optica

High-dimensional intracity quantum cryptography with structured photons: supplementary material

Alicia Sit[1], Frédéric Bouchard[1], Robert Fickler[1], Jérémie Gagnon-Bischoff[1], Hugo Larocque[1], Khabat Heshami[2], Dominique Elser[3,4], Christian Peuntinger[3,4], Kevin Günthner[3,4], Bettina Heim[3,4], Christoph Marquardt[3,4], Gerd Leuchs[1,3,4], Robert W. Boyd[1,5], and Ebrahim Karimi[1,6,*]

[1]Physics Department, Centre for Research in Photonics, University of Ottawa, Advanced Research Complex, 25 Templeton, Ottawa ON K1N 6N5, Canada

[2]National Research Council of Canada, 100 Sussex Drive, Ottawa ON K1A 0R6, Canada

[3]Max-Planck-Institut für die Physik des Lichts, Staudtstraße 2, 91058 Erlangen, Germany

[4]Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany

[5]Institute of Optics, University of Rochester, Rochester, New York, 14627, USA

[6]Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran

*Corresponding author: ekarimi@uottawa.ca

Published 24 August 2017

This document provides supplementary information to "High-dimensional intracity quantum cryptography with structured photons," https://doi.org/10.1364/optica.4.001006.

https://doi.org/10.6084/m9.figshare.5248189

1. MUTUALLY UNBIASED BASIS

Given a set of bases $\alpha_0, \ldots, \alpha_n$ of dimension d, they are said to be mutually unbiased with respect to one another if they satisfy the following condition,

$$|^{j}\langle\alpha_i|\alpha_{i'}\rangle^{j'}|^2 = \begin{cases}\delta_{j,j'} & \forall\ i = i' \\ \frac{1}{d} & \forall\ i \neq i'\end{cases};\quad i \in \{0,1,...n\},\ \ j \in \{1,2,..,d\}. \tag{S1}$$

For dimensions where d is a power of a prime, $d+1$ mutually unbiased bases (MUBs) can be found. For 2-dimensional quantum key distribution (QKD) protocols, photons can be encoded using polarization and orbital angular momentum (OAM). We represent states of light that have a particular polarization and OAM value using a compound ket notation. In this way, if a photon has a certain polarization Π and carries ℓ units of OAM, it is written as $|\Pi, \ell\rangle$.

The two MUBs of dimension 2 are given by,

$$\begin{aligned}\{|\zeta\rangle^i\} &= \left\{\frac{1}{\sqrt{2}}\left(|L,-\ell\rangle + |R,+\ell\rangle\right), \frac{1}{\sqrt{2}}\left(|L,-\ell\rangle - |R,+\ell\rangle\right)\right\},\\ \{|\xi\rangle^j\} &= \left\{\frac{1}{\sqrt{2}}\left(|L,-\ell\rangle + i\,|R,+\ell\rangle\right), \frac{1}{\sqrt{2}}\left(|L,-\ell\rangle - i\,|R,+\ell\rangle\right)\right\}.\end{aligned} \tag{S2}$$

In dimension 4, the natural basis is $|k\rangle \in \{|H,\ell\rangle, |H,-\ell\rangle, |V,\ell\rangle, |V,-\ell\rangle\}$, and the two sets of MUBs $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$ were generated by the following matrices,

$$\mathcal{M}_0^{ik} = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},$$

$$\mathcal{M}_1^{jk} = \frac{1}{2}\begin{pmatrix}1&i&1&-i\\1&i&-1&i\\1&-i&1&i\\-1&i&1&i\end{pmatrix}, \tag{S3}$$

such that $|\psi\rangle^i = \mathcal{M}_0^{ik}|k\rangle$ and $|\varphi\rangle^j = \mathcal{M}_1^{jk}|k\rangle$. This results in the following states:

$$\{|\psi\rangle^i\} = \{|H,+\ell\rangle, |H,-\ell\rangle, |V,+\ell\rangle, |V,-\ell\rangle\}, \tag{S4}$$

$$\begin{aligned}\{|\varphi\rangle^j\} = \Big\{&\frac{1}{\sqrt{2}}(|L,\ell\rangle + |R,-\ell\rangle), \frac{1}{\sqrt{2}}(|L,\ell\rangle - |R,-\ell\rangle),\\ &\frac{1}{\sqrt{2}}(|L,-\ell\rangle + |R,\ell\rangle), \frac{1}{\sqrt{2}}(|L,-\ell\rangle - |R,\ell\rangle)\Big\}.\end{aligned} \tag{S5}$$

