Multiplexing scheme for simplified entanglement-based large-alphabet quantum key distribution

Citation for published version:

Digital Object Identifier (DOI):
10.1103/PhysRevA.91.052313

Link:
Link to publication record in Heriot-Watt Research Portal

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Physical Review A

General rights
Copyright for the publications made accessible via Heriot-Watt Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
Heriot-Watt University has made every reasonable effort to ensure that the content in Heriot-Watt Research Portal complies with UK legislation. If you believe that the public display of this file breaches copyright please contact open.access@hw.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
Multiplexing scheme for simplified entanglement-based large-alphabet quantum key distribution

Adetunmise C. Dada
SUPA, Institute for Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 1AS, United Kingdom
(Received 22 March 2015; published 15 May 2015)

We propose a practical quantum cryptographic scheme which combines high information capacity, such as provided by high-dimensional quantum entanglement, with the simplicity of a two-dimensional Clauser-Horne-Shimony-Holt (CHSH) Bell test for security verification. By applying a state combining entanglement in a two-dimensional degree of freedom, such as photon polarization, with high-dimensional correlations in another degree of freedom, such as photon orbital angular momentum (OAM) or path, the scheme provides a considerably simplified route towards security verification in quantum key distribution (QKD) aimed at exploiting high-dimensional quantum systems for increased secure key rates. It also benefits from security against collective attacks and is feasible using currently available technologies.

DOI: 10.1103/PhysRevA.91.052313 PACS number(s): 03.67.Dd, 03.65.Ud, 03.67.Ac, 42.50.Ex

I. INTRODUCTION

Cryptography is one of the most promising applications of quantum science [1]. With the recent demonstrations of high-dimensional two-photon entanglement using time bins [2,3] and photon orbital angular momentum (OAM) [4,5], large-alphabet entanglement-based quantum key distribution (QKD) systems become closer to their real-world implementations and applications. The traditional approach to large-alphabet QKD based on Bell’s theorem involves encoding a key in a high-dimensional degree of freedom, such as photon OAM, and verifying the security of the generated key using a test of a Bell inequality which requires projective measurements in high-dimensional mutually unbiased bases [6]. This is a straightforward generalization of the original protocol introduced by Ekert in 1991 (E91) [1,7] and its modifications, such as proposed in Ref. [8].

E91-based protocols have been demonstrated for qubits using polarization [9] and time-energy entanglement [10]. A Bell-type test of energy-time entangled qutrits has also been realized [11]. Reported Bell-test-based QKD experiments using OAM qutrits [12] have implemented a randomized selection of dichotomous measurements instead of full projective measurements in a three-dimensional state space. Although projective measurement for detection of high-dimensional OAM states of light with up to 11 different outcomes is now within reach [13,14], it still remains an experimental challenge to perform them in arbitrary qudit bases. In the case of high-dimensional time-bin states, such measurements would require multipath interferometric setups which become too cumbersome to implement for a high number of dimensions. Although a scheme for large-alphabet QKD has been proposed and realized using energy-time entanglement [15], the applicability of this scheme is specific to this kind of entanglement and the security verification is highly device dependent as it places stringent conditions on timing resolutions of the detectors, which limits key generation rates.

Security verification of quantum key distribution schemes is a complicated problem in general. Security proofs have been provided for Bell-test-based QKD against so-called collective attacks [16] as well as the most general coherent attacks in the standard security scenarios [17]. However, proofs of device-independent security against these sophisticated attacks are not yet available in the case of entangled qudits requiring Bell tests generalized to high dimensions [18].

Here, we propose an approach to large-alphabet entanglement-based QKD which circumvents these problems by avoiding the need to perform high-dimensional unitary rotations required for measurements in different mutually unbiased bases, resulting in a much simplified measurement setup. The scheme presented here also benefits from security proofs for QKD based on entangled qubits against collective attacks. Our approach is in principle applicable to any system in which it is possible to create bipartite two-dimensional entanglement in one degree of freedom and high-dimensional correlations in another. Although we use an example with photon polarization and OAM to illustrate the protocol, the principle can be applied to other systems using other degrees of freedom to encode large secret keys.

