QUANTUM SECURITY
at all distance scales

Experimental Quantum Conference Key Agreement Using a Photonic Graph State

Joseph Ho | QCrypt, August 2021

Alexander Pickston, Federico Grasselli, Francesco Graffitti, Christopher L. Morrison, Massimiliano Proietti, Andres Ulibarrena, and Alessandro Fedrizzi

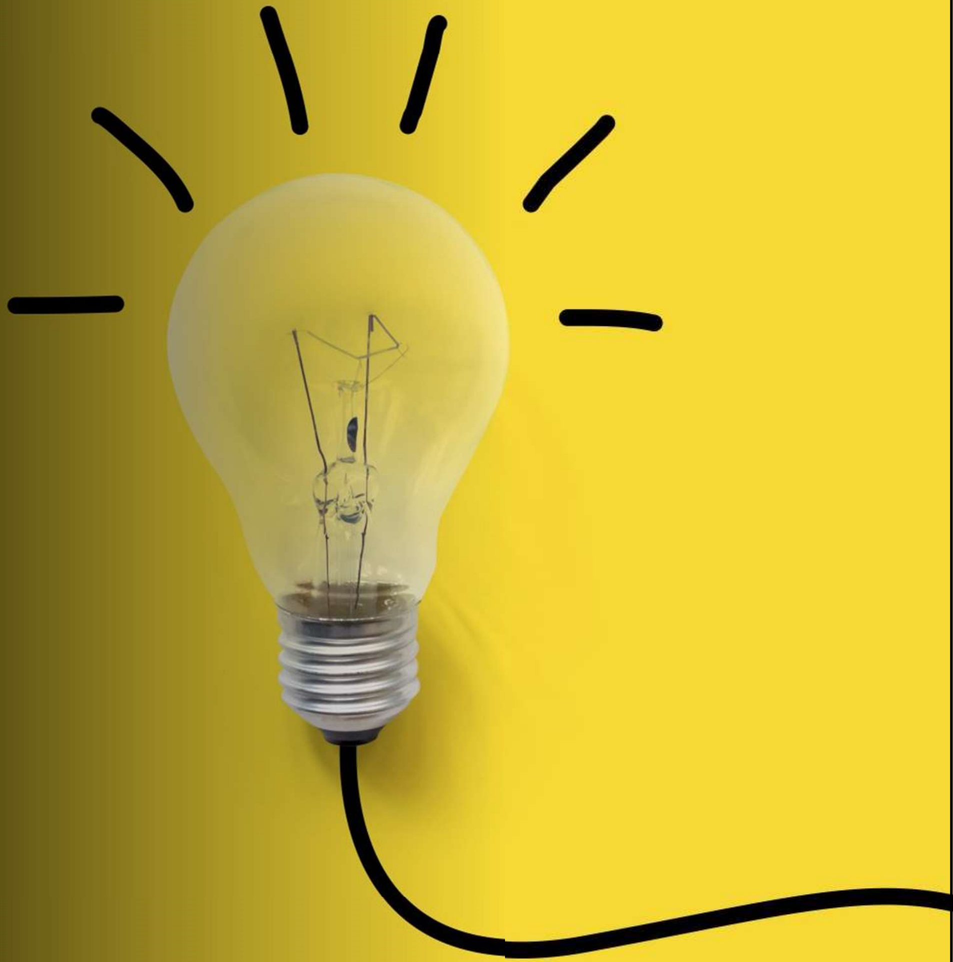
QUANTUM COMMUNICATIONS HUB

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

Engineering and Physical Sciences Research Council

