Full characterization of a high-dimensional quantum communication channel

Frédéric Bouchard,1 Felix Hufnagel,1 Dominik Koutný,2 Aazad Abbas,1 Alicia Sit,1 Khabat Heshami,3,1 Robert Fickler,1 and Ebrahim Karimi1,4
1Department of Physics, University of Ottawa, 25 Templeton Street, Ottawa, Ontario, K1N 6N5 Canada
2Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic.
3National Research Council of Canada, 100 Sussex Drive, Ottawa, Ontario K1A 0R6, Canada
4Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran.

The characterization of quantum processes, e.g. communication channels, is an essential ingredient for establishing quantum information systems. For quantum key distribution protocols, the amount of overall noise in the channel determines the rate at which secret bits are distributed between authorized partners. In particular, tomographic protocols allow for the full reconstruction, and thus characterization, of the channel. Here, we perform quantum process tomography of high-dimensional quantum communication channels with dimensions ranging from 2 to 5. We can thus explicitly demonstrate the effect of an eavesdropper performing an optimal cloning attack or an intercept-resend attack during a quantum cryptographic protocol. Our study shows that the process matrix enables a more detailed understanding of the channel conditions compared to a coarse-grained measure, such as quantum bit error rates. This full characterization technique allows us to distinguish eavesdropping attempts and optimize the quantum key distribution performance under asymmetric experimental conditions.

INTRODUCTION

Quantum information science has witnessed the emergence of a wide range of new technologies and applications [1]. Quantum cryptography [2], quantum computation [3] and quantum sensing [4] are examples of promising venues for a possible next technological revolution. In order to construct complex quantum machines or quantum networks, a full characterization of its building blocks is critical. A method for reconstructing the action of a component in a quantum system is known as quantum process tomography (QPT) [5, 6]. Previously, QPT has been performed to characterize several quantum physical systems, such as liquid-state NMR [7, 8], photonic qubits [9], atoms in optical lattices [10], trapped ions [11], solid-state qubits [12], continuous-variable quantum states [13], semiconductor quantum dot qubits [14] and, recently, nonlinear optical systems [15]. Another class of important quantum systems that can benefit from full characterization are quantum channels and components for quantum key distribution (QKD) and quantum communications [16, 17], where, so far, quantum channels may be categorized as optical fibre [18], line-of-sight free-space [19] and ground-to-satellite (satellite-to-ground) [20] links.

The benefits of fully characterizing quantum communication channels lie at a better understanding of possible error sources and, more importantly, on the detection of the potential presence of an eavesdropper, namely Eve, tapping into the quantum channel. Usually, her presence is revealed in the form of noise introduced in the channel. The authorized partners, typically referred to as Alice and Bob, may estimate noise levels in the channel to assess the amount of leaked information to Eve. After this error assessment, Alice and Bob may perform classical post-processing protocols, such as privacy amplification [21], in order to remove Eve’s leaked information. Conventional methods for secure key rate analysis rely on symmetry assumptions to associate an average (coarse-grained over all preparation and measurement settings) bit error rate parameter to a reduction in secure key rates. However, experimental errors often tend to break symmetries which motivates numerical techniques towards QKD [22].

While usual QKD schemes rely on encoding quantum information in two-level systems, i.e. qubits, a particular class of QKD schemes is known as high-dimensional QKD protocols [23, 24]. High-dimensional schemes have the potential advantage of tolerating larger noise levels in the channel and carrying more than one bit of information per carrier. So far, a full characterization of high-dimensional processes based on QPT has not been achieved experimentally. With the emergence of high-dimensional quantum information, QPT will become an essential tool for the characterization of complex experiments dealing with high-dimensional quantum states. As a physical implementation, the orbital angular momentum (OAM) of photons represents a promising route for high-dimensional encoding due to the maturity of its generation and detection schemes [25, 26]. OAM states, corresponding to helical wavefronts of the form exp(iℓϕ), where the OAM value ℓ is an integer and ϕ is the azimuthal coordinate, may be realized using single phase elements. Computer-generated holograms displayed on a spatial light modulator (SLM) provide a simple and versatile method for generating and manipulating these modes [27]. High-dimensional QKD has been demonstrated experimentally using OAM in the laboratory [28, 30], in intra-city free-space links [31, 33] and, recently, in other types of quantum links [24].

