La Rivista del Nuovo Cimento (2026) 49:475–504
https://doi.org/10.1007/s40766-026-00084-9

REVIEW

Photonic qudit entanglement and its applications to quantum key distribution

Jinwon Yoo[1] · Luca Castello[1] · Stefania Sciara[1,2] · Domenico Bongiovanni[1] · David J. Moss[3] · Roberto Morandotti[1]

Received: 23 April 2026 / Accepted: 27 August 2026 / Published online: 21 October 2026
© The Author(s) 2026

Abstract

High-dimensional quantum key distribution (QKD) based on entangled qudits has emerged as a promising route for advancing the performance and practicality of quantum communication. By extending beyond the qubit framework, qudit entanglement enables the encoding of multiple bits per particle and offers greater robustness against noise, loss, and eavesdropping. In this review, we present qudit-based entanglement QKD protocols and their experimental demonstrations. We first introduce the basic concepts of qudits and provide an overview of foundational qubit-based entanglement QKD schemes, such as Ekert '91 (E91) and Bennett–Brassard–Mermin '92 (BBM92), which establish the core principles of entanglement-based secure key generation. Subsequently, we examine the generalization of these protocols to entangled qudits, highlighting how higher dimensionality enhances secure key rates and noise tolerance. Finally, we survey experimental demonstrations of qudit-based entanglement QKD across photonic platforms and outline prospects, showing that high-dimensional entanglement can be reliably generated, distributed, and measured for QKD with high stability and scalability. Remarkably, these achievements not only verify the feasibility of practical high-dimensional QKD, but also demonstrate clear advantages over qubit-based systems. Overall, theoretical frameworks and experimental realizations reviewed here position photonic qudit-based entanglement QKD as a promising resource for scalable, high-speed, and secure quantum communication networks, unveiling its potential as a central component in the future of quantum information technologies.

✉ Stefania Sciara
Stefania.Sciara@etsmtl.ca

✉ Roberto Morandotti
Roberto.Morandotti@inrs.ca

1 Institut national de la recherche scientifique – Centre Énergie Matériaux et Télécommunications (INRS-EMT), 1650 boulevard Lionel-Boulet, Varennes, QC J3X 1P7, Canada

2 Département de génie électrique, École de technologie supérieure (ÉTS), Montréal, QC, Canada

3 Optical Sciences Centre, Swinburne University of Technology, Hawthorn, VIC 3122, Australia

Keywords Quantum key distribution · Qudit · Entanglement · Quantum photonics

1 Introduction

The field of quantum information science has transitioned from fundamental theoretical exploration to a robust era of experimental realization. This progress is underscored by a series of landmark achievements in quantum optics, which have demonstrated the ability to generate and control large-scale quantum states with unprecedented precision [1–6]. From the generation of nonclassical light [3, 7–11] and the observation of two-photon interference [12, 13] to the distribution of entanglement [14–20], these foundational milestones have proven the feasibility of harnessing quantum mechanical effects for complex tasks. Such advancements in hardware and protocol design have paved the way for practical applications that transcend the limits of classical physics. Among these, quantum key distribution (QKD) stands as the most mature technology, offering a paradigm shift in secure communications.

QKD enables communicating parties to establish a shared cryptographic key, whose security is guaranteed by the laws of quantum mechanics [21–23]. In its earliest form—often referred to as a prepare-and-measure scheme—one party prepares individual quantum signals in one of several possible states and sends them to the other party, who measures these states [21, 24–26]. Any attempt by an eavesdropper to intercept or measure the quantum system inevitably introduces disturbances that manifest as excess errors, allowing the legitimate parties to assess the channel's security. A particularly powerful realization is entanglement-based QKD. Entangled particles are distributed between the communicating parties, and their nonclassical correlations are exploited to both generate a secret key and test for the presence of the undesired eavesdropper [22, 27, 28]. Beyond reproducing the essential security features of prepare-and-measure schemes, entanglement-based implementations naturally connect to tests of nonlocal correlations [22, 27]. Moreover, they can relax assumptions regarding the trustworthiness of the key-distribution source [22, 27]. Since its first demonstrations [29, 30], QKD has progressed from theoretical proposals to practical implementations, ranging from laboratory experiments [31–33] to deployed network trials [34–36]. Traditionally, most entanglement-based QKD systems have relied on two-level quantum states—qubits [22, 27, 31]. While qubit-based entanglement QKD has been pivotal in establishing the feasibility of quantum-secure communication, restricting the encoding to only two quantum states per carrier limits the amount of information that can be transmitted. In addition, qubit-level encoding constrains the protocol's tolerance to noise.

In recent years, high-dimensional entanglement QKD has emerged as a powerful extension of the original qubit-based framework [37–39]. In this approach, information is encoded into quantum systems with more than two levels—referred to as *qudits* [37, 40–43]. Increasing the number of distinct states per quantum particle expands the accessible Hilbert space for communication and offers several advantages. First, a higher information capacity per successful detection event can be achieved, which can be exploited to increase the secure key rate [37, 44]. Second, many high-dimensional protocols are more resilient to noise and errors, since the relative impact

of disturbances is reduced in a larger state space [45–47]. Third, the protocol security can be enhanced by allowing high-dimensional systems to use a richer set of measurement settings and more complex encoding schemes, which, in turn, raises the difficulty for eavesdroppers to obtain information undetected [44, 45, 48]. Together, these benefits make high-dimensional entanglement QKD particularly attractive for practical communication scenarios, where losses, noise, and operational imperfections are unavoidable.

Photonics offers natural, versatile platforms for realizing high-dimensional quantum systems [37, 41, 43, 49]. In particular, photonic qudits are defined by encoding information in discrete sets of modes associated with specific degrees of freedom, such as time, frequency, orbital angular momentum (OAM), or path, which form the basis states of a high-dimensional system. Depending on the encoding, these states can be transmitted and measured with high fidelity over long distances in both optical fiber and free-space channels, being naturally compatible with existing telecommunication infrastructure [50–52] and satellite links [53–55]. These properties make photonic qudits a powerful resource for generating and distributing high-dimensional entanglement over long distances and, in particular, for implementing advanced entanglement-based QKD protocols [37–39].

Over the past few years, several reviews have provided comprehensive overviews of high-dimensional prepare-and-measure QKD protocols, including photonic implementations and performance [37, 56]. In contrast, the corresponding landscape for high-dimensional entanglement-based QKD remains comparatively underexplored. Although qudit-based entanglement QKD protocols constitute a crucial and complementary class of schemes alongside prepare-and-measure approaches, no unified review has systematically consolidated this area [16, 39, 57]. Therefore, a dedicated survey is needed to explore the current state of the art, identify open challenges, and guide future developments.

In this review, we provide a comprehensive overview of photonic qudits and their applications to entanglement-based QKD. We begin by introducing qudits and high-dimensional entanglement. Then, we summarize qubit-based entanglement QKD as a reference framework to clarify its operating principles and establish a baseline for comparison. Building on this foundation, we discuss extensions to qudit-based entanglement QKD schemes, review representative experimental realizations on photonic platforms, and outline pathways toward scalable quantum communication infrastructures. Throughout our discussion, we highlight both opportunities and practical challenges that accompany the adoption of high-dimensional approaches. Ultimately, we convey how photonic qudits not only deepen our understanding of quantum information science, but also pave the way for practical, next-generation secure communication systems.

2 High-dimensional quantum information

Quantum information protocols are conventionally formulated in terms of qubits. High-dimensional quantum information instead exploits physical systems that support more than two distinct levels, thus providing access to a larger alphabet and a richer

structure of quantum correlations. In this section, we introduce the basic properties of qudits and then discuss the entanglement of bipartite qudit systems as a key resource for high-dimensional quantum communications.

2.1 Qudit

A quantum system is a physical entity governed by the rules of quantum mechanics, such as superposition [58] and entanglement [59]. The possible states of such a system are described within a mathematical structure called the Hilbert space $\mathcal{H}$ of dimension d^N, where N is the number of constituent quantum systems and d is the number of accessible levels per system. Physically realizable pure states are represented by a unit vector $|\psi\rangle \in \mathcal{H}$, which fully specifies the system's measurable properties, including its energy [60], momentum [60], polarization [49], or spin [60]. The qubit residing in the two-dimensional Hilbert space constitutes the simplest quantum vector [61], whose computational basis consists of two orthonormal states $\{|0\rangle, |1\rangle\}$. The general qubit state can be expressed as $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$, with complex coefficients c_0, $c_1 \in \mathbb{C}$ satisfying the normalization condition $|c_0|^2 + |c_1|^2 = 1$.

In the context of high-dimensional quantum information, one considers qudits whose Hilbert space has dimension $d > 2$ [37, 42, 43]. The standard orthonormal basis in this space is

$$\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}, \tag{1}$$

where each basis state $|k\rangle$ represents the system occupying the kth level. A general qudit state is then written as:

$$|\psi\rangle = \sum_{k=0}^{d-1} c_k |k\rangle, \tag{2}$$

with $c_k \in \mathbb{C}$ satisfying the normalization condition $\sum_{k=0}^{d-1} |c_k|^2 = 1$. The increased dimensionality results in a higher quantum information capacity per single carrier. Specifically, the information content (expressed in bits) of a single qudit can be quantified as the logarithm of the dimension of its Hilbert space, as

$$\text{Information per qudit} = \log_2 d \ \ \text{(bits)}. \tag{3}$$

In comparison, a single qubit can carry an information content of $\log_2 2 = 1$ bit. Thus, a single qudit has the same information capacity as $\log_2 d$ qubits. For example, a qutrit ($d = 3$) carries $\log_2 3 \approx 1.585$ bits, while a ququart ($d = 4$) yields $\log_2 4 = 2$ bits. This logarithmic scaling highlights the enhanced information capacity of qudits, and their use in QKD protocols can directly translate into higher key generation rates.

2.2 Bipartite qudit entanglement

Entanglement is a uniquely quantum phenomenon, where the state of a composite system cannot be expressed as independent states of its constituent subsystems [59]. The concept of entanglement traces its origin to the early days of quantum theory. Erwin Schrödinger coined the term *entanglement* and emphasized that it is "not one but rather the characteristic trait of quantum mechanics" [62]. He formalized the idea by describing the quantum states of two systems that cannot be decomposed into independent subsystem states. Mathematically, a bipartite state $|\Psi\rangle$ in a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is said to be entangled if it cannot be written as a product of local states

$$|\Psi\rangle \neq |\psi\rangle_A \otimes |\psi\rangle_B, \tag{4}$$

where $|\psi\rangle_A \in \mathcal{H}_A$ and $|\psi\rangle_B \in \mathcal{H}_B$ are the local states, while the symbol $\otimes$ denotes the tensor product. Such states exhibit nonclassical correlations that arise from coherent superpositions across the two subsystems—coherence that cannot be reduced to any mixture of locally defined states [63]. This coherence is at the heart of quantum entanglement and underpins its power as a resource in quantum communication [22, 27, 59]. A standard example of bipartite entangled states is the canonical maximally entangled qudit state, known as Bell states [64], given by:

$$|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle_A |k\rangle_B. \tag{5}$$

Bell states serve as fundamental resources for quantum communication protocols such as quantum state teleportation [65–67] and entanglement-based QKD [16, 39, 57]. In addition to this canonical form, other forms of the entangled state can be obtained by applying local unitary transformations on the subsystems [64, 68]. As an example, any state of the form

$$|\psi_d\rangle = (U_A \otimes U_B)|\Phi_d\rangle, \tag{6}$$

with unitary operators U_A and U_B acting on the qudits A and B, respectively, remains entangled. Since the local unitary operations do not affect entanglement [69], $|\psi_d\rangle$ shares the same entanglement properties as the Bell state $|\Phi_d\rangle$. This can be used in high-dimensional quantum communication protocols, including QKD. Compared to their qubit counterparts, qudit Bell states provide access to a broader set of correlations and offer improved robustness to noise in QKD [45], as discussed in Sects. 3 and 4.

