

QUANTUM MECHANICS

High-dimensional quantum cloning and applications to quantum hacking

Frédéric Bouchard,¹ Robert Fickler,¹ Robert W. Boyd,^{1,2} Ebrahim Karimi^{1,3*}

Attempts at cloning a quantum system result in the introduction of imperfections in the state of the copies. This is a consequence of the no-cloning theorem, which is a fundamental law of quantum physics and the backbone of security for quantum communications. Although perfect copies are prohibited, a quantum state may be copied with maximal accuracy via various optimal cloning schemes. Optimal quantum cloning, which lies at the border of the physical limit imposed by the no-signaling theorem and the Heisenberg uncertainty principle, has been experimentally realized for low-dimensional photonic states. However, an increase in the dimensionality of quantum systems is greatly beneficial to quantum computation and communication protocols. Nonetheless, no experimental demonstration of optimal cloning machines has hitherto been shown for high-dimensional quantum systems. We perform optimal cloning of high-dimensional photonic states by means of the symmetrization method. We show the universality of our technique by conducting cloning of numerous arbitrary input states and fully characterize our cloning machine by performing quantum state tomography on cloned photons. In addition, a cloning attack on a Bennett and Brassard (BB84) quantum key distribution protocol is experimentally demonstrated to reveal the robustness of high-dimensional states in quantum cryptography.

INTRODUCTION

High-dimensional information is a promising field of quantum information science that has matured over the last years. It is known that, by using not only qubits but also qudits, that is, d -dimensional quantum states, it is possible to encode more information on a single carrier, increase noise resistance in quantum cryptography protocols (1), and investigate fundamental properties of nature (2). Photonic systems have been shown to be promising candidates in quantum computation and cryptography for many proof-of-principle demonstrations as well as for “flying” quantum carriers to distribute high-dimensionally encoded states. Orbital angular momentum (OAM) of light, which provides an unbounded state space, has long been recognized as a potential high-dimensional degree of freedom for conducting experiments on the foundations of quantum mechanics (3, 4), quantum computation (5), and cryptography (6). The main characteristic of photons carrying OAM is their twisted wavefront, characterized by an $\exp(i\ell\varphi)$ phase term, where ℓ is an integer and φ is the azimuthal coordinate (7). In the context of quantum information, OAM states of photons have the advantage of representing quantum states belonging to an infinitely large, but discrete, Hilbert space (8). Finite subspaces of dimension d can be considered as laboratory realizations of photonic qudits. Here, we adopt the OAM degree of freedom of single photons to achieve high-dimensional quantum cloning and perform quantum hacking on a high-dimensional quantum communication channel. Although perfect cloning of unknown quantum states is forbidden (9), it is interesting to ask how similar to the initial quantum state the best possible quantum clone can be. The answer is given in terms of the cloning fidelity \mathcal{F} , which is defined as the overlap between the initial state to be cloned and that of the cloned copies. This figure of merit is a measure of the accuracy of a cloned copy obtained from a specific cloner. Schemes that achieve the best pos-

sible fidelity are called optimal quantum cloning and play an important role in quantum information (10). For instance, an optimal state estimation yields a bounded fidelity of $\mathcal{F}_{\text{est}} = 2/(1+d)$, where d is the dimension of the quantum state (11). Optimal quantum cloning turns out to be a more efficient way of broadcasting the quantum state of a single system because it yields a fidelity that is always higher than that of optimal state estimation, which has been experimentally realized for low-dimensional photonic states (12–15). Moreover, this enhancement in fidelity grows larger with higher-dimensional quantum states, further motivating experimental investigations of high-dimensional quantum cloning. Hence, high-dimensional optimal quantum cloning machines are of great importance whenever quantum information is to be transmitted among multiple individuals without knowledge of the input quantum state. Here, we concentrate on the $1 \rightarrow 2$ universal optimal quantum cloning machine, for which the optimal fidelity of the two cloned copies is given by $\mathcal{F}_{\text{clo}} = 1/2 + 1/(1+d)$, where d is the dimension of the Hilbert space of the states that are to be cloned (16).

RESULTS

Optimal quantum cloning with OAM states of single photons

We use the symmetrization method to realize a universal optimal quantum cloning machine for high-dimensional OAM states (17, 18). In this method, the quantum state that is to be cloned, namely, $|\psi\rangle$, is sent to one of the input ports of a nonpolarizing beam splitter. In the other input port, a completely mixed state of the appropriate dimension, given by $\hat{\rho}_{\text{mix}} = I_d/d$, is sent, where I_d is the d -dimensional identity matrix. The symmetrization method relies on the well-known two-photon interference effect at a 50:50 beam splitter first proposed by Hong *et al.* (19). When two indistinguishable single photons enter a beam splitter, one into each input port, the photons will “bunch” because of their bosonic nature and exit the beam splitter together through the same output port. This principle is the essence of the symmetrization method for optimal quantum cloning. When both input photons are interfering at the beam splitter, two “cloned” photons will

¹Department of Physics, University of Ottawa, 25 Templeton Street, Ottawa, Ontario K1N 6N5, Canada. ²Institute of Optics, University of Rochester, Rochester, NY 14627, USA. ³Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran.

