communications physics

A Nature Portfolio journal

Article

https://doi.org/10.1038/s42005-025-02376-8

High-dimensional quantum key distribution with Qubit-like states

Check for updates

Lukas Scarfe [1] ✉, Rojan Abolhassani [1], Frédéric Bouchard [2], Aaron Z. Goldberg [2], Khabat Heshami [1,2], Francesco Di Colandrea [1,3] & Ebrahim Karimi [1,2,4]

Quantum key distribution (QKD) protocols most often use two conjugate bases in order to verify the security of the quantum channel. In the majority of protocols, these bases are mutually unbiased to one another, which is to say they are formed from balanced superpositions of the entire set of states in the opposing basis. Here, we introduce a high-dimensional QKD protocol using qubit-like states, referred to as Fourier-qubits (or F-qubits). In our scheme, each F-qubit is a superposition of only two computational basis states with a relative phase that can take d distinct values, where d is the dimension of the computational basis. This non-mutually-unbiased approach allows us to bound the information leaked to an eavesdropper, maintaining security in high-dimensional quantum systems despite the states' seemingly two-dimensional nature. By simplifying state preparation and measurement, our protocol offers a practical alternative for secure high-dimensional quantum communications. We experimentally demonstrate this protocol for a noisy high-dimensional QKD channel using the orbital angular momentum degree of freedom of light and discuss the potential benefits for encoding in other degrees of freedom.

Quantum Key Distribution (QKD) promises an information-theoretically secure method to distribute shared keys guaranteed by the fundamental laws of physics[1–3]. In order to distribute a secure key over an untrusted channel, Alice and Bob must prepare, exchange, and measure quantum states with few errors, which are not trivial tasks[4]. This difficulty has spawned many QKD protocols that can be more easily implemented with realistic devices and improve the secure key rates despite the practical challenges[5–7].

High-dimensional (HD) QKD protocols have attracted growing interest in recent years[8,9]. Indeed, by encoding information into a higher-dimensional Hilbert space, secure keys can be distributed with a higher density of information per photon[10]. In addition, these protocols can tolerate a greater error rate introduced by either an eavesdropper or simple channel noise[11]. While these benefits are enticing, the reality is that, up to this point, nearly all commercial QKD systems operate with two-dimensional QKD protocols[12]. Likewise, most fundamental research is focused on two-dimensional implementations[13]. The main reason is that encoding information in a high-dimensional Hilbert space poses significant technical challenges[14], with the complexity of experimental setups scaling proportionally to the dimensionality of the protocol. In contrast, a two-dimensional QKD system can process the polarisation degree of freedom, offering the advantage of cost-effective and straightforward passive generation and detection equipment.

The go-to QKD protocol, BB84, requires two mutually unbiased bases (MUB), where each basis consists of states in a balanced superposition of every state in the opposing basis. The two most common bases chosen are the computational (logical) basis and the Fourier basis[11,15,16]. In the d-dimensional implementation, the use of the Fourier basis requires precisely generating and measuring superpositions of d states.

In this work, we introduce a set of "qubit-like" states to be used in QKD alongside the logical basis in lieu of the Fourier basis. These states are qubit-like in the sense that they are only constructed as superpositions of two logical states, with a relative phase difference between them that is one of the d roots of unity. Because of the binary nature of these states, and their relation to the well-known quantum Fourier transform (QFT), we refer to these states as Fourier-qubits (or F-qubits). This reduction in the complexity of the states allows for simpler generation and detection[17]. While previous works with qubit-like states used them to increase the error tolerance up to the theoretical limit of 50%, the key rate remains that of a two-dimensional protocol, which is 1 bit per sifted photon[18,19]. Additionally, a recent work using a subset of the F-qubit states has shown that using qubit-like states in a HD protocol can greatly increase the information density of a time-bin coherent pulse-based QKD channel, albeit without an increase in error tolerance at higher dimensions[20]. Here, the F-qubits are used to complement the logical basis, whose states' generation and detection are the most simple,

[1]Nexus for Quantum Technologies, University of Ottawa, Ottawa, ON, Canada. [2]National Research Council of Canada, Ottawa, ON, Canada. [3]Dipartimento di Fisica, Università degli Studi di Napoli Federico II, Complesso Universitario di Monte Sant'Angelo, Napoli, Italy. [4]Institute for Quantum Studies, Chapman University, Orange, CA, USA. ✉e-mail: lscar039@uottawa.ca

and estimate the information leaked to a potential eavesdropper. This feature allows our QKD protocol to maintain the high-dimensional benefit of increased information density of $\log_2(d)$ bits per sifted photon, as well as the feature of error tolerance increasing with dimension, all while using relatively simple quantum states.