3 Entanglement-based QKD

QKD enables two (or more) remote parties, conventionally referred to as Alice and Bob, to establish a shared secret key whose security is rooted in the principles of quantum mechanics. Unlike classical cryptographic schemes, whose security relies

on computational assumptions [70, 71], QKD achieves information-theoretic security guaranteed by quantum phenomena, such as the no-cloning theorem, which prohibits perfect copying of unknown quantum states [72].

The first QKD protocol, BB84, proposed by Bennett and Brassard in 1984 [21], is a prepare-and-measure scheme. Alice encodes random bits in quantum states, and Bob measures them in randomly chosen bases. Any attempt by an eavesdropper (Eve) to intercept and measure the quantum states inevitably introduces errors, allowing Alice and Bob to detect the eavesdropper's presence and discard compromised data.

An alternative approach, entanglement-based QKD, distributes pairs of entangled systems to Alice and Bob (see Fig. 1), who then perform independent measurements in randomly selected bases. After many measurement rounds, Alice and Bob publicly compare the bases used in their measurements and retain only the events compatible with key generation—a process known as *sifting*. This approach offers several advantages over prepare-and-measure schemes. Most notably, it removes the requirement for a trusted source: the presence of genuine entanglement, verified directly from measurement statistics, certifies the security of the key [48]. Additionally, entanglement-based protocols enable device-level security verification based on observed correlations [73]. Foundational entanglement-based protocols include Ekert '91 (E91) [22], which links

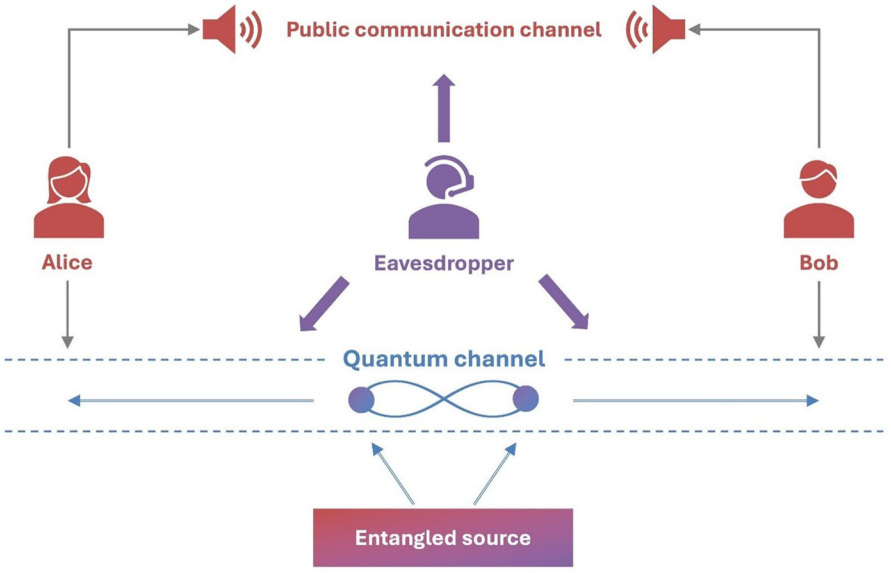


Fig. 1 Entanglement-based quantum key distribution protocol architecture. An entangled source generates pairs of particles and distributes one particle to Alice and the other to Bob through a quantum channel. Alice and Bob independently and randomly choose a measurement basis from a predefined set of settings and record their detection outcomes. After quantum transmission, they communicate over an authenticated classical channel to announce their measurement settings and disclose a subset of measurement outcomes for parameter estimation, enabling detection of eavesdropping attempts and estimating correlation strength and error rate. Based on this analysis, they can assess the security of the shared data. Once security is confirmed, the correlated outcomes obtained from their measurements constitute a shared key that can be directly used for secure communication

the security of the key to Bell's inequality violation, and Bennett–Brassard–Mermin '92 (BBM92) [27], which instead establishes secure keys through entanglement correlations without relying on Bell tests.

In this section, we present the original qubit-based entanglement QKD protocols, E91 and BBM92. We discuss their operating principles, measurement configurations, and security analyses to establish the essential features of entanglement-based QKD. These foundations also provide the groundwork for understanding high-dimensional entanglement-based QKD schemes, where entanglement is exploited in larger Hilbert spaces to enhance performance and robustness.

3.1 E91

Proposed by Ekert [22], the E91 protocol was the first QKD scheme to explicitly exploit quantum entanglement as a resource for the security of the generated secret key. A source distributes pairs of entangled qubits, sending one qubit to Alice (A) and the other to Bob (B). The security of the key is guaranteed by the violation of Bell's inequality, ensuring that any eavesdropping attempt disturbs the quantum correlations and is detectable. Ideally, Alice and Bob share a maximally entangled Bell state described by:

$$|\Phi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B). \tag{7}$$

In each measurement round, they independently and randomly select one of three possible operators: $(A_1,\ A_2,\ A_3)$ for Alice and $(B_1,\ B_2,\ B_3)$ for Bob. After all measurements, Alice and Bob publicly announce which operators they used. Only the events corresponding to the A_1–B_1 settings are used for key generation, while the remaining data are used to verify security. The operators A_1 and B_1 correspond to measurements along the Pauli-Z matrix [60], whose eigenvectors are

$$Z : \{|0\rangle,\ |1\rangle\}. \tag{8}$$

When both parties measure on this basis, their results are perfectly correlated: if Alice obtains $|0\rangle$, Bob obtains $|0\rangle$, and likewise for $|1\rangle$. These correlated outcomes generate the shared secret key.

To test eavesdropping, Alice and Bob estimate the strength of quantum correlations of the shared Bell state using the measurement operators–$(A_2,\ A_3)$ and $(B_2,\ B_3)$—defined by:

$$A_a = M(\alpha_a),\ B_b = M(\beta_b),\ (a,\ b = 2,\ 3), \tag{9}$$

with

$$M(\theta) = \cos(\theta)X + \sin(\theta)Y, \tag{10}$$

where X and Y operators are Pauli-X and -Y matrices [60]. The eigenvectors associated with these operators are

$$|+_\theta\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + e^{i\theta}|1\rangle\Big),\ |-_\theta\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - e^{i\theta}|1\rangle\Big), \tag{11}$$

where $\theta = \alpha_a$ or β_b denotes the measurement angle chosen by Alice or Bob, respectively. For the qubit Bell state, the quantum correlation between Alice's and Bob's measurement outcomes for setting A_a and B_b is quantified by the expectation value

$$E(A_a,\ B_b) = P(A_a = B_b) - P(A_a \neq B_b), \tag{12}$$

where $P(A_a = B_b)$ and $P(A_a \neq B_b)$ are the probabilities that their outcomes are equal or different, respectively. This characterizes the degree of correlation between their measurement results for each pair of settings. To test for nonlocal correlations, Alice and Bob compute the Clauser–Horne–Shimony–Holt (CHSH) parameter [74]:

$$S = E(A_2,\ B_2) + E(A_2,\ B_3) + E(A_3,\ B_2) - E(A_3,\ B_3), \tag{13}$$

which must satisfy $|\ S\ | \leq 2$ for any local realistic theory. For the measurement settings described by the angles

$$\alpha_2 = 0, \quad \alpha_3 = \frac{\pi}{2}, \quad \beta_2 = \frac{3\pi}{4}, \quad \beta_3 = -\frac{3\pi}{4}, \tag{14}$$

quantum mechanics predicts

$$|\ S\ | = 2\sqrt{2}, \tag{15}$$

which gives the maximal quantum violation.

While a CHSH violation certifies the presence of nonlocal correlations and is therefore necessary to detect eavesdropping in a device-independent manner [75], secure key generation further requires that the observed Bell parameter S satisfies the security thresholds established by device-independent QKD (DIQKD) [73]. In DIQKD, physical measurement devices are treated as untrusted "black boxes", with security derived solely from observed classical input–output statistics without relying on assumptions about their internal calibration. Under this framework, and for collective attacks processed with one-way classical post-processing, the asymptotic secure key rate $\mathrm{SKR}_{\mathrm{sift}}$ extracted from A_1-B_1 measurement outcomes explicitly incorporates S:

$$\mathrm{SKR}_{\mathrm{sift}} \geq N_{\mathrm{sift}}\left[1 - f_{\mathrm{EC}}h_2(Q) - h_2\left(\frac{1+\sqrt{(S/2)^2-1}}{2}\right)\right], \tag{16}$$

where N_{sift} denotes the sifted key rate obtained from measurement outcomes in the A_1-B_1 key-generating basis, $Q = P(A_1 \neq B_1)$ is the corresponding quantum bit

error rate, $f_{\mathrm{EC}} \geq 1$ is the error-correction efficiency factor, and $h_2(x) = -(1-x)\log_2(1-x) - x\log_2 x$ is the binary entropy function [48, 73]. For ideal error correction ($f_{\mathrm{EC}} = 1$), extracting a positive secret key rate ($\mathrm{SKR}_{\mathrm{sift}} > 0$) requires the CHSH violation S to satisfy the general condition:

$$S > 2\sqrt{1 + \left[2\, h_2^{-1}(1 - h_2(Q)) - 1\right]^2}, \tag{17}$$

where $h_2^{-1}(\cdot)$ denotes the inverse binary entropy function. This explicitly shows that the required CHSH violation S grows with the error rate Q.

As an explicit illustration, consider a depolarizing channel acting on the shared Bell state, for which $S = 2\sqrt{2}(1-2Q)$ [73]. A quantum bit error rate of $Q = 12\%$ then corresponds to $S \approx 2.15$: the local-realistic bound $|\ S\ | \leq 2$ is violated, yet this value falls well short of the $S \approx 2.56$ demanded by Eq. (17), so that no secret key can be extracted. Over such a channel, a positive secret key rate requires Q below approximately 7.1%, that is, S above approximately 2.42 [73]. A Bell violation is therefore a necessary, but by no means sufficient, condition for secure key generation.

In this protocol, Alice and Bob evaluate the violation of Bell's inequality in their shared entanglement, thereby certifying the security of their shared key without assuming trust in the entanglement source. However, the protocol is inherently inefficient, as only a small subset of measurement-setting combinations is used for key generation, while the remaining settings are devoted to correlation estimation and eavesdropping testing [76, 77].

3.2 BBM92

In 1992, Bennett, Brassard, and Mermin proposed another type of entanglement-based QKD protocol, known as BBM92 [27]. Compared to the E91 scheme, which requires three measurement settings per party, the BBM92 protocol employs a simpler structure involving only two mutually unbiased bases (MUBs). This reduction in measurement settings streamlines implementation while still enabling secure key generation from entanglement.