*Corresponding author. Email: ekarimi@uottawa.ca

jointly exit one of the output ports. We note that this cloning scheme does not require knowledge of the input state and applies to any arbitrary state. This property is a result of the “universality” of the cloning machine and shows the versatility of our scheme. Each state of the output cloned photon is represented by a reduced density matrix obtained by tracing over the other photon. Because both cloned photons are characterized by an identical cloned state, the cloner is thus said to be “symmetric.” Hence, the symmetrization method is considered to be a symmetric optimal universal quantum cloning machine (UQCM). In our experiment, we implement a high-dimensional version of this UQCM with OAM states of single photons (see Fig. 1). We generate and measure the OAM states by manipulating the phase front of the photons using a liquid crystal phase-only spatial light modulator (SLM) (see the Supplementary Materials for a more detailed experimental discussion).

Cloning fidelity

To characterize the quality of our UQCM, we use two different approaches to evaluate the yielding cloning fidelities: measuring the probability of successful cloning and full-state tomography of the cloned photons. In this first series of measurements, we evaluate the cloning fidelity, \mathcal{F}_ψ , of a given arbitrary input state, $|\psi\rangle$, from the probability of finding both output cloned photons in

the state $|\psi\rangle$, that is, $\mathcal{P}(|\psi\rangle, |\psi\rangle)$. This probability can be obtained experimentally by means of coincidence measurements: $\mathcal{F}_\psi = \mathcal{P}(|\psi\rangle, |\psi\rangle) = (N(|\psi\rangle, |\psi\rangle) + \sum_{i \neq \psi} N(|\psi\rangle, |i\rangle)) / N_{\text{tot}}$, where $N(|i\rangle, |j\rangle)$ represents the number of coincidence measurements between the states $|i\rangle$ and $|j\rangle$, N_{tot} is the total number of coincidence measurements (that is, $N_{\text{tot}} = N(|\psi\rangle, |\psi\rangle) + 2\sum_{i \neq \psi} N(|\psi\rangle, |i\rangle)$), and $|i\rangle$ and $|j\rangle$ represent elements of the basis containing $|\psi\rangle$. The factor of 2 that appears in the definition of N_{tot} is a result of the symmetric nature of our cloning machine, where $N(|i\rangle, |j\rangle) = N(|j\rangle, |i\rangle)$. Further, one can obtain from normalization, $\mathcal{P}(|i\rangle, |\psi\rangle) = N(|i\rangle, |\psi\rangle) / N_{\text{tot}}$, for $i \neq \psi$. Here, we note that the optimal cloning fidelity depends on the HOM interference visibility \mathcal{V} through the relation

$$\mathcal{F}(\mathcal{V}) = \frac{1}{2} + \frac{1}{1+d} \left(\frac{2\mathcal{V}}{1+\mathcal{V}} \right)$$

Dimensionality and universality of the cloning machine

Compared to a full tomographic reconstruction, this method requires fewer measurements and thus enables us to characterize the cloning fidelity of our cloner under a wider range of circumstances. For instance, the effect of dimensionality on a UQCM is a crucial point for any optimal cloning schemes. As mentioned previously, increasing the