We theoretically prove that our protocol is secure from the most general coherent attack by an eavesdropper by demonstrating that the F-qubits can be used to indirectly measure the phase error rate. Additionally, we experimentally demonstrate the generation and detection of these modes in a noisy lab-scale channel using spatial modes of light in a 4-dimensional Hilbert space. In our test, the channel supports our F-qubit-based QKD protocol with a measured sifted key rate above 1 bit per sifted photon. We foresee our protocol being useful in implementations where high-dimensional QKD is desirable, such as high-bitrate and low-noise channels that are bandwidth-limited by the detector recovery time. Additionally, any system where the complexity of the quantum state scales with dimensionality will benefit from the implementation of the F-qubits.

Methods

Protocol

In our protocol, information is encoded onto qudits living in a d-dimensional Hilbert space. In particular, Alice and Bob prepare and measure their qudits in two separate bases. In the logical basis, information is encoded in states of the form $|\psi_n\rangle = |n\rangle$, where $n \in \{0, 1, \ldots, d-1\}$. Alice randomly selects n, serving as her raw key, and transmits the state $|n\rangle$ over an untrusted channel. Upon reception, Bob projects his incoming state on the same basis and uses the measurement outcome n' as his raw key. By iterating this process, Alice and Bob generate a raw key and use an authenticated classical channel to compare a small subset of their keys, estimating the error rate E_d to perform error reconciliation.

In order to bound Eve's leaked information, Alice and Bob also prepare and measure states in a second basis containing the F-qubit states:

$$|\phi_{jk}^m\rangle = (|j\rangle + \omega_d^m|k\rangle)/\sqrt{2}, \tag{1}$$

where $\omega_d = e^{2\pi i/d}$, $j \in \{0, 1 \ldots, d-2\}$, $k \in \{1, 2, \ldots, d-1\}$, with $j < k$, and $m \in \{0, 1, \ldots, d-1\}$. A depiction of these modes in a time-bin implementation can be seen in Fig. 1. More precisely, Alice randomly selects a triplet (j, k, m), preparing the state $|\phi_{jk}^m\rangle$. Bob performs a measurement in the same F-qubit basis, projecting onto $|\phi_{j'k'}^{m'}\rangle$. Via classical communications, Alice and Bob can determine the probability of obtaining errors in the F-qubit basis. This information is used to estimate the phase error rate, E_d', to bound the information leaked to an eavesdropper as in BB84.

Finally, as in other high-dimensional BB84-like protocols, the secret key rate per sifted photon is given by[21]

$$R = \log_2(d) - h^{(d)}(E_d) - h^{(d)}(E_d'), \tag{2}$$

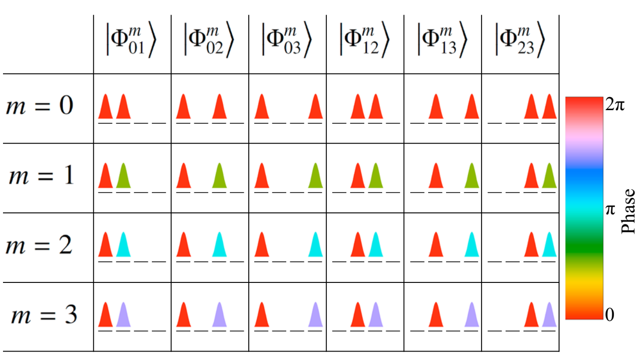

Fig. 1 | *F*-qubits in a 4-dimensional time-bin-based protocol. The logical basis consists of chopped Gaussian modes that are separated into time-bins $|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$. False colours encode the relative phase information.

where $h^{(d)}(x) = -x\log_2(x/(d-1)) - (1-x)\log_2(1-x)$ is the d-dimensional Shannon entropy function, and E_d and E_d' are the channel dit error and phase error rates, respectively.