Here, we demonstrate the benefits of a full characterization of a quantum channel through quantum process tomography. This full characterization will allow us to complement the numerical approach in [22] to optimize secure key rates under specific experimental conditions and to develop new protocols lacking symmetry that may outperform existing approaches. Moreover, we characterize the effect of an eavesdropper performing a high-dimensional optimal cloning attack and two types of intercept-resend attack. We further show, that from
the experimentally reconstructed process, we may determine the source of the errors present in our high-dimensional quantum communication channel.

**RESULTS**

Theory of quantum process tomography: Let us set the stage by introducing the basic concepts of QPT. The goal of QPT is to determine the completely positive map $\mathcal{E}$ representing the action of the system on any $d$-dimensional input state $\rho_{in}$. The output state is then given by $\rho_{out} = \mathcal{E}(\rho_{in})$. The process is typically represented as,

$$\mathcal{E}(\rho) = \sum_{m,n} \chi_{mn} \hat{A}_m \rho \hat{A}_n^\dagger,$$

(1)

where the $\hat{A}_m$ operators form a complete basis typically given by the Pauli operators or the Gell-Mann operators in higher dimensions. The trace-preserving positive Hermitian $d^2 \times d^2$ matrix $\chi_{mn}$, defined as the process matrix, completely and uniquely characterizes the action of the process $\mathcal{E}$. We may note that QPT may also be performed for non-trace-preserving maps $[35]$. A convenient alternative description of processes is given by the Choi-Jamiolkowski isomorphism (CJI), which states that every completely positive map can be represented as an operator acting on a $d^2$-dimensional Hilbert space. Such an operator, known as the Choi matrix $\rho_{E}$, can be defined as the result of the channel acting upon one part of a maximally entangled state, $|\Phi\rangle$.

$$\rho_{E} = (\mathbb{I} \otimes \mathcal{E})|\Phi\rangle\langle\Phi|,$$

(2)

The output state is thus given accordingly,

$$\rho_{out} = \text{Tr}_{in} \left( \rho_{in} \otimes \mathbb{I} \rho_{E} \right),$$

(3)

where $T$ denotes the transposition, $\mathbb{I}$ is the $d$-dimensional identity operator and $\text{Tr}_{in} [\cdot]$ represents the partial trace over the input state’s Hilbert space. In order to perform QPT, a set of tomographically complete states are sent into the channel and state tomography is performed on the output states. In our case, we consider states belonging to mutually unbiased bases (MUB) in dimension $d$, which are known for dimensions that are powers of prime numbers $[36]$. A MUB projector is given by $\Pi_{\alpha}^{(n)}$, where $\alpha \in \{1,\ldots,d+1\}$ and $m \in \{1,\ldots,d\}$. The complete and orthogonality relations are respectively given by, $\sum_{\alpha,m} \Pi_{\alpha}^{(n)} / (d+1) = \mathbb{I}$ and $\text{Tr}(\Pi_{\alpha}^{(n)} \Pi_{\beta}^{(n)}) = \delta_{\alpha \beta} \delta_{mn} + (1 - \delta_{\alpha \beta})/d$, $\delta_{ij}$ is the Kronecker delta. With the help of the CJI, one can derive Born rule–like expressions for probabilities,

$$p_{m,n}^{(\alpha,\beta)} = \text{Tr} \left[ \Pi_{\alpha}^{(n)} \mathcal{E} \left( \Pi_{\beta}^{(m)} \right) \right] = \text{Tr} \left[ \left( \Pi_{\alpha}^{(n)} \right)^T \otimes \Pi_{\beta}^{(m)} \right] \rho_{E}$$

(4)

This equation underlies the relation between quantum process tomography and quantum state tomography. The Choi matrix, $\rho_{E}$, is experimentally reconstructed using the maximum–likelihood estimation. Better algorithms have also been recently proposed for QPT $[37]$. Finally, the process matrix is directly obtained from the Choi matrix.