An entangled-pair source distributes one qubit to Alice and the other to Bob, ideally prepared in a Bell state. Each party independently and randomly measures its qubit in one of two MUBs, chosen as the eigenbases of the Pauli-Z and -X operators:

$$Z : \{|0\rangle, |1\rangle\}; \qquad X : |\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}. \tag{18}$$

The security of BBM92 can be analyzed using the Koashi–Preskill framework [78], which relies on the principle of complementarity between two measurement bases. Specifically, complementarity means that information about one observable (e.g., the Z basis) cannot be obtained without disturbing the complementary observable (e.g., the X basis). A randomly selected subset of the measurement data is then publicly disclosed to estimate the quantum bit error rate (QBER) in each basis. QBER is defined

as the fraction of measurement rounds in which Alice and Bob's outcomes deviate from the ideal correlation pattern expected for the shared Bell state in that basis. In the specific case that the Bell state is $|\Phi_2\rangle = (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)/\sqrt{2}$, the QBER in each basis is given by:

$$Q_Z = 1 - \frac{\left(N_{00}^{(Z)} + N_{11}^{(Z)}\right)}{N_Z}, \qquad Q_X = 1 - \frac{\left(N_{++}^{(X)} + N_{--}^{(X)}\right)}{N_X}, \tag{19}$$

where N_Z (N_X) is the total number of measurement rounds in the Z (X) basis. $N_{kk}^{(Z)}$ with $k \in \{0, 1\}$ denotes the number of measurement rounds where both parties obtain an outcome k in the Z basis; $N_{ss}^{(X)}$ with $s \in \{+, -\}$ is defined analogously for the X basis. Alice and Bob extract the sifted key from Z-basis measurements. The observed error rate Q_Z determines how much information must be revealed during error correction. Then, complementarity connects Z and X bases. If Eve attempts to learn Alice's or Bob's Z-basis outcomes, her interaction with the quantum systems generally disturbs the shared entanglement state and the coherence revealed by measurements in the complementary X basis. Thus, a low X-basis error rate Q_X indicates that the shared state retains strong X-basis correlations. This can only occur if Eve has not gained significant information about their Z-basis key. Therefore, a small Q_X strictly limits Eve's information and ensures the security of the final key.

After bounding Eve's information using the observed QBERs, Alice and Bob proceed to distill a secure key from their Z-basis raw data. The asymptotic secret key fraction is determined by the information revealed during error correction and the information Eve may access. Error correction requires the disclosure of approximately $f_{\mathrm{EC}} h_2(Q_Z)$ bits per signal to reconcile discrepancies in their Z-basis outcomes, where $f_{\mathrm{EC}} \geq 1$ accounts for the inefficiency of the error-correction code and $h_2(\cdot)$ denotes the binary entropy function $h_2(Q) = -(1-Q)\log_2(1-Q) - Q\log_2 Q$ that quantifies the uncertainty associated with a key bit affected by an error rate Q [79]. The remaining information Eve could have obtained is removed through privacy amplification [80], which compresses the reconciled Z-basis string according to the observed X-basis error rate Q_X. This contribution can be quantified using the binary entropy $h_2(Q_X)$. Combining these terms, the asymptotic secure key rate is [81, 82]:

$$\mathrm{SKR}_{\mathrm{sift}} \geq N_{\mathrm{sift}}[1 - f_{\mathrm{EC}}\, h_2(Q_Z) - h_2(Q_X)], \tag{20}$$

where N_{sift} denotes the sifted key rate obtained from the Z-basis measurements. This procedure ensures that any information Eve may hold is eliminated, yielding an information-theoretically secure key.

For the protocol to be secure, the secret key rate must remain positive. Assuming identical error rates in the two bases, $Q_Z = Q_X = Q_{\mathrm{th},2}$, the threshold QBER can be obtained by setting the secret key fraction per sifted bit to zero:

$$1 - f_{\mathrm{EC}}\, h_2\big(Q_{\mathrm{th},2}\big) - h_2\big(Q_{\mathrm{th},2}\big) = 0 \Rightarrow (1 + f_{\mathrm{EC}})\, h_2(Q_{\mathrm{th},2}) = 1. \tag{21}$$

This condition marks the boundary between a regime where a positive secret key can be generated and one in which key extraction is impossible. For an ideal error correction ($f_{\mathrm{EC}} = 1$), it yields

$$Q_{\mathrm{th},2} \approx 0.11, \tag{22}$$

indicating that the protocol remains secure as long as the observed QBER does not exceed approximately 11% [48]. Although BBM92 does not include a Bell-test step, its security can be rigorously quantified by evaluating the QBER in the matching measurement bases, which bounds the information Eve can access.

While the above expressions define the asymptotic benchmarks for entanglement-based protocols (such as E91 and BBM92), practical QKD evaluations require transitioning from ideal assumptions to physical deployment conditions. Real-world systems operate with finite sample sizes (or finite key lengths N), where statistical fluctuations during parameter estimation require worst-case confidence bounds, reducing the secret key rate and imposing a minimum block size threshold for key extraction [48, 83]. The resulting statistical penalty scales as the inverse square root of the block size, so that the asymptotic expressions given above are recovered only in the limit of infinitely long keys. Additionally, key rates must be evaluated under a composable security framework [84] to ensure the generated keys remain secure when deployed in downstream cryptographic protocols, incorporating an explicit overall failure parameter $\varepsilon_{\mathrm{QKD}}$ across parameter estimation, error correction, and privacy amplification, conventionally decomposed into a correctness and a secrecy contribution. The same considerations apply to the high-dimensional protocols discussed in Sect. 4, where the finite-size penalty is incurred in each of the d-dimensional bases used for parameter estimation.

4 High-dimensional entanglement QKD

Having introduced qubit-based entanglement QKD protocols, we now extend the discussion to the qudit regime. High-dimensional entanglement enlarges the accessible state space and hence the information capacity of each quantum carrier. Higher dimensionality improves protocol robustness, enabling more efficient and resilient key distribution than standard qubit-based schemes. In the following, we review the generalization of entanglement-based QKD protocols to higher dimensions, focusing on the qudit versions of the fundamental E91 and BBM92 schemes.

4.1 Qudit-based E91

For high-dimensional systems with $d > 2$, the standard E91 protocol can be extended naturally to entangled qudits [45, 57, 85]. In this framework, two parties share a qudit Bell state of the form

$$|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle_A |k\rangle_B. \tag{23}$$

In each measurement round, the two parties randomly choose a measurement basis among three possible settings: (A_1, A_2, A_3) for Alice and (B_1, B_2, B_3) for Bob. The bases A_1 and B_1 correspond to measurements in the computational basis, i.e., the eigenvectors of the generalized Pauli-Z operator Z_d [86, 87], given by:

$$Z_d : \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}. \tag{24}$$

When both parties measure in this basis, they use the outcomes to generate the shared sifted key. Because the shared symbol is d-dimensional, each measurement yields one of d possible outcomes (0,1, ..., $d-1$). As a result, the amount of information obtained per successful measurement increases from 1 bit (in the qubit case) to $\log_2 d$ bits.

To verify the protocol's security, we employ a generalized Bell-type inequality known as the Collins–Gisin–Linden–Massar–Popescu (CGLMP) inequality [46]. This serves as the high-dimensional extension of the CHSH inequality and is expressed as:

$$I_d \equiv E(A_2, B_2) + E(A_2, B_3) + E(A_3, B_2) + E(A_3, B_3), \tag{25}$$

where the four correlation terms $E(A_a, B_b)$ represent the expectation values of joint measurement outcomes between Alice's and Bob's respective settings:(A_2, A_3) and (B_2, B_3). Specifically, the four quantum correlations are defined as [46]:

$$E(A_2, B_2) \equiv \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right) \{P(A_2 = B_2 + k) - P(A_2 = B_2 - k - 1)\}, \tag{26A}$$

$$E(A_2, B_3) \equiv \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right) \{P(B_3 = A_2 + k) - P(B_3 = A_2 - k - 1)\}, \tag{26B}$$

$$E(A_3, B_2) \equiv \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right) \{P(B_2 = A_3 + k + 1) - P(B_2 = A_3 - k)\}, \tag{26C}$$

$$E(A_3, B_3) \equiv \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right) \{P(A_3 = B_3 + k) - P(A_3 = B_3 - k - 1)\}. \tag{26D}$$

Each term $P(A_a = B_b + k)$ in Eq. (26A–26D) is defined as:

$$P(A_a = B_b + k) \equiv \sum_{j=0}^{d-1} P(A_a = j + k,\ B_b = j), \tag{27}$$

which represents the probability that the measurement outcomes of A_a and B_b differ by k modulo d. Analogously, $P(B_b = A_a + k)$ can be written as:

$$P(B_b = A_a + k) \equiv \sum_{j=0}^{d-1} P(B_b = j + k,\ A_a = j). \tag{28}$$

For any local realistic model, the CGLMP inequality $I_d \leq 2$ must hold. However, quantum mechanics allows violation of this bound when Alice and Bob share a qudit Bell state. In the standard CGLMP test, the measurement settings A_2, A_3 and B_2, B_3 are defined as phase-shifted MUBs with eigenvectors given by:

$$|k\rangle_{A_a} = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \exp\left(i \frac{2\pi j}{d}(\alpha_a + k)\right) |j\rangle_A, \tag{29A}$$

$$|l\rangle_{B_b} = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \exp\left(i \frac{2\pi j}{d}(\beta_b - l)\right) |j\rangle_B. \tag{29B}$$

Here, $|j\rangle_A$ and $|j\rangle_B$ denote the local computational bases of Alice's and Bob's subsystems, while the parameters α_a and β_b introduce controlled phase shifts that distinguish the two measurement settings for each party. By applying these MUBs to the qudit Bell state, one can calculate the quantum-mechanical probability distribution of all possible measurement outcome combinations, such as:

$$\begin{aligned} P_{QM}(A_a = k,\ B_b = l) &= \frac{1}{d^3} \left| \sum_{j=0}^{d-1} \exp\left(i \frac{2\pi j}{d}(k - l + \alpha_a + \beta_b)\right) \right|^2 \\ &= \frac{1}{d^3} \frac{\sin^2[\pi(k - l + \alpha_a + \beta_b)]}{\sin^2[\pi(k - l + \alpha_a + \beta_b)/d]}. \end{aligned} \tag{30}$$

If the phase parameters are chosen as:

$$\alpha_2 = 0, \quad \alpha_3 = \frac{1}{2}, \quad \beta_2 = \frac{1}{4}, \quad \beta_3 = -\frac{1}{4}, \tag{31}$$

the CGLMP correlation can be expressed as:

$$I_{d,\,QM} = 4d \sum_{k=0}^{[d/2]-1} \left(1 - \frac{2k}{d-1}\right)\left(q_k - q_{-(k+1)}\right), \tag{32}$$

where

$$q_k = \frac{1}{2d^3 \sin^2[\pi(k + 1/4)/d]}. \tag{33}$$

Under these optimal parameters, the measurement bases are aligned to maximize the quantum probabilities contributing positively to the correlation sum. For instance, for 3-level Bell states, the theoretical value is $I_{3,\mathrm{QM}} = 2.873$, while for 4-level Bell states it increases to $I_{4,\mathrm{QM}} = 2.896$. Consequently, higher-dimensional entanglement yields a larger violation of the local-realistic bound, thereby certifying stronger nonlocal correlations. However, whether this translates into an improved secret key rate depends on the adopted security model and key-rate analysis.

Unlike the binary CHSH scenario, which yields a simple closed-form lower bound on the DIQKD secret key rate, as shown in Eq. (16), the CGLMP inequality does not admit a closed-form expression for the secret key rate. Instead, within the DIQKD framework, the secret key rate can be obtained by calculating the lower bound on Eve's conditional entropy from the observed CGLMP violation using semidefinite programming hierarchies [88, 89].