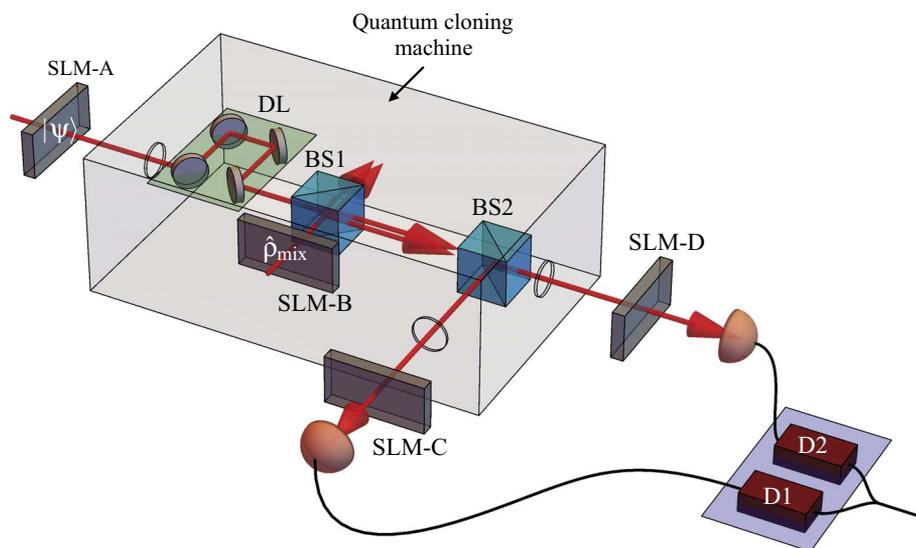
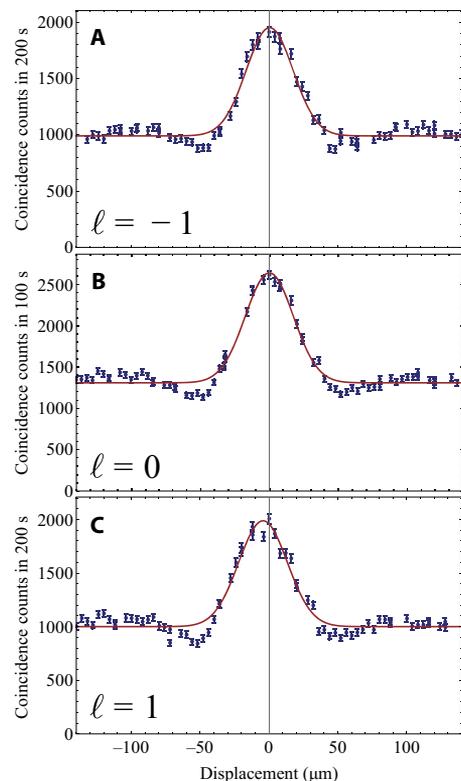


Fig. 1. Simplified sketch of the experimental design. The input quantum state $|\psi\rangle$ is imprinted on a single photon using an SLM-A. The single photon is subsequently sent to the cloning machine for optimal cloning. The cloning machine consists of a delay line (DL), to adjust the arrival time of the input photon, a second photon that is in a completely mixed state when exiting SLM-B, and a first beam splitter (BS1). The two photons are made to arrive at the beam splitter simultaneously using the DL. The two photons exiting one of the output ports of the first beam splitter together are separated at a second beam splitter (BS2) and are sent out of the cloning machine. The cloned photons are then detected and characterized using detectors (D1 and D2) and SLMs (SLM-C and SLM-D), respectively. (A to C) Examples of Hong-Ou-Mandel (HOM) coalescence curves for input photons of $\ell = -1, 0, 1$, respectively (top to bottom). The curve is obtained by recording the coincidences between the output ports of BS2 for various delays of one of the input photons. Examples of enhancement peaks of $R_{\ell=-1} = 1.97 \pm 0.08$, $R_{\ell=0} = 2.02 \pm 0.08$, and $R_{\ell=1} = 1.99 \pm 0.09$ are obtained experimentally, and agree with the theoretical value of $R_{\text{th}} = 2$, corresponding to a visibility of $\mathcal{V} = 1$.



dimensionality of the input quantum states results in a decrease of the cloning fidelity. This decrease in cloning fidelity can serve as an intuitive explanation for the superiority of high-dimensional quantum cryptography. In our experiment, we measure the cloning fidelity of our cloning machine for different input states belonging to the computational OAM basis of various dimensions $d \in \{2, 3, 4, 5, 6, 7\}$. We find near-perfect agreement of the experimentally evaluated cloning fidelities to the theoretical predictions of the high-dimensional $1 \rightarrow 2$ symmetric optimal UQCM (see Fig. 2). In addition, we experimentally verify the universality of our cloning machine by performing quantum cloning of every state of all $d + 1$ OAM mutually unbiased bases (MUBs) (see Fig. 3A) (20, 21). Once more, we find near-optimal cloning fidelities for all MUBs, thus demonstrating the viability and universality of our optimal quantum cloner (see the Supplementary Materials). Note that MUBs and their elements are playing an important role in quantum communication and information, as basis states used in quantum cryptographic protocols (22) and quantum state tomography (23), for example.

Optimal cloning of a Gaussian state

As a second series of measurements for a complete characterization of our UQCM, we fully reconstruct the high-dimensional cloned quantum states by means of quantum state tomography. Moreover,

our UQCM should be able to clone the state regardless of the input state and its complex structure in the high-dimensional state space. An exemplary and visually interesting high-dimensional state is the so-called Gaussian state given by the following superposition

$$|\psi_{\text{Gauss}}\rangle = \mathcal{N} \sum_{\ell=-3}^{\ell=3} \exp[-(\ell/2)^2] |\ell\rangle$$