**Experimental results:** Our experiment consists of three components: the generation stage, the quantum channel and the detection stage, which are owned by Alice, Eve and Bob, respectively. We implement the prepare-and-measure QKD scheme with heralded single-photons using the OAM degree of freedom, see Fig. 1. The single photon pairs, consisting of the signal and idler, are generated by spontaneous parametric downconversion (SPDC) at a type I $\beta$-barium borate (BBO) crystal. The nonlinear crystal is pumped by a quasi-continuous wave laser operating at a wavelength of 355 nm. The generated photon pairs are coupled to single-mode optical fibres (SMF) in order to filter their spatial modes to the fundamental Gaussian mode. A coincidence rate of 30 kHz is measured, directly at the source, within a coincidence time window of 2 ns. We use the detection of the idler photon as the heralding trigger for the signal photon, thereby realizing a
FIG. 2. Process matrix of high-dimensional quantum channels. The real part of the experimentally reconstructed process matrices are presented for dimensions ranging from 2 to 5 in the case of (a-d) an ideal quantum channel, (e-h) a universal symmetric optimal quantum cloning attack, (i-l) a universal intercept-resend attack and (m-p) an intercept-resend attack only using two MUB. The theoretical results are represented by the wire-grid.

Heralded single photon source with a measured second-order coherence of $g^{(2)}(0) = 0.015 \pm 0.004$. The heralded signal photon is sent to SLM-A corresponding to Alice’s generation stage. The OAM states are produced using a phase-only holography technique [27]. Alice’s heralded photon is subsequently sent over the quantum channel, considered here as a black box between Alice and Bob. At Bob’s receiver, we perform a state-projection over the required states, which we realize by a mode filter implemented through a phase-flattening hologram and coupling into a SMF [38, 39]. In particular, Alice and Bob perform QPT using MUB [40], which are experimentally realized using OAM states. The computational bases ($\alpha = 1$) are given by $|\ell\rangle; \ell = -d/2, ..., d/2; \ell \neq 0$ and $|\ell\rangle; \ell = -(d - 1)/2, ..., (d - 1)/2$ for even and odd dimensions, respectively, for symmetry considerations. The second basis is given by the discrete Fourier transform, i.e. $|\phi_k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega_{d}^{kj} |j\rangle; k = 0, ..., d - 1$, where $\omega_{d} = \exp(i2\pi/d)$. The explicit form of the other MUB elements can be found elsewhere [41].

Ideal quantum communication channel: In the case of an ideal quantum channel, i.e. no eavesdropper, the real parts of the experimentally reconstructed process matrices are shown in Fig. 2 (a-d) for dimensions ranging from $d = 2$ to 5. Ideal processes, where $\tilde{E}(\rho) = \rho$, are described by process matrices given by $\tilde{\chi}_{ij} = \delta_{i0}\delta_{j0}$. Deviations of our reconstructed ideal process matrices from the theory are attributed to imperfections in generation and detection of the distributed quantum states, i.e. the OAM modes. As higher dimensions are
considered, larger crosstalk among the OAM modes is observed, which further deteriorates the experimentally reconstructed process matrix. In order to describe the quality or performance of the quantum channel, several figures of merit are available to describe our process \[42\]. One such figure is the process fidelity which is defined as \( F_P = \text{Tr}(\chi_{\text{exp}} F) \). For the ideal quantum channel, \( F_P \) can be directly obtained from the process matrix \( \chi_{\text{ideal}} \), i.e. \( F_P = \chi_{\text{ideal}} \). Moreover, the average fidelity, \( \bar{F} \), of the process can be defined as the state fidelity between the output and the input averaged over all possible states with the convenient relation \( \bar{F} = (d F_P + 1)/(d + 1) \). Similarly, the average purity is defined as the purity of the outgoing states averaged over all possible states and describes the level of mixture introduced by the process. It can be related to the average fidelity according to \( \bar{P} = (1 - 2 \bar{F} + d \bar{F}^2)/(d - 1) \), respectively. The experimentally obtained process fidelities, average fidelities and average purities for the ideal channel are shown in Fig. 3 for dimensions ranging from \( d = 2 \) to 5.