Results

Proof of security

Assuming the transmitted qudit is generated by an ideal single-photon source, the action of an eavesdropper, Eve, can be generally modeled as a coherent attack given by the unitary transformation U_{Eve}:

$$U_{\text{Eve}}|\eta_k\rangle|e_{00}\rangle = \sum_{j=0}^{d-1} c_{kj}|\eta_j\rangle|e_{kj}\rangle, \tag{3}$$

where $|e_{kj}\rangle$ is Eve's ancilla state and $|\eta_k\rangle$ is extracted from the Fourier-conjugate basis:

$$|\eta_k\rangle = \frac{1}{\sqrt{d}}\sum_{n=0}^{d-1}\omega_d^{kn}|n\rangle. \tag{4}$$

Without loss of generality, we assume $c_{kj} \geq 0$ and $\langle e_{kj}|e_{rs}\rangle = \delta_{kr}\delta_{js}$.

The dit error rate of the Fourier basis, E_d', depends on the probability that Bob obtains a measurement of $|\eta_n\rangle$ conditioned on the fact that Alice prepares $|\eta_\ell\rangle$:

$$p(\eta_n|\eta_\ell) = \text{Tr}\left[|\eta_n\rangle\langle\eta_n|U_{\text{Eve}}|\eta_\ell\rangle\langle\eta_\ell| \otimes |e_{00}\rangle\langle e_{00}|U_{\text{Eve}}^\dagger\right] = c_{\ell n}^2. \tag{5}$$

We are now interested in relating the probability outcomes $p(\eta_n|\eta_\ell)$ in the Fourier basis to the measured probability outcomes of the qubit-like states. To do so, we use the fact that the F-qubit states can be rewritten in terms of the Fourier basis states as

$$\left|\phi_{jk}^m\right\rangle = \frac{1}{\sqrt{2d}}\sum_\ell\left(\omega_d^{-j\ell} + \omega_d^{(m-k\ell)}\right)|\eta_\ell\rangle. \tag{6}$$

The probability that Bob obtains $|\phi_{j'k'}^{m'}\rangle$ conditioned on the fact that Alice prepares $|\phi_{jk}^m\rangle$ is thus given by

$$p\left(\phi_{j'k'}^{m'}|\phi_{jk}^m\right) = \frac{4}{d^2}\sum_{\ell n}\cos^2\left[\frac{\pi(m-(k-j)\ell)}{d}\right]\cos^2\left[\frac{\pi(m'-(k'-j')n)}{d}\right]p(\eta_n|\eta_\ell). \tag{7}$$

This relation can be inverted to find the probability outcomes $p(\eta_n|\eta_\ell)$ in the Fourier basis given the probability outcomes of the F-qubits,

$$\begin{aligned} p(\eta_n|\eta_\ell) = \frac{4}{d^4}\sum_{j<k}\sum_{j'<k'}\sum_{m,m'}\left(\beta + \sum_{p=0}^{d-1}\exp\left(\frac{2\pi i}{d}p\left(m-(k-j)\ell\right)\right)\right) \\ \left(\beta + \sum_{p'=0}^{d-1}\exp\left(\tfrac{2\pi i}{d}p'\left(m'-(k'-j')n\right)\right)\right)p\left(\phi_{j'k'}^{m'}|\phi_{jk}^m\right), \end{aligned} \tag{8}$$

where $\beta = (2-d)/(d-1)$. For the full derivation of this relation, refer to Supplementary Note 3. Recall that the result of Eq. (2) is expressed in terms of the dit error rate (E_d) and the phase error rate (E_d') of the computational basis. Eve's leaked information is given by $I_{AE} \leq h^{(d)}(E_d')$[22], where I_{AE} is the mutual information between Alice and Eve. Explicitly, the dit error rate in the Fourier basis is given by

$$E_d' = \frac{1}{d}\sum_{\ell \neq n} p(\eta_n|\eta_\ell). \tag{9}$$

Using the fact that the dit error rate in the Fourier basis is equal to the phase error in the computational basis[23], we have then linked the probability outcomes of the F-qubits to phase error rate of the computational basis.

With both the dit and phase error rates in the channel, Alice and Bob can perform error correction and generate a secure key so long as both errors are below the tolerable threshold[24].

Finally, the secret key rate per sifted photon is given by

$$\begin{aligned} R &= \log_2(d) - h^{(d)}(E_d) - I_{\mathrm{AE}} \\ &\geq \log_2(d) - h^{(d)}(E_d) - h^{(d)}(E_d'). \end{aligned} \tag{10}$$

We have shown the protocol to be secure under what is considered a collective attack[25], which could be extended to general attacks[26].