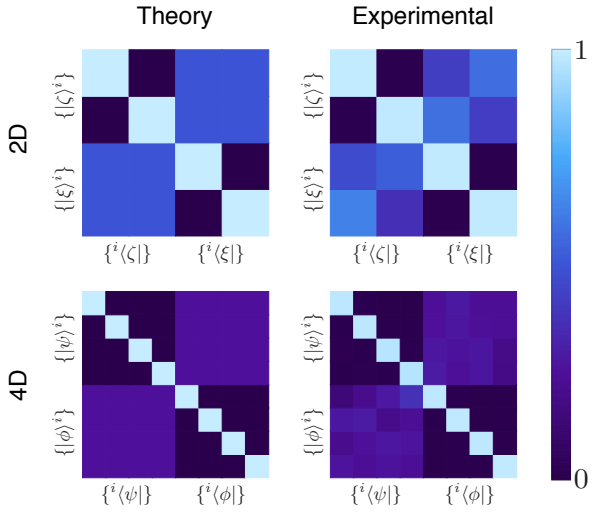

Fig. S1. Visualization of MUBs in d=2 and d=4 Theoretical probability-of-detection matrices (left column) for dimensions 2 and 4 using Eq. (S2) and Eqs. (S4–S5) by applying Eq. (S1). The probability-of-detection matrices as measured in the laboratory (right column) give bit error rates of 0.83% and 1.83% in dimensions 2 ($\ell = 2$) and 4 ($\ell = 2$), respectively.

Figure S1 shows a visual representation of the 2D (top row) and 4D (bottom row) MUBs using Eq. (S1), comparing the theoretical probability-of-detection matrix to the experimental one as measured in the laboratory, i.e. without the intra-city link. The quantum bit error rate is calculated as one minus the average of the on-diagonal elements. The calculated quantum bit error rates from the experimentally measured matrices are 0.83% and 1.83% in dimensions 2 ($\ell = 2$) and 4 ($\ell = 2$), respectively.

2. GENERATION OF IMPLEMENTED MUBS IN $D = 2$ AND 4

In order to create structured photons possessing both polarization and OAM, we utilize patterned liquid crystal devices known as q-plates. Q-plates coherently couple spin (i.e. polarization) to orbital angular momentum such that $\ell = \pm 2q$, where q is the topological charge of the liquid crystal distribution. The action of a q-plate is as follows:

$$|L,0\rangle \xrightarrow{q-plate} |R,+2q\rangle\,, \tag{S6}$$

$$|R,0\rangle \xrightarrow{q-plate} |L,-2q\rangle\,. \tag{S7}$$

Since q-plates are linear devices, a photon in a superposition of $|L,0\rangle$ and $|R,0\rangle$ will be mapped to a state in a superposition of $|R,+2q\rangle$ and $|L,-2q\rangle$. Thus, just as waveplates are used to transform polarization states on the Poincaré sphere, waveplates in combination with a q-plate perform the same transformations on a hybrid OAM-Poincaré sphere.

The MUBs in dimension 2, $\{|\zeta\rangle^i\}$ and $\{|\xi\rangle^j\}$ are generated using the sequence of a half-wave plate (HWP) followed by a q-plate. The waveplate angles are given in (S8).

state	HWP
$\|\zeta\rangle^1$	0°
$\|\zeta\rangle^2$	+45°
$\|\xi\rangle^1$	+22.5°
$\|\xi\rangle^2$	−22.5°

(S8)

The MUBs in dimension 4, $\{|\psi\rangle^i\}$ and $\{|\varphi\rangle^j\}$ are generated by sandwiching a q-plate between either HWPs or QWPs. If photons pass left to right through the following optical elements, the waveplate angles that Alice uses to generate $\{|\psi\rangle^i\}$ are given in the (S9), and $\{|\varphi\rangle^j\}$ in (S10).

state	QWP before QP	QWP after QP
$\|\psi\rangle^1$	−45°	−45°
$\|\psi\rangle^2$	+45°	+45°
$\|\psi\rangle^3$	−45°	+45°
$\|\psi\rangle^4$	+45°	−45°

(S9)

state	HWP before QP	HWP after QP
$\|\varphi\rangle^1$	0°	0°
$\|\varphi\rangle^2$	+45°	0°
$\|\varphi\rangle^3$	0°	–
$\|\varphi\rangle^4$	+45°	–

(S10)

Bob uses the same waveplate angles, but mirrors the sequence of waveplates as Alice has in order to project his received photons onto a particular state.

3. EXPERIMENTAL DATA

Coincidence counts are accumulated per 200 ms. For each of Bob's measurements, he records fifty data points. Bob obtains a probability-of-detection matrix by averaging the data points for each measurement and then normalizing over each state that Alice sends. The states that Alice sends and the states that Bob projects onto are labelled on the left and top, respectively, of each matrix below.