Having quantified the experimental imperfections, we can now investigate the case of an imperfect quantum channel. As a starting point, we consider a general class of trace-preserving processes which creates mixtures from some input state. The result of such an action on an input state, say \( \rho_{\text{in}} = |0\rangle \langle 0| \), is given by the output state \( \rho_{\text{out}} = F |0\rangle \langle 0| + (1 - F)/(d - 1) \sum_{i=1}^{d-1} |i\rangle \langle i| \), where \( F = \langle \psi_{\text{in}} | \rho_{\text{out}} | \psi_{\text{in}} \rangle \) is the state fidelity. It can be shown that the process matrix associated to this decoherence process is given by

\[
\chi_{ij} = \frac{(1 - F)}{2(d - 1)} \delta_{ij} + \left( \frac{F(d + 1) - 1}{d} \right) \frac{1}{2(d - 1)} \delta_{0i} \delta_{0j}. \tag{5}
\]

**Optimal quantum cloning attack:** A special case of such a process is the so-called universal optimal cloning attack. In this scenario, Eve sends the incoming photon to an optimal cloning machine which produces two imperfect copies of the incoming photon, out of which she keeps one and sends the other to Bob. Later on, Eve may decide to perform a measurement on her copy in order to obtain information from Alice and Bob’s shared photon. For the case of universal optimal cloning, Eve’s copying machine has the effect of symmetrically introducing errors on the outgoing state. The cloning fidelity is defined as \( F_{\text{cl}} = 1/2 + 1/(1 + d) \). Universal optimal cloning machines have been realized experimentally using the symmetrization method \[43\]-\[47\], where both cloned photons possess the same cloning fidelity. At the heart of the symmetrization technique for optimal cloning is the Hong-Ou-Mandel interference effect \[48\]. For indistinguishable photons incident at the input port of a balanced beam splitter, a two-photon interference effect occurs which forbids the photons to exit the beam splitter from different output ports. Surprisingly, a slight modification of the Hong-Ou-Mandel experiment leads to a universal optimal symmetric cloning machine. In this case, the second photon needs to be in a \( d \)-dimensional completely mixed state and is fed into the second input port of the beam splitter at exactly the same time. As the representation of the mixed state is the same in any bases, this scheme is universal, i.e. works for any state of the Hilbert space. When the two photons exit the beam splitter from the same output port, optimal cloning has been successful. A second beam splitter is then used to separate the two photons, e.g. one photon goes to Bob and the other one stays at Eve. We then experimentally perform the universal optimal cloning machine in the quantum channel for dimensions up to 5 and perform, again, a full characterization of the attack on the channel through QPT, see Fig. 2 e-h and Fig. 3.
**Intercept-resend attack:** Another eavesdropping scheme that achieves processes with lower average fidelities is the so-called intercept-resend attack, see Fig. 2. In contrast to the above described optimal cloning attack, Eve directly measures the received photon information, where she randomly performs her measurement in bases uniformly chosen at random (intercept). She then prepares a photon in the observed state and transmits it to Bob (resend). When considering the intercept-resend over all MUB, the fidelity of the states at the output of the channel is given by $F_K = 2/(1 + d)$. We experimentally perform the intercept-resend attack in our quantum channel by means of two SLMs, i.e. SLM-E1 and SLM-E2, with a SMF in between. The first SLM (SLM-E1) along with the SMF acts as the intercept section, while the second SLM (SLM-E2) acts as the resend. In the universal case, Eve randomly chooses $\alpha = 1, ..., d + 1$ and $m = 1, ..., d$ and simultaneously displays phase elements equivalent to $|\psi_m^{(\alpha)}\rangle$ and $|\psi_m^{(\alpha)}\rangle$ on the SLM-E1 and SLM-E2, respectively. Next, we consider a non-symmetric process that introduces noise in a way that is not independent of the input state. An example of such an attack is the intercept-resend strategy considering 2 MUB, which corresponds to the seminal BB84 QKD protocol [2]. In this case, Alice and Bob encode their random bits only in 2 MUB. Hence, Eve may only consider those 2-MUB for her intercept-resend attack. In this case, the process matrix has a different form from that introduced earlier for symmetric decoherence. Using the same experimental configuration as that presented previously, we perform the intercept-resend attack considering the computational and the discrete Fourier transform bases. The real part of the theoretical process matrices for the 2-MUB intercept-resend attack are shown in Fig. 2. Interesting structures in the process matrices can be seen, demonstrating yet again the illustrative power of QPT and the process matrix in characterizing quantum processes, such as quantum channels in quantum communication settings.