where \mathcal{N} is a normalization constant. We experimentally generate the Gaussian state of dimension $d = 7$ and perform full quantum state tomography on one of the output cloned photons. The theoretically expected and experimentally achieved results are shown in Fig. 3B. The cloned Gaussian state has a fidelity of 0.80 ± 0.03 with respect to the theoretically expected cloned density matrix. Thus, for an arbitrary complex input state $|\psi_{\text{Gauss}}\rangle$, the experimental cloning fidelity, $\mathcal{F} = \langle \psi_{\text{Gauss}} | \hat{\rho}_{\text{cl}} | \psi_{\text{Gauss}} \rangle$, of our UQCM obtained from complete quantum state tomography can be estimated to be around 0.40 ± 0.01 . In comparison to the average fidelity obtained previously for $d = 7$ of 0.59 ± 0.02 , which we evaluated from success probabilities, the lower fidelity value can be explained by measurement errors and cross-talk among spatial modes for several MUBs. For complete state tomography, these errors have a stronger adverse effect, and a much larger number of measurements (56 measurements in dimension 7),

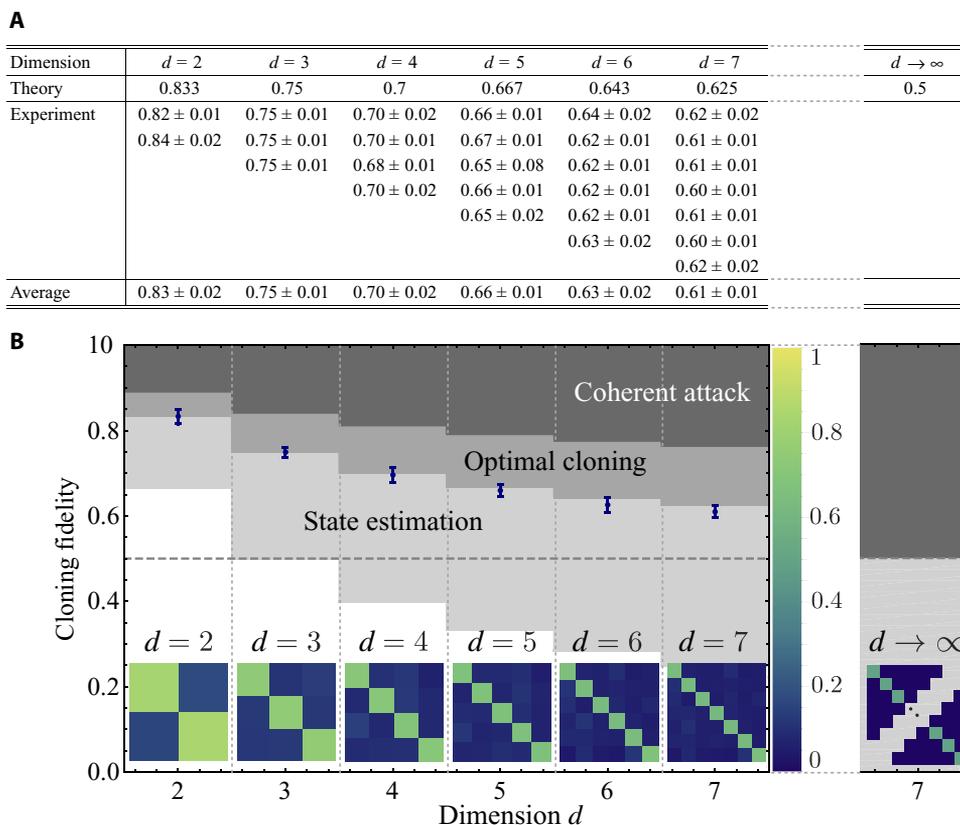


Fig. 2. Optimal cloning fidelity for various dimensions. (A) Experimental values of the cloning fidelities are shown for each d number of elements of the logical basis, along with theoretical values, for various dimensions d . (B) The average cloning fidelities (blue dots) are plotted for various dimensions, along with probability matrices $\mathcal{P}(|i\rangle, |\psi\rangle)$ of detecting a cloned photon in any output state $|i\rangle$ of the OAM logical basis, given an input state $|\psi\rangle$ of the same basis. The diagonal elements of the probability matrices correspond to the cloning fidelity of each element of the basis. The light and dark gray shaded areas correspond to fidelities not accessible by state estimation and $1 \rightarrow 2$ optimal symmetric UQCM, respectively. In quantum cryptography, a more effective class of quantum hacking, namely, coherent attacks (1), yields larger fidelities illustrated by the dim gray shaded area.