Implementation

We test the generation and detection of these modes in a hypothetical orbital angular momentum (OAM) based protocol through a noisy short-distance free-space optical channel. In particular, we use Laguerre-Gaussian (LG) beams, each carrying a discrete value of OAM, ℓ[27], forming a 4-dimensional Hilbert space. The phase and intensity of the spatial modes are shown and labeled in Fig. 2. The *F*-qubit modes are generated by impinging a 633 nm beam from a HeNe laser onto a spatial light modulator (SLM) displaying a grated hologram designed to precisely control phase and intensity[28] of an output beam. The traditional Fourier basis consists of small areas of intensity located around a ring. Due to their small intensity distributions, SLMs have a low efficiency in both generation and detection of the modes as compared to the *F*-qubits, which have a larger intensity distribution that utilizes more of the SLMs' active area. The beam carrying the *F*-qubit, along with a Gaussian beam of the same wavelength and opposite polarisation, are sent through a channel with noise simulated by a turbulent cell, as well as an adaptive optics system as a corrective element[29]. A simplified experimental setup is shown in Fig. 3. Further information on the use of the noisy channel and the adaptive optics system can be found in Supplementary Note 1. As our security proof is as of now only valid for a single-photon model, our tolerable error rates should be considered in the case of a perfect single-photon source.

The *F*-qubit mode is sent to another SLM where a projective measurement is performed using intensity and phase masking[30]. Each generated mode is projectively measured on all states. These measurements are normalized to create a probability outcome matrix shown in Fig. 4 according to the procedure outlined in Supplementary Note 2. This probability outcome matrix of the *F*-qubit basis is then used to calculate the phase error rate, as shown in Eqs. (8), (9). We calculate the phase error rate, E_d', by minimizing the distance between left and right sides of Eq. (7). This minimization is performed in order to avoid unphysical solutions present due to detector noise. Using measurements of the computational basis, we directly determine the bit error rate in the channel.

In our noisy channel, we find that the dit error rate, E_d, is 2.89%, and the phase error rate, E_d', is 6.91%. After error correction and privacy amplification, the resulting sifted key rate in this channel, as given in Eq. (2), would be $R = 1.28$ bits per photon.

Conclusions

We have introduced a high-dimensional quantum key distribution protocol that uses qubit-like states in the secondary basis. Due to their qubit-like nature, the preparation and detection of *F*-qubits is significantly less complex than traditional MUB states, while maintaining the benefits of high-dimensional protocols, namely the increase in information density and error tolerance. By fixing the number of modes within each state to two, we fix the measurement complexity regardless of the dimension of the system, which has been shown to reduce errors in the detection stage[31]. We have experimentally implemented these qubit-like modes in a noisy lab-scale OAM-based QKD channel, achieving a sifted key rate above 1 bit per sifted photon.

The *F*-qubit basis is overcomplete and is constructed of $d^2(d-1)/2$ states, with a factor of d^2 more states than the traditional BB84 protocol. This is not a problem in the limit of infinite key length, but it should be considered for real-world implementations. Nevertheless, this issue can be alleviated with an unbalanced basis choice[23], wherein the *F*-qubits are only used to estimate the error rate of the channel and not for key generation, and are generated at a lower rate than the logical basis. This, in addition to the

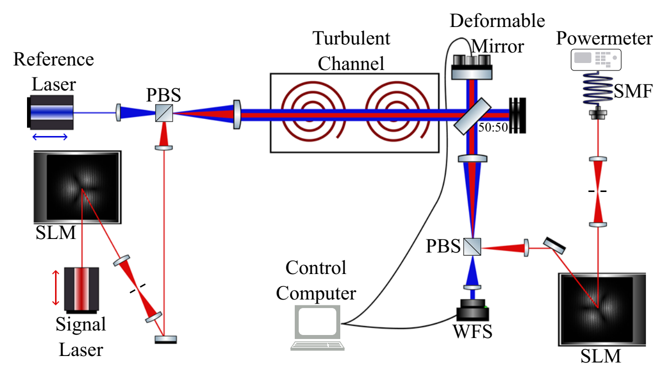

Fig. 3 | Experimental setup to generate and measure the *F*-qubit modes encoded using orbital angular momentum (OAM) in a noisy channel. The reference and signal lasers are both of wavelength 633 nm, with the red and blue representing orthogonal polarisations. The mode of the reference beam is a Gaussian, expanded to approximate a plane wave that is used as a probe of the turbulence measured by the wavefront sensor (WFS). The signal laser is impinged on a spatial light modulator (SLM), which is used to apply the phase and intensity of the *F*-qubit modes encoded as a superposition of LG modes carrying OAM. These beams are made to propagate co-linearly using a polarising beam splitter (PBS) and sent through the turbulent channel. They are subsequently separated after being corrected by the adaptive optics mirror. The *F*-qubit mode is projectively measured using a second SLM and coupled into a single-mode fibre (SMF).

