Pathways for entanglement based quantum communication in the face of high noise

Xiao-Min Hu, Chao Zhang, Yu Guo, Fang-Xiang Wang, Wen-Bo Xing, Cen-Xiao Huang, Bi-Heng Liu, Yun-Feng Huang, Chuan-Feng Li, Guang-Can Guo, Xiaoqin Gao, Matej Pivoluska, and Marcus Huber

arXiv:2011.03005 — accepted to PRL

School of Physical Sciences
University of Science and Technology of China

ÖAW IQOQI Vienna

VCQ

TU WIEN

u Ottawa

UNIVERSITAS MASARYKIANA BRUNENSIS

SAV

Motivation for noise resistant QKD

- QKD is a leading application of quantum information science
- Practical implementations are susceptible to noise
- Noise hinders:

1. Achievable key rates
2. Transmission distances

- Improving noise resistance is one of the key remaining challenges
- We approach the problem by encoding information into d-dimensional photonic degrees of freedom (qudits)

Can large-alphabet encoding help?

- Using large alphabet encodings into *d*-dimensional physical degrees of freedom (qudits) instead of binary encoding (qubits) was proposed already more than 20 years ago[1]
- Better noise resistance and key rates were anticipated
- Practical manipulation of qudits became possible much more recently
- Existing practical implementations brought better achievable key rates[2], but not better noise resistance
- Reason: In practice, noise increases non-trivially with dimension *d*

[1] H. Bechmann-Pasquinucci and W. Tittel, **Phys. Rev. A 61, 062308 (2000)**
[2] N. T. Islam, C. C. W. Lim, C. Cahall, B. Qi, J. Kim,and D. J. Gauthier, **Quantum Science and Technology 4,035008 (2019)**

QKD implementation and analysis details

- Entanglement based
- Discrete variables
- Trusted devices
- Asymptotic key rates

Three main ideas

1. Qudit entanglement is in practice more noise resistant than qubit entanglement[3] – entanglement in subspaces can be detected even for very noisy channels
2. Noise resistance of qudit entanglement can be leveraged to noise resistant QKD with simultaneous subspace encoding [4]
3. Encoding information into path degree of freedom of photons is a very versatile technique allowing for high-fidelity multi-outcome measurements, required for subspace QKD[5]

[3] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, M. Huber, **Phys. Rev. X 9, 041042 (2019)**

[4] M. Doda, M. Huber, G. Murta, M. Pivoluska, M. Plesch, and C. Vlachou, **Phys. Rev. Applied15, 034003 (2021)**

[5] X.-M. Hu, W.-B. Xing, B.-H. Liu, Y.-F. Huang, C.-F. Li,G.-C. Guo, P. Erker, and M. Huber, **Phys. Rev. Lett.125, 090503 (2020)**

