for higher-dimensional Hilbert spaces. To this end, we first informally introduce the qudit Pauli group Π_d. It has two generators $X_d, Z_d \in \Pi_d$ defined as

$$X_d = \sum_{k=0}^{d-1} |k \oplus 1\rangle\langle k|, \tag{13a}$$

$$Z_d = \sum_{k=0}^{d-1} \omega^k |k\rangle\langle k|, \tag{13b}$$

where $\omega = \exp 2\pi i/d$ and $\oplus$ is addition modulo d. An arbitrary element of Π_d is then $X_d^\alpha Z_d^\beta$ for $0 \leqslant \alpha, \beta \leqslant d - 1$.

From other useful properties of the qudit Pauli group let us recall that the special case of Weyl commutation relations [16]) reads

$$X_d Z_d = Z_d X_d e^{i\zeta_d}. \tag{14}$$

Hence, the eigenvector v_d in the equation $X_d Z_d v_d = e^{i\lambda_d} v_d$ is also an eigenvector of $X_d^\alpha Z_d^\alpha$ (up to a phase). This is because

$$X_d^\alpha Z_d^\alpha = (X_d Z_d)^\alpha e^{i\kappa\zeta_d}, \tag{15}$$

where $\kappa = (\alpha^2 - \alpha)/2$ counts the total number of passes of Z_d through X_d. But v_d is also an eigenvector of the rhs (up to a phase).

Choi–Jamiołkowski representation of quantum channels

A remarkable way of representing a quantum channel is known as the Choi–Jamiołkowski isomorphism [37, 38]. Let $\mathcal{N}$ be the quantum channel. Then there exists a positive semi-definite map $R_{\mathcal{N}}$, sometimes called *Choi matrix*, that represents the action of the channel via

$$\mathcal{N} \circ \varrho_A = \text{Tr}_A[(\varrho_A^\top \otimes \text{id}_B) R_{\mathcal{N}}]. \tag{16}$$

The channel $\mathcal{N}$ is trace-preserving if its Choi matrix satisfies $\text{Tr}_B R_{\mathcal{N}} = \text{id}_A$. Conversely, any quantum channel $\mathcal{N}$ gives rise to a Choi matrix

$$R_{AB}(\mathcal{N}) = (\text{id}_A \otimes \mathcal{N}) \circ \Phi_{AA'}, \tag{17}$$

where $\Phi_{AA'} = \sum_{i=1}^{d_A} |i\rangle_A |i\rangle_{A'}$ is an un-normalized maximally entangled state. The physical interpretation of the Choi matrix is as if the communicating parties shared a maximally entangled qudit pair. Instead of sending the actual qudit through the channel one sends a half of a maximally entangled state. The Choi matrix is usually derived from another channel representation (Kraus maps, for example) but almost all QKD schemes allow its direct construction. This leads to the so-called diagonal Bell state. To see this, recall that the states in many QKD schemes are always sent in one of the MUB bases. That means that the number of possible errors can be enumerated—one just needs to find the error generators causing a bit flip in at least one of the bases. These are precisely the elements of the Pauli group Π_d and so the Choi matrix reads

$$\tilde{R}_{AB}(\mathcal{N}) = \sum_{\alpha,\beta=0}^{d-1} \lambda_{\alpha\beta} (\text{id} \otimes X_d^\alpha Z_d^\beta) \tilde{\Phi}_{AA'}. \tag{18}$$

Starting from (18), the operation $\circ$ in (17) becomes an ordinary matrix multiplication and the tilde indicates a normalized state. The probability error coefficients satisfy $1 \geqslant \lambda_{\alpha\beta} \geqslant 0$ together with $\sum_{\alpha,\beta=0}^{d-1} \lambda_{\alpha\beta} = 1$.

3. Derivation of the 2- and 3-MUB QKD adversarial channels for qudits and their asymptotic secret key rates

We adopt and reformulate the method of adversarial channel derivation from [5]. A concise version also appears in appendix A of [6].

---

[9] A more general idea, that we will not discuss further, is the possibility already envisaged in [4] to go beyond entanglement distillation protocols in order to establish classical secret correlations. It indeed turns out that one can distribute so-called 'private states' [36] for this purpose. This is precisely the situation where $Q^{(1)}(\mathcal{N}) = 0$ but $P^{(1)}(\mathcal{N}) > 0$.

2 MUBs

The error analysis is straightforward. In the bit basis (the eigenvectors of Z_d), the errors are caused by X_d^α (there is $d-1$ of them) and $X_d^\alpha Z_d^\beta$ for all $\alpha, \beta > 0$ (there is $(d-1)^2$ of them in total). Hence the measured error rate in the bit basis reads

$$Q_b = (d-1)\lambda_Z + (d-1)^2\lambda_?, \tag{19}$$

where $\lambda_Z \equiv \lambda_{0\beta}$ and $\lambda_?$ is the rest. Similarly for the phase basis, by setting $\lambda_X \equiv \lambda_{\alpha 0}$ we obtain

$$Q_p = (d-1)\lambda_X + (d-1)^2\lambda_?. \tag{20}$$

It is common and experimentally reasonable [6] to set the error rates equal $Q_b = Q_p \equiv Q$. The normalization condition yields

$$\lambda_{00} = 1 - 2Q + (d-1)^2\lambda_? \tag{21}$$

and it is perhaps clear that $\lambda_?$ is a free parameter that needs to be determined by taking the best Eve's strategy. Following [5], the most general quantum attack is a collective attack. A collective attack is Eve's interaction with a passing qubit one by one with an eventual collective measurement deferred until the quantum transmission is over. In this light, the maximum amount of information provided to Eve is given by the *minimized* coherent information equation (7) which we readily rewrite as

$$Q(\mathcal{N}, \tilde{\Phi}_{AA'}) = H(B)_{\tilde{R}} - H(AB)_{\tilde{R}}. \tag{22}$$

Indeed, the normalized Choi matrix $\tilde{R}$ serves a double purpose: it is a channel representation but also an output of the channel whose input is maximally entangled with the reference system A (see equation (17)). The minimized rhs can be immediately evaluated

$$\min_{\lambda_?} Q(\mathcal{N}, \tilde{\Phi}_{AA'}) = \min_{\lambda_?}[H(B)_{\tilde{R}} - H(AB)_{\tilde{R}}], \tag{23a}$$

$$= \log d + \min_{\lambda_?} \sum_{\alpha,\beta=0}^{d-1} \lambda_{\alpha\beta} \log \lambda_{\alpha\beta}, \tag{23b}$$

$$= \log d + \min_{\lambda_?}[(1 - 2Q + (d-1)^2\lambda_?)\log[1 - 2Q + (d-1)^2\lambda_?]$$
$$+ 2(d-1)\frac{Q - (d-1)^2\lambda_?}{d-1} \log \frac{Q - (d-1)^2\lambda_?}{d-1}$$
$$+ (d-1)^2\lambda_? \log \lambda_?]. \tag{23c}$$