Normalized raw data for probability-of-detection matrix in dimension 2 as measured across the intra-city link using a q=1/2-plate, as shown in Fig. 3a of the main text (top row):

	${}^1\langle\zeta\|$	${}^2\langle\zeta\|$	${}^1\langle\xi\|$	${}^2\langle\xi\|$
$\|\zeta\rangle^1$	0.971	0.029	0.421	0.579
$\|\zeta\rangle^2$	0.062	0.938	0.677	0.323
$\|\xi\rangle^1$	0.731	0.269	0.959	0.041
$\|\xi\rangle^2$	0.459	0.541	0.068	0.932

(S11)

Target corrected data from (S11):

	${}^1\langle\zeta\|$	${}^2\langle\zeta\|$	${}^1\langle\xi\|$	${}^2\langle\xi\|$
$\|\zeta\rangle^1$	0.972	0.028	0.351	0.649
$\|\zeta\rangle^2$	0.050	0.950	0.653	0.347
$\|\xi\rangle^1$	0.725	0.275	0.961	0.039
$\|\xi\rangle^2$	0.463	0.537	0.069	0.931

(S12)

Normalized raw data for probability-of-detection matrix in dimension 4 as measured across the intra-city link:

	${}^1\langle\psi\|$	${}^3\langle\psi\|$	${}^2\langle\psi\|$	${}^4\langle\psi\|$	${}^1\langle\varphi\|$	${}^2\langle\varphi\|$	${}^3\langle\varphi\|^3$	${}^4\langle\varphi\|$
$\|\psi\rangle^1$	0.918	0.019	0.051	0.012	0.252	0.245	0.275	0.228
$\|\psi\rangle^3$	0.020	0.937	0.038	0.005	0.190	0.192	0.312	0.306
$\|\psi\rangle^2$	0.012	0.156	0.816	0.012	0.279	0.277	0.289	0.155
$\|\psi\rangle^4$	0.149	0.009	0.018	0.824	0.152	0.195	0.384	0.269
$\|\varphi\rangle^1$	0.319	0.125	0.325	0.231	0.869	0.039	0.064	0.029
$\|\varphi\rangle^2$	0.252	0.217	0.239	0.292	0.038	0.822	0.042	0.098
$\|\varphi\rangle^3$	0.185	0.177	0.447	0.191	0.065	0.027	0.872	0.037
$\|\varphi\rangle^4$	0.207	0.205	0.381	0.208	0.030	0.134	0.036	0.800

(S13)

Target corrected data from (S13), as shown in Fig. 3a of the main text (bottom row):

	${}^1\langle\psi\|$	${}^3\langle\psi\|$	${}^2\langle\psi\|$	${}^4\langle\psi\|$	${}^1\langle\varphi\|$	${}^2\langle\varphi\|$	${}^3\langle\varphi\|^3$	${}^4\langle\varphi\|$
$\|\psi\rangle^1$	0.924	0.035	0.011	0.031	0.272	0.232	0.254	0.243
$\|\psi\rangle^3$	0.024	0.960	0.012	0.004	0.197	0.213	0.260	0.330
$\|\psi\rangle^2$	0.005	0.052	0.930	0.013	0.239	0.301	0.301	0.159
$\|\psi\rangle^4$	0.049	0.004	0.029	0.918	0.094	0.242	0.433	0.232
$\|\varphi\rangle^1$	0.376	0.108	0.321	0.195	0.874	0.033	0.065	0.028
$\|\varphi\rangle^2$	0.273	0.197	0.255	0.275	0.035	0.825	0.045	0.096
$\|\varphi\rangle^3$	0.200	0.132	0.511	0.157	0.060	0.016	0.889	0.035
$\|\varphi\rangle^4$	0.186	0.163	0.365	0.287	0.026	0.129	0.043	0.803

Normalized raw data for probability-ofdetection matrix in dimension 4 on a turbulent night:

	${}^1\langle\psi\|$	${}^3\langle\psi\|$	${}^2\langle\psi\|$	${}^4\langle\psi\|$	${}^1\langle\varphi\|$	${}^2\langle\varphi\|$	${}^3\langle\varphi\|^3$	${}^4\langle\varphi\|$
$\|\psi\rangle^1$	0.741	0.032	0.043	0.184	0.370	0.168	0.364	0.098
$\|\psi\rangle^3$	0.096	0.722	0.138	0.044	0.120	0.432	0.221	0.228
$\|\psi\rangle^2$	0.043	0.177	0.755	0.025	0.276	0.247	0.197	0.281
$\|\psi\rangle^4$	0.101	0.041	0.047	0.811	0.122	0.433	0.332	0.113
$\|\varphi\rangle^1$	0.126	0.471	0.197	0.206	0.707	0.051	0.144	0.098
$\|\varphi\rangle^2$	0.211	0.234	0.352	0.203	0.110	0.694	0.079	0.117
$\|\varphi\rangle^3$	0.265	0.285	0.259	0.191	0.195	0.056	0.632	0.117
$\|\varphi\rangle^4$	0.478	0.146	0.185	0.191	0.048	0.103	0.075	0.775

