Quantum key distribution overcoming extreme noise: simultaneous subspace coding using high-dimensional entanglement

Mirdit Doda, Marcus Huber, Gláucia Murta, Matej Pivoluska, Martin Plesch, Chrysoula Vlachou

Motivation

QKD challenge: Low key rate and the high susceptibility to noise.
Is using high dimensional (HD) protocols a solution?

- More information per photon
- Better noise resistance
- Theoretical HD QKD studies suggest better rates and noise resistance

Why aren't we using HD QKD protocols in practice?

- Noise increases with dimension
- Noise differs for different experimental platforms (which one is the best one for existing protocols?)
- Noise in HD protocols comes with larger error correction overhead

Inspired by recent HD entanglement distribution noise resistance study [1] we show that extremely noisy entanglement can be indeed used for QKD in practice, beating qubit protocols in practical implementations!

Simultaneous subspace coding QKD protocol

General idea: Use a $d \times d$ dimensional entangled quantum system to perform multiple instances of a QKD protocol simultaneously in non-overlapping subspaces of size k.
Protocol:

1. Untrusted source distributes ρ_{AB} (ideally maximally entangled)
2. Two types of measurement:

A_1 Alice's computational basis measurement
A_2 Alice's subspace MUB measurement
B_1 Bob's computational basis measurement
B_2 Bob's subspace MUB measurement

			d=9	k=3			
Alice	A1	A1	A2	A1	A1	A2	A2
x	0	–	5	1	7	4	–
x'	0	–	2	–	1	1	–
Keep?	✓	✗	✓	✗	✓	✓	✗
y'	2	–	2	–	1	0	–
y	2	–	5	7	7	3	–
Bob	B1	B2	B2	B1	B1	B2	B1
Subspace (m)	0	–	1	–	2	1	–

3. Keys are post-processed (parameter estimation + error correction + privacy amplification) in each subspace simultaneously

Key rate and white noise

For each subspace m, we lower bound Devetak-Winter rate [2]:

$$K_m \geq H(X_m|E_T) - H(X_m|Y_m).$$

Total key rate is given by

$$K_{TOT} = \sum_m P(M=m)K_m\,.$$

We lower bound $H(X_m|E_T)$ by min-entropy $H_{min}(X_m|E_T)$, and

$$H_{min}(X_m|E_T) \geq -\log_2\left(\frac{\sqrt{W_k^m} + \sqrt{(k-1)\left(1-W_k^m\right)}}{k}\right),$$

where

$$W_k^m = \sum_{i=0}^{k-1} P(ii|22,m)\,.$$

The error correction overhead $H(X_m|Y_m)$ can be estimated directly from measurement data.
If we apply this to the isotropic state with visibility v,

$$K_{TOT}^{iso}(d,v,k) \geq \left(\frac{vd+k-vk}{d}\right)\log_2\left(\frac{k}{\left(\sqrt{vd+1-v}+(k-1)\sqrt{1-v}\right)^2}\right)$$
$$+\left(\frac{vd+1-v}{d}\right)\log_2(vd+1-v) + \frac{(k-1)(1-v)}{d}\log_2(1-v)\,.$$

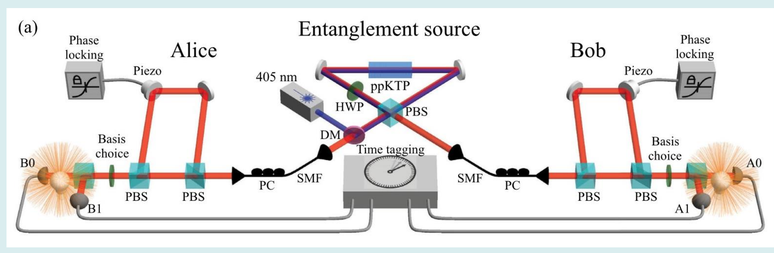
Important facts:

1. For d even and $k=2$, critical visibility is $v > \frac{1}{1+0.0893d}$, thus for any ***fixed*** visibility, there is large enough d, for which we can obtain positive key rate.
2. **The above information is misleading, because v is a function of dimension d which depends on the actual implementation!**

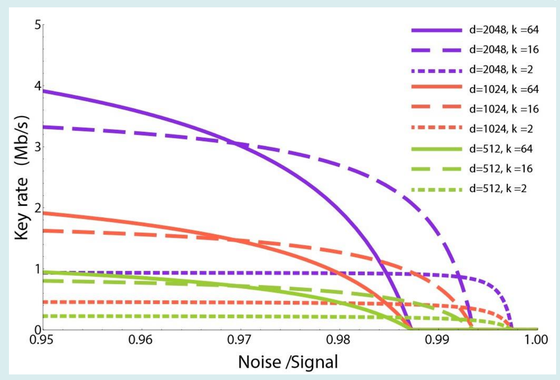
Error model

a) Source produces entangled photons according to Poisson distribution with mean λ photons per second;
b) With probability P_L each photon gets lost;
c) Detectors receive mean ν environmental photons per second;
d) Detectors have μ dark counts per second and efficiency P_C.