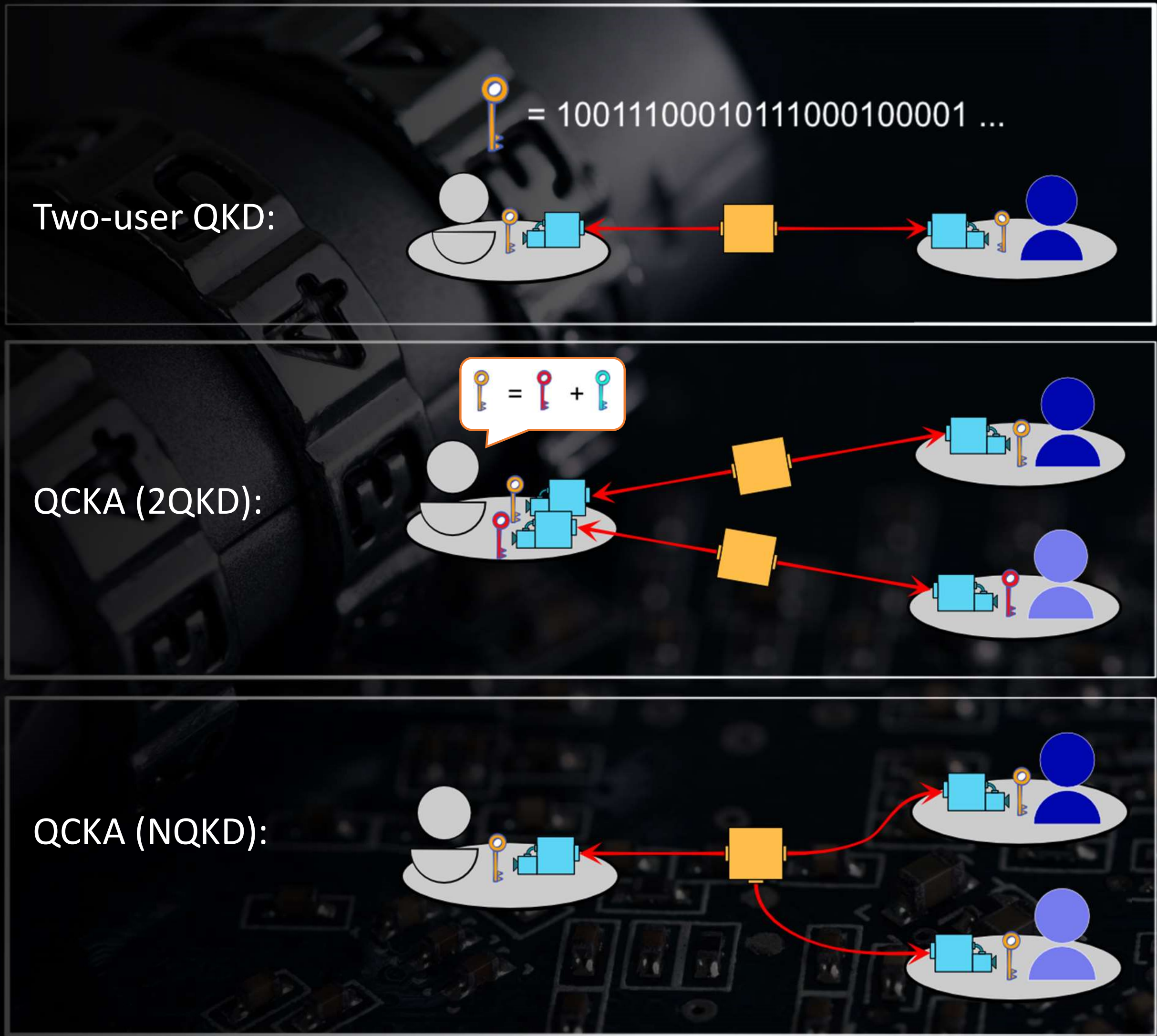
Outline

- Conference key agreement at a glance
  - Previous experiment using GHZ states
- Quantum networks and graph states
  - Conference key agreement: NQKD vs 2QKD
- Experimental setup
  - 6-photon graph, GHZ states and Bell pairs
  - Results: measured key rate
- Summary



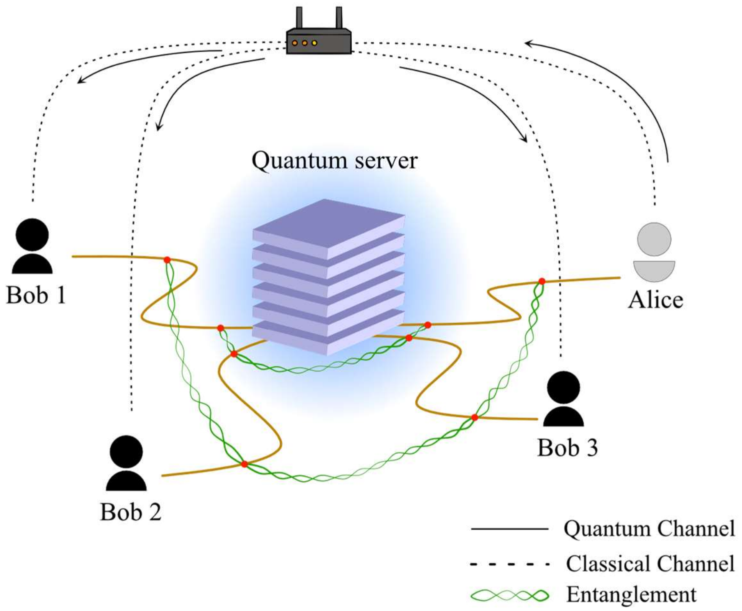
Quantum Conference Key Agreement

Allows N users to share a common, secret key for group-wide encryption.