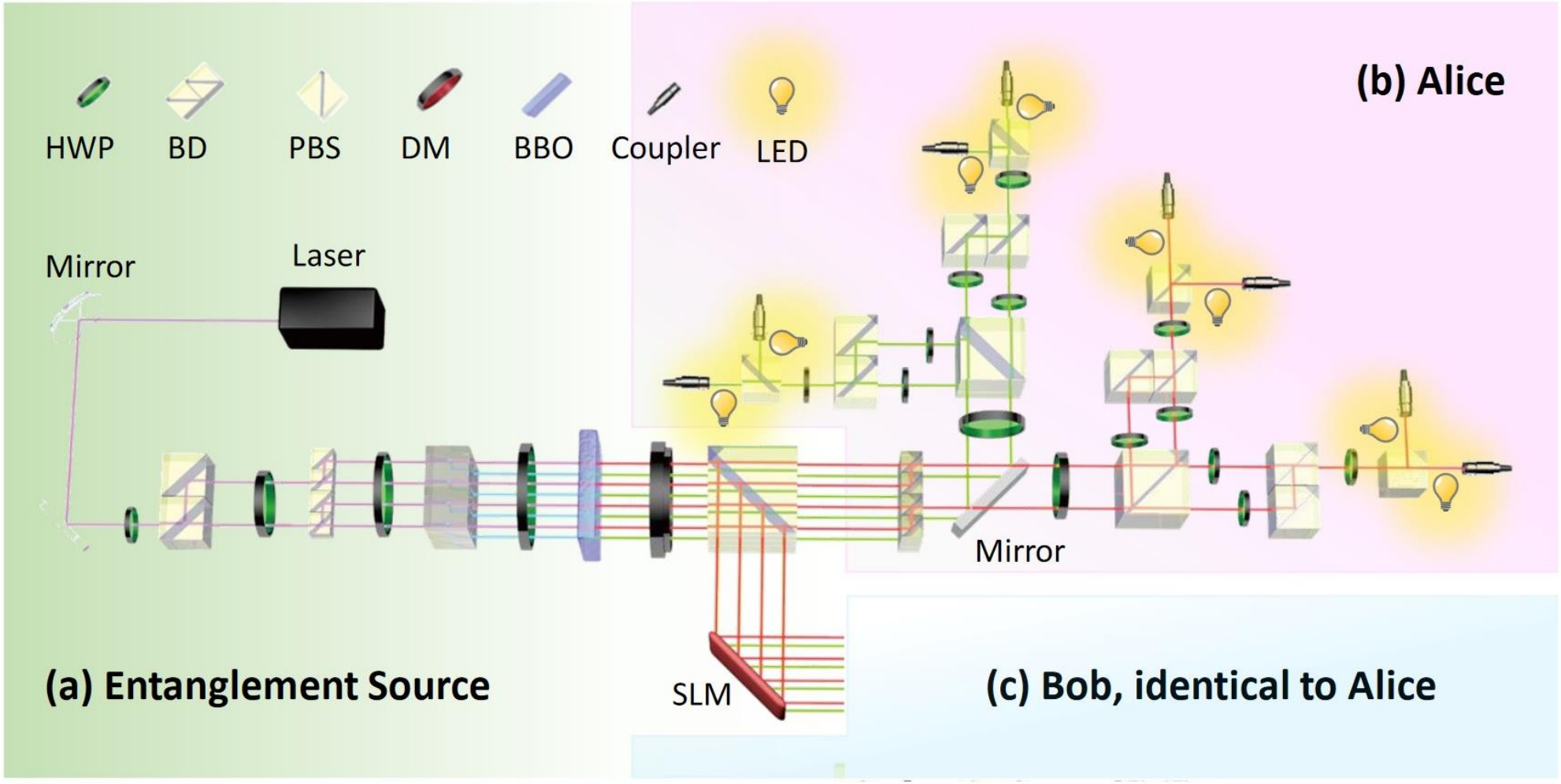
QKD with subspace encoding

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 $d \times d$ maximally entangled state $|\psi\rangle_d = \sum_{i=0}^{d-1} \frac{1}{\sqrt{d}} |ii\rangle$)
2. Two types of measurement chosen at random:
   - A_k/B_k – Alice's/Bob's computational basis measurement
     (Example $d = 4, k = 2 : \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$)
   - A_t/B_t – Alice's/Bob's subspace MUB measurement
     (Example $d = 4, k = 2 : \{|0\rangle + |1\rangle, |0\rangle - |1\rangle, |2\rangle + |3\rangle, |2\rangle - |3\rangle\}$)
3. Subspace post-selection: Only outcomes in the same subspace are kept
4. Key rate fraction in subspace of size k: $K \geq \log_2(k) - H(\vec{e}_k) - H(\vec{e}_t)$