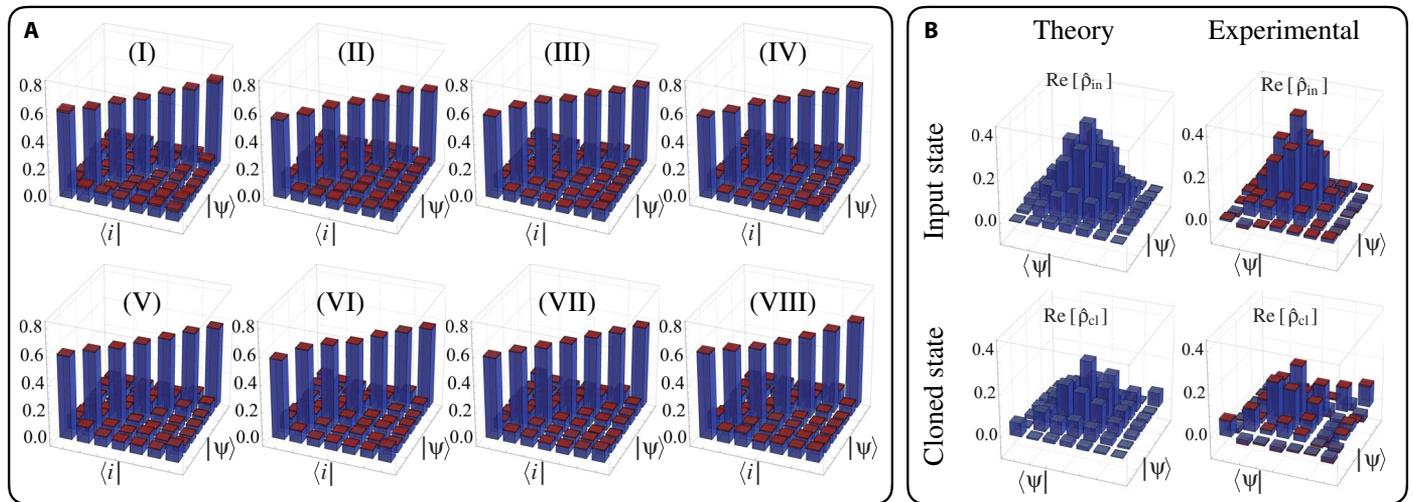


Fig. 3. Cloning fidelities for various MUBs and cloning of Gaussian states in dimension $d = 7$. (A) Probability $\mathcal{P}(|j\rangle, |\psi\rangle)$ of detection of an output cloned state $|j\rangle$ given an input state $|\psi\rangle$, where $|j\rangle$ and $|\psi\rangle$ belong to a specific MUB. This set of measurement is repeated for all $d + 1$ MUBs (I) to (VIII), in dimension 7. The on-diagonal elements represent the cloning fidelities for each element of a given basis. (B) Theoretical and experimental high-dimensional cloning of a Gaussian state. The cloned fidelity is obtained by calculating the overlap of the reduced density matrix of the cloned state with the input state. The experimental reduced density matrix of the cloned state is obtained by full quantum state tomography. The experimentally reconstructed density matrices of the Gaussian state before and after cloning are shown along with their theoretical counterparts.

that is, $d(d + 1)$, are required (see the Supplementary Materials). However, both methods show that our implementation of a symmetric UQCM can be used to clone any arbitrarily complex quantum state up to dimension 7, without a significant deterioration of the optimal state fidelities. Hence, cloning of high-dimensional quantum states encoded in the OAM degree of freedom might become a building block of future high-dimensional quantum information applications.

Cloning attack in quantum cryptography

As a final test of the ability to clone high-dimensional quantum states, we implement a cloning attack into a high-dimensional quantum key distribution (QKD) scheme. In a QKD protocol, a sender (Alice) and receiver (Bob) use quantum states to distribute a random, secret key shared between both parties. The shared key is then used to communicate an encrypted message through a classical channel, using the perfectly secure one-time pad protocol. The security of QKD derives from the fact that the presence of an eavesdropper (Eve) will result in the introduction of errors in the shared key, which can originate, for example, from the nonperfect but optimal cloning done by the eavesdropper (24). Note that the dimensionality of the quantum states used to distribute the key directly affects the cloning fidelity and thus the amount of errors introduced by a possible cloning attack.

We first perform a high-dimensional QKD using the seminal BB84 protocol (22), extended using OAM states of dimension $d = 7$. An eavesdropper with access to a high-dimensional UQCM then performs individual attacks on the QKD channel. In our experiment, the first MUB is given by the logical OAM basis $\{|\ell\rangle; \ell = -3, -2, -1, 0, 1, 2, 3\}$, and the second MUB is given by the Fourier angle basis $\{|\phi_i\rangle; i = 1, 2, 3, 4, 5, 6, 7\}$. Projective measurements are shown with and without the cloning attack in Fig. 4 (A and B), respectively. The lower fidelity due to a cloning attack is readily visible. A visually compelling illustration of the effect of an eavesdropper on Alice and Bob's shared key can be given by directly using the established raw sifted key, without performing further