The very essence of large-alphabet QKD is the possibility of a large rate of key generation. In practice, for a given entanglement-based QKD system, the minimum applicable coincidence detection time window \( \Delta t \) is an important factor limiting the maximum rate at which it is possible to generate secure keys per run, i.e., a single transmission and detection of the source state. As the number of dimensions offered by the source state increases, the maximum possible key rate per run for a given \( \Delta t \) also increases. The development of OAM sorters makes genuine large-alphabet key generation using up to 11-dimensional OAM entanglement feasible. This will also allow for a higher data rate per photon pair, as the detection of the photonic qudits would not need to be implemented as (probabilistic) dichotomous measurements, as has been the case in previous experiments [4,12]. It is also straightforward to implement projective measurements in computational (unrotated) time-bin bases. In what follows, we first describe the existing generalizations of the E91 protocol. We will describe the source state, measurement setup, and security considerations for our proposed scheme. Finally, we conclude with a few remarks on the realizability of the proposed experimental implementations.

\( ^{a.c.dada@hw.ac.uk} \)
II. GENERALIZED E91 PROTOCOL

To establish our scheme, let us first review the basic entanglement-based large-alphabet QKD resulting from a direct generalization of the E91 protocol and its variants. Assume a source producing photon pairs in the state

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_A \otimes |j\rangle_B. \tag{1}$$

Here we use the notation $|x,y\rangle \equiv |x\rangle \otimes |y\rangle$, where $\otimes$ denotes tensor product. In terms of OAM eigenstates $|\ell\rangle$, for example, this may be written as the maximally entangled state

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{\ell=|\ell|/2}^{\ell=+|\ell|/2} h(\ell) |\ell\rangle_A \otimes |-\ell\rangle_B, \tag{2}$$

where $h(\ell) = 1$ for all $\ell$ when $d$ is odd, and $h(\ell \neq 0) = 1$, $h(0) = 0$ when $d$ is even.

In a Bell inequality test experiment, each of the communicating parties Alice (A) and Bob (B) will have a photon OAM detector with outcomes depending on two settings or measurements, $\{A_1,A_2\}$ and $\{B_1,B_2\}$ respectively, which maximize Bell inequality violation. For the QKD scheme, there is an additional setting for each detector, i.e., $A_3$ for Alice and $B_3$ for Bob, chosen to produce perfect correlations. In a variant of Ekert’s scheme modified for increased key generation efficiency [8,17,18], only Alice’s detector uses $|\Phi\rangle$ when $d=2$. Only cases in which the combination of measurement settings involve $A_1 \otimes B_1$ are used for this test, while the remaining results are discarded. After basis reconciliation, Bob announces his data for the Bell inequality check, and Alice computes the value of the Bell parameter $S$. If $S > 2$, then the key is secure and the eavesdropper, Eve, will not have gained any useful information on the key. The secret key can then be used in any cryptographic communication between Alice and Bob.

Implementing the above requires full projective measurements in the OAM state basis $\{|\ell\rangle\}$ in a $d$-dimensional subspace, corresponding to $A_1, B_1$. This may be realized, e.g., for up to $d = 11$ using OAM mode sorters as mentioned above. However, full projective measurements whose operators have eigenstates which are OAM superpositions are also required. It is nontrivial to realize such measurements because they require unitary operations within the high-dimensional OAM subspace being considered before the OAM detection. The implementations of such operations are difficult to derive in general and have not yet been realized experimentally.