**SECRET KEY RATES**

Finally, we show that the full characterization enables an enhanced estimation of the information leakage to an adversary eavesdropper. This results in a more accurate and favourable estimation of the achievable secret key rate, $K$, of the channel for a given QKD protocol. The first step to calculate the secret key rate of a channel is by evaluating the quantum bit error rate (QBER), $e_B$, from the raw key shared by Alice and Bob. Analytical formulae are derived to obtain the secret key rate as a function of the QBER. For instance, the BB84 protocol [2] in dimension $d$ has the following simple analytical formula,

$$K^{(d)}(e_B) = \log_2(d) - 2 h^{(d)}(e_B),$$

where $h^{(d)}(x) := -x \log_2(x/(d - 1)) - (1 - x) \log_2(1 - x)$ is the $d$-dimensional Shannon entropy. An extension of the $d$-dimensional BB84 protocol to tomographically complete measurements is known as the six-state protocol for the specific case of $d = 2$. For dimensions that are power of prime numbers, all $d + 1$ MUB are adopted. The secret key rate of this $(d + 1)$ MUB protocol as a function of the QBER is given by,

$$K^{(d)}(e_B) = \log_2((d + 1)/d) - \frac{d + 1}{d} e_B \log_2(d + 1). \quad (7)$$

Nonetheless, using such analytical formulae has a number of drawbacks. First, it only considers sifted data and assumes perfect unbiasedness among different MUB. This assumption may increase the resulting secret key rate, but does not consist of an adequate representation of the channel and may lead to an underestimation of Eve’s leaked information. Moreover, the secret key rate is obtained from a coarse-graining of the individual QBER per measurement settings. Thus, given this single parameter, a pessimistic estimation of the secret key rate is obtained due to the limited knowledge of the channel. Following the method described in [22], a more appropriate mean by which the secret key rate of a channel may be estimated is by considering the Devetak-Winter formula [49]. To do so, we recast our prepare-and-measure QKD protocol into an entanglement-based scheme using the source-replacement scheme [50], where Alice and Bob share pairs of entangled photons represented by the density matrix $\rho_{AB}$. The secret key rate is then obtained according to,

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

where $\rho_{AB}$ is the tripartite density matrix shared by Alice, Bob and Eve, respectively; $\mathcal{C}$ is the set of physical density
matrices that is consistent with the experimental constraints, e.g. QBER; $H(X|Y) := H(\rho_{XY}) - H(\rho_Y)$ is the conditional von Neumann entropy, with $H(\rho) = -\text{Tr}[\rho \log_2 \rho]$; $Z_A$ and $Z_B$ are the sets of positive operator valued measures (POVM) associated with Alice’s and Bob’s measurement settings, respectively. Finally, $\rho_{Z_AZ_B}$ and $\rho_{Z_AE}$ are given by,

$$\rho_{Z_AZ_B} = \sum_{jk} \text{Tr} \left[ (Z_A^j \otimes Z_B^k) \rho_{AB} \right] |j\rangle\langle j| \otimes |k\rangle\langle k|, \quad (9)$$

$$\rho_{Z_AE} = \sum_{j} |j\rangle\langle j| \otimes \text{Tr}_A \left[ (Z_A^j \otimes \hat{1}) \rho_{AE} \right]. \quad (10)$$