error correction and privacy amplification, as a one-time pad to share an encrypted message, for example, an image of their favorite optical phenomenon. We experimentally simulate such a situation by performing the high-dimensional BB84 protocol with and without Eve's attack using our UQCM. In a real-world QKD, experimental errors will always be introduced in the raw key, leading to a slightly deteriorated image after Bob's decryption (see Fig. 4A). However, if Eve performs her cloning attack while Alice and Bob are trying to establish their key, the errors increase significantly, which is then directly visible in Bob's decrypted image (see Fig. 4B). The quantum bit error rate (QBER) is given by 0.16 and 0.57, without and with the cloning attack, respectively. In the absence of an eavesdropper, the QBER is well below the error bound for security in dimension 7, that is, $D_{\text{coh}} = 23.72\%$ (1). Thus, error correction and privacy amplification may be performed in order for Alice and Bob to obtain a completely secure and errorless shared key. However, in the presence of the eavesdropper, the QBER is well above the bound in dimension 7, immediately revealing the presence of Eve. Furthermore, the mutual information between Alice and Bob may be calculated from

$$I_{\text{AB}}^d = \log_2(d) + (1 - e_{\text{B}}^N) \log_2(1 - e_{\text{B}}^N) + e_{\text{B}}^N \log_2(e_{\text{B}}^N / (d - 1))$$

where e_{B}^N is Bob's error rate (25). Experimental values of 1.73 and 0.36 bits per photon were obtained for Alice and Bob's mutual information without and with the cloning attack, respectively. In addition, we performed quantum hacking to a two-dimensional QKD protocol (BB84). In this case, the QBER is given by 0.19 and 0.007, with and without the cloning attack, which is well above and below the security bound in dimension 2, that is, $D_{\text{coh}}(2) = 11.00\%$, respectively. Hence, it is clear that high-dimensional quantum cryptography leads to higher signal disturbance in the presence of an optimal cloning attack, resulting in a larger tolerance to noise in the quantum channel.

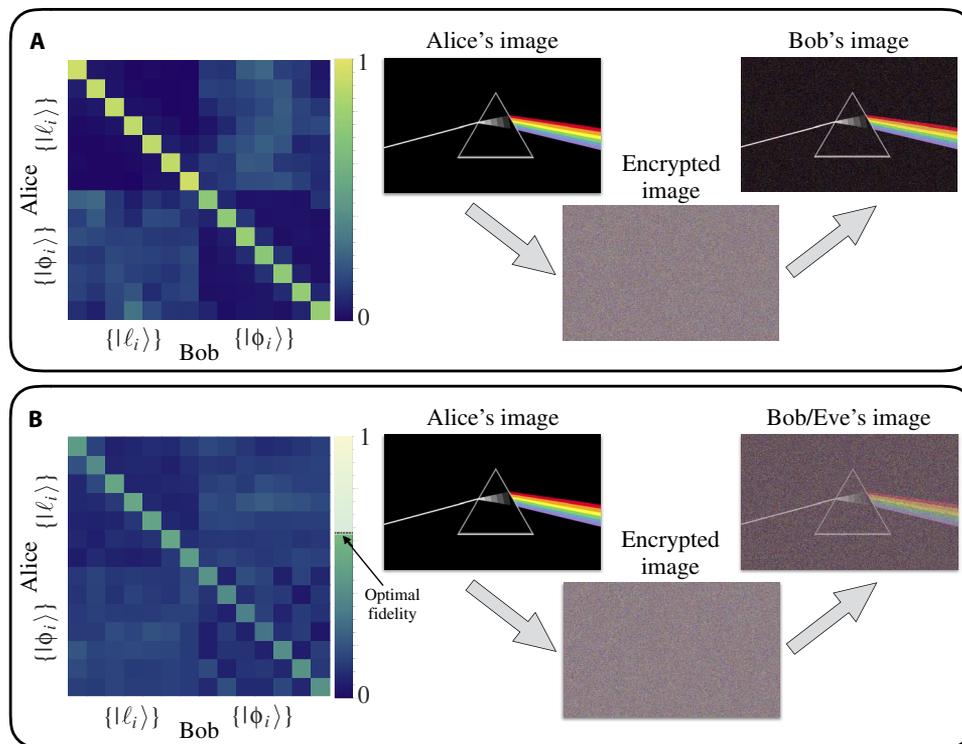


Fig. 4. High-dimensional QKD without and with quantum hacking. (A) Experimental probability matrices obtained from projective measurements are shown on the left side. The bases selected by Alice and Bob are indicated on the vertical and horizontal axes, respectively. On the right, we show Alice's initial message and Bob's decrypted message. (B) Experimental probability matrices with the presence of an eavesdropper having access to a symmetric optimal UQCM. Similarly, Alice's initial message is shown along with the decrypted message obtained by both Bob and Eve. One may note that for the BB84 protocol, the symmetric UQCM does not lead to the optimal individual attack. Rather, our UQCM results in the optimal individual attack for the QKD protocol exploiting all $d + 1$ available MUBs. In the simpler case of the BB84 protocol, the optimal attack consists of the asymmetric Fourier-covariant cloner (1, 26), which cannot be straightforwardly implemented in our experimental setup.