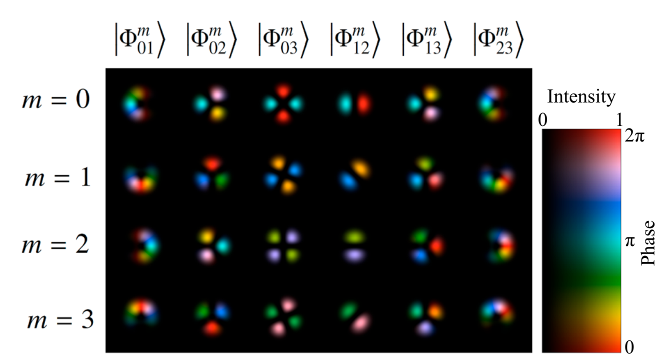

Fig. 2 | *F*-qubits in a 4-dimensional orbital angular momentum (OAM) based protocol. The logical basis consists of a set of LG modes, carrying discrete units of OAM, $|\ell\rangle$, $\ell \in \{-2, -1, 1, 2\}$. False colours and opacity encode the phase and amplitude information, respectively.

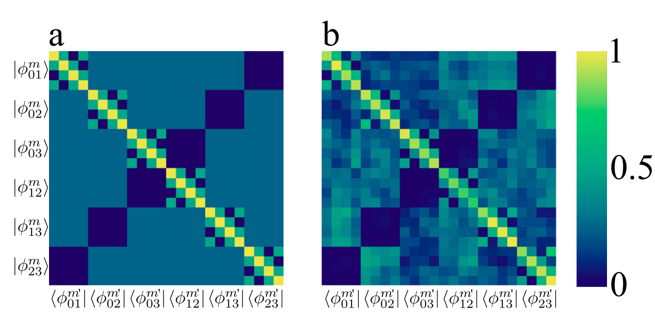

Fig. 4 | Probability outcome matrices of *F*-qubit basis in 4 dimensions. Each subgroup of 4 × 4 is representative of $|\langle\phi^m_{i,j}|\phi^{m'}_{i',j'}\rangle|^2$ where $m, m' \in \{0, \ldots d-1\}$. **a** Theoretical probability outcome matrix with no errors. **b** Experimentally measured probability outcome matrix through our noisy channel using orbital angular momentum encoding as described by Fig. 2.

significant increase of the number of modes used, could significantly increase the block size of the exchanged bits required to perform real-world QKD with this protocol.

A common issue facing QKD systems is that the bandwidth of the channel is restricted by the limitation of single-photon-detector recovery times[32]. These types of channels are particularly suited to implementing high-dimensional QKD in order to increase the information density per photon; meanwhile the simplicity of the *F*-qubits makes them useful in many different high-dimensional encoding schemes. For example, the implementation in a time-bin encoding simply requires a variable-length interferometer. Beyond QKD, we feel that these modes will have use in fields other than quantum communications, such as quantum sensing and imaging.

Data availability

Data from the results presented in this paper may be obtained from the authors upon reasonable request.

Received: 9 May 2025; Accepted: 14 October 2025;
Published online: 25 November 2025