4.2 Qudit-based BBM92

Similar to the E91 scheme, the BBM92 protocol can also be generalized to high-dimensional systems [16, 39, 44, 45] by distributing maximally entangled qudit states, such as the canonical Bell state $|\Phi_d\rangle$. In each measurement round, Alice and Bob independently choose between two MUBs. The first is the computational basis

$$Z_d : \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}, \tag{34}$$

corresponding to the eigenbasis of the generalized Pauli-Z operator [86, 87]. The second is the Fourier basis for Alice

$$X_{d,A} : \{|f_{s_A}\rangle\}_{s_A=0}^{d-1},\ |f_{s_A}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \exp\left(i \frac{2\pi j s_A}{d}\right) |j\rangle, \tag{35}$$

and the inverse Fourier basis for Bob

$$X_{d,B} : \{|f_{s_B}{}'\rangle\}_{s_B=0}^{d-1},\ |f_{s_B}{}'\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \exp\left(-i \frac{2\pi j s_B}{d}\right) |j\rangle, \tag{36}$$

where $|f_{s_A}\rangle$ and $|f_{s_B}{}'\rangle$ are the eigenbases of the generalized Pauli-X operator X_d and its inverse, respectively [86, 87]. When Alice and Bob measure in matching bases—either both selecting the computational basis Z_d, or selecting the Fourier-pair ($X_{d,A}$ for Alice and $X_{d,B}$ for Bob)—their outcomes are perfectly correlated. Specifically, measurements in the computational basis yield identical outcomes, while measurements

in the Fourier-pair yield outcomes satisfying $s_A = s_B$. Each local outcome corresponds to one of d possible symbols and thus carries $\log_2 d$ bits of raw information. As in the qubit case, Z_d and the Fourier pair $\{X_{d,A},\ X_{d,B}\}$ constitute a pair of maximally complementary measurement bases, such that precise information in one basis implies maximal uncertainty in the other. This complementarity is exploited by using the measurement rounds in which both parties choose the Z_d basis to form the sifted key, while the X_d-basis (Fourier) outcomes are reserved for parameter estimation, providing a measure of disturbance and bounding the information potentially available to an eavesdropper. To quantify the disturbance, Alice and Bob reveal a randomly chosen subset of their data and compute their QBERs:

$$Q_{Z_d} = 1 - \frac{1}{N_{Z_d}} \sum_{k=0}^{d-1} N_{kk}^{(Z_d)}, \qquad Q_{X_d} = 1 - \frac{1}{N_{X_d}} \sum_{s=0}^{d-1} N_{ss}^{(X_d)}, \tag{37}$$

where N_{Z_d} (N_{X_d}) is the total number of Z_d (X_d) basis measurements and $N_{kk}^{(Z_d)}$ ($N_{ss}^{(X_d)}$) are the measurement rounds where both parties reported the same measurement outcome k (s) in the Z_d (X_d) basis. The quantity Q_{Z_d} determines the amount of classical communication needed to correct any mismatches between Alice's and Bob's keys, while Q_{X_d} bounds Eve's information through complementarity. Since this error-correction step operates on d-level symbols, the appropriate measure of uncertainty is the d-ary entropy:

$$h_d(Q) = -(1-Q)\log_2(1-Q) - Q\,\log_2\left(\frac{Q}{d-1}\right), \tag{38}$$

which characterizes the uncertainty associated with a symmetric d-ary error model with total probability Q. Including error-correction inefficiencies, the asymptotic d-ary secure key rate is [39]:

$$\mathrm{SKR}_{\mathrm{sift}}^{(d)} \geq N_{\mathrm{sift}}^{(d)} \left[\log_2 d - f_{\mathrm{EC}}\, h_d(Q_{Z_d}) - h_d(Q_{X_d})\right], \tag{39}$$

where $f_{\mathrm{EC}} \geq 1$ accounts for the inefficiency of the employed error-correction code and $N_{\mathrm{sift}}^{(d)}$ is the unrevealed sifted key rate obtained from the Z_d-basis measurements. In practical qudit deployments, these asymptotic key rates must be adjusted for finite-sample statistical fluctuations across all d-dimensional parameter-estimation bases and evaluated within a composable security framework, following the finite-size formalism detailed at the end of Sect. 3.2.

To isolate the effect of the dimension d on the protocol performance, we consider a symmetric scenario in which the error rates in the two MUBs are equal, $Q_{Z_d} = Q_{X_d} = Q_{\mathrm{th},d}$. The QBER threshold $Q_{\mathrm{th},d}$ is defined by the condition that the secret key fraction per sifted symbol vanishes,

$$\log_2 d - (f_{\mathrm{EC}} + 1)\, h_d(Q_{\mathrm{th},d}) = 0. \tag{40}$$

In the ideal case of perfect error correction, where the efficiency attains its optimal value $f_{\mathrm{EC}} = 1$, the threshold condition for a non-zero secret key rate reduces to

$$\log_2 d - 2\, h_d(Q_{\mathrm{th},d}) = 0. \tag{41}$$

Equation (41) shows that the threshold is reached when the information carried by each measurement outcome, $\log_2 d$, is exactly balanced by the uncertainty introduced by errors in the two bases. Since increasing the dimension raises $\log_2 d$, more noise (that is, a larger $Q_{\mathrm{th},d}$) is required to reach this balance. For example, in the ideal case, one finds [39, 45, 90]:

$$\begin{aligned} d = 3: &\quad Q_{\mathrm{th},3} \approx 0.1595, \\ d = 4: &\quad Q_{\mathrm{th},4} \approx 0.1893, \\ d = 8: &\quad Q_{\mathrm{th},8} \approx 0.2470. \end{aligned} \tag{42}$$

The threshold value increases with dimension, demonstrating the enhanced robustness of high-dimensional QKD. For comparison, the corresponding threshold for the standard qubit-based BBM92 protocol ($d = 2$) is $Q_{\mathrm{th},2} \approx 0.11$ (see Sect. 3.2), whereas for $d = 8$ the tolerated error rate is more than twice that of the qubit protocol.

The high-dimensional extensions of both E91 and BBM92 protocols illustrate the main advantages of qudit-based entanglement QKD over their qubit counterparts: each detection event can carry more than one bit of secure information, and the protocols tolerate higher levels of noise and disturbance before the secret key rate vanishes. The high-dimensional BBM92 protocol preserves the simple two-basis structure, and unlike E91, does not require a Bell test, whereas high-dimensional E91 naturally retains the ability to certify security via stronger Bell-type inequality violations in larger Hilbert spaces. Nevertheless, these benefits come at the price of increased experimental complexity, including more demanding state preparation and mode control, tighter stability requirements, and more intricate detection in larger outcome spaces [16, 39, 57]. In the next section, we review the most representative experimental implementations of qudit-based entanglement QKD and assess their practical advantages.

5 Experimental QKD with entangled photonic qudits

QKD implementations have largely benefited from photonic platforms, as photons are naturally suited for transmitting quantum information over long distances with minimal decoherence [50, 91]. Their weak interaction with the environment, along with well-established techniques for generating, manipulating, and detecting single photons, makes photonics an ideal platform for quantum communication protocols, including quantum state teleportation [92–94] and QKD. In particular, photonic degrees of freedom such as OAM [57, 95], path [16, 96], frequency [97–100], and time [5, 39, 101] offer flexible, scalable encodings for high-dimensional quantum systems.

For instance, OAM modes provide a theoretically unbounded alphabet that enables multi-level encoding [57, 95]; path encoding can be implemented using integrated photonic circuits offering stability and compactness [16, 96]; frequency encoding exploits spectrally distinct modes that are naturally compatible with commercial telecommunication infrastructure [4, 5, 97–100, 102]; time-bin encoding allows for stable long-distance transmission and ensures compatibility with existing telecommunication fiber infrastructure [5, 39, 101]. These properties collectively make photonic qudits a highly versatile resource for realizing high-dimensional entanglement-based QKD schemes that combine practicality, scalability, and enhanced security.

In this section, we turn to experimental realizations of qudit-based entanglement QKD schemes. By leveraging these photonic degrees of freedom, several pioneering works have demonstrated the feasibility of generating, transmitting, and measuring high-dimensional entangled states for secure key distribution. These experiments mark an essential step toward practical high-dimensional quantum communication systems, illustrating how photonic qudits can be efficiently implemented and integrated into existing optical infrastructures.

5.1 Qutrit-based E91 protocol implementation with OAM

One of the earliest qudit-based entanglement QKD demonstrations was reported by Gröblacher et al. [57], who implemented an E91 protocol using entangled qutrits encoded in the OAM of photons (see Fig. 2). OAM originates from the helical phase structure of an optical field and can take discrete quantized values of angular momentum, providing a high-dimensional degree of freedom for encoding quantum information. In their experiment, a type-I β-barium-borate (BBO) crystal was pumped by an Ar^+ laser at 351 nm to produce photon pairs via spontaneous parametric down-conversion (SPDC) [103]. SPDC is a nonlinear optical process in which a pump photon is spontaneously converted into two lower-energy photons—called the signal and idler—while satisfying energy and momentum conservation. The down-converted photons were energy-degenerate and spectrally filtered with a narrowband filter centered at 702 nm to ensure indistinguishability. The OAM degree of freedom of each photon defined a three-dimensional Hilbert space spanned by the Laguerre–Gaussian modes. The OAM of each pump photon is conserved when all beams are aligned collinearly in the SPDC process [104, 105]. This conservation enables the generation of photon pairs entangled in the form of a qutrit Bell state, expressed as:

$$|\psi_3\rangle = \alpha|0\rangle_s|0\rangle_i + \beta|1\rangle_s|2\rangle_i + \gamma|2\rangle_s|1\rangle_i, \tag{43}$$

with measured coefficients $\alpha = 0.642 \pm 0.009$, $\beta = 0.546 \pm 0.009$, and $\gamma = 0.539 \pm 0.009$. Here, $|0\rangle \equiv \mathrm{LG}_{0,0}$, $|1\rangle \equiv \mathrm{LG}_{0,+1}$, $|2\rangle \equiv \mathrm{LG}_{0,-1}$ and the subscripts s and i label signal and idler photons, respectively. Note that the state in Eq. (43) can be regarded as a locally transformed version of the canonical Bell state $|\Phi_3\rangle$ [68], where a permutation operation on Bob's modes exchanges $|1\rangle_B$ and $|2\rangle_B$.