DISCUSSION

In conclusion, we showed the feasibility of high-dimensional optimal quantum cloning of OAM states of single photons. This scheme was further used to perform a cloning attack to a secure quantum channel, revealing the robustness of high-dimensional quantum cryptography upon quantum hacking. Moreover, studying the effect of dimensionality and universality on optimal quantum cloning reveals its advantage over optimal state estimation in quantum information schemes, where unknown quantum states must be distributed.

MATERIALS AND METHODS

The experimental setup can be divided into three parts: a single-photon source, a HOM interferometer, and a cloning characterization apparatus (see fig. S1). Single-photon pairs were generated by the process of spontaneous parametric down-conversion at a nonlinear type I β -barium borate crystal illuminated by a quasi-continuous wave ultraviolet laser operating at a wavelength of 355 nm. The single photons were spatially filtered to the fundamental Gaussian mode by coupling the generated pairs to single-mode optical fibers, with a measured coincidence rate of 30 kHz, within a coincidence time window of 5 ns. The partner photons were each made to illuminate an SLM, to generate the desired photonic states, and subsequently sent at a 50:50 nonpolarizing beam splitter, one at each input port. The path taken by the photons, generated at the nonlinear crystal to get to the beam splitter, must be equidistant for both photons of a given pair to observe the two-photon interference effect. This can be achieved with a precision of tens of micrometers using a

programmable translational stage. Polarizers and interference filters were inserted in the path of each photon. The photons were then made indistinguishable in arrival time, polarization, and frequency. On the other hand, the spatial modes of the photons were kept as a degree of freedom representing photonic quantum states for the UQCM. Following the HOM interference beam splitter, the bunched photons were sent to a second beam splitter, separating them for further coincidence detection. Last, the separated output cloned photons were detected and characterized with SLMs followed by single-mode optical fibers.

SUPPLEMENTARY MATERIALS

Supplementary material for this article is available at <http://advances.sciencemag.org/cgi/content/full/3/2/e1601915/DC1>

Supplementary Text

fig. S1. Detailed experimental setup.

fig. S2. Experimental cloning fidelities for every element of each MUB in dimension 7.

fig. S3. Projective measurements of the input and cloned Gaussian state.

REFERENCES AND NOTES

1. N. J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Security of quantum key distribution using d -level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
2. M. Krenn, M. Huber, R. Fickler, R. Lapkiewicz, S. Ramelow, A. Zeilinger, Generation and confirmation of a (100×100) -dimensional entangled quantum system. *Proc. Natl. Acad. Sci. U.S.A.* **111**, 6243–6247 (2014).
3. A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, E. Andersson, Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities. *Nat. Phys.* **7**, 677–680 (2011).