Time-bin encoding

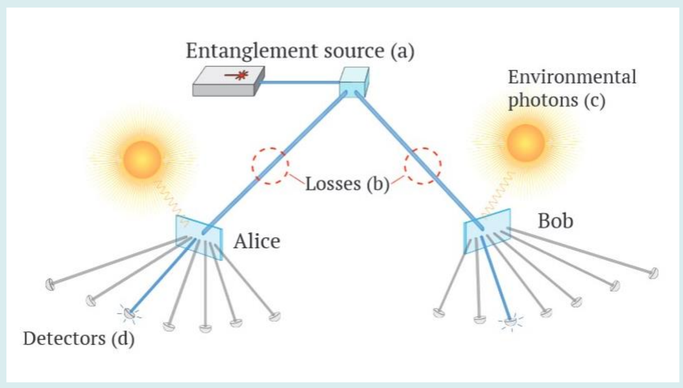


Setup: Source produces a state of two entangled photons, with two degrees of freedom: the time of arrival t of the photon at the respective labs of Alice and Bob and their polarization. The time of can be discretized by considering time bins of size t_b and setting a time frame F outside of which a photon is ``lost''. Taking F to be a multiple of t_b we have effectively a discrete system of dimension $d = \frac{F}{t_b}$.

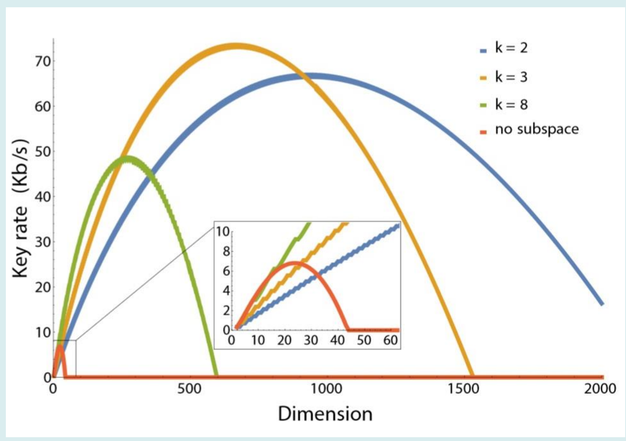


Noise-to-signal ratio is the average number of non-entangled photons that arrive in the lab (including singles and taking into account detector inefficiencies) divided by the overall average number of clicks per second, assuming that these quantities are the same for both parties.

Spatial encoding



Setup: Source produces states entangled in infinite dimensional spatial degree of freedom (e.g. angular momentum). This is projected down to d modes on each side. Notable difference to time-bin encoding is that each party now requires d detectors. For values of d above certain threshold dark counts become the dominant source of noise.



Parameters used: $P_C = 60\%; P_L = 98{,}4\%; \mu = 300; \nu = 2000;$
$\lambda = 40000; \Delta t = 10^{-7}s$

Acknowledgements: MH acknowledges funding from the Austrian Science Fund (FWF) through the START project Y879-N27.CV acknowledges support from the Belgian Fonds de la Recherche Scientifique -- FNRS, under grant no R.50.05.18.F (QuantAlgo). The QuantAlgo project has received funding from the QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union's Horizon 2020 Programme. GM is funded by the Deutsche Forschungsgemeinschaft (DFG, German ResearchFoundation) under Germany's Excellence Strategy – Cluster of ExcellenceMatter and Light for Quantum Computing (ML4Q) EXC 2004/1 – 390534769.MD, MPi and MPI acknowledge funding from VEGA project 2/0136/19. MPi and MPI additionally acknowledge GAMU project MUNI/G/1596/2019.

Bibliography
[1] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber
Phys. Rev. X 9, 041042, 2019
[2] I. Devetak and A. Winter, Proceedings of the Royal So-ciety of London Series A461, 207,2005