As illustrated in Fig. 2, each arm of the platform contained two phase holograms acting as OAM mode transformers mounted on motorized translation stages

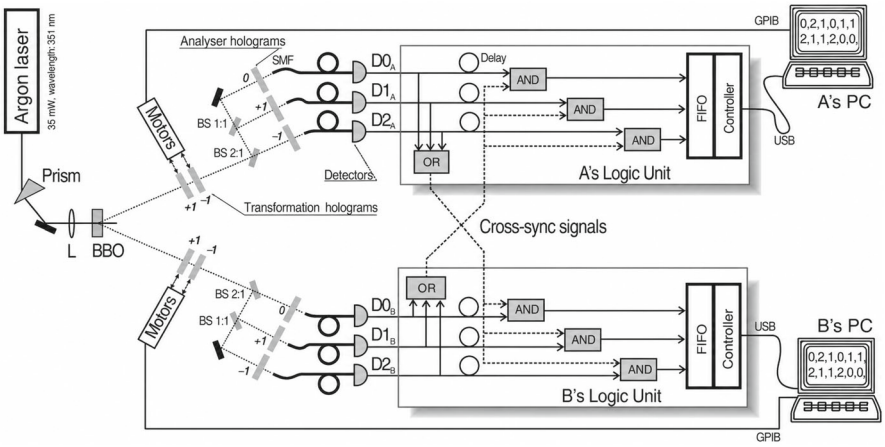


Fig. 2 Experimental setup for qutrit-based E91 QKD protocol with OAM. The entangled photon pairs are generated by pumping a BBO crystal with an Ar^+ laser operating at a wavelength of 351 nm. In each down-conversion arm, two phase holograms mounted on computer-controlled stepper motors manipulate the qutrit Bell state. Mode analysis is performed probabilistically using a combination of beam splitters, mode-selecting holograms, and single-mode fibers, enabling discrimination among the three orthogonal spatial modes $\mathbf{LG}_{0,-1}$, $\mathbf{LG}_{0,0}$, and $\mathbf{LG}_{0,1}$. Two logic units process the resulting detection events independently and identify coincidence counts using synchronized timing signals. Each local measurement outcome, represented by the value 0, 1, or 2, is stored in a first-in–first-out (FIFO) buffer. The computer collects these outcomes and, after basis reconciliation, analyzes the coincidence data to verify security and to generate the final secret key shared between the two parties. Reprinted with permission from [57]. © Deutsche Physikalische Gesellschaft. Reproduced by permission of IOP Publishing CC BY-NC-SA

for fine displacement control. Horizontal translation of the holograms implemented the measurement bases $(A_1,\ A_2,\ A_3)$ and $(B_1,\ B_2,\ B_3)$. Mode analysis was performed probabilistically using OAM analyzers consisting of beam splitters, mode-selection holograms, and single-mode fibers, resulting in a detection probability of 1/3 per photon. Two computers independently recorded detection events (one for Alice and one for Bob), and coincidences were identified via cross-synchronization signals. The maximal measured qutrit Bell parameter for the QKD run was $I_3 = 2.688 \pm 0.171$, exceeding the classical bound by ~ 4 standard deviations, thereby confirming strong violation of local realism, which served as the eavesdropping check of the protocol. The sifted key consisted of 150 ternary digits (trits), which contained 14 symbol errors. Following classical error, a final secure key of 72 trits was obtained. This experiment demonstrated the capability of implementing high-dimensional QKD through free-space propagation, showing that OAM modes can maintain quantum correlations even in open-air channels. The successful realization of qutrit-based entanglement distribution revealed the potential of this approach for long-distance free-space quantum communication, particularly in future Earth-to-satellite quantum links [53–55], where maintaining high-dimensional entanglement could significantly enhance information capacity and noise resilience.

5.2 Qutrit-based BBM92 protocol implementation with path encoding

Zheng et al. demonstrated (2023) a high-dimensional BBM92 protocol implemented entirely on silicon photonic chips [16]. They reported the first realization of an entanglement-based QKD protocol operating in higher dimensions on a fully complementary metal–oxide–semiconductor (CMOS)-compatible silicon photonic platform (see Fig. 3A), marking an important step toward scalable chip-level quantum networks. The experimental system comprised a central server chip and three node chips (Fig. 3B). The server generated entangled photon pairs via spontaneous four-wave

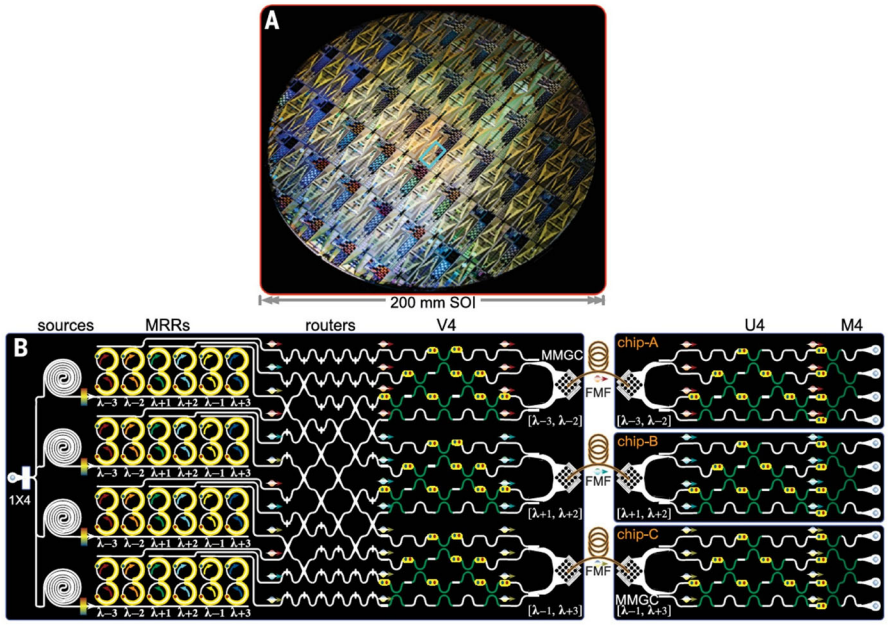


Fig. 3 Experimental setup for qutrit-based BBM92 QKD protocol with on-chip path encoding. **A** Photograph of the 200-mm silicon-on-insulator wafer that contains CMOS-compatible integrated quantum-networking chipsets fabricated by standard lithography. Each chipset includes a server chip and multiple-node chips, forming a self-contained quantum-network module. **B** Circuit diagram of one networking module. The architecture consists of a central server chip that generates and distributes multiple pairs of high-dimensional entangled photons to three node chips (labeled chip-A, B, and C). The server integrates four nonlinear photon-pair sources based on spontaneous four-wave mixing in silicon nanowaveguides, followed by arrays of coupled microring resonators (MRRs) that perform wavelength demultiplexing and remultiplexing. Each photon pair is encoded across four distinct on-chip paths, defining a four-dimensional logical basis $|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$. These photons are then routed through multimode grating couplers (MMGCs) into few-mode fiber (FMF) links, ensuring that the constituent photons of each pair are directed to distinct receiver nodes. The triangular interferometric meshes labeled $\boldsymbol{V}_4$ on the server and $\boldsymbol{U}_4$ on the node chips represent programmable linear-optical circuits capable of implementing arbitrary unitary transformations for selecting the measurement bases. The $\boldsymbol{M}_4$ sections denote measurement interferometers used for projective detection. Green elements correspond to reconfigurable beam splitters, and yellow regions indicate thermo-optic phase shifters. Reproduced from Y. Zheng et al., "Multichip multidimensional quantum networks with entanglement retrievability", *Science* 381, 221–226 (2023), https://doi.org/10.1126/science.adg8159, AAAS [16]

mixing (SFWM) in four integrated nanowaveguide sources pumped by a continuous-wave laser at 1558.17 nm. In this nonlinear process, two pump photons are annihilated, creating a signal-idler photon pair at distinct wavelengths. The broadband biphoton spectrum was then divided into multiple correlated wavelength channels by arrays of coupled microring resonators (MRRs), which act as precise wavelength demultiplexers. Each entangled pair was encoded in four distinct on-chip paths, defining a four-dimensional logical basis $|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$.

After generation, the paths of each photon in a correlated pair were recombined and routed so that one photon of the pair was directed to one node chip, and its partner to another. This routing was accomplished through a carefully engineered network of on-chip waveguide crossings and MRR-based wavelength multiplexers. For example, photons with specific wavelength pairs ($\lambda_{\pm 3}$, $\lambda_{\pm 2}$, and $\lambda_{\pm 1}$) were assigned to connect distinct pairs of node chips: one wavelength channel links nodes A and C, another connects A and B, and the third connects B and C. In each case, the two photons forming an entangled pair occupied matched path modes on the server chip, which were coherently combined into a single output waveguide for transmission through a few-mode fiber (FMF). This multiplexed arrangement allowed simultaneous distribution of multiple entangled states among all nodes in the network. Each fiber thus carried one photon from each entangled pair in a superposition of four hybrid polarization-mode states. After transmission, the corresponding node chip demultiplexed and converted the modes back into path encoding for measurement. The successful recovery of path correlations between nodes confirmed that entanglement was preserved through the chip–fiber–chip channels.

Building on this entanglement distribution, Zheng et al. implemented an entanglement-based QKD experiment between two node chips. Although the network supported up to 4-level (ququart) entanglement, the QKD tests were performed for qubit and qutrit cases, using the corresponding qudit Bell states of the form

$$|\Phi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_s|0\rangle_i + |1\rangle_s|1\rangle_i\right), \tag{44A}$$

$$|\Phi_3\rangle = \frac{1}{\sqrt{3}}\left(|0\rangle_s|0\rangle_i + |1\rangle_s|1\rangle_i + |2\rangle_s|2\rangle_i\right). \tag{44B}$$

The protocol follows the BBM92 scheme generalized to higher dimensions. Specifically, each user measures their photon in one of two MUBs: the computational basis and the Fourier basis, chosen randomly for each detection event. The experimental results demonstrated the advantage of high-dimensional encoding for QKD. In the qubit regime, the system achieved 0.301 ± 0.033 bits of secure key per coincidence, with a QBER of 4.6%, which is well below the security threshold of 11% [27, 45]. Instead, extending the encoding to qutrits increased the secure key to 0.346 ± 0.037 bits per coincidence, with a QBER of approximately 10.3%, remaining below the corresponding security threshold of 15.95% [45]. Such achieved key rates confirmed that higher-dimensional encoding improves the key capacity per detected photon, even in the presence of fiber-induced modal crosstalk. Furthermore, secure key rates indicate

that the qutrit case maintains positive key generation even at higher error levels than in the qubit case, illustrating the robustness of the high-dimensional approach.

A key significance of this work lies in the complete integration of main QKD components, including entangled-photon sources, multiplexers, routing networks, and measurement circuits, onto mass-manufacturable silicon photonic chips. The system demonstrates that high-dimensional entanglement can be generated, distributed over chip–fiber–chip links, and measured entirely within a fully integrated platform.

5.3 BBM92 protocol implementation with time-bin ququarts

A recent experimental breakthrough by Yu et al. demonstrated a qudit-based BBM92 protocol using picosecond-spaced, time-bin-encoded photons on an integrated photonic platform [39]. The realization of high-dimensional, entanglement-based QKD is implemented entirely within a fiber-pigtailed chip system operating in the telecommunication C-band, marking a major advance toward scalable and high-speed quantum communication over standard optical fiber networks. The experimental platform combined a programmable on-chip interferometer cascade (OIC) integrated with a 45-cm-long spiral waveguide fabricated on a CMOS-compatible substrate (see Fig. 4). Within the OIC, multiple unbalanced Mach–Zehnder interferometers were connected in cascade, forming a reconfigurable network capable of coherently splitting a single pump pulse into a sequence of subpulses with controlled temporal spacing. When the pulse trains were injected into the spiral waveguide, SFWM generated C-band photon