Equality (23b) follows from $\mathrm{Tr}_A[\tilde{R}_{AB}] = \mathrm{id}/d$ (the channel represented by R_{AB} ($\tilde{R}_{AB}$) is unital). We also used the fact that $\tilde{R}_{AB}$ is Bell-diagonal in order to calculate $H(AB)_{\tilde{R}}$ using equations (19)–(21). From (23c), by setting $\frac{\mathrm{d}}{\mathrm{d}\lambda_?}[Q(\mathcal{N}, \tilde{\Phi}_{AA'})] = 0$, we find the stationary point

$$\lambda_? = \frac{Q^2}{(d-1)^2} \tag{24}$$

and $\frac{\mathrm{d}^2}{\mathrm{d}^2\lambda_?}[Q(\mathcal{N}, \tilde{\Phi}_{AA'})]|_{(24)} = \frac{(d-1)^4}{(Q-1)^2 Q^2 \ln 2} > 0$ reveals a minimum for all d and Q. Then

$$\lambda_Z = \lambda_X = \frac{Q(1-Q)}{d-1} \tag{25}$$

and as a result we get

$$\mathcal{N}_d^{2\mathrm{MUBs}}(\varrho) = (1-Q)^2\varrho + \frac{Q(1-Q)}{d-1}\sum_{\alpha=1}^{d-1} X_d^{\alpha}\varrho X_d^{\alpha\dagger} + \frac{Q(1-Q)}{d-1}\sum_{\beta=1}^{d-1} Z_d^{\beta}\varrho Z_d^{\beta\dagger}$$
$$+ \frac{Q^2}{(d-1)^2}\sum_{\alpha,\beta=1}^{d-1} X_d^{\alpha}Z_d^{\beta}\varrho(X_d^{\alpha}Z_d^{\beta})^{\dagger} \tag{26}$$

also called the BB84 channel for $d = 2$. The secret key rates obtained by plugging equation (24) into equation (23c) read

$$Q^{(1)}(\mathcal{N}_d^{2\mathrm{MUBs}}) = \log d + 2[Q\log Q + (1-Q)\log(1-Q) - Q\log(d-1)] \tag{27}$$

and are plotted in figure 1 for $d = 2$ to 7. For $d = 2$ the rate goes to zero for $Q \approx 0.11$ which is the famous threshold derived in [39].
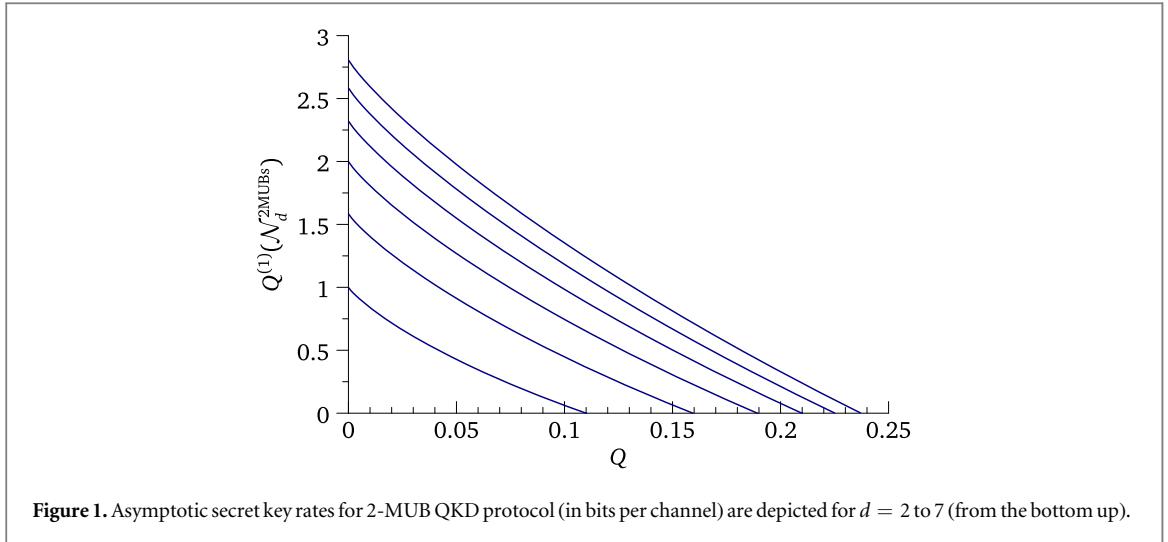
Figure 1. Asymptotic secret key rates for 2-MUB QKD protocol (in bits per channel) are depicted for $d = 2$ to 7 (from the bottom up).

2 MUBs via equation (11)

We can recover one of our earlier results also from equation (11). First, since $H(X) = H(B) = \log d$ and by using equation (4) together with the identity $H(B) - H(B|X) = H(X) - H(X|B)$ we get

$$H(X|B) = H(B|X) = -(1 - Q)\log(1 - Q) - Q \log Q + Q \log(d - 1). \tag{28}$$

The channel $\mathcal{N}_d^{2\text{MUBs}}$ is unital: $\mathcal{N}_d^{2\text{MUBs}} : \frac{\text{id}_d}{d} \mapsto \frac{\text{id}_d}{d}$. Therefore, Bob's information is classical (knowing the basis he perfectly measures the raw bit value), $Y \equiv B$ and $H(X|B) = H(X|Y)$. We also find

$$\frac{H(E)}{2} = H(E|X) \equiv H(B|X)$$

and by using $H(E) - H(E|X) = H(X) - H(X|E)$ we get

$$H(X|E) = \log d - H(E|X). \tag{29}$$

Putting it all together, we obtain

$$r_1^{(d,2\text{MUBs})} = \log d + 2[(1 - Q)\log(1 - Q) + Q \log Q - Q \log(d - 1)] \equiv Q^{(1)}(\mathcal{N}_d^{2\text{MUBs}}) \tag{30}$$

in accordance with equation (27).

The reason for the repetition of the previous analysis is two-fold. Besides showing that our earlier approach via quantum/private capacity is valid and arguably more perspicuous, the secret key rates of the form of equation (11) enable a nice interpretation of the entropic quantities and a direct comparison with the results coming from the finite key size analysis performed in [28], which is based on the one-shot entropic uncertainty relations. The second point will be discussed in detail in section 4. To illustrate the first point, note that for $d = 2$ we may rewrite equation (11) in an even more familiar form [6]

$$r_1^{(d,2\text{MUBs})} = 1 - h(Q) - \text{leak}_{\text{EC}}, \tag{31}$$

where $h(Q) \stackrel{\text{df}}{=} -(1 - Q)\log(1 - Q) - Q \log Q$ is the binary Shannon entropy and $\text{leak}_{\text{EC}} = h(Q)$ is the information leaked to Eve during the error correction (information reconciliation) procedure.

Going back to a general d, typically, $\text{leak}_{\text{EC}} > H(X|Y)$ (recall $Y \equiv B$ from below equation (28)). This is because the algorithms performing this purely classical part do not typically achieve the Shannon limit [19]. For our purposes we consider this step to be perfect: $\text{leak}_{\text{EC}} = H(X|Y)$.