Hence, every additional experimental measurement is included in the minimization, which results in a greater, or equal, secret key rate. In the limiting case where we have a full characterization of the channel, $\rho_{AB}$ is fully reconstructed and is given by the Choi matrix, $\rho_{CE}$, mentioned earlier. Thus the secret key rate may be directly calculated from $\rho_{AB}$,

$$K = H(Z_A|E) - H(Z_A|Z_B), \quad (11)$$

where all experimental measurements are taken into consideration, even for the case of mismatching MUB. Going back to the prepare-and-measure scheme, we can now determine the corresponding set of POVMs. At Alice’s preparation stage, we have $Z_A = \{|0\rangle, \ldots, |d-1\rangle\}$. However, at Bob’s measuring stage, we consider two different sets of POVMs, i.e. $Z_B^{\text{out}} = \{|0\rangle, \ldots, |d-1\rangle\}$ and $Z_B^{\text{in}} = \{|0\rangle, \hat{1} \otimes |0\rangle\}$, where the former corresponds to a sorting-type measurement and the latter corresponds to a filter-type measurement, i.e. “click” or “no-click”. We note that in the case of a filter-type configuration, the secret key rate is upper-bounded by 1 bit per sifted photon. By doing so, we demonstrate the flexibility of our method which allows one to incorporate specific details about the experimental configuration and study its effect on the overall achievable secret key rate from a given QKD system. For the full characterization of our high-dimensional quantum channel via QPT with no explicit eavesdropping strategy applied, we calculate the corresponding secret key rate and compare it to a coarse-grained estimation of the channel, see Fig. 4. We observe that for larger dimensions, the coarse-grained secret key rate performs poorly compared to the achievable secret key rate obtained from a full characterization of the channel. This may be due to the fact that as one considers higher-dimensional states, the symmetry assumption involved in coarse-graining is increasingly not fulfilled. Therefore, full characterization of quantum channels may offer a means by which the full potential of high-dimensional protocols is exploited. In highly asymmetric scenarios, which is often the case due to systematic errors such as misalignments, full characterization may even surpass the performance of coarse-grained protocols even when considering the lower sifting efficiency of tomographic protocols.

In summary, full characterization of quantum processes via QPT is an invaluable tool for high-dimensional quantum information processing. In particular, the complexity resulting from the generation and detection of the high-dimensional states involved may be fully characterized. In the study of quantum channels for quantum communications, full characterization via QPT turns out to be a beneficial resource that allows one to take full advantage of the potential high-dimensional nature of the protocols at play to increase the overall secret key rate.

[1] Dowling, J. P. & Milburn, G. J. Quantum technology: the second quantum revolution. Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 361, 1655–1674 (2003).

[2] Bennett, C. H. & Brassard, G. Proceedings of the ieee international conference on computers, systems, and signal processing, bangalore, india, 1984 (1984).

[3] Nielsen, M. A. & Chuang, I. Quantum computation and quantum information (2002).

[4] Degen, C., Reinhard, F. & Cappellaro, P. Quantum sensing. Rev. Mod. Phys. 89, 035002 (2017).

[5] Chuang, I. L. & Nielsen, M. A. Prescription for experimental determination of the dynamics of a quantum black box. J. Mod. Opt. 44, 2455–2467 (1997).

[6] Poyatos, J., Cirac, J. I. & Zoller, P. Complete characterization of a quantum process: the two-bit quantum gate. Phys. Rev. Lett. 78, 390 (1997).

[7] Nielsen, M. A., Knill, E. & Laflamme, R. Complete quantum teleportation using nuclear magnetic resonance. Nature 396, 52 (1998).

[8] Childs, A. M., Chuang, I. L. & Leung, D. W. Realization of quantum process tomography in nmr. Phys. Rev. A 64, 012314 (2001).

[9] O’Brien, J. L. et al. Quantum process tomography of a controlled-not gate. Phys. Rev. Lett. 93, 080502 (2004).

[10] Myrskog, S., Fox, J., Mitchell, M. & Steinberg, A. Quantum process tomography on vibrational states of atoms in an optical lattice. Phys. Rev. A 72, 013615 (2005).

[11] Riebe, M. et al. Process tomography of ion trap quantum gates. Phys. Rev. Lett. 97, 220407 (2006).

[12] Howard, M. et al. Quantum process tomography and linblad estimation of a solid-state qubit. New Journal of Physics 8, 33 (2006).

[13] Lobino, M. et al. Complete characterization of quantum-optical processes. Science 322, 563–566 (2008).