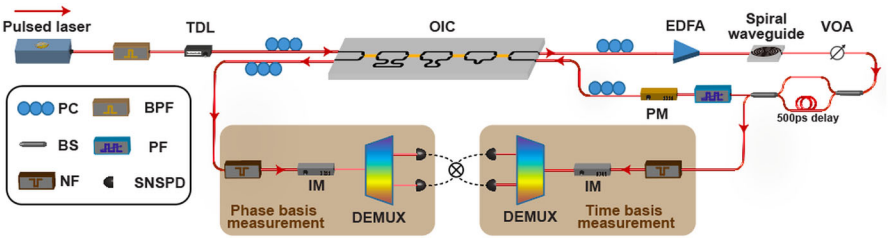


Fig. 4 Experimental setup for ququart-based BBM92 QKD protocol with ultrafast time-bin encoding. A programmable on-chip interferometer cascade (OIC) coherently splits an input pump pulse into four subpulses with equal amplitudes and 64-ps temporal spacing. Pump pulses drive spontaneous four-wave mixing in an integrated spiral waveguide, producing the four-dimensional time-bin Bell state between signal and idler photons. Using two beam splitters (BS) with a 500-ps delay line, photons are probabilistically routed either to the time- or phase-measurement setups, arriving simultaneously or with a 500-ps delay, thereby enabling the random selection of measurement bases for Alice and Bob. Measurements in the time basis are performed through temporal gating, while those in the phase basis are realized by applying phase modulation (PM) followed by temporal gating on the resulting time-bin superpositions. Temporal gating is implemented using two intensity modulators (IMs), one per measurement basis. The sifted keys are extracted from coincidence detections on the time basis, and the system security is evaluated from the bit error rates in both bases. This integrated configuration enables stable and phase-coherent implementation of entanglement QKD at a 1 GHz clock rate, offering a compact, fiber-compatible platform for high-dimensional quantum communication. *TDL* tunable delay line, *EDFA* erbium-doped fiber amplifier, *VOA* variable optical attenuator, *DEMUX* demultiplexer, *PC* polarization controller, *BPF* band-pass filter, *PF* programmable filter, *NF* notch filter, *SNSPD* superconducting nanowire single-photon detector. Reprinted from [39] under the Creative Commons Attribution 4.0 International License (CC BY 4.0)

pairs entangled in the time-bin degree of freedom. The pairs were then spectrally filtered and distributed to two receivers through dense wavelength-division multiplexing channels. Leveraging this capability, the BBM92 scheme has been realized using a ququart Bell state of the form

$$|\Phi_4\rangle = \frac{1}{2}\big(|0\rangle_s|0\rangle_i + |1\rangle_s|1\rangle_i + |2\rangle_s|2\rangle_i + |3\rangle_s|3\rangle_i\big), \tag{45}$$

where $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ denote four time-bin basis states ordered by increasing arrival time at the single-photon detectors, with adjacent bins separated by 64 ps. In this scheme, Alice and Bob each received one photon from an entangled pair (from the spiral waveguide) and performed measurements in one of two MUBs: the time basis (equivalent to the computational basis), defined by the discrete time-of-arrival of the photons, and the phase basis (equivalent to the Fourier basis), formed by coherent superpositions of the time bins. Measurements in the time and phase bases were randomly selected using a beam splitter-based delay scheme with a 500-ps temporal delay. Coincidence outcomes were recorded for matching bases between Alice and Bob and used to generate a shared secret key. The time-bin spacing was comparable to the 52 ps timing jitter of the superconducting nanowire single-photon detectors used in the experiment, so temporal gating was employed to isolate the relevant modes and suppress crosstalk between adjacent bins. The system operated stably over several hours with low background noise and maintained synchronization at a pump repetition rate of 1 GHz, enabling processing speeds comparable to those of standard telecommunication systems. The measured average secure key rate reached 2.04 kbit/s, while the average QBERs were 10.97% in the time basis and 13.05% in the phase basis—within the 18.93% security threshold for the ququart BBM92 protocol. The protocol scheme was also extended over a 60-km fiber link comprising telecom-compatible modules (single-mode and dispersion-compensating fibers), yielding a secret key rate of 37 bit/s. The measured secret key rate was mainly affected by two factors: the low efficiency of the entanglement source and the losses introduced by the external temporal gating, used to isolate the relevant time bins and suppress crosstalk between adjacent bins. Temporal gating is required because the timing jitter of the superconducting nanowire single-photon detectors (SNSPDs, 52 ps) approaches the temporal mode spacing of the entangled qudits (64 ps). If SNSPDs with higher timing resolution (e.g., < 30 ps) were used, secret key rates of up to 102.8 kbit/s and 1.93 kbit/s could be achieved in the short-distance and long-distance configurations, respectively.

The significance of this work lies in realizing an application-ready, chip-integrated platform for entanglement-based QKD. The monolithic interferometric architecture provides phase-stable, programmable control of multiple time bins, enabling high-dimensional operation at GHz speeds and compatibility with wavelength-multiplexed fiber links. With further optimization of detector performance and on-chip active phase control, the same system could generate and process time-bin entangled states with 8 temporal modes, paving the way for dense, multi-user quantum networks. The experiment by Yu et al. thus establishes a scalable foundation for implementing high-dimensional entanglement-based QKD in practical, fiber-integrated quantum communication systems.

5.4 Systematic comparison

Sections 5.1 through 5.3 reviewed three distinct high-dimensional entanglement-based QKD implementations spanning different physical degrees of freedom, integration levels, and operational environments: a bulk free-space system utilizing OAM qutrits for open-air propagation [57], a fully integrated silicon photonic platform exploiting spatial path encoding for multi-node on-chip networks [16], and a telecom-compatible fiber-integrated chip system leveraging picosecond time-bin ququarts for high-speed transmission [39]. While each platform successfully demonstrates the information-capacity and error-tolerance advantages of higher-dimensional Hilbert spaces, they exhibit distinct performance trade-offs dictated by their underlying optical sources and channel architectures. To provide a clear side-by-side evaluation, Table 1 systematically compares their key physical parameters and operational performance metrics.

In summary, the choice of physical platform and degree of freedom fundamentally dictates the operational domain of high-dimensional QKD. Future progress across all three paradigms will rely on hardware-level optimizations to enhance the secret key generation rate and reduce the error rate.

Table 1 Systematic comparison of representative high-dimensional entanglement-based QKD implementations

Degree of freedom	OAM [57]	Path [16]	Time-bin [39]
Protocol	E91	BBM92	BBM92
Qudit level	$d = 3$	$d = 2, 3$	$d = 4$
Physical platform	Bulk optics	Integrated photonic chip/fiber	Integrated photonic chip/fiber
Photon-pair source	Type-I BBO crystal (SPDC)	Nanowaveguide array (SFWM)	Spiral waveguide (SFWM)
Operating optical band	Near infrared	Telecom C-band	Telecom C-band
Transmission channel	Free-space	FMF	SMF/DCF
Error rate	9.33% (14/150 errors in sifted key)	4.6% ($d = 2$); 10.3% ($d = 3$)	Time basis: 10.97%; Phase basis: 13.05%
Secret key yield	72 trits (Total post-processed)	0.301 bits/coincidence ($d = 2$); 0.346 bits/coincidence ($d = 3$)	2.04 kbit/s (few-meter SMF); 37 bit/s (60-km SMF + DCF)

The three works quote their performance using different figures of merit (total post-processed key length, key fraction per coincidence, and key rate in bit/s); the original units are retained here, and the corresponding entries should therefore not be read as directly comparable numbers

SPDC spontaneous parametric down-conversion, *SFWM* spontaneous four-wave mixing, *BBO* β-barium-borate, *FMF* few-mode fiber, *SMF* single-mode fiber, *DCF* dispersion-compensating fiber

6 Frequency-bin entanglement for scalable high-dimensional QKD

Frequency-bin entanglement is a considerably promising resource for high-dimensional entanglement-based QKD toward future quantum communication networks. Such states are naturally generated in nonlinear optical processes (SPDC or SFWM), either directly as sets of discrete resonant modes (e.g., in microring resonators) or as broadband photon pairs that are subsequently mapped onto a discrete set of frequency bins by spectral filtering [4, 5, 97–100, 102]. In this framework, entanglement-based QKD protocols can be implemented by distributing frequency-bin entanglement between Alice and Bob through optical fibers. Two recent experiments have adopted this scheme by implementing the qubit-based BBM92 protocol (see Fig. 5) [106, 107] with a frequency-bin Bell state of the form

$$|\Phi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_s|0\rangle_i + |1\rangle_s|1\rangle_i\right), \tag{46}$$

where $|0\rangle$ and $|1\rangle$ denote the qubit states encoded in two distinct frequency modes of each photon. Although the two works used different platforms—one based on two microring resonators integrated into a silicon photonic chip [106], while the other on a periodically poled lithium niobate waveguide [107]—the overall architecture is rather similar. In both cases, measurements in the Z basis are implemented by spectrally separating the two frequency bins with narrowband filters and detecting them independently. Measurements in the X basis are realized via electro-optic phase modulation that mixes the two frequency bins, followed by spectral [106] or temporal [107] discrimination of the resulting interference pattern. Alice and Bob randomly choose between these two bases, where the randomness is reproduced either with beamsplitters that direct photons toward different analysis paths [106] or by continuously driving the electro-optic modulators so that both bases are effectively sampled [107]. The two groups demonstrate low QBER well below the qubit-based BBM92 security threshold of 11% and positive secret key rates over tens of kilometers of optical fiber.

These qubit-level demonstrations also provide a clear pathway toward high-dimensional entanglement-based QKD using frequency qudits. Modern sources of frequency-bin entanglement naturally support many spectral modes—far more than the two bins used to encode a qubit—and experiments have already shown the generation and control of high-dimensional frequency-entangled Bell states [4, 5, 97–100, 102]. By selecting and coherently addressing larger sets of frequency bins, the same hardware can be extended to encode qudits in the frequency domain. On the measurement side, complex spectral phase masks sandwiched between electro-optic phase modulators enable the implementation of generalized mutually unbiased bases for qudits [108, 109]. However, current realizations are intrinsically lossy and further constrained by the need for multi-tone radio-frequency driving [108, 109].

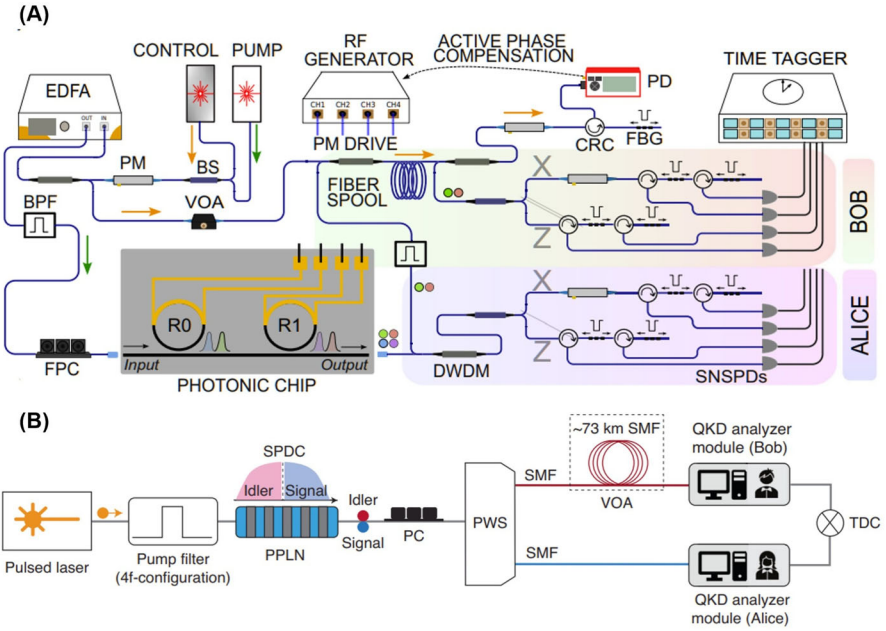


Fig. 5 Experimental setups for qubit-based BBM92 QKD protocol with frequency-bin entanglement. **A** In the integrated implementation, a continuous-wave laser amplified by an erbium-doped fiber amplifier (EDFA) is phase modulated and spectrally filtered (BPF) to generate a frequency comb that pumps two microring resonators (R0, R1) on a silicon photonic chip, which produce frequency-bin entangled photon pairs via SFWM. The pairs are sent through a fiber spool acting as the quantum channel and then demultiplexed by a dense wavelength-division multiplexer (DWDM) toward Alice and Bob. Each party performs Z- and X-basis measurements using electro-optic phase modulators, circulators (CRCs), and fiber Bragg gratings (FBGs), with active phase compensation provided by a classical pilot tone monitored on a photodiode (PD). Detection is carried out with superconducting nanowire single-photon detectors (SNSPDs), and all time tags are registered by a common time-tagger unit. Reproduced from Ref. [106] under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. **B** A pulsed pump laser, which is spectrally shaped with a $4f$-configuration filter, drives SPDC in a PPLN waveguide, producing frequency-correlated signal–idler pairs. A polarization controller (PC) and a programmable wavelength switch (PWS) select a pair of frequency bins that define the logical qubit states and distribute the photons through standard single-mode fibers (SMFs) to Alice and Bob. A variable optical attenuator (VOA) and up to ~ 73 km of SMF emulate channel loss. At each user, a QKD analyzer module based on electro-optic modulation, filtering and frequency-to-time mapping implements projective measurements in the computational Z basis and in superposition X basis, with detection events recorded by a time-to-digital converter (TDC). Reproduced from Ref. [107] under the Creative Commons Attribution 4.0 International License