4. J. Harris, F. Bouchard, E. Santamato, W. H. Zurek, R. W. Boyd, E. Karimi, Quantum probabilities from quantum entanglement: Experimentally unpacking the Born rule. *New J. Phys.* **18**, 053013 (2016).
5. F. Cardano, F. Massa, H. Qassim, E. Karimi, S. Slussarenko, D. Paparo, C. de Lisio, F. Sciarrino, E. Santamato, R. W. Boyd, L. Marrucci, Quantum walks and wavepacket dynamics on a lattice with twisted photons. *Sci. Adv.* **1**, e1500087 (2015).
6. M. Mirhosseini, O. S. Magaña-Loaizal, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, R. W. Boyd, High-dimensional quantum cryptography with twisted light. *New J. Phys.* **17**, 033033 (2015).
7. L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, J. Woerdman, Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes. *Phys. Rev. A* **45**, 8185–8189 (1992).
8. G. Molina-Terriza, J. P. Torres, L. Torner, Twisted photons. *Nat. Phys.* **3**, 305–310 (2007).
9. W. K. Wootters, W. H. Zurek, A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).
10. N. Gisin, S. Massar, Optimal quantum cloning machines. *Phys. Rev. Lett.* **79**, 2153 (1997).
11. D. Bruß, C. Macchiavello, Optimal state estimation for d -dimensional quantum systems. *Phys. Lett. A* **253**, 249–251 (1999).
12. A. Lamas-Linares, C. Simon, J. C. Howell, D. Bouwmeester, Experimental quantum cloning of single photons. *Science* **296**, 712–714 (2002).
13. W. T. M. Irvine, A. L. Linares, M. J. A. de Dood, D. Bouwmeester, Optimal quantum cloning on a beam splitter. *Phys. Rev. Lett.* **92**, 047902 (2004).
14. E. Nagali, L. Sansoni, F. Sciarrino, F. De Martini, L. Marrucci, B. Piccirillo, E. Karimi, E. Santamato, Optimal quantum cloning of orbital angular momentum photon qubits through Hong–Ou–Mandel coalescence. *Nat. Photonics* **3**, 720–723 (2009).
15. E. Nagali, D. Giovannini, L. Marrucci, S. Slussarenko, E. Santamato, F. Sciarrino, Experimental optimal cloning of four-dimensional quantum states of photons. *Phys. Rev. Lett.* **105**, 073602 (2010).
16. P. Navez, N. J. Cerf, Cloning a real d -dimensional quantum state on the edge of the no-signaling condition. *Phys. Rev. A* **68**, 032313 (2003).
17. M. Ricci, F. Sciarrino, C. Sias, F. De Martini, Teleportation scheme implementing the universal optimal quantum cloning machine and the universal NOT gate. *Phys. Rev. Lett.* **92**, 047901 (2004).
18. F. Sciarrino, C. Sias, M. Ricci, F. De Martini, Quantum cloning and universal NOT gate by teleportation. *Phys. Lett. A* **323**, 34–39 (2004).
19. C. K. Hong, Z. Y. Ou, L. Mandel, Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **59**, 2044 (1987).
20. T. Durt, B.-G. Englert, I. Bengtsson, K. Zyczkowski, On mutually unbiased bases. *Int. J. Quantum Inf.* **8**, 535 (2010).
21. A. Klappenecker, M. Rötteler, Constructions of mutually unbiased bases, in *Finite Fields and Applications* (Springer, 2004), pp. 137–144.
22. C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, paper presented at the International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.
23. R. B. A. Adamson, A. M. Steinberg, Improving quantum state estimation with mutually unbiased bases. *Phys. Rev. Lett.* **105**, 030406 (2010).
24. K. Bartkiewicz, K. Lemr, A. Černoč, J. Soubusta, A. Miranowicz, Experimental eavesdropping based on optimal quantum cloning. *Phys. Rev. Lett.* **110**, 173601 (2013).
25. W.-H. Zhang, L. Ye, Optimal asymmetric phase-covariant and real state cloning in d dimensions. *New J. Phys.* **9**, 318 (2007).
26. H. Fan, H. Imai, K. Matsumoto, X.-B. Wang, Phase-covariant quantum cloning of qudits. *Phys. Rev. A* **67**, 022317 (2003).

Acknowledgments

Funding: This work was supported by the Canada Research Chairs Program and Canada Foundation for Innovation. F.B. acknowledges the support of the Vanier Canada Graduate Scholarships Program of the Natural Sciences and Engineering Research Council of Canada (NSERC). R.F. acknowledges the support of the Banting postdoctoral fellowship of the NSERC. All authors acknowledge the support of the Max Planck–University of Ottawa Center for Extreme and Quantum Photonics. **Author contributions:** F.B. and E.K. conceived the idea. F.B., R.F., R.W.B., and E.K. designed the experiment. F.B. performed the experiment and analyzed the data. F.B. and E.K. wrote the manuscript with the help of other authors. All authors discussed the results and contributed to the text of the manuscript. **Competing interests:** The authors declare that they have no competing interests. **Data and materials availability:** All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials. Additional data related to this paper may be requested from the authors.

Submitted 13 August 2016

Accepted 14 December 2016

Published 3 February 2017

10.1126/sciadv.1601915

Citation: F. Bouchard, R. Fickler, R. W. Boyd, E. Karimi, High-dimensional quantum cloning and applications to quantum hacking. *Sci. Adv.* **3**, e1601915 (2017).

This article is published under a Creative Commons license. The specific license under which this article is published is noted on the first page.

For articles published under [CC BY](#) licenses, you may freely distribute, adapt, or reuse the article, including for commercial purposes, provided you give proper attribution.

For articles published under [CC BY-NC](#) licenses, you may distribute, adapt, or reuse the article for non-commercial purposes. Commercial use requires prior permission from the American Association for the Advancement of Science (AAAS). You may request permission by clicking [here](#).

The following resources related to this article are available online at <http://advances.sciencemag.org>. (This information is current as of February 3, 2017):

Updated information and services, including high-resolution figures, can be found in the online version of this article at:

<http://advances.sciencemag.org/content/3/2/e1601915.full>

Supporting Online Material can be found at:

<http://advances.sciencemag.org/content/suppl/2017/01/30/3.2.e1601915.DC1>

This article **cites 24 articles**, 3 of which you can access for free at:

<http://advances.sciencemag.org/content/3/2/e1601915#BIBL>

Science Advances (ISSN 2375-2548) publishes new articles weekly. The journal is published by the American Association for the Advancement of Science (AAAS), 1200 New York Avenue NW, Washington, DC 20005. Copyright is held by the Authors unless stated otherwise. AAAS is the exclusive licensee. The title *Science Advances* is a registered trademark of AAAS