III. PROPOSED SCHEME

A. State preparation

We propose a state which replaces the need for measurements in high-dimensional rotated bases with the simplicity of a two-dimensional CHSH Bell test for the verification of the security of generated key. To appreciate how our source state relates to hybrid entangled states, consider the state expressed in terms of the composite OAM and polarization basis states $|\ell,P\rangle$ (where $\ell$ denotes the OAM, $\ell = -\infty,\ldots, +\infty$; and $P$ denotes the polarization $P = H, V$) as

$$|\Phi_n\rangle = \frac{1}{\sqrt{2d}} \sum_{n=-[d/2]}^{n=+[d/2]} |2n,H\rangle_A \otimes |2n,H\rangle_B$$

$$+ |2n-1,V\rangle_A \otimes |2n+1,V\rangle_B. \tag{3}$$

with $n \neq 0$ for even $d$. Note that this state combines $2d$-dimensional orbital angular momentum entanglement and polarization entanglement in a way similar to but quite different from the cases of the so-called hyperentangled [22], hypoentangled [23], or entangled entangled [24] states. In hyperentanglement, a measurement of OAM will not destroy polarization entanglement and vice versa. In hypoentanglement, measuring either polarization or OAM destroys entanglement in the other degree of freedom. Here measuring OAM completely destroys polarization entanglement, but the converse is not true. We note that the division of the subspaces (e.g., into odd and even OAM parities in this example) can also be done in other ways, depending on the specific realization and experimental convenience. State (3) can be rewritten, as

$$|\Phi_n\rangle = \frac{1}{\sqrt{d}} \sum_{n=-[d/2]}^{n=+[d/2]} |\phi\rangle_n, \text{ } n \neq 0 \text{ for even } d. \tag{4}$$

Here $|\phi\rangle_n$ is an entangled state within the $n$th OAM subspace. Although this state is (hypo)entangled in both polarization and OAM, only the classical correlation in OAM is strictly necessary for our scheme.

Our source state is of the form

$$|\Phi_{\text{source}}^{P/D}\rangle = \sum_{n=-[d/2]}^{n=+[d/2]} |\phi\rangle_n^{P/D}, \tag{5}$$

where $|\phi\rangle_n^{P/D}$ is an entangled state in polarization within an OAM subspace specified by $n$. The source state could be obtained either by postselection or deterministically (denoted by superscripts $P$ and $D$ respectively) as outlined below.
where \( \tau \) is a real-valued coupling coefficient which is proportional to the product of the pump amplitude and the coupling constant between the electromagnetic field and the nonlinear crystal. The source state for our scheme can then be obtained by final postselection on the state represented by Eq. (3). This can be done by registering only the values of \( n \) for which both Alice and Bob have a single detection per OAM subspace in one run. To achieve this, it suffices to use detectors which distinguish among zero, one, and more than one photon. Such detectors have been experimentally demonstrated [27,28]. Also, actual photon-number-resolving detectors have been realized (e.g., see Refs. [29,30]) with increased detection efficiencies [31].

2. State preparation: Deterministic case

A more suitable approach, however, is to prepare the source state in a deterministic way by, e.g., using an array of \( d \) polarization-entangled-photon sources (EPS) generating exactly one photon pair at a time. Existing semiconductor quantum dot (QD) systems provide a suitable platform for single-photon generation [32,33], as well as generation of entangled photon pairs on demand with high efficiency [34]. Rapid experimental progress is also being made towards implementing arrays consisting of several QD high-fidelity-entangled-photon-pair emitters on the same chip [35]. Here, we propose a setup utilizing \( d \) EPS (see Fig. 2). OAM of \( \ell = n \), for example, is then individually imprinted on photons emitted by the \( n \)th source to yield state \( |\phi_n\rangle \), resulting in basis states that are assigned as shown below. The photons in an entangled pair are usually generated using the biexciton-exciton-vacuum cascade and are separable based on their wavelength. Individual photons from different pairs may then be combined into one beam using an OAM combiner (i.e., a coherent OAM sorter operated in reverse) to obtain the source state \( |\Phi_n^{\ell}\rangle \) [Eq. (5)]. For this case, the entangled state \( |\Phi_n^{\ell}\rangle \)
implement the randomly chosen measurement. HWP3 and PBS6 are used for polarization analysis in the Bell test. As in Fig. 1, OAM sorting (e.g., using beam splitters) on Alice’s and Bob’s side. For the Bell test, Alice (Bob) sets the half-wave plate (HWP3) orientation angle to

is used to resolve the qubit subspaces and/or establish the key.