Implementation using path entanglement



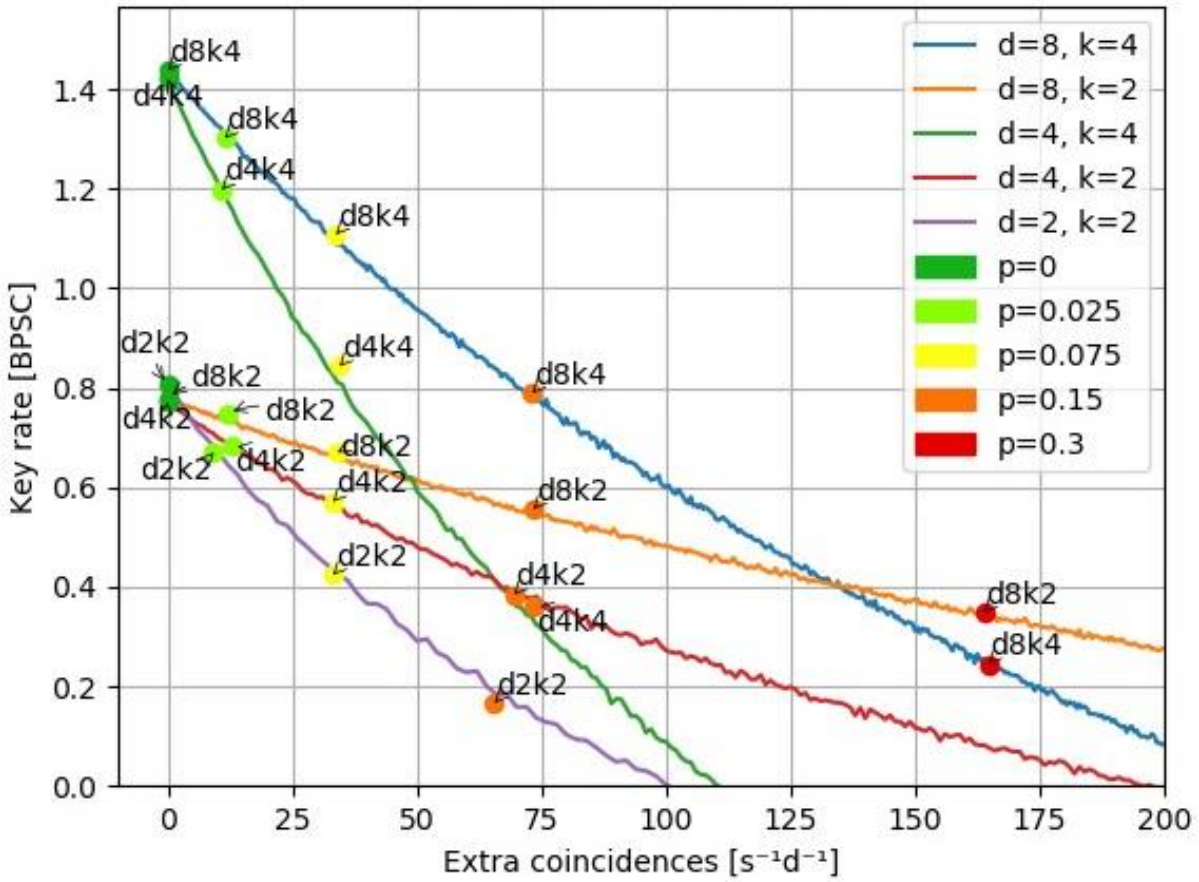
Noise simulation

- We use 16 adjustable LEDs to simulate noisy environment (1 for each coupler)
- This allows us to precisely control extra singles S injected in each detector per second
- Each lab therefore receives dS extra singles per second
- In our experiment we can disregard multi-click events as they are very rare and the number of extra coincidences per second is estimated as

$$\boldsymbol{C = 2 \times d \times S \times d \times S \times \tau}$$

- Coincidence window length is $\tau = 5 \times 10^{-9} s$
- How to fairly compare protocols with different d and k?