Murta et al., Adv. Quan. Technol. 3, 2000025 (2020)

Quantum Conference Key Agreement - NQKD



Epping et al., NJP, 19, 093012 (2017)
Grasselli et al., NJP, 20, 113014 (2018)

N-BB84 Protocol

Distribute GHZ state each round

Perform sequence of measurements

Estimate security parameters

Error correction and privacy amplification on raw key

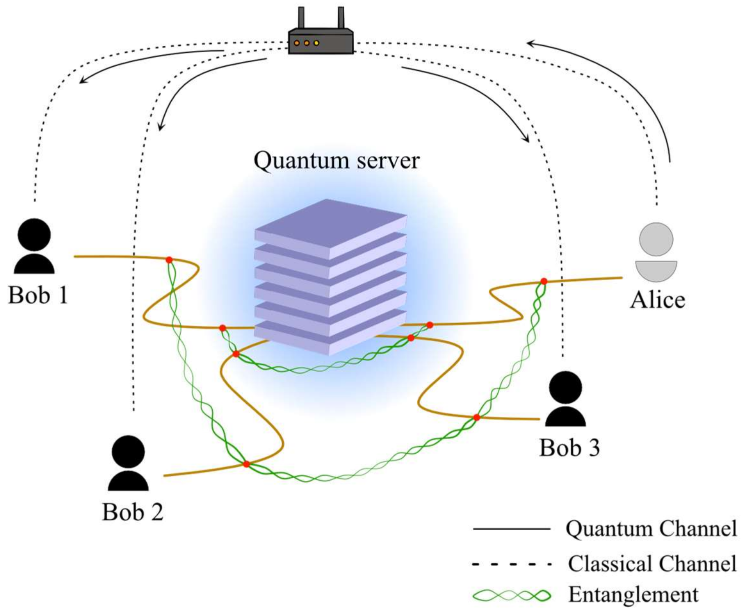
Distribute $|GHZ\rangle = \frac{|0\rangle^{\otimes N} + |1\rangle^{\otimes N}}{\sqrt{2}}$ for a total of L rounds

In each round, measure qubit according to preshared sequence:

Type-I: $\hat{Z}$ for key generation

Type-II: $\hat{X}$ for parameter estimation, $m = L \cdot p$

Quantum Conference Key Agreement - NQKD



Epping et al., NJP, 19, 093012 (2017)
Grasselli et al., NJP, 20, 113014 (2018)

N-BB84 Protocol

Distribute GHZ state each round

Perform sequence of measurements

Estimate security parameters

Error correction and privacy amplification on raw key

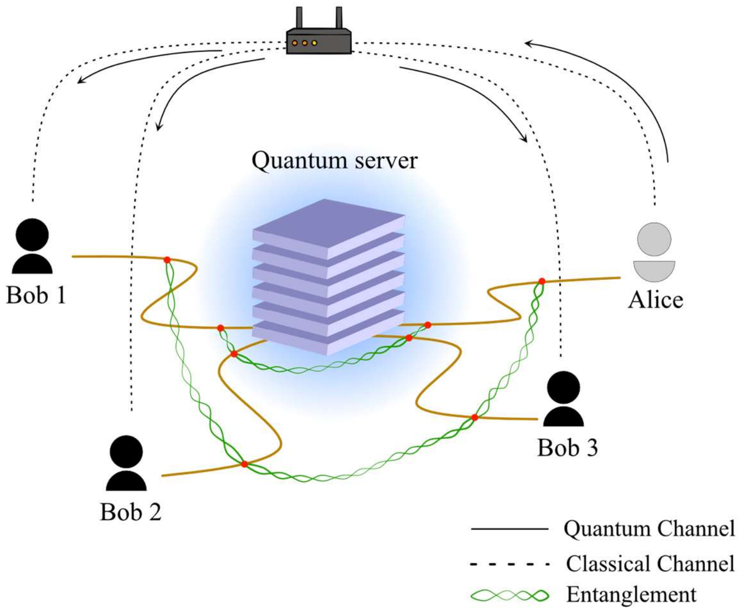
Estimate security parameters:

- Disclose subset of m type-I rounds
- Disclose all m type-II rounds
- Evaluate:

$$QBER = \max\left\{Q^m_{AB_i}\right\} \qquad \text{where, } Q^m_{AB_i} = \left(1 - \left\langle \sigma_Z^A\, \sigma_Z^{B_i} \right\rangle\right)/2$$

$$Q^m_X = \left(1 - \langle \sigma_X^{\otimes N} \rangle\right)/2$$

Quantum Conference Key Agreement - NQKD



Epping et al., NJP, 19, 093012 (2017)
Grasselli et al., NJP, 20, 113014 (2018)

N-BB84 Protocol

- Distribute GHZ state each round
- Perform sequence of measurements
- Estimate security parameters
- Error correction and privacy amplification on raw key

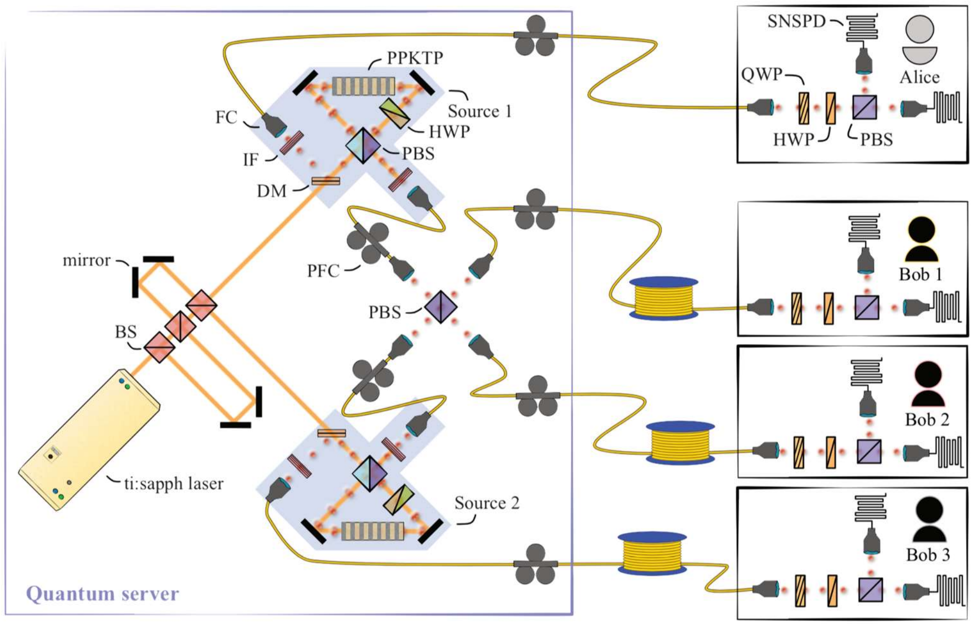
Raw key: $n = L - 2m$

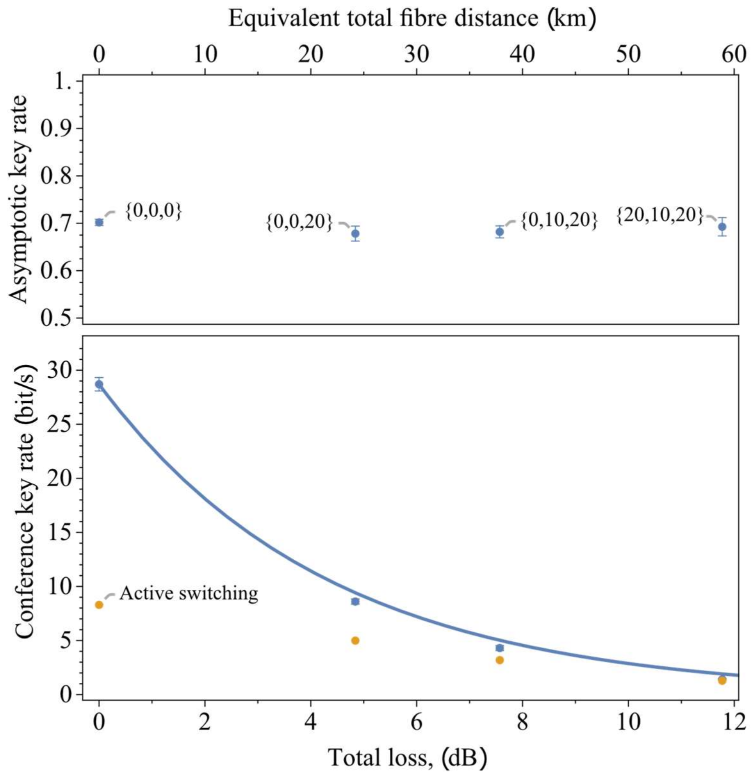
Apply multi-user error correction and privacy amplification