(b) Suggested measurement setup for Alice (Bob). Measurements 1, 2, and 3, i.e., 

the source state using an array of single-entangled-photon-pair sources (EPS), spatial light modulators (SLMs), splitters, and OAM combiners.

channel), and

and

To achieve the simultaneous measurements for the case of

orthogonal polarizations of Alice’s and Bob’s photons within

above, Alice and Bob need to first perform local operations

except for a change in the basis state assignment of the

method of state preparation.

We note that the source state [Eq. (5)] is essentially the

|n,H⟩′|n,V⟩′ = |n,H⟩A ⊗ |n,V⟩B,  

|V,A⟩n,H⟩′ = |n,VA⟩H ⊗ |n,H⟩B,  

|V,A⟩n,V⟩′ = |n,VA⟩V ⊗ |n,V⟩B.

Note that this only causes a transformation of the basis states defined in Eq. (7) as follows:

\[
\begin{align*}
\hat{Q}_A &= \sum_{n=1}^{d} |2n,H⟩_A \langle 2n,H|_A + |2n,V⟩_A \langle 2n - 1, V|_A, \\
\hat{Q}_B &= \sum_{n=1}^{d} |2n,H⟩_B \langle 2n,H|_B + |2n,V⟩_B \langle 2n - 1, V|_B.
\end{align*}
\]

A combination of a HWP and a PBS can now carry out the Bell-test polarization measurements (A1,2 or B1,2) for each value of n.

We can write the CHSH inequality in the nth subspace as

\[
S_n = E_n(A_1, B_1) - E_n(A_1, B_2) + E_n(A_2, B_1) + E_n(A_2, B_2) \leq 2,
\]

where the correlation coefficients of the measurement A_i performed by Alice and B_j by Bob are defined as

\[
P_n(A_i = B_j) = P_n(A_i = B_j) - P_n(A_i \neq B_j).
\]

P_n(A_i = B_j) and P_n(A_i \neq B_j) are probabilities for equal and unequal outcomes respectively, determined experimentally using the coincidence rates within each nth subspace. The detector settings for the CHSH Bell inequality violation could be specified as measurements in the bases \{|m+⟨θ⟩⟩, |m−⟨θ⟩⟩\},
where
\[ |m_+(\theta)\rangle = -\cos(2\theta)|\pm 2n, H\rangle + \sin(2\theta)|\pm 2n, V\rangle, \]
\[ |m_-(\theta)\rangle = \sin(2\theta)|\pm 2n, H\rangle + \cos(2\theta)|\pm 2n, V\rangle. \] (16)

In the ± sign above, + applies to Alice and − applies to Bob. A half-wave plate oriented at an angle $\theta$ rotates the measurement basis of a polarizing beam splitter (PBS), i.e., $|\langle H |, |V \rangle \rangle$ to $|\langle m_+(\theta) |, |m_-(\theta) \rangle \rangle$). If we set
\[ \theta_1^a = 0, \theta_2^a = \pi/8, \theta_1^b = \pi/16, \text{and} \theta_2^b = 3\pi/16 \] (17)
as values of $\theta$ for $A_1, A_2, B_1$, and $B_2$ respectively so that Alice and Bob always measure in bases which are mutually unbiased with respect to each other, then we will ensure the commutativity of Alice’s and Bob’s measurement outcomes and get the maximal violation of $2\sqrt{2}$ for each nth subspace of state (5).