7 Discussions and perspectives

The development of qudit-based entanglement QKD protocols has marked a significant step toward advancing the performance and scalability of quantum communication. By extending entanglement into higher-dimensional Hilbert spaces, these protocols can offer notable advantages, including enhanced secure key rates, improved noise tolerance, and stronger resilience against eavesdropping, which surpass the capabilities of their qubit-based counterparts. Such merits have driven diverse experimental

demonstrations across various photonic platforms, underscoring the opportunities that high-dimensional systems offer for next-generation quantum networks.

Experimental demonstrations of qudit-based entanglement QKD have confirmed that high-dimensional encoding can be realized across multiple photonic degrees of freedom, including OAM [57], path [16], and temporal [39] modes. These achievements demonstrate that photonic qudit entanglement not only increases information capacity but also provides greater robustness against noise and experimental imperfections. Time-bin entanglement operating at gigahertz repetition rates, for instance, has enabled secure key generation at kilobit-per-second rates—an encouraging step toward bridging the gap between proof-of-principle experiments and deployable QKD systems [39]. The ability to generate, distribute, and measure high-dimensional entanglement at such high clock rates demonstrates strong compatibility with scalable, high-speed quantum communication infrastructures. In parallel, frequency-qudit entanglement combines several attractive features for high-dimensional QKD. It can be generated and directly transmitted using off-the-shelf telecommunication components, offering seamless compatibility with existing optical infrastructures [4, 5, 97–100, 102]. In addition, the manipulation and measurement of frequency-entangled qudits can be implemented entirely within a single-mode fiber using commercially available electro-optic components, eliminating the need for bulk or interferometric optics [4, 5, 97–100, 102]. This approach allows reconfigurable control of frequency-bin superpositions, substantially simplifying system design while minimizing phase drift [110]. The ability to access a large number of well-defined and inherently stable spectral modes further supports the realization of high-dimensional states. Demonstrations of up to eight-dimensional frequency Bell states highlight this potential [98], and existing implementations of frequency-qubit BBM92 further indicate the feasibility of extending such approaches to a scalable, high-dimensional regime [106, 107].

Integrating high-dimensional encoding into practical networks introduces several technical challenges. Generating and manipulating high-dimensional entangled states typically requires precise phase and amplitude control across multiple modes, which becomes challenging in real network environments where interferometric paths drift and mode alignment fluctuates [51, 111–114]. Furthermore, a higher dimensionality exacerbates crosstalk in multimode systems, and maintaining coherence across all basis states becomes increasingly difficult over long distances [101, 115–117]. These factors constrain channel stability, synchronization, and detection efficiency—critical issues that must be addressed before high-dimensional systems can operate reliably in large-scale networks.

The progress in photonic qudit-based entanglement QKD highlights both the opportunities and challenges inherent to high-dimensional approaches. These advances have validated their theoretical advantages and provided the groundwork for scalable, high-rate implementations. Moving forward, the successful integration of qudit entanglement into telecom-compatible platforms, together with advances in frequency multiplexing [14, 16–18, 118], will be crucial for realizing large-scale, efficient, and robust quantum communication infrastructure.

Acknowledgements R.M. acknowledges support from the Canada Research Chair program, from NSERC, through the following projects: Discovery Grant, AQUA ALLRP 587602-23, QuEnSi ALLRP 578468-22, Consortium on Integrated Quantum Photonics with Ferroelectric Materials ALLRP 587352-23, HyperSpace ALLRP 569583-21, and from FRQNT, through the project AdéQuATS FRQNT 328872.

Author contributions J.Y. and L.C. wrote the initial draft, with feedback from S.S. and D.B. D.J.M. and R.M. supervised the work. All authors revised and approved the final manuscript.

Funding See Acknowledgements.

Data availability The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of interest The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999)
2. X.-L. Wang, L.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li, H. Lu, Y. Hu, X. Jiang, C.-Z. Peng, L. Li, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, J.-W. Pan, Phys. Rev. Lett. **117**, 210502 (2016)
3. P. Thomas, L. Ruscio, O. Morin, G. Rempe, Nature **608**, 677 (2022)
4. M. Kues, C. Reimer, P. Roztocki, L.R. Cortés, S. Sciara, B. Wetzel, Y. Zhang, A. Cino, S.T. Chu, B.E. Little, D.J. Moss, L. Caspani, J. Azaña, R. Morandotti, Nature **546**, 622 (2017)
5. C. Reimer, S. Sciara, P. Roztocki, M. Islam, L. Romero Cortés, Y. Zhang, B. Fischer, S. Loranger, R. Kashyap, A. Cino, S.T. Chu, B.E. Little, D.J. Moss, L. Caspani, W.J. Munro, J. Azaña, M. Kues, R. Morandotti, Nat. Phys. **15**, 148 (2019)
6. C. Reimer, M. Kues, P. Roztocki, B. Wetzel, F. Grazioso, B.E. Little, S.T. Chu, T. Johnston, Y. Bromberg, L. Caspani, D.J. Moss, R. Morandotti, Science **351**, 1176 (2016)
7. P. Roztocki, M. Kues, C. Reimer, B. Wetzel, S. Sciara, Y. Zhang, A. Cino, B.E. Little, S.T. Chu, D.J. Moss, R. Morandotti, Opt. Express **25**, 18940 (2017)
8. C. Reimer, L. Caspani, M. Clerici, M. Ferrera, M. Kues, M. Peccianti, A. Pasquazi, L. Razzari, B.E. Little, S.T. Chu, D.J. Moss, R. Morandotti, Opt. Express **22**, 6535 (2014)
9. J. Claudon, J. Bleuse, N.S. Malik, M. Bazin, P. Jaffrennou, N. Gregersen, C. Sauvan, P. Lalanne, J.-M. Gérard, Nat. Photonics **4**, 174 (2010)
10. L. Sapienza, M. Davanço, A. Badolato, K. Srinivasan, Nat. Commun. **6**, 7833 (2015)
11. C. Reimer, M. Kues, L. Caspani, B. Wetzel, P. Roztocki, M. Clerici, Y. Jestin, M. Ferrera, M. Peccianti, A. Pasquazi, B.E. Little, S.T. Chu, D.J. Moss, R. Morandotti, Nat. Commun. **6**, 8236 (2015)
12. C.K. Hong, Z.Y. Ou, L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987)
13. K.M.A. Yousef, M. D'Alessandro, M. Yeh, N. Sinclair, M. Loncar, F. Capasso, Science **389**, 416 (2025)
14. S. Wengerowsky, S.K. Joshi, F. Steinlechner, H. Hübel, R. Ursin, Nature **564**, 225 (2018)

15. M. Pompili, S.L.N. Hermans, S. Baier, H.K.C. Beukers, P.C. Humphreys, R.N. Schouten, R.F.L. Vermeulen, M.J. Tiggelman, L.D.S. Martins, B. Dirkse, S. Wehner, R. Hanson, Science **372**, 259 (2021)
16. Y. Zheng, C. Zhai, D. Liu, J. Mao, X. Chen, T. Dai, J. Huang, J. Bao, Z. Fu, Y. Tong, X. Zhou, Y. Yang, B. Tang, Z. Li, Y. Li, Q. Gong, H.K. Tsang, D. Dai, J. Wang, Science **381**, 221 (2023)
17. J. Liu, D. Liu, Z. Jin, Z. Lin, H. Li, L. You, X. Feng, F. Liu, K. Cui, W. Zhang, Y. Huang, Sci. Adv. **10**, eado9822 (2024)
18. Y.-R. Fan, Y. Luo, K. Guo, J.-P. Wu, H. Zeng, G.-W. Deng, Y. Wang, H.-Z. Song, Z. Wang, L.-X. You, G.-C. Guo, Q. Zhou, Light Sci. Appl. **14**, 189 (2025)
19. Y. Zheng, H. Wang, X. Jia, J. Huang, H. Yuan, C. Zhai, J. Dai, J. Shi, L. Zhang, X. Zhang, M. Zhuang, J. Liu, J. Mao, T. Dai, Z. Fu, Y. Jiao, Y. Shi, D. Dai, X. Wang, Y. Li, Q. Gong, Z. Yuan, L. Chang, J. Wang, Nature **651**, 68 (2026)
20. Y. Huang, Y. Yang, H. Li, J. Wang, J. Qiu, Z. Qi, Y. Zhang, Y. Li, Y. Zheng, X. Chen, Nat. Photonics **20**, 87 (2026)
21. C.H. Bennett, G. Brassard, Theor. Comput. Sci. **560**, 7 (2014)
22. A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
23. H.-K. Lo, M. Curty, K. Tamaki, Nat. Photonics **8**, 595 (2014)
24. C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992)
25. D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998)
26. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003)
27. C.H. Bennett, G. Brassard, N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992)
28. X. Ma, C.-H.F. Fung, H.-K. Lo, Phys. Rev. A **76**, 012307 (2007)
29. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, N. Gisin, Appl. Phys. Lett. **70**, 793 (1997)
30. C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptol. **5**, 3 (1992)
31. T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000)
32. W. Tittel, J. Brendel, H. Zbinden, N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000)
33. C. Gobby, Z.L. Yuan, A.J. Shields, Appl. Phys. Lett. **84**, 3762 (2004)
34. M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J.F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A.W. Sharpe, A.J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R.T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z.L. Yuan, H. Zbinden, A. Zeilinger, New J. Phys. **11**, 075001 (2009)
35. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J.F. Dynes, A.R. Dixon, A.W. Sharpe, Z.L. Yuan, A.J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, A. Zeilinger, Opt. Express **19**, 10387 (2011)
36. Y. Shi, S.M. Thar, H.S. Poh, J.A. Grieve, C. Kurtsiefer, A. Ling, Appl. Phys. Lett. **117**, 124002 (2020)
37. D. Cozzolino, B. Da Lio, D. Bacco, L.K. Oxenløwe, Adv. Quantum Technol. **2**, 1900038 (2019)
38. M. Zahidy, D. Ribezzo, C. De Lazzari, I. Vagniluca, N. Biagi, R. Müller, T. Occhipinti, L.K. Oxenløwe, M. Galili, T. Hayashi, D. Cassioli, A. Mecozzi, C. Antonelli, A. Zavatta, D. Bacco, Nat. Commun. **15**, 1651 (2024)
39. H. Yu, S. Sciara, M. Chemnitz, N. Montaut, B. Crockett, B. Fischer, R. Helsten, B. Wetzel, T.A. Goebel, R.G. Krämer, B.E. Little, S.T. Chu, S. Nolte, Z. Wang, J. Azaña, W.J. Munro, D.J. Moss, R. Morandotti, Nat. Commun. **16**, 171 (2025)
40. A. Mair, A. Vaziri, G. Weihs, A. Zeilinger, Nature **412**, 313 (2001)
41. M. Erhard, M. Krenn, A. Zeilinger, Nat. Rev. Phys. **2**, 365 (2020)
42. Y. Wang, Z. Hu, B.C. Sanders, S. Kais, Front. Phys. (2020). https://doi.org/10.3389/fphy.2020.589504
43. M. Kues, C. Reimer, J.M. Lukens, W.J. Munro, A.M. Weiner, D.J. Moss, R. Morandotti, Nat. Photonics **13**, 170 (2019)
44. H. Bechmann-Pasquinucci, W. Tittel, Phys. Rev. A **61**, 062308 (2000)
45. N.J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002)