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Computer Sci.* **560**, 7–11 (2014).
2. Gottesman, D. & Lo, H.-K. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Inf. Theory* **49**, 457–475 (2003).
3. Zahidy, M. et al. Practical high-dimensional quantum key distribution protocol over deployed multicore fiber. *Nat. Commun.* **15**, 1651 (2024).
4. Zhang, H. et al. Noise-reducing quantum key distribution. *Rep. Prog. Phys.* **88**, 016001 (2024).
5. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87**, 194108 (2005).
6. Yin, Z.-Q. et al. Measurement-device-independent quantum key distribution with uncharacterized qubit sources. *Phys. Rev. A* **88**, 062322 (2013).
7. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509**, 475–478 (2014).
8. Vagniluca, I. et al. Efficient time-bin encoding for practical high-dimensional quantum key distribution. *Phys. Rev. Appl.* **14**, 014051 (2020).
9. Sit, A. et al. High-dimensional intracity quantum cryptography with structured photons. *Optica* **4**, 1006–1010 (2017).
10. Bechmann-Pasquinucci, H. & Tittel, W. Quantum cryptography using larger alphabets. *Phys. Rev. A* **61**, 062308 (2000).
11. Cerf, N. J., Bourennane, M., Karlsson, A. & Gisin, N. Security of quantum key distribution using *d*-level systems. *Phys. Rev. Lett.* **88**, 127902 (2002).
12. Oesterling, L., Hayford, D. & Friend, G. Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 156–161 (2012).
13. Bedington, R., Arrazola, J. M. & Ling, A. Progress in satellite quantum key distribution. *npj Quantum Inf.* **3**, 30 (2017).
14. Cozzolino, D., Da Lio, B., Bacco, D. & Oxenløwe, L. K. High-dimensional quantum communication: Benefits, progress, and future challenges. *Adv. Quantum Technol.* **2**, 1900038 (2019).
15. Cozzolino, D. et al. Orbital angular momentum states enabling fiber-based high-dimensional quantum communication. *Phys. Rev. Appl.* **11**, 064058 (2019).
16. Forbes, A., Youssef, M., Singh, S., Nape, I. & Ung, B. Quantum cryptography with structured photons. *Appl. Phys. Lett.* **124**, 110501 (2024).
17. Wang, S. et al. Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme. *Quantum Sci. Technol.* **3**, 025006 (2018).
18. Chau, H. F. Quantum key distribution using qudits that each encode one bit of raw key. *Phys. Rev. A* **92**, 062324 (2015).
19. Chau, H. F., Wang, Q. & Wong, C. Experimentally feasible quantum-key-distribution scheme using qubit-like qudits and its comparison with existing qubit- and qudit-based protocols. *Phys. Rev. A* **95**, 022311 (2017).
20. Sulimany, K. et al. High-dimensional coherent one-way quantum key distribution. *npj Quantum Inf.* **11**, 16 (2025).
21. Sheridan, L. & Scarani, V. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A* **82**, 1–4 (2010).
22. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000).
23. Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18**, 133–165 (2005).
24. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441–444 (2000).
25. Biham, E. & Mor, T. Bounds on information and the security of quantum cryptography. *Phys. Rev. Lett.* **79**, 4034–4037 (1997).
26. Renner, R. & Cirac, J. I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **102**, 110504 (2009).
27. Allen, L., Beijersbergen, M. W., Spreeuw, R. J. C. & Woerdman, J. P. Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes. *Phys. Rev. A* **45**, 8185–8189 (1992).
28. Bolduc, E., Bent, N., Santamato, E., Karimi, E. & Boyd, R. W. Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram. *Opt. Lett.* **38**, 3546–3549 (2013).
29. Scarfe, L. et al. Fast adaptive optics for high-dimensional quantum communications in turbulent channels. *Commun. Phys.* **8**, 79 (2025).
30. Bouchard, F. et al. Measuring azimuthal and radial modes of photons. *Opt. Express* **26**, 31925–31941 (2018).
31. Lib, O., Sulimany, K., Araújo, M., Ben-Or, M. & Bromberg, Y. High-dimensional quantum key distribution using a multi-plane light converter. *Opt. Quantum* **3**, 182–188 (2025).
32. Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J. & Gauthier, D. J. Provably secure and high-rate quantum key distribution with time-bin qudits. *Sci. Adv.* **3**, e1701491 (2017).

Acknowledgements

This work was supported by Canada Research Chairs; Canada First Research Excellence Fund (CFREF); National Research Council of Canada High-Throughput and Secure Networks (HTSN) Challenge Program; and the Alliance Consortia Quantum Grant (QUINT, ARAQNE). Francesco Di Colandrea further acknowledges support from the PNRR MUR project PE0000023-NQSTI.

Author contributions

L.S. & E.K. conceived of the idea. F.B. & A.Z.G. worked on the proof of security. L.S. & R.A. performed the experiment. F.D.C. performed the numerical simulations. L.S., R.A., & F.D.C. analyzed the data. L.S. & F.B. wrote the first draft of the manuscript. K.H. & E.K. supervised the project. All authors contributed to the final version of the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s42005-025-02376-8.

Correspondence and requests for materials should be addressed to Lukas Scarfe.

Peer review information *Communications Physics* thanks Kfir Sulimany and the other, anonymous, reviewer(s) for their contribution to the peer review of this work. A peer review file is available.