[14] Kim, D. et al. Quantum control and process tomography of a semiconductor quantum dot hybrid qubit. Nature 511, 70 (2014).

[15] Jacob, K. V., Mirasola, A. E., Adhikari, S. & Dowling, J. P. Quantum process tomography of linear and quadratically nonlinear optical systems. arXiv preprint arXiv:1801.10555 (2018).

[16] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. Rev. Mod. Phys. 74, 145 (2002). Ndagano, B., Envenu and Perez-Garcia, Benjamin and Roux, Filippos S and McLaren, Melanie and Rosales-Guzman, Carmelo and Zhang, Yingwen and Mouane, Othmane and Hernandez-Aranda, Raoul I and Konrad, Thomas and Forbes, Andrew

[17] Bienvenu, N., Perez-Garcia, B., Roux, F. S., McLaren, M., Rosales-Guzman, C., Zhang, Y., Mouane, O., Hernandez-Aranda, R. I., Konrad, T. & Forbes, A. Characterizing quantum
channels with non-separable states of classical light. *Nat. Phys.* **13**, 397 (2017).

[18] Muller, A., Zbinden, H. & Gisin, N. Underwater quantum coding. *Nature* **378**, 449 (1995).

[19] Buttler, W. et al. Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.* **81**, 3283 (1998).

[20] Yin, J. et al. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.* **119**, 200501 (2017).

[21] Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE T. Inform. Theory* **41**, 1915–1923 (1995).

[22] Coles, P. J., Metodiev, E. M. & Lütkenhaus, N. Numerical approach for unstructured quantum key distribution. *Nature Commun.* **7**, 11712 (2016).

[23] Erhard, M., Fickler, R., Krenn, M. & Zeilinger, A. Twisted photons: New quantum perspectives in high dimensions. *Light: Sci. & Appl.* **7**, 17146 (2018).

[24] Molina-Terriza, G., Torres, J. P. & Torner, L. Twisted photons. *Advances in Optics and Photonics* **8**, 200–227 (2016).

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

[26] Sit, A. Experimental quantum process tomography of non-trace-preserving maps. *Phys. Rev. A* **82**, 042307 (2010).

[27] Forbes, A., Dudley, A. & McLaren, M. Creation and detection of optical modes with spatial light modulators. *Advances in Optics and Photonics* **8**, A20–A23 (2014).

[28] Mair, A., Vaziri, A., Weihs, G. & Zeilinger, A. Entanglement of the orbital angular momentum states of photons. *Nature* **412**, 313–316 (2001).

[29] Durt, T., Englert, B.-G., Bengtsson, I. & Žyczkowski, K. On mutually unbiased bases. *Int. J. Quantum Inf.* **8**, 535–640 (2010).

[30] Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 461, 207–235 (The Royal Society, 2005).

[31] Hbounding, I. Precise quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).

[32] Nagali, E. et al. Optimal quantum cloning of orbital angular-momentum photon qubits through hong–ou–mandel coherence. *Nature Photonics* **3**, 720 (2009).

[33] Nagali, E. et al. Experimental optimal cloning of four-dimensional quantum states of photons. *Phys. Rev. Lett.* **105**, 073602 (2010).

[34] Bouchard, F., Fickler, R., Boyd, R. W. & Karimi, E. High-dimensional quantum cloning and applications to quantum hacking. *Science Adv.* **3**, e1601915 (2017).

[35] Hong, C.-K., Ou, Z.-Y. & Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044 (1987).

[36] Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).

Acknowledgments This work was supported by Canada Research Chair (CRC); Canada Foundation for Innovation (CFI); Canada Excellence Research Chairs, Government of Canada (CERC); Canada First Research Excellence Fund (CFREF); Natural Sciences and Engineering Research Council of Canada (NSERC). D.K. would like to acknowledge the project no IGA-PrF-2018-003.

Author Information Correspondence and requests for materials should be addressed to ekarimi@uottawa.ca.

Competing interests The authors declare no competing financial interests.

Data availability statement The data that support the plots and analysis within this paper and other findings of this study are available from the corresponding author upon reasonable request.