Comparison 1 – Isotropic noise

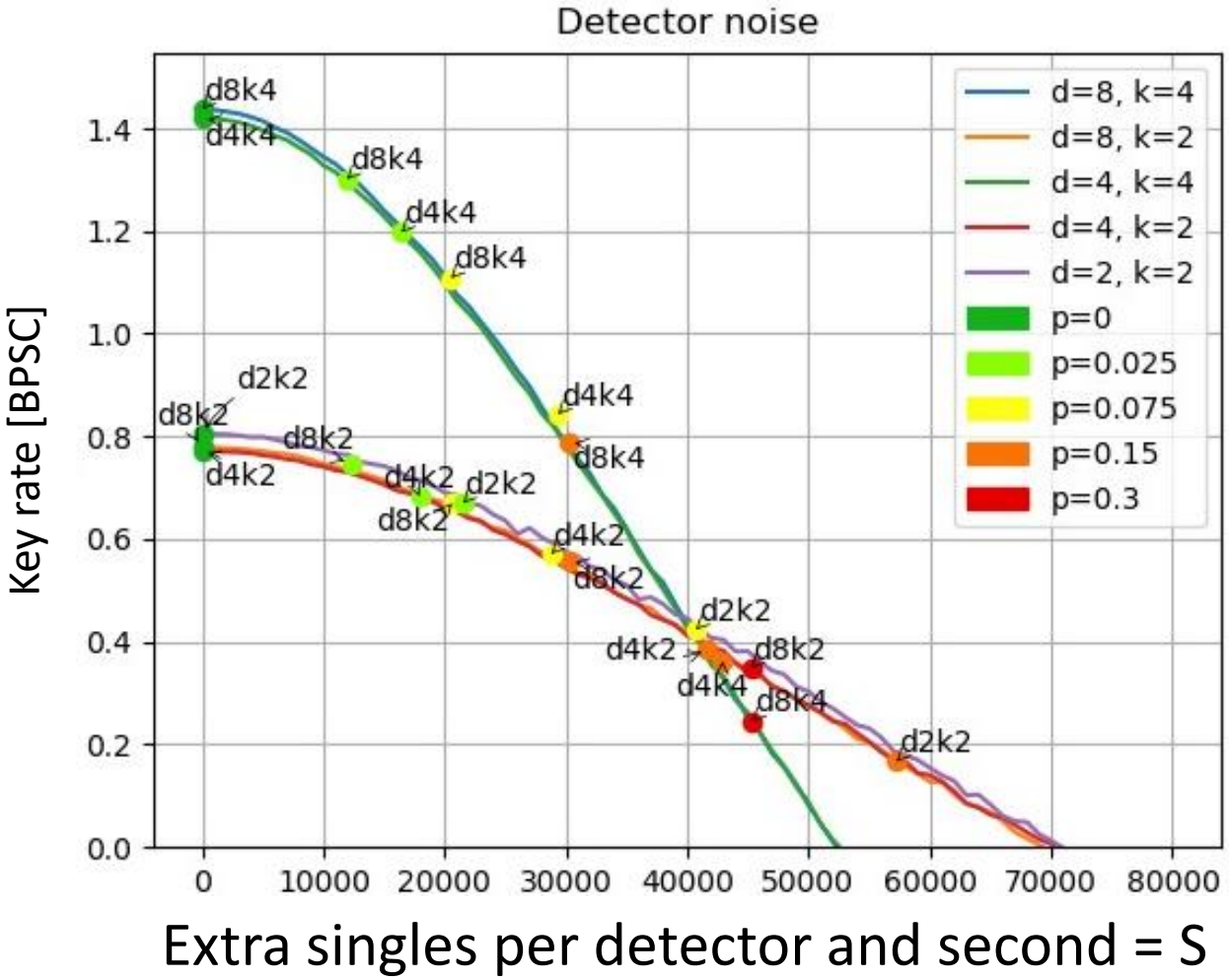


Extra Coincidences $= C/d$

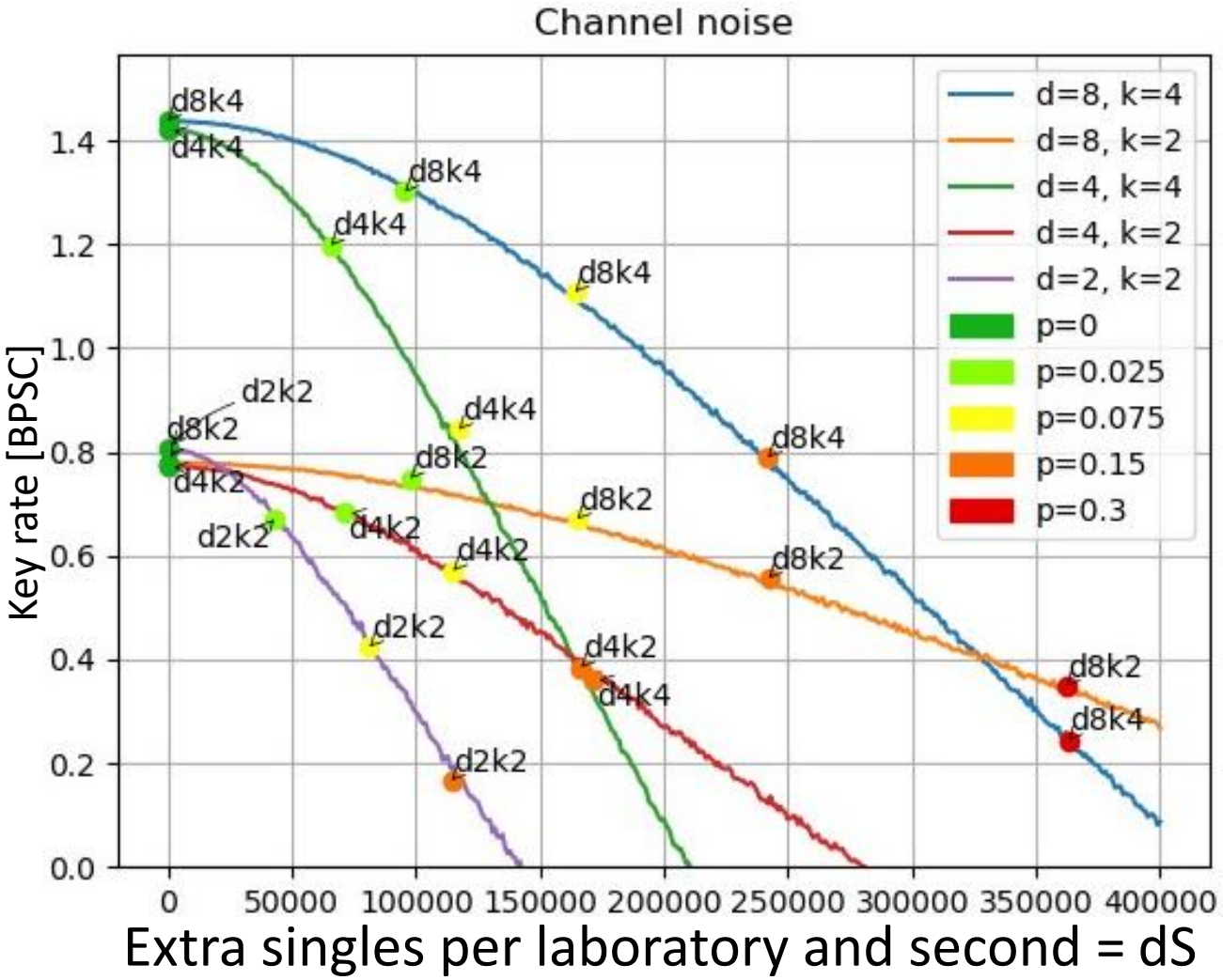
$\Leftrightarrow$

$$\rho_d = (1-p)\rho_d^{\mathrm{ent}} + p\frac{I_{d^2}}{d^2},$$