Obtaining the statistical data for the Bell test requires either carrying out a detection which resolves both polarization and OAM or, as illustrated in Fig. 1(b), reversing operation $\hat{Q}(\hat{A})$ to re-establish OAM-polarization entanglement (using SLM2 and PBS4), and then carrying out OAM detection. We define the operations to reverse $\hat{Q}(\hat{A})$ as
\[ \hat{Q}_A = \sum_{n=1}^{d} (2n, H)_A (2n, H|_A + |2n, V\rangle}_A (2n + 1, V|_A), \]
\[ \hat{Q}_B = \sum_{n=1}^{d} (-2n, H)_B (-2n, H|_B + -2n, V\rangle}_B (-2n + 1, V|_B). \] (19)

Since the state within the nth subspace [Eq. (6)] is maximally entangled, it gives a maximal violation of the CHSH inequality based on operator (18)
\[ S_n(|\phi\rangle_n \langle \phi|_n) = \text{Tr} (\hat{S}_n |\phi\rangle_n \langle \phi|_n) = 2\sqrt{2} \geq 2. \] (20)

2. Measurement: Deterministic case

When the state is prepared deterministically as described in Sec. III A 2, operators $\hat{Q}_A$ and $\hat{Q}_B$ [Eqs. (12) and (19)] are not necessary for the measurements. As in the nondeterministic case, the Bell test is carried out using a combination of a HWP and PBS [see Fig. 2(b)], but photon number resolution and final postselection are not required. Due to the difference in basis assignment in this case, we redefine the detector settings for the CHSH Bell inequality violation as measurements in the bases $|m_+(\theta)\rangle, |m_-(\theta)\rangle$, where
\[ |m_+(\theta)\rangle' = -\cos(2\theta)|n, H\rangle + \sin(2\theta)|n, V\rangle, \]
\[ |m_-(\theta)\rangle' = \sin(2\theta)|n, H\rangle + \cos(2\theta)|n, V\rangle. \] (21)

The optimum settings (specified by $\theta$) for the HWP are the same as in Eq. (17) above, and the resulting Bell operator for this case [see Eq. (11)] is
\[ \hat{S}_n = \sqrt{2}(|H, A|_n \langle H, A, B|_n + |V, A, B\rangle_n \langle V, A, B|_n \]
\[ + |H, A, B\rangle_n \langle V, A, B|_n + |V, A, B\rangle_n \langle H, A, B|_n \]
\[ - |H, A, B\rangle_n \langle H, A, B|_n - |V, A, B\rangle_n \langle V, A, B|_n \]
\[ + |H, A, B\rangle_n \langle V, A, B|_n + |V, A, B\rangle_n \langle H, A, B|_n \}. \] (22)

The state represented by Eq. (10) is also maximally entangled within the nth subspace for this case, and it gives a maximal violation of the CHSH inequality based on operator (22) when the key has not been eavesdropped.

C. Security against collective attacks

Any eavesdropping of the key is essentially a measurement strategy that will destroy polarization entanglement which is used to establish the key. This in turn degrades the CHSH Bell inequality violation [1] in any respective OAM subspaces. A collective attack is one in which the eavesdropper (Eve) applies the same operation on each of Alice’s and Bob’s particles, but has no other limitations. In particular, she is allowed to have access to a string of qubits from Alice or Bob at one time, and to other dimensions of their particle states, even possibly unknown to Alice or Bob. Since Eq. (5) is a product state of $d$ entangled qubits pairs, our scheme is essentially a multiplexing of multiple polarization-entangled qubit pairs by means of a higher-dimensional degree of freedom, followed by independently testing the CHSH Bell inequality simultaneously—Eve’s access to one or more source states in our scheme is equivalent to her access to a string of qubits on which she can perform joint (coherent) measurements. Therefore, the security of our scheme is completely guaranteed by the security of the individual qubit-based schemes against collective attacks [16]. This, in turn, implies security against the most general, so-called coherent attacks [16,39] if an application of the exponential quantum de Finetti theorem can be made [40]. This is indeed the case in our scheme (under the assumption of finite-dimensional subsystems) because our source state is invariant under permutation of Alice and Bob, and their measurement outcomes are commutative, as mentioned above [Eq. (17)]. These results apply fully to our large-alphabet protocol since it is equivalent to simultaneous but independent 2-qubit secure protocols. The total bit rate generated securely against collective attacks as a function of Bell parameters $S_n$ can therefore be written as [17]
\[ r \geq \sum_n 1 - h(Q_n) - h \left(1 + \sqrt{(S_n/2)^2 - 1}\right) \]. (23)
bit-error rate (QBER) $Q$, and Bell parameter for each channel is the same, i.e., $Q_n = Q$ and $S_n = S$ respectively for all $n$. Our scheme shows a $d$-fold enhancement in secure key rate.