3 MUBs

The existence of three MUBs generated by the Pauli elements Z_d, X_d and $X_d Z_d$ for any d [16] is good news and it makes senses to study the secret key rates for the 3-MUB QKD protocols. The error analysis is a bit more intricate. In the bit (Z_d) and phase (X_d) basis the errors are generated by the X_d^α and $X_d^\alpha Z_d^\beta$ and by Z_d^β and $X_d^\alpha Z_d^\beta$, respectively, assuming $\alpha, \beta > 0$. In the bit-phase basis (the basis spanned by the eigenvectors of $X_d Z_d$) the errors are caused by X_d^α, Z_d^β ($\alpha, \beta > 0$) and those *not* of the form $X_d^\alpha Z_d^\alpha$ for $\alpha > 0$. This is shown in equation (15).

Let us first do some counting: for a given d there is in total $d^2 - 1$ error operators $X_d^\alpha Z_d^\beta$ by excluding an identity. It contains $d - 1$ of X_d^α operators and $d - 1$ of Z_d^β operators. There is also $d - 1$ of $X_d^\alpha Z_d^\alpha$ operators

for $\alpha > 0$. Hence, the number of operators of the form $X_d^\alpha Z_d^\beta$ (α, $\beta > 0$, $\alpha \neq \beta$) causing errors in the $X_d Z_d$ basis must be

$$d^2 - 1 - 3(d - 1) = (d - 2)(d - 1).$$

As a result we get from equation (18) the following error rates:

$$Q_b = (d - 1)\lambda_Z + (d - 1)\lambda_X + (d - 2)(d - 1)\lambda_{XZ}, \tag{32a}$$

$$Q_p = (d - 1)\lambda_Z + (d - 1)\lambda_? + (d - 2)(d - 1)\lambda_{XZ}, \tag{32b}$$

$$Q_{b-p} = (d - 1)\lambda_X + (d - 1)\lambda_? + (d - 2)(d - 1)\lambda_{XZ}. \tag{32c}$$

The coefficients λ_Z, λ_X are defined as before and $\lambda_{XZ} = \lambda_{\alpha\alpha}$ for $0 < \alpha \leqslant d - 1$. We again set the error rates equal: $Q_b = Q_p = Q_{b-p} \equiv Q$. The normalization condition becomes

$$\lambda_{00} + (d - 1)\lambda_Z + (d - 1)\lambda_X + (d - 1)\lambda_? + (d - 2)(d - 1)\lambda_{XZ} = 1 \tag{33}$$

and we find

$$\lambda_{00} = 1 - Q - (d - 1)\lambda_?, \tag{34a}$$

$$\lambda_X = \lambda_Z = \lambda_?, \tag{34b}$$

$$\lambda_{XZ} = \frac{Q - 2(d - 1)\lambda_?}{(d - 2)(d - 1)} \tag{34c}$$

for $d > 2$. The channel is of the following form

$$\mathcal{N}_d^{\text{3MUBs}}(\varrho) = (1 - Q - (d - 1)\lambda_?)\varrho + \lambda_? \left[\sum_{\alpha=1}^{d-1} X_d^\alpha \varrho X_d^{\alpha\dagger} + \sum_{\beta=1}^{d-1} Z_d^\beta \varrho Z_d^{\beta\dagger} + \sum_{\gamma=1}^{d-1} X_d^\gamma Z_d^\gamma \varrho (X_d^\gamma Z_d^\gamma)^\dagger \right]$$

$$+ \frac{Q - 2(d - 1)\lambda_?}{(d - 2)(d - 1)} \sum_{\alpha \neq \beta=1}^{d-1} X_d^\alpha Z_d^\beta \varrho (X_d^\alpha Z_d^\beta)^\dagger. \tag{35}$$

The minimization procedure similar to equation (23) leads to an analytical solution (too long to paste here) of the following cubic equation

$$\lambda_?^3 = (1 - (d - 1)\lambda_? - Q)\left[\frac{-2(d - 1)\lambda_? + Q}{(d - 2)(d - 1)} \right]^2. \tag{36}$$

The resulting secret key rates are given by

$$Q^{(1)}(\mathcal{N}_d^{\text{3MUBs}}) = \log d + (Q - 2(d - 1)\lambda_?)\log \frac{Q - 2(d - 1)\lambda_?}{(d - 2)(d - 1)}$$

$$+ 3(d - 1)\lambda_? \log \lambda_? + (1 - Q - (d - 1)\lambda_?)\log(1 - Q - (d - 1)\lambda_?) \tag{37}$$

and are plotted in figure 2. By comparing with figure 1 we can see that the tolerable threshold values are much better than for the corresponding 2-MUB protocol. Our results perfectly agree (in the overlapping cases) with a numerical study from [26] as well as the secret key rates and thresholds from [24]. The $d = 2$ case must be analyzed separately and it is the well-known six-state protocol [13]. The channel is the qubit depolarizing channel (see again [6], appendix A)

$$\mathcal{N}_2^{\text{3MUBs}}(\varrho) = (1 - 3Q/2)\varrho + Q/2(X_2 \varrho X_2 + Y_2 \varrho Y_2 + Z_2 \varrho Z_2). \tag{38}$$

Then

$$Q^{(1)}(\mathcal{N}_2^{\text{3MUBs}}) = 1 - S(\{q_i\}), \tag{39}$$

where $q_i = \{1 - 3/2Q, Q/2, Q/2, Q/2\}$. The one-shot capacity becomes zero for the threshold value $Q \approx 0.126$ [6, 40].

4. Non-asymptotic secret key rates for the 2- and 3-MUB QKD d-level protocols

The condition for a secret key generated when the resources are not unlimited is formally identical to equation (1). However, equation (1) cannot this time be satisfied arbitrarily well. More precisely, for finite-length private codes, ϵ is chosen sufficiently small and it becomes an input parameter of the secret key generation protocol. The task can be further reformulated—it is often advantageous to investigate separately two conditions: (i) *correctness*

$$\Pr[K_A \neq K_B] \leqslant \epsilon_{\text{cor}}, \tag{40}$$

Figure 2. Qudit secret key rates for the 3-MUB QKD protocol for $d = 2$ (the bottom curve) to 7 (the upmost curve) in bits per channel are plotted. For the special case $d = 2$ equation (32) simplify and no optimization is needed. The resulting channel is equation (38).

where the key string is allowed to be different with a non-zero probability ϵ_{cor}, and (ii) *secrecy*

$$\left\| \varrho_{AE} - \frac{1}{|K|} \sum_{k \in K} |k\rangle\langle k|_A \otimes \tau_E \right\|_1 \leqslant \epsilon_{\mathrm{sec}}. \tag{41}$$