Fractional secure key rate (asymptotic limit):

$$AKR = \frac{\ell}{L} = 1 - h(QBER) - h(Q_X)$$

Quantum Conference Key Agreement - Experiment





Proietti, et al., Sci Adv, eabe0395 (2021)

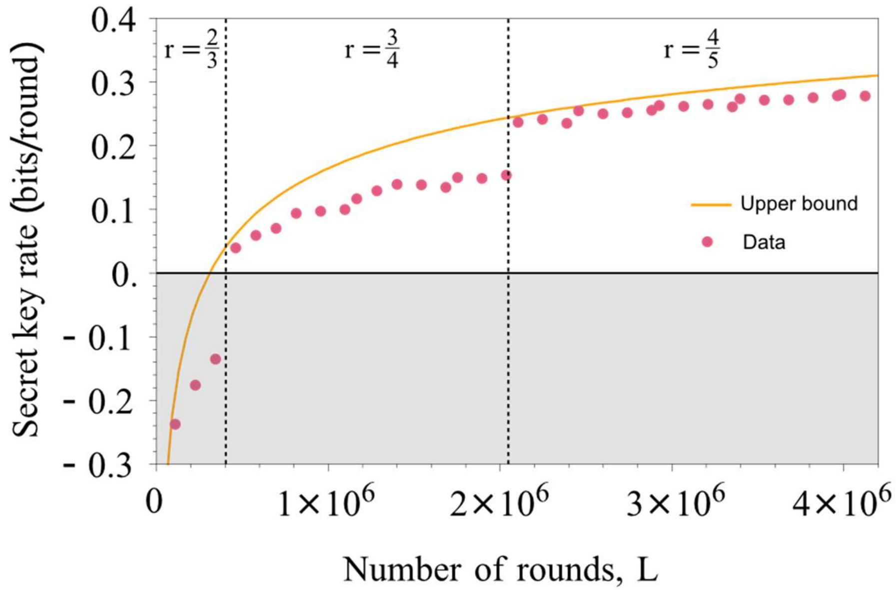
Quantum Conference Key Agreement - Experiment

Finite key rate:

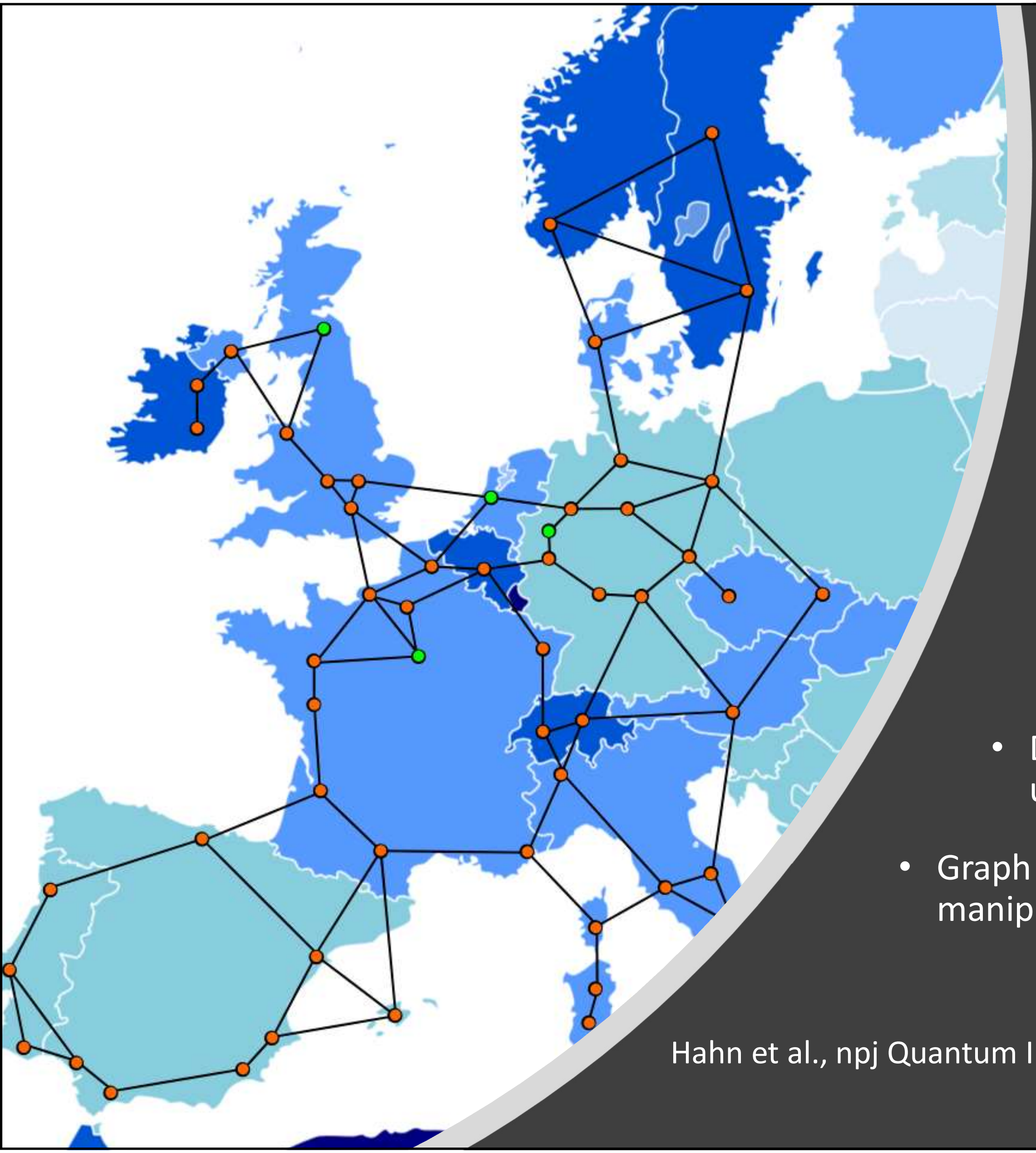
$$\frac{\ell}{L} = \frac{n}{L}[1 - h(Q_X^m + 2\xi_X)$$
$$- h(\mathrm{QBER}^m + 2\xi_Z)] - \log_2 \left[\frac{2(N-1)}{\epsilon_{EC}}\right]^{\frac{1}{L}}$$
$$- 2\log_2 \left[\frac{1 - 2(N-1)\epsilon_{PE}}{2\epsilon_{PA}}\right]^{\frac{1}{L}} - h(p)\,,$$

see Grasselli et al., NJP, 20, 113014 (2018).

- Multi-party error correction, LDPC codes
- Standard privacy amplification, Toeplitz matrix



Proietti, et al., Sci Adv, eabe0395 (2021)