IV. CONCLUSION

Our scheme offers significant advantages over current generalized E91 schemes. It results in a greatly simplified security verification and key generation setup which does not get more complicated with increasing $d$, except for an increase in the number of output ports of the OAM sorting device. It thereby provides a route to boosting the secure key rates in entanglement-based QKD without the usual increased complexity of Bell tests in high dimensions. It also benefits from the relative tolerance of two-dimensional Bell tests to measurement error. Although it is known that the amount of violation for an actual $D$-dimensional Bell test increases with $D$, these increments are marginal even in the ideal case and level off as $D$ increases [20,43]. Also, the high sensitivity of the complicated measurement setup to errors will usually overwhelm these increments even for modest values of $D$, resulting in smaller violations than in the qubit case. Another advantage of our scheme where an SPDC source is used is that nonmaximal high-dimensional entanglement will not generally degrade the verification of security. For example, the spiral bandwidth [44] of the SPDC source will not generally degrade Bell violation, but will only limit the effective number of OAM channels in the nondeterministic case. In contrast, if generalized OAM-based Bell tests are used without procrustean filtering, then a small spiral bandwidth might cause a failure of the Bell test for an entangled state [4].

In summary, this paper has described a practical scheme in which a single CHSH-Bell test setup combined with a full projective measurement is sufficient for security verification even for a large-alphabet scheme capable of arbitrarily large key rates per run. The scheme is simpler to implement than existing generalizations of E91 protocol to high dimensions because it circumvents measurements in mutually unbiased bases in high dimensions while maintaining capacity for large key rates and security against collective attacks. A second significant advantage is that nonmaximal high-dimensional entanglement will not necessarily degrade the verification of security. We point out that the scheme is realizable using current technology by mentioning two examples for generating applicable source states, namely, spontaneous parametric down conversion and, more suitably, source of single pairs of entangled photons, such as semiconductor quantum dots. From the point of view of real-world applications of high-dimensional QKD based on photon OAM in free space, judicious selection of basis states [45,46] will increase resilience against decoherence induced by atmospheric turbulence in a free space implementation. Although this can be applied within the framework of this scheme, implementations with time bins [10,47] or paths appear especially promising for long-distance applications. The complexity of security verification in large-alphabet entanglement-based QKD makes it apparent that the simplified scheme presented here will likely enable otherwise infeasible secure key rates in QKD, enabling more practical implementations of entanglement-based technologies.

ACKNOWLEDGMENTS

The author acknowledges the Engineering and Physical Sciences Research Council (EPSRC [Grants No. EP/I023186/1 and No. EP/K015338/1]) and the Scottish Universities Physics Alliance (SUPA) for funding; Brian Gerardot and Gerald Buller for support; and Ryan Warburton, Jonathan Leach and Miles Padgett for stimulating discussions.

---


FIG. 3. (Color online) Comparison of the minimum secure key rate $r_{\text{min}}$ as a function of the Bell parameter $S$ and the quantum bit-error rate (QBER) $Q$, in a single run, for our scheme with a qubit-based E91-type protocol [17,18]. We assume that the quantum bit-error rate $Q$ and Bell parameter for each channel is the same, i.e., $Q_n = Q$ and $S_n = S$ respectively for all $n$. Our scheme shows a $d$-fold enhancement in secure key rate.