This means that an adversary is decoupled from the resulting secret key sequence by a small (but fixed) amount ϵ_{sec}. Due to composability [41], the errors add up and the overall security parameter is bounded: $\epsilon \leqslant \epsilon_{\mathrm{cor}} + \epsilon_{\mathrm{sec}} + \epsilon_{\mathrm{PA}}$ [10]. Similarly to the asymptotic analysis, the 'measure' of decoupling, ϵ_{sec}, is related, through the decoupling lemma [5]

$$\epsilon_{\mathrm{sec}} \leqslant 2\varepsilon + 2^{-\frac{1}{2}}(-\ell + H_{\min}^{\varepsilon}(X^n|E^n)_{\varrho} - n\mathrm{leak}_{\mathrm{EC}}), \tag{42}$$

to the smooth min-entropy

$$H_{\min}^{\varepsilon}(A|B)_{\varrho} \stackrel{\mathrm{df}}{=} \max_{\substack{\varrho' \text{ s.t.} \\ \|\varrho - \varrho'\|_1 \leqslant \varepsilon}} H_{\min}(A|B)_{\varrho'}, \tag{43}$$

where

$$H_{\min}(A|B)_{\varrho} \stackrel{\mathrm{df}}{=} \max_{\substack{\sigma_B \text{ s.t.} \\ 0 < \mathrm{Tr}\,\sigma_B \leqslant 1}} \sup_{\xi \in \mathbb{R}}[\varrho_{AB} - 2^{-\xi}\mathrm{id}_A \otimes \sigma_B \leqslant 0]. \tag{44}$$

We will also need the max-entropy definition

$$H_{\max}(A|B)_{\varrho} \stackrel{\mathrm{df}}{=} \sup_{\sigma_B} \log\left[\mathrm{Tr}\left[\left(\sqrt{\varrho_{AB}}\,(\mathrm{id}_A \otimes \sigma_B)\sqrt{\varrho_{AB}}\right)^{1/2}\right]\right]^2, \tag{45}$$

where for two commuting distributions $\varrho \to P$ and $\sigma \to Q$ the optimization can be performed [42].

Given the secrecy parameter ϵ_{sec}, the secret key of the length $\ell \stackrel{\mathrm{df}}{=} nr^{(\varepsilon,n)}$ can be extracted whenever

$$r^{(\varepsilon,n)} \leqslant \frac{1}{n} H_{\min}^{\varepsilon}(X^n|E^n)_{\varrho} - \mathrm{leak}_{\mathrm{EC}}. \tag{46}$$

The secret key rate is achievable [27]. Given the security parameters ε in (42), the constructed code satisfies the decoupling condition. In coding theory, the statement of achievability is usually proved by a random construction via a direct coding theorem. This is precisely the construction found in section 5.4 of [5]. The original derivation from [5] has been further elaborated on and sharpened providing increasingly better estimates for the secret key rate. For the most important contributions, we should not forget to mention [19–21, 23] and mainly [28] culminating in [29] whose extension to the QKD qudit protocols will be presented in the next section. Also note the similarity between equation (11) and equation (46). Indeed, this is not a coincidence, the latter can be seen as a finite-key version of the former [5, 19]. The conditional entropy belongs to a parametric

---

[10] We took the liberty of ignoring the possibility of failure ϵ_{PA} during the privacy amplification (PA) step and the probability of failure ϵ_{cor} of correctly estimating Alice's key, equation (40). Both parameters are undoubtedly important for the overall secret key rate in the non-asymptotic scenario. They manifest themselves as additional exponents in equation (42) in the form proportional to $-\log[1/\epsilon]$. The errors are chosen independently as part of the protocol [19, 28] but our main interest lies in ϵ_{sec} and so we will study the key rate as its function. For a practical piece of advice as what to do in the deployed scenario, where all parameters must be set, we point the reader to [22] and also [29].

family of the so-called Rényi entropies and both the min- and max-entropy, equations (44) and (45), are family members with an operational meaning relevant for QKD [23]. Furthermore, we have the equipartition property

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H_{\max}^{\varepsilon}(X^n | E^n)_{\varrho} = \lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H_{\min}^{\varepsilon}(X^n | E^n)_{\varrho} = H(X|E)_{\varrho}. \tag{47}$$

An important advance in the security of the finite-key size QKD using two MUBs was possible due to the use of the uncertainty relation for smooth entropies:

$$H_{\min}^{\varepsilon}(X^n | E^n)_{\varrho} + H_{\max}^{\varepsilon}(X^n | Y^n)_{\varrho} \geqslant n \log d \tag{48}$$

[42] explains the physical interpretation in detail so we will only say that uncertainty relations in general limit the knowledge in one basis if a measurement is performed in the complementary basis. In this case, the complementary basis (the eigenvectors of the Pauli Z_d basis) is used exclusively for the sacrificed portion of the sifted key and this consequently serves for an estimation of the preserved part of the sifted key (which itself is transmitted in the basis spanned by the eigenvectors of the Pauli X_d matrix).

Bounds on the finite secret key rate

The direct evaluation of the smooth min-entropy for $0 \ll n < \infty$ in equation (46) is not straightforward. There exists a couple of methods to estimate it and the most advanced analysis so far, based on the smooth entropy uncertainty relations, appeared in [29] following [28]. We present its generalization to the qudit scenario for the 2-MUB QKD protocol. This approach provides the best secret key rate known to the authors but it cannot be extended to the case of 3 MUBs in a straightforward manner. In this case we use another strategy via the study of the asymptotic behavior of the smooth min-entropy. This bound already appeared in [23] and we improve it by recent insights based on the *conditional entropy variance* (the so-called second-order approximation of the quantum coding rate [43]). For the sake of comparison, we evaluate these bounds also for the 2-MUB qudit protocol. Here, the finite-key corrections come from two sources. First, it is the approximations of the smooth min-entropy and the smooth quantities in general. The second source of corrections is the error rate estimation phase, where a part of the sifted key is sacrificed in order to estimate the error rate of the data used to extract the actual secret key.

To proceed, we will recapitulate the relevant parts (see footnote 6) of the qudit 2- and 3-MUB QKD protocol in order to apply the methods of [28]. For the case of 2 MUBs, we may adopt the same protocol definition as in Box 1 of [28]. In particular, an asymmetric choice of the complementary bases is used [30], one for the raw key whose length will be labeled n and the other one of the length k used solely in the parameter estimation step. Hence, the total length of the sifted key is $N = n + k$. The difference compared to [28] is the calculation of the average error λ subsequently used for the parameter estimation. As a pure formality—instead of the modulo two addition of the publicly announced bit sequences of the length k (used to count the number of differing bits), the communicating parties may use

$$\lambda \overset{\mathrm{df}}{=} \sum_{i=1}^{k} 1\{x_i \neq y_i | X\} = \sum_{i=1}^{k} \left\lceil \frac{x_i \ominus y_i}{d} \right\rceil, \tag{49}$$