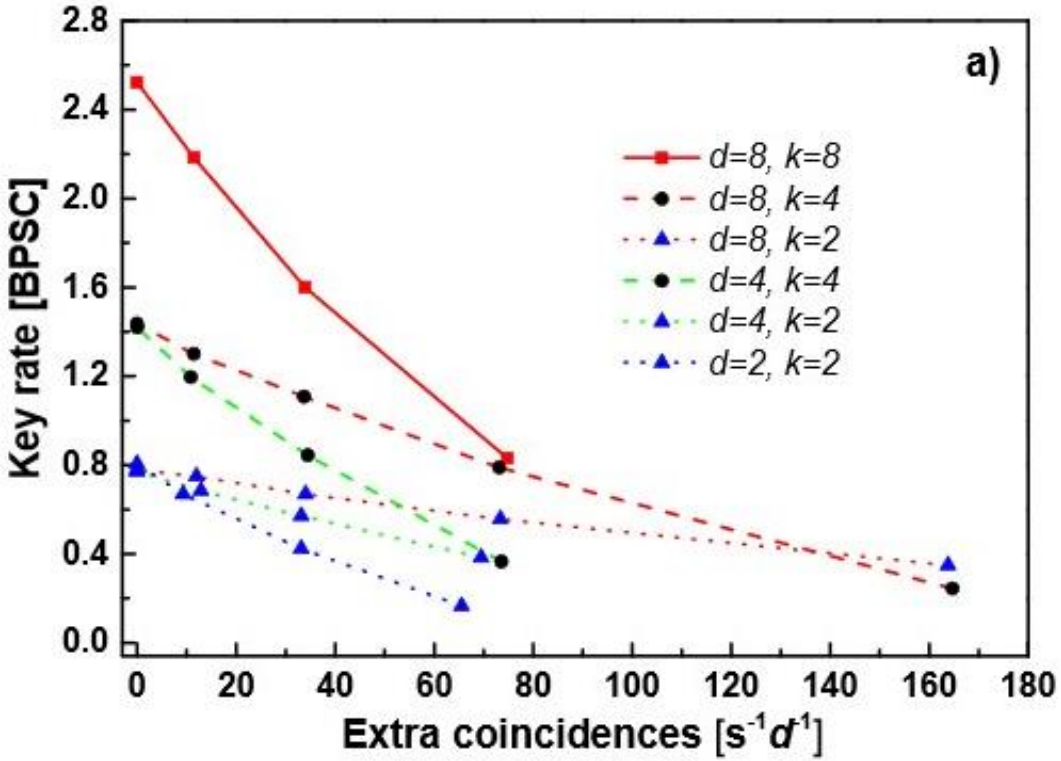
Comparison 2 – Detector noise

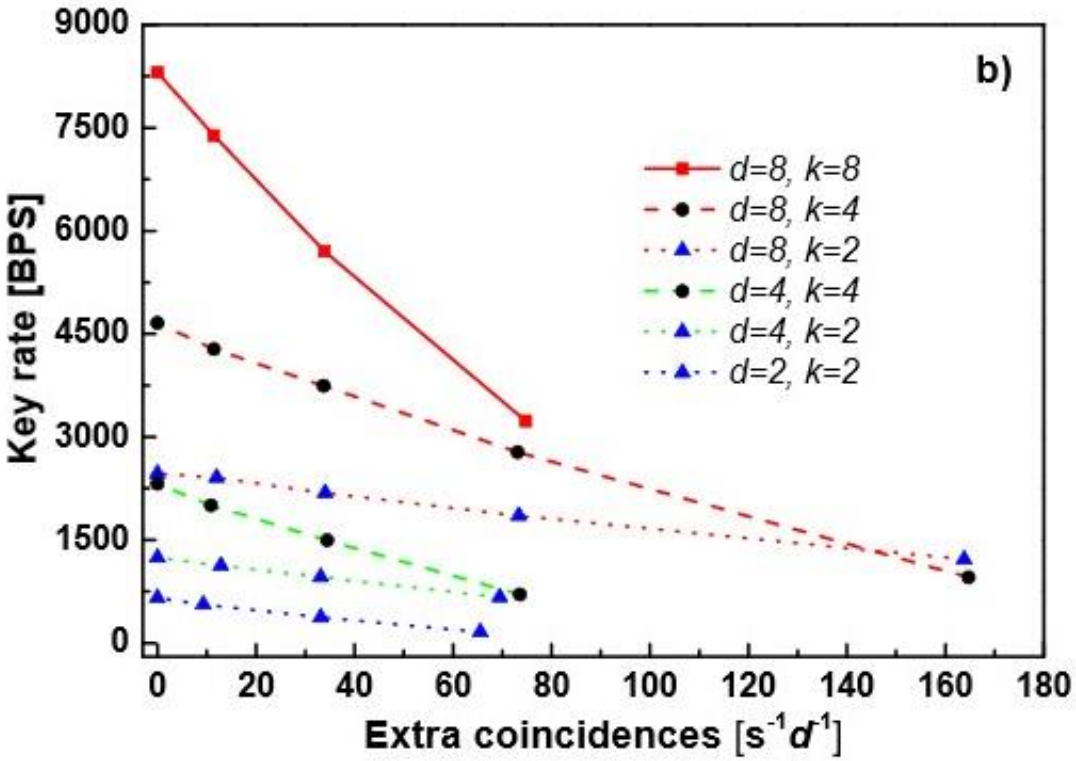


Comparison 3 – Channel noise



Key rate in bits per second





- BBO crystal heating limits pump laser power in practice
- Doubling d allows us to double the pump laser power

Future directions

- Using multiple MUB measurements
- Improving the detection modules so that the number of detectors does not scale with dimension

Thank you !