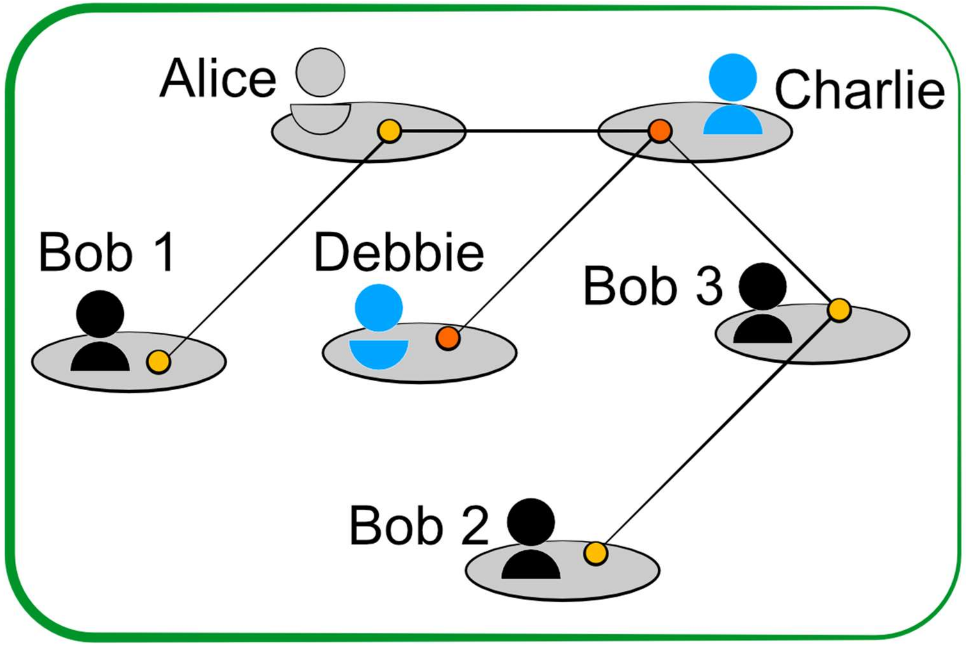
QCKA in Networks

- Future multi-node quantum networks will have finite channels
- In constrained networks, NQKD can use GHZ states to reduce congestion versus 2QKD with Bell pairs
- Delivering different entanglement resources to connected users poses challenges
- Graph states provide a useful framework for describing and manipulating complex entanglement in networks

Hahn et al., npj Quantum Inf. 5, 76 (2019)

Epping et al., NJP, 19, 093012 (2017)

Six-photon Graph for QCKA

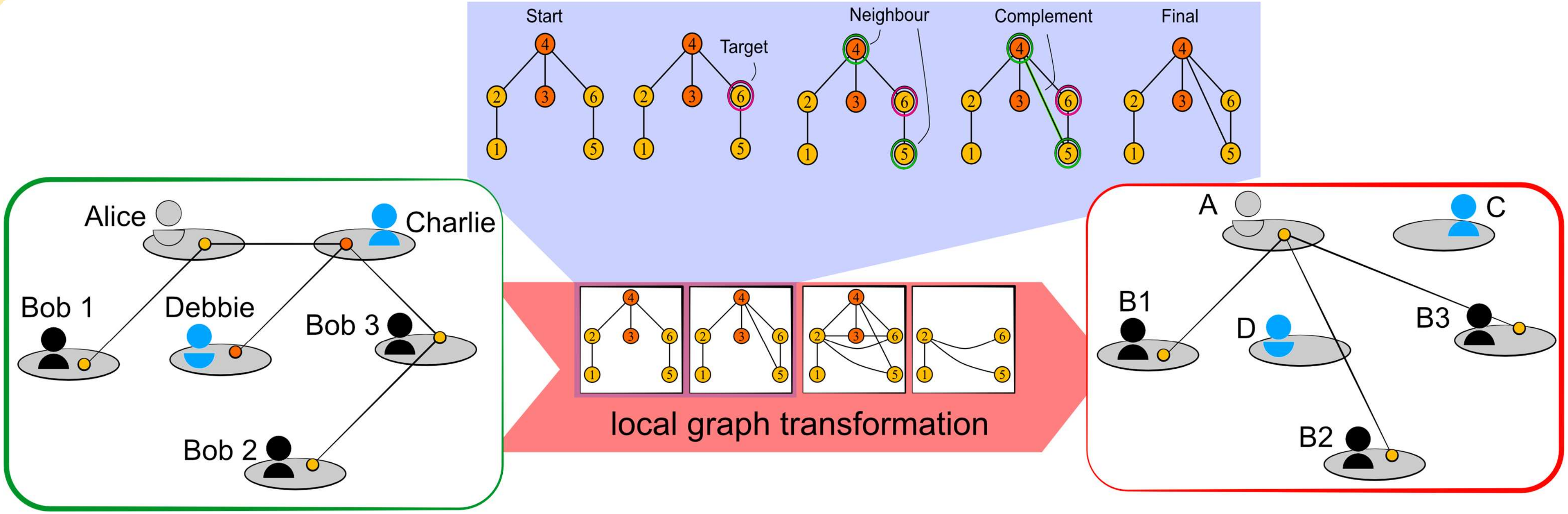


- Graph state created in a network
  - Nodes → qubit-encoded photon
  - Edges → pairwise interaction
- Using local complementation (LC) techniques to transform graph and distribute entanglement resources

Hahn et al., npj Quantum Inf. 5, 76 (2019)

Adcock et al., Quantum Sci. Tech. 4, 015010 (2019)