where $\ominus$ stands for the modulo d subtraction and $1\{\omega | A\}$ denotes the set indicator function defined for two sets $\Omega \subset A$ as $1\{\omega | A\} = 1$ whenever $\omega \in \Omega$ and zero otherwise. In the parameter estimation phase, the sacrificed portion of the sifted sequence of the length k over d letters (transmitted in the Pauli Z_d basis) is used to estimate the error rate in the portion of the length n transmitted in the Pauli X_d basis. Analogously to [28], we are penalized by effectively increasing the error rate by $\nu = \sqrt{\frac{N(k+1)\ln \frac{2}{\varepsilon}}{k^2(N-k)}}$ due to the finiteness of the statistics. More precisely, the estimate of large deviations for an independent and identically distributed random process sampled without replacement due to Serfling is used [44].
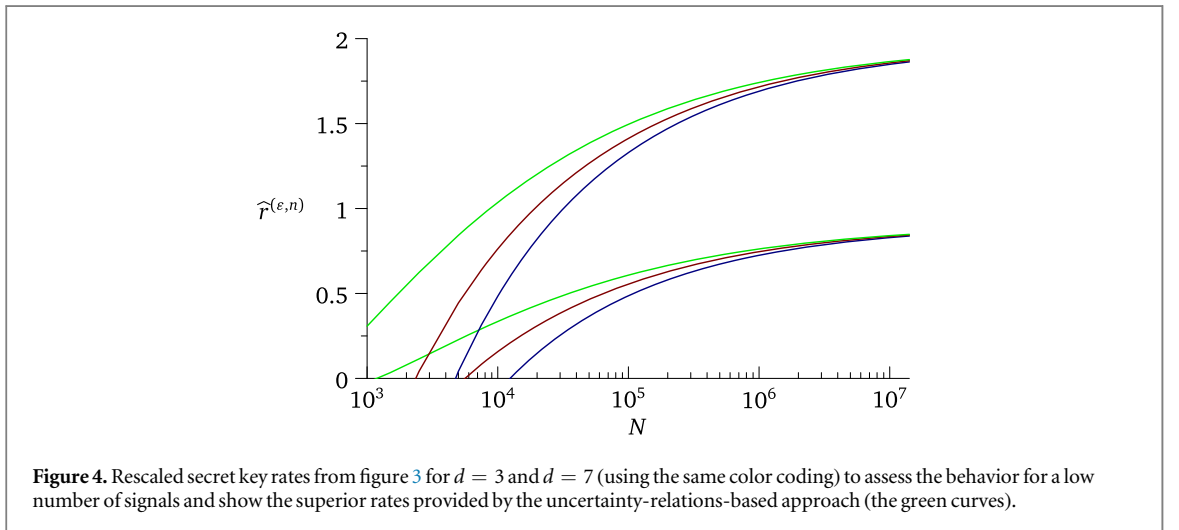
For three MUBs, the QKD protocol must be modified only such that the Pauli X_d basis will be used for the key extraction and the Z_d and $X_d Z_d$ basis for the parameter estimation step. So the communicating parties will be instructed to switch the bases accordingly with equal probabilities for the Z_d and $X_d Z_d$ bases. In this case, the uncertainty relations based approach does not provide the best secret key rates and the smooth min-entropy from equation (42) must be estimated differently (see equation (56) onwards).

A useful upper bound on the classical max-entropy is given by the probability distribution support (the set over which the probability distribution is positive [5]) leading to

$$H_{\max}(X|Y)_P \leqslant \log|\mathrm{supp}[P(X|Y=y)]| = \log|\{x \in \{0, 1, \ldots, d-1\}; \Pr[X=x|Y=y] > 0\}|. \tag{50}$$

Here we generalize the result from [29] (claim 9) and show that the rhs satisfies

$$\log|\{x \in \{0, 1, \ldots, d-1\}; \Pr[X=x|Y=y] > 0\}| \leqslant n(h(Q+\nu) + (Q+\nu)\log(d-1)) \tag{51}$$

Figure 3. Secret key rates based on the finite-key length analysis for $d = 2 \ldots 7$ 2-MUB QKD protocol. For each d, a triple of curves (blue/red/green) corresponds to increasingly better key rates. The worst rate (blue) is provided by optimizing the lower expression in equation (63). The middle (red) curve comes from the second-order analysis in the upper expression equation (63). The highest (green) rate is given by optimizing equation (55) based on uncertainty relation for smooth entropies we obtained for any d. We set $Q = 0.05$, $\varepsilon = 10^{-10}$ and $N = n + k$ is the length of the sifted string of d letters.

Figure 4. Rescaled secret key rates from figure 3 for $d = 3$ and $d = 7$ (using the same color coding) to assess the behavior for a low number of signals and show the superior rates provided by the uncertainty-relations-based approach (the green curves).

for the 2-MUB protocol. We start as in [28]

$$\left|\{x \in \{0, 1, \ldots, d-1\}; \Pr[X = x | Y = y] > 0\}\right| \leqslant \sum_{x \in \{0, \ldots, d-1\}^n} 1\{\lambda < n(Q + \nu)\}, \tag{52a}$$
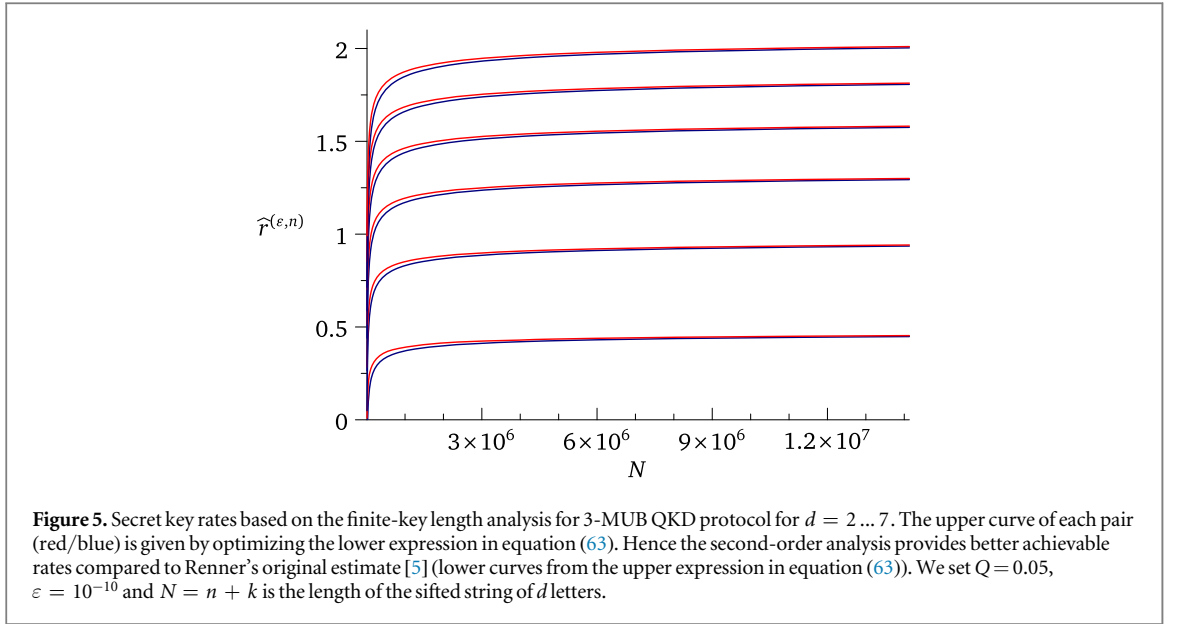
$$= \sum_{\lambda=0}^{n} \binom{n}{\lambda}(d - 1)^{\lambda} 1\{\lambda < n(Q + \nu)\}, \tag{52b}$$

$$= \sum_{\lambda=0}^{n(Q+\nu)} \binom{n}{\lambda}(d - 1)^{\lambda}, \tag{52c}$$

$$\leqslant 2^{n(h(Q+\nu))}(d - 1)^{n(Q+\nu)}. \tag{52d}$$

The new term $(d - 1)^{\lambda}$ in the first equality comes from an additional number of errors caused by a larger (d-letter) alphabet. The last line comes from $\sum_{\lambda=0}^{n(Q+\nu)} \binom{n}{\lambda} \leqslant 2^{n(h(Q+\nu))}$, valid for $0 \leqslant Q + \nu \leqslant 1/2$, and by taking into account $0 \leqslant \lambda \leqslant n(Q + \nu)$. Upon taking the logarithm we obtain (51). This, on the other hand, allows us to bound the min-entropy from equation (42) via equation (48):

$$H_{\min}^{\varepsilon}(X^n | E^n)_{\varrho} \geqslant n(\log d - h(Q + \nu) - (Q + \nu)\log(d - 1)). \tag{53}$$