(S14)

4. NUMERICAL APPROACH FOR THE SECRET KEY RATE CALCULATION

Here we use a numerical approach to calculate the secret key rate for the MUBs in the current experiment that are shown in Eqs. (S3–S5). The secret key rate calculation below relies on the dual optimization problem that has recently been introduced as an efficient numerical approach for unstructured quantum key distribution [1]. The main result in [1] indicates that the achievable secure key rate is lower bounded by the following maximization problem,

$$K \geq \frac{\Theta}{\ln 2} - H(Z_A|Z_B), \tag{S15}$$

where

$$\Theta := \max_{\vec{\lambda}} \left(-\left\| \sum_j Z_A^j R(\vec{\lambda}) Z_A^j \right\| - \vec{\lambda}\cdot\vec{\gamma} \right), \tag{S16}$$

and

$$R(\vec{\lambda}) := \exp\left(-\mathbb{1} - \vec{\lambda}\cdot\vec{\Gamma}\right). \tag{S17}$$

Here Z_A (Z_B) denotes the measurement performed by Alice (Bob) to derive the raw key, and $\vec{\gamma} = \{\gamma_i := \mathrm{Tr}(\rho_{AB}\Gamma_i)\}$ are determined through average value of experimental measurements.

For the generalized BB84 in dimension $d = 4$ with two MUBs, the experimental constraints can be summarized to

$$\text{Key-map POVM:} \quad Z_A = \left\{ |\psi\rangle^i\langle\psi|, \text{for} \quad i = 1\cdots d = 4 \right\} \tag{S18}$$

$$\text{Constraints:} \quad \langle\mathbb{1}\rangle = 1 \tag{S19}$$

$$\langle \mathbf{E_X} \rangle = Q \tag{S20}$$

$$\langle \mathbf{E_Z} \rangle = Q \tag{S21}$$

where $\mathbf{E}_{\mathbf{Z}\,(\mathbf{X})}$ are coarse-grained error operators in $\mathcal{M}_{0\,(1)}$ MUBs and defined as

$$\mathbf{E_X} = \mathbb{1} - \sum_i^{d=4} |\psi\rangle^i\langle\psi| \otimes |\psi\rangle^i\langle\psi| \tag{S22}$$

$$\mathbf{E_Z} = \mathbb{1} - \sum_i^{d=4} |\varphi\rangle^i\langle\varphi| \otimes |\varphi\rangle^i\langle\varphi|. \tag{S23}$$

Eqs. (S4) and (S5) show the definition for $|\psi\rangle^i$ and $|\varphi\rangle^i$ basis states.

Figure S2 shows the numerical result of the optimization problem in Eq. (S15) with MUBs in Eqs. (S4,S5) in comparison with the theoretical key rates in [2, 3]. This numerical approach may be extended to find secret key rate per signal with two-way classical communications to tolerate higher qubit error rates [4].

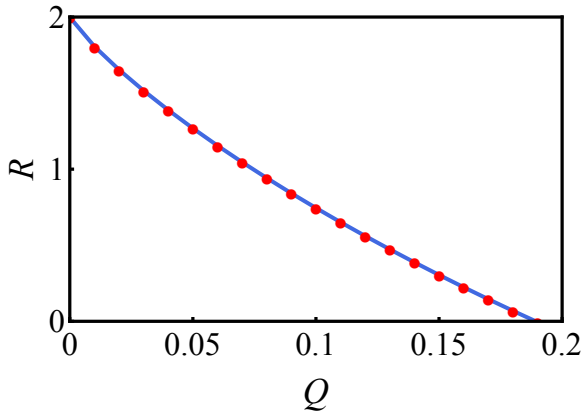

Fig. S2. Secret key rate per signal for BB84 in d=4 with 2 MUBs Solution to the numerical optimization problem in Eq. (S15) are shown for different values of average error rates (red dots). As it can be seen, the numerical optimization saturates the bound and shows a good agreement with the theory from [2, 3]. For more details on the numerical approach see [1].

REFERENCES

1. P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, "Numerical approach for unstructured quantum key distribution," Nature Communications **7**, 11712 (2016).
2. A. Ferenczi, and N. Lütkenhaus, "Symmetries in quantum key distribution and the connection between optical attacks and optimal cloning," Physical Review A **85**, 052310 (2012).
3. L. Sheridan, and V. Scarani, "Security proof for quantum key distribution using qudit systems," Physical Review A **82**, 030301 (2010).

4. G. M. Nikolopoulos, K. S. Ranade, and G. Alber, "Error tolerance of two-basis quantum-key-distribution protocols using qudits and two-way classical communication," Physical Review A **73**, 032325 (2006).