46. D. Collins, N. Gisin, N. Linden, S. Massar, S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002)
47. D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski, A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000)
48. V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, Rev. Mod. Phys. **81**, 1301 (2009)
49. S. Slussarenko, G.J. Pryde, Appl. Phys. Rev. **6**, 041303 (2019)
50. N. Gisin, R. Thew, Nat. Photonics **1**, 165 (2007)
51. F. Steinlechner, S. Ecker, M. Fink, B. Liu, J. Bavaresco, M. Huber, T. Scheidl, R. Ursin, Nat. Commun. **8**, 15971 (2017)
52. A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, H. Zbinden, Phys. Rev. Lett. **121**, 190502 (2018)
53. T. Roger, R. Singh, C. Perumangatt, D.G. Marangon, M. Sanzaro, P.R. Smith, R.I. Woodward, A.J. Shields, Sci. Adv. **9**, eadj5873 (2023)
54. J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A.K. Ekert, J.-W. Pan, Nature **582**, 501 (2020)
55. S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, J.-W. Pan, Nature **549**, 43 (2017)
56. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, J.-W. Pan, Rev. Mod. Phys. **92**, 025002 (2020)
57. S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, A. Zeilinger, New J. Phys. **8**, 75 (2006)
58. P.A.M. Dirac, *The Principles of Quantum Mechanics* (Oxford University Press, Oxford, 1981), pp.10–18
59. R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009)
60. J.J. Sakurai, J. Napolitano, *Modern Quantum Mechanics* (Cambridge University Press, Cambridge, 2020), pp.1–61
61. M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, 2010), pp.13–17
62. E. Schrödinger, Math. Proc. Camb. Philos. Soc. **31**, 555 (1935)
63. R.F. Werner, Phys. Rev. A **40**, 4277 (1989)
64. C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993)
65. Y.-H. Luo, H.-S. Zhong, M. Erhard, X.-L. Wang, L.-C. Peng, M. Krenn, X. Jiang, L. Li, N.-L. Liu, C.-Y. Lu, A. Zeilinger, J.-W. Pan, Phys. Rev. Lett. **123**, 070505 (2019)
66. X.-M. Hu, C. Zhang, B.-H. Liu, Y. Cai, X.-J. Ye, Y. Guo, W.-B. Xing, C.-X. Huang, Y.-F. Huang, C.-F. Li, G.-C. Guo, Phys. Rev. Lett. **125**, 230501 (2020)
67. H. Zhang, L. Wan, T. Haug, W.-K. Mok, S. Paesani, Y. Shi, H. Cai, L.K. Chin, M.F. Karim, L. Xiao, X. Luo, F. Gao, B. Dong, S. Assad, M.S. Kim, A. Laing, L.C. Kwek, A.Q. Liu, Sci. Adv. **8**, eabn9783 (2022)
68. B. Wu, J. Jiang, J. Zhang, G. Tian, X. Sun, Phys. Rev. A **98**, 022304 (2018)
69. O. Gühne, G. Tóth, Phys. Rep. **474**, 1 (2009)
70. D.J. Bernstein, T. Lange, Nature **549**, 188 (2017)
71. R.L. Rivest, A. Shamir, L. Adleman, Commun. ACM **21**, 120 (1978)
72. W.K. Wootters, W.H. Zurek, Nature **299**, 802 (1982)
73. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007)
74. J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969)
75. N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, Rev. Mod. Phys. **86**, 419 (2014)
76. D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, P.G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000)
77. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002)
78. M. Koashi, J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003)
79. G. Brassard, L. Salvail, in *Advances in Cryptology—EUROCRYPT '93*. ed. by T. Helleseth (Springer, Berlin, 1994)
80. C.H. Bennett, G. Brassard, C. Crepeau, U.M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995)
81. I. Devetak, A. Winter, Proc. R. Soc. A: Math. Phys. Eng. Sci. **461**, 207 (2005)
82. P.W. Shor, J. Preskill, Phys. Rev. Lett. **85**, 441 (2000)
83. M. Tomamichel, C.C.W. Lim, N. Gisin, R. Renner, Nat. Commun. **3**, 634 (2012)

84. M. Ben-Or, M. Horodecki, D.W. Leung, D. Mayers, J. Oppenheim, in Theory of Cryptography Conference (Springer, Berlin, Heidelberg, 2005), pp. 386–406
85. T. Durt, N.J. Cerf, N. Gisin, M. Żukowski, Phys. Rev. A **67**, 012311 (2003)
86. J. Schwinger, Proc. Natl. Acad. Sci. **46**, 570 (1960)
87. K. Siudzińska, Phys. Rev. A **102**, 062615 (2020)
88. L. Masanes, S. Pironio, A. Acín, Nat. Commun. **2**, 238 (2011)
89. M. Araújo, M. Huber, M. Navascués, M. Pivoluska, A. Tavakoli, Quantum **7**, 1019 (2023)
90. L. Sheridan, V. Scarani, Phys. Rev. A **82**, 030301 (2010)
91. J.L. O'Brien, A. Furusawa, J. Vučković, Nat. Photonics **3**, 687 (2009)
92. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, Nature **390**, 575 (1997)
93. I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, N. Gisin, Nature **421**, 509 (2003)
94. J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang, X.-D. Cai, P. Xu, G.-S. Pan, J.-J. Jia, Y.-M. Huang, H. Yin, J.-Y. Wang, Y.-A. Chen, C.-Z. Peng, J.-W. Pan, Nature **488**, 185 (2012)
95. F. Wang, M. Erhard, A. Babazadeh, M. Malik, M. Krenn, A. Zeilinger, Optica **4**, 1462 (2017)
96. J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J.W. Silverstone, Q. Gong, A. Acín, K. Rottwitt, L.K. Oxenløwe, J.L. O'Brien, A. Laing, M.G. Thompson, Science **360**, 285 (2018)
97. P. Imany, J.A. Jaramillo-Villegas, O.D. Odele, K. Han, D.E. Leaird, J.M. Lukens, P. Lougovski, M. Qi, A.M. Weiner, Opt. Express **26**, 1825 (2018)
98. H.-H. Lu, K.V. Myilswamy, R.S. Bennink, S. Seshadri, M.S. Alshaykh, J. Liu, T.J. Kippenberg, D.E. Leaird, A.M. Weiner, J.M. Lukens, Nat. Commun. **13**, 4338 (2022)
99. M. Clementi, F.A. Sabattoli, M. Borghi, L. Gianini, N. Tagliavacche, H. El Dirani, L. Youssef, N. Bergamasco, C. Petit-Etienne, E. Pargon, J.E. Sipe, M. Liscidini, C. Sciancalepore, M. Galli, D. Bajoni, Nat. Commun. **14**, 176 (2023)
100. S. Seshadri, H.-H. Lu, D.E. Leaird, A.M. Weiner, J.M. Lukens, Phys. Rev. Lett. **129**, 230505 (2022)
101. T. Ikuta, H. Takesue, Sci. Rep. **8**, 817 (2018)
102. P. Imany, J.A. Jaramillo-Villegas, M.S. Alshaykh, J.M. Lukens, O.D. Odele, A.J. Moore, D.E. Leaird, M. Qi, A.M. Weiner, Npj Quantum Inf. **5**, 59 (2019)
103. C. Couteau, Contemp. Phys. **59**, 291 (2018)
104. S. Franke-Arnold, S.M. Barnett, M.J. Padgett, L. Allen, Phys. Rev. A **65**, 033823 (2002)
105. J.P. Torres, G. Molina-Terriza, L. Torner, J. Opt. B Quantum Semiclass. Opt. **7**, 235 (2005)
106. N. Tagliavacche, M. Borghi, G. Guarda, D. Ribezzo, M. Liscidini, D. Bacco, M. Galli, D. Bajoni, Npj Quantum Inf. **11**, 60 (2025)
107. A. Khodadad Kashi, M. Kues, Light Sci. Appl. **14**, 49 (2025)
108. H.-H. Lu, N.B. Lingaraju, D.E. Leaird, A.M. Weiner, J.M. Lukens, Opt. Express **30**, 10126 (2022)
109. H.-H. Lu, J.M. Lukens, N.A. Peters, O.D. Odele, D.E. Leaird, A.M. Weiner, P. Lougovski, Phys. Rev. Lett. **120**, 030502 (2018)
110. M. Shin, H. Shin, Curr. Opt. Photonics **9**, 443 (2025)
111. G. Vallone, D. Dequal, M. Tomasin, F. Vedovato, M. Schiavon, V. Luceri, G. Bianco, P. Villoresi, Phys. Rev. Lett. **116**, 253601 (2016)
112. J. Jin, S. Agne, J.-P. Bourgoin, Y. Zhang, N. Lütkenhaus, T. Jennewein, Phys. Rev. A **97**, 043847 (2018)
113. R. Valivarthi, M. Grimeau Puigibert, Q. Zhou, G.H. Aguilar, V.B. Verma, F. Marsili, M.D. Shaw, S.W. Nam, D. Oblak, W. Tittel, Nat. Photonics **10**, 676 (2016)
114. Q.-C. Sun, Y.-L. Mao, S.-J. Chen, W. Zhang, Y.-F. Jiang, Y.-B. Zhang, W.-J. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang, T.-Y. Chen, L.-X. You, X.-F. Chen, Z. Wang, J.-Y. Fan, Q. Zhang, J.-W. Pan, Nat. Photonics **10**, 671 (2016)
115. H. Cao, S.-C. Gao, C. Zhang, J. Wang, D.-Y. He, B.-H. Liu, Z.-W. Zhou, Y.-J. Chen, Z.-H. Li, S.-Y. Yu, J. Romero, Y.-F. Huang, C.-F. Li, G.-C. Guo, Optica **7**, 232 (2020)
116. X.-M. Hu, W.-B. Xing, B.-H. Liu, D.-Y. He, H. Cao, Y. Guo, C. Zhang, H. Zhang, Y.-F. Huang, C.-F. Li, G.-C. Guo, Optica **7**, 738 (2020)
117. L. Bulla, K. Hjorth, O. Kohout, J. Lang, S. Ecker, S.P. Neumann, J. Bittermann, R. Kindler, M. Huber, M. Bohmann, R. Ursin, M. Pivoluska, Phys. Rev. A **107**, L050402 (2023)
118. F. Appas, F. Baboux, M.I. Amanti, A. Lemaître, F. Boitier, E. Diamanti, S. Ducci, Npj Quantum Inf. **7**, 118 (2021)