Figure 5. Secret key rates based on the finite-key length analysis for 3-MUB QKD protocol for $d = 2 \ldots 7$. The upper curve of each pair (red/blue) is given by optimizing the lower expression in equation (63). Hence the second-order analysis provides better achievable rates compared to Renner's original estimate [5] (lower curves from the upper expression in equation (63)). We set $Q = 0.05$, $\varepsilon = 10^{-10}$ and $N = n + k$ is the length of the sifted string of d letters.

Hence, we get for (46)

$$r^{(\varepsilon,n)} \leqslant \log d - h(Q + \nu) - (Q + \nu)\log(d - 1) - \text{leak}_{\text{EC}} \tag{54}$$

and so finally the optimized secret key rate is given by

$$\widehat{r}^{(\varepsilon,n)} \leqslant \max_{k} \frac{N - k}{N}[\log d - h(Q + \nu) - (Q + \nu)\log(d - 1) - \text{leak}_{\text{EC}}]. \tag{55}$$

The numerical optimization was done by choosing a target number of sifted signals N, the error rate Q and the security parameter ϵ. The result of optimization is the highest rate and also the number k of sacrificed bits needed to achieve it. Another option, we did not pursue, was to set the target number n of raw bits and optimize the rate over k sa well. The choice depends more on practical requirements. As expected, in the limit of $N \to \infty$ or $n \to \infty$, we recover equations (27) and (30). This is because $\nu \to 0$ and $\frac{N - k}{N} = \frac{n}{n + k} \to 1$.

The smooth min-entropy estimates reveal the rate of convergence in equation (47). The first such estimate widely used in the literature was provided by Renner [5] (corollary 3.3.7)

$$\frac{1}{n}H_{\min}^{\varepsilon}(X^n|E^n)_{\varrho} \geqslant H(X|E)_{\varrho} - (2\log\text{rank}\varrho_X + 3)\sqrt{\frac{1}{n}\log\frac{2}{\varepsilon}}. \tag{56}$$

A better estimate comes from the recent advances in finite block length quantum coding [43] through

$$\frac{1}{n}H_{\min}^{\varepsilon}(X^n|E^n)_{\varrho} \geqslant H(X|E)_{\varrho} + \Phi^{-1}(\varepsilon^2)\sqrt{\frac{V(X|E)}{n}}, \tag{57}$$

where

$$V(\varrho\|\sigma) \stackrel{\text{df}}{=} \text{Tr}[\varrho(\log\varrho - \log\sigma - D(\varrho\|\sigma))^2] \tag{58}$$

is the relative entropy variance and

$$D(\varrho\|\sigma) \stackrel{\text{df}}{=} \text{Tr}[\varrho(\log\varrho - \log\sigma)] \tag{59}$$

is the quantum relative entropy [45]. Then, as a special case, we obtain the quantum conditional entropy and the conditional entropy variance [34]
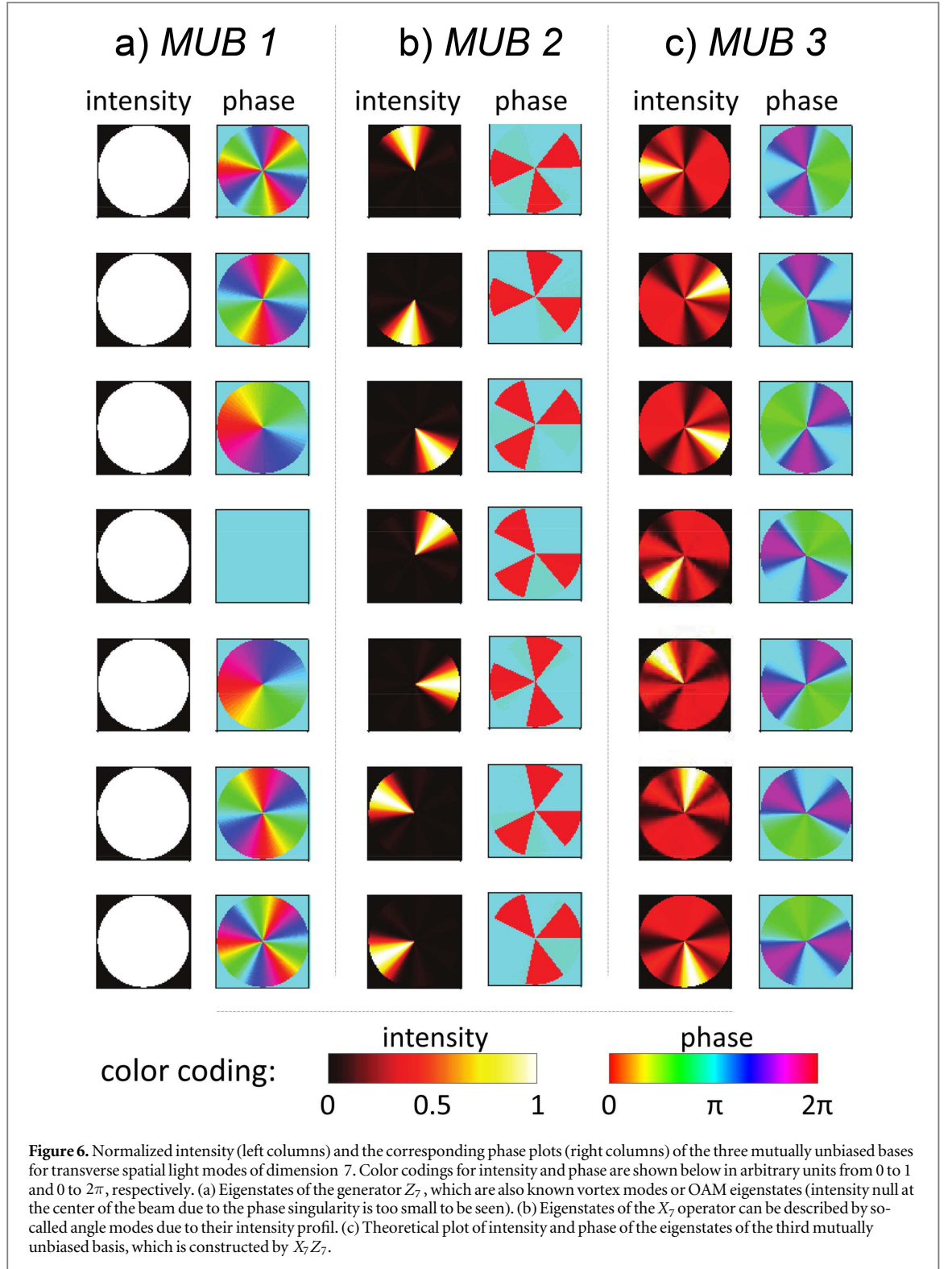
$$H(A|B)_{\varrho} = -D(\varrho_{AB}\|\text{id}_A \otimes \varrho_B), \tag{60}$$

$$V(A|B)_{\varrho} = V(\varrho_{AB}\|\text{id}_A \otimes \varrho_B). \tag{61}$$

The expression $\Phi^{-1}(x) = -\sqrt{2}\ \text{inv}\left[(1 - \text{Erf}(2x))\right]$ stands for the inverse of the complementary cumulative Gaussian distribution function. The previously mentioned large deviation estimate of the smooth min-entropy manifests itself by replacing $f(Q) = H(X|E)_{\varrho}$ with

$$f(Q + \nu) = \widetilde{H}(X|E)_{\varrho} \leqslant f(Q) \tag{62}$$

in equations (56) and (57).

Figure 6. Normalized intensity (left columns) and the corresponding phase plots (right columns) of the three mutually unbiased bases for transverse spatial light modes of dimension 7. Color codings for intensity and phase are shown below in arbitrary units from 0 to 1 and 0 to 2π, respectively. (a) Eigenstates of the generator Z_7, which are also known vortex modes or OAM eigenstates (intensity null at the center of the beam due to the phase singularity is too small to be seen). (b) Eigenstates of the X_7 operator can be described by so-called angle modes due to their intensity profil. (c) Theoretical plot of intensity and phase of the eigenstates of the third mutually unbiased basis, which is constructed by $X_7 Z_7$.

Combining equation (46) and the estimates in equations (56) and (57) together with equation (62) we get an achievable upper bound for the secret key rate

$$\hat{r}^{(\varepsilon,n)} \leqslant \max_k \frac{N-k}{N} \left[\widetilde{H}(X|E) - \text{leak}_{\text{EC}} - \begin{cases} (2\log\text{rank}\varrho_X + 3)\sqrt{\frac{1}{N-k}\log\frac{2}{\varepsilon}} \\ -\Phi^{-1}(\varepsilon^2)\sqrt{\frac{V(X|E)}{N-k}}. \end{cases} \right]. \tag{63}$$

The optimized secret key rate $\hat{r}^{(\varepsilon,n)}$ is plotted as the two lower curves in figure 3 for the 2-MUB protocol and in figure 5 for the 3-MUB protocol. Then, the overall number of secret key bits is given by $(N-k)\log d$ for k found in equation (63). Figure 4 shows the d = 3 and d = 7 cases from figure 3 on a semilogarithmic scale.

5. Discussion and conclusions

With the promising results of an increased secret key rate at hand, we now turn to laboratory implementations of discrete high-dimensional state spaces. Although the presented theoretical analysis is valid for any experimental realization, we focus on one prominent example, namely transverse spatial light modes. Encoding high-dimensional quantum states on the orbital angular momentum (OAM) of photons is a vibrant field in which technologies to generate and manipulate the states have matured over the last 15 years. Here, the eigenstates of two MUBs can be intuitively understood as the complementary variables, OAM and angular position (ANG). They correspond to the generators Z_d and X_d, respectively, which we introduced earlier (equation (13)). High-dimensional states of both MUBs have been used in previous experiments to demonstrate complementarity as well as high-dimensionality of the generated quantum states [46–48]. More importantly, their advantage in high-dimensional QKD has been demonstrated recently [10] and experimental techniques for efficiently sorting the encoded qudits are well established [49, 50].

In figure 6, we give an example of the eigenmodes of all three MUBs for dimension $d = 7$: the OAM-basis Z_7, the ANG-basis X_7 and the eigenstates of $X_7 Z_7$. The typical vortex of OAM carrying light modes and their according helical phase dependence (from which the OAM stems) can be seen (figure 6(a)) as well as the angular-shaped intensity of the states in the second MUBs (figure 6(b)). The modes of the third MUB are more complex in their intensity and phase profile (figure 6(c)), which leads to open questions of how practical such modes are in a laboratory setting. Although modern techniques to generate complex light fields with high fidelity and efficiency are well known [51], the efficient sorting of a general set of spatial modes remains difficult. Possible techniques will need to be efficient and to work on the single photon level. Both requirements are fulfilled for established sorting devices that are used for OAM and ANG modes but no direct techniques is known yet, which sorts the modes of the third basis. One way to circumvent this lack of an efficient direct sorting would be to transfer the transverse spatial degree of freedom into different optical paths, e.g. as described [52]. Once transferred, it is known how to realize any unitary transformation on the state, and thus an efficient detection could be done in any basis [53]. Here, the fast progress in integrated quantum optics might a promising way to realize such a so-called multiport even for dimensions as high as $d = 7$ [54, 55].

In summary, we calculated secret key rates and tightly estimated achievable upper bounds on acceptable errors for an asymptotic and finite key length scenario in high-dimensional QKD schemes. We were able not only to reproduce and streamline already known bounds but mainly we (i) adapted the uncertainty-relations-based method to high-dimensional QKD with two MUBs leaving us with non-zero secret key rates even for a relatively small number of signals and (ii) extended the findings to a QKD scheme involving 3 MUBs basis. Given the assured existence of 3 MUBs in any dimension, our results are not limited to dimensions where the exact number of MUBs is known and they can be readily applied to laboratory implementations. Additionally, we give an example for a possible physical implementation, transverse spatial modes, for which mature techniques in generating all possible qudit-states exist and devices to efficiently sort the states of two MUBs are established. Hence, an important future challenge is to develop a practical device that efficiently sorts the modes of the third MUB. Given the derived increase in the secret key rate, the development of such a novel sorter will further boost high-dimensional QKD schemes and their real-world implementations.

Acknowledgments

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Int. Conf. on Computers, Systems and Signal Processing* pp 175–9

[2] Wootters W K and Zurek W H 1982 A single quantum cannot be cloned *Nature* **299** 802–3

[3] Milonni P W and Hardies M L 1982 Photons cannot always be replicated *Phys. Lett.* A **92** 321–2

[4] Devetak I 2005 The private classical capacity and quantum capacity of a quantum channel *IEEE Trans. Inf. Theory* **51** 44–55

[5] Renner R 2005 Security of QKD *PhD Thesis* ETH arXiv:quant-ph/0512258

[6] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution *Rev. Mod. Phys.* **81** 1301

[7] Cerf N, Bourennane M, Karlsson A and Gisin N 2002 Security of quantum key distribution using *d*-level systems *Phys. Rev. Lett.* **88** 127902

[8] Ali-Khan I, Broadbent C and Howell J 2007 Large-alphabet quantum key distribution using energy-time entangled bipartite states *Phys. Rev. Lett.* **98** 060503

[9] Walborn S, Lemelle D, Almeida M and Ribeiro P 2006 Quantum key distribution with higher-order alphabets using spatially encoded qudits *Phys. Rev. Lett.* **96** 090501

[10] Mirhosseini M, Magaña-Loaiza O S, O'Sullivan M N, Rodenburg B, Malik M, Lavery M P J, Padgett M J, Gauthier D J and Boyd R W 2015 High-dimensional quantum cryptography with twisted light *New J. Phys.* **17** 033033

[11] Malik M, Rodenburg B, Mirhosseini M, Leach J, Lavery M P J, Padgett M J and Boyd R W 2012 Influence of atmospheric turbulence on optical communications using orbital angular momentum for encoding *Opt. Express* **20** 13195–200

[12] Rodenburg B, Mirhosseini M, Malik M, Magaña-Loaiza O S, Yanakas M, Maher L, Steinhoff N K, Tyler G A and Boyd R W 2014 Simulating thick atmospheric turbulence in the lab with application to orbital angular momentum communication *New J. Phys.* **16** 033020

[13] Bruss D 1998 Optimal eavesdropping in quantum cryptography with six states *Phys. Rev. Lett.* **81** 3018

[14] Wootters W K and Fields B D 1989 Optimal state-determination by mutually unbiased measurements *Ann. Phys., NY* **191** 363–81

[15] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 A new proof for the existence of mutually unbiased bases *Algorithmica* **34** 512–28

[16] Thomas D, Berthold-Georg E, Ingemar B and Karol Ż 2010 On mutually unbiased bases *Int. J. Quantum Inf.* **8** 535–640

[17] Bechmann-Pasquinucci H and Peres A 2000 Quantum cryptography with 3-state systems *Phys. Rev. Lett.* **85** 3313

[18] Bruss D and Macchiavello C 2002 Optimal eavesdropping in cryptography with three-dimensional quantum states *Phys. Rev. Lett.* **88** 127901

[19] Scarani V and Renner R 2008 Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing *Phys. Rev. Lett.* **100** 200501

[20] Abruzzo S, Kampermann H, Mertz M and Bruß D 2011 Quantum key distribution with finite resources: secret key rates via Rényi entropies *Phys. Rev. A* **84** 032321

[21] Bratzik S, Mertz M, Kampermann H and Bruß D 2011 Min-entropy and quantum key distribution: nonzero key rates for 'small' numbers of signals *Phys. Rev. A* **83** 022330

[22] Cai R Y Q and Scarani V 2009 Finite-key analysis for practical implementations of quantum key distribution *New J. Phys.* **11** 045024

[23] Renner R, Gisin N and Kraus B 2005 Information-theoretic security proof for quantum-key-distribution protocols *Phys. Rev. A* **72** 012332

[24] Ferenczi A and Lütkenhaus N 2012 Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning *Phys. Rev. A* **85** 052310

[25] Sheridan L and Scarani V 2010 Security proof for quantum key distribution using qudit systems *Phys. Rev. A* **82** 030301

[26] Coles P J, Metodiev E M and Lütkenhaus N 2016 Numerical approach for unstructured quantum key distribution *Nat. Commun.* **7** 11712

[27] Renner R private correspondence

[28] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 Tight finite-key analysis for quantum cryptography *Nat. Commun.* **3** 634

[29] Tomamichel M and Leverrier A 2015 A rigorous and complete proof of finite key security of quantum key distribution arXiv:1506.08458

[30] Hoi-Kwong L, Hoi-Fung C and Ardehali M 2005 Efficient quantum key distribution scheme and a proof of its unconditional security *J. Cryptol.* **18** 133–65

[31] Hayashi M and Tsurumaru T 2012 Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths *New J. Phys.* **14** 093014

[32] Hayashi M 2015 Quantum wiretap channel with non-uniform random number and its exponent and equivocation rate of leaked information *IEEE Trans. Inf. Theory* **61** 5595–622

[33] Tomamichel M and Hayashi M 2013 A hierarchy of information quantities for finite block length analysis of quantum tasks *IEEE Trans. Inf. Theory* **59** 7693–710

[34] Li K *et al* 2014 Second-order asymptotics for quantum hypothesis testing *Ann. Stat.* **42** 171–89

[35] Smith G 2008 Private classical capacity with a symmetric side channel and its application to quantum cryptography *Phys. Rev. A* **78** 022306

[36] Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2005 Secure key from bound entanglement *Phys. Rev. Lett.* **94** 160502

[37] Man-Duen C 1975 Completely positive linear maps on complex matrices *Linear Algebr. Appl.* **10** 285–90

[38] Andrzej J 1972 Linear transformations which preserve trace and positive semidefiniteness of operators *Rep. Math. Phys.* **3** 275–8

[39] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441

[40] Hoi-Kwong L 2001 Proof of unconditional security of six-state quantum key distribution scheme *Computation* **1** 81–94

[41] Müller-Quade J and Renner R 2009 Composability in quantum cryptography *New J. Phys.* **11** 085006

[42] Tomamichel M 2012 A framework for non-asymptotic quantum information theory arXiv:1203.2142

[43] Tomamichel M, Berta M and Renes J M 2016 Quantum coding with finite resources *Nat. Commun.* **7** 11419

[44] Serfling R J 1974 Probability inequalities for the sum in sampling without replacement *Ann. Stat.* **2** 39–48

[45] Umegaki H 1962 Conditional expectation in an operator algebra, iv (entropy and information) *Kodai Math. Semin. Rep.* **14** 59–85

[46] Leach J, Jack B, Romero J, Jha A K, Yao A M, Franke-Arnold S, Ireland D G, Boyd R W, Barnett S M and Padgett M J 2010 Quantum correlations in optical angle-orbital angular momentum variables *Science* **329** 662–5

[47] Krenn M, Huber M, Fickler R, Lapkiewicz R, Ramelow S and Zeilinger A 2014 Generation and confirmation of a (100 × 100)-dimensional entangled quantum system *Proc. Natl Acad. Sci.* **111** 6243–7

[48] Edgar M P, Tasca D S, Izdebski F, Warburton R E, Leach J, Agnew M, Buller G S, Boyd R W and Padgett M J 2012 Imaging high-dimensional spatial entanglement with a camera *Nat. Commun.* **3** 984

[49] Mirhosseini M, Malik M, Shi Z and Boyd R W 2013 Efficient separation of the orbital angular momentum eigenstates of light *Nat. Commun.* **4** 2781

[50] Berkhout G, Lavery M, Courtial J, Beijersbergen M and Padgett M 2010 Efficient sorting of orbital angular momentum states of light *Phys. Rev. Lett.* **105** 153601

[51] Arrizón V, Ruiz U, Carrada R and González L A 2007 Pixelated phase computer holograms for the accurate encoding of scalar complex fields *J. Opt. Soc. Am. A* **24** 3500–7

[52] Fickler R, Lapkiewicz R, Huber M, Lavery M P J, Padgett M J and Zeilinger A 2014 Interface between path and orbital angular momentum entanglement for high-dimensional photonic quantum information *Nat. Commun.* **5** 4502

[53] Reck M, Zeilinger A, Bernstein H J and Bertani P 1994 Experimental realization of any discrete unitary operator *Phys. Rev. Lett.* **73** 58

[54] Carolan J *et al* 2015 Universal linear optics *Science* **349** 711–6

[55] Huber M, Ramelow S, Zeilinger A, Schaeff C and Polster R 2015 Experimental access to higher-dimensional entangled quantum systems using integrated optics *Optica* **2** 523–9