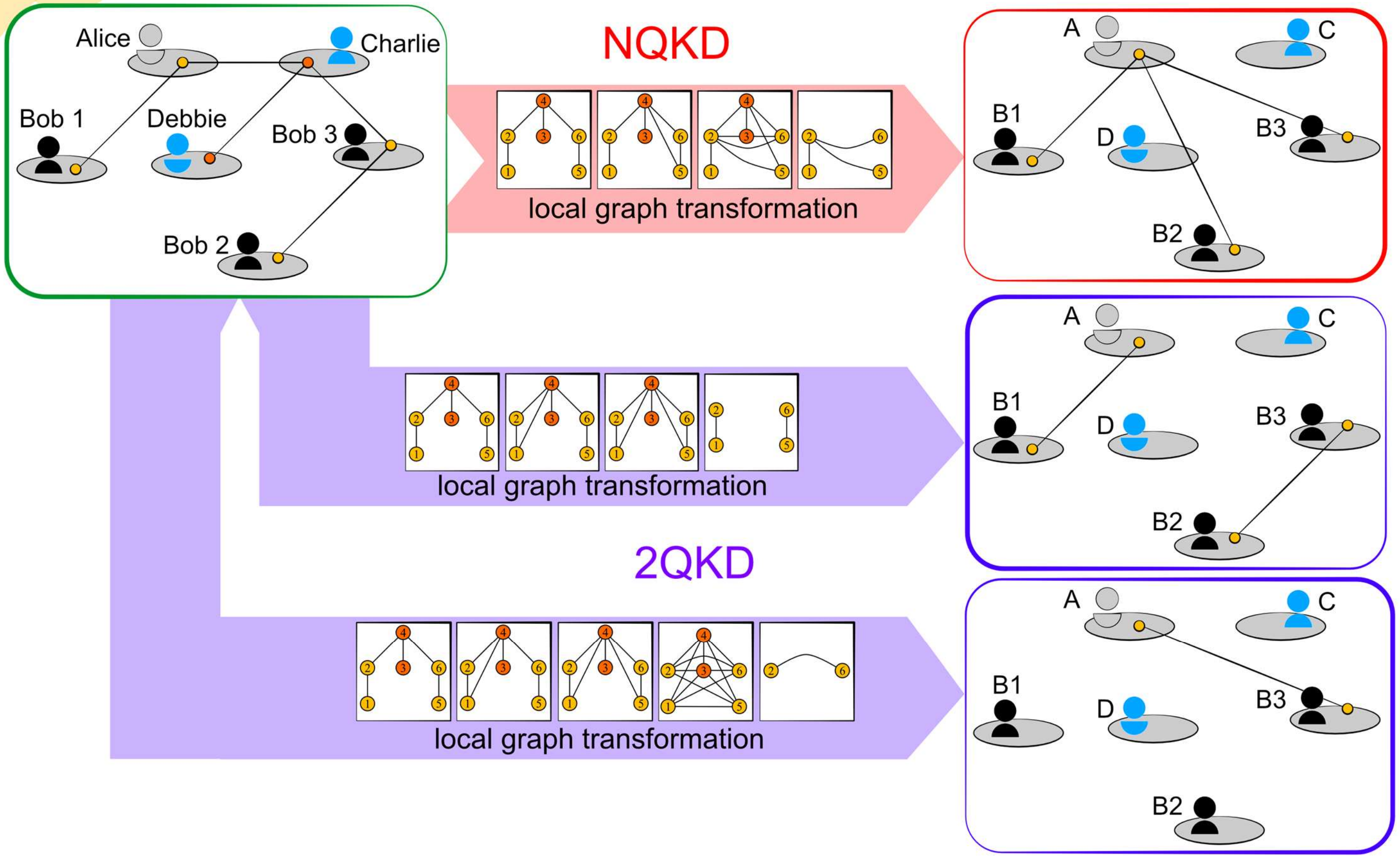
Six-photon Graph for QCKA



Hahn et al., npj Quantum Inf. 5, 76 (2019)

Adcock et al., Quantum Sci. Tech. 4, 015010 (2019)

Six-photon Graph for QCKA



NQKD protocol

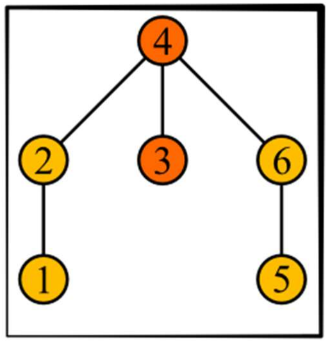
- Obtain GHZ state
- Measure security parameters
- Evaluate AKR from N-BB84 scheme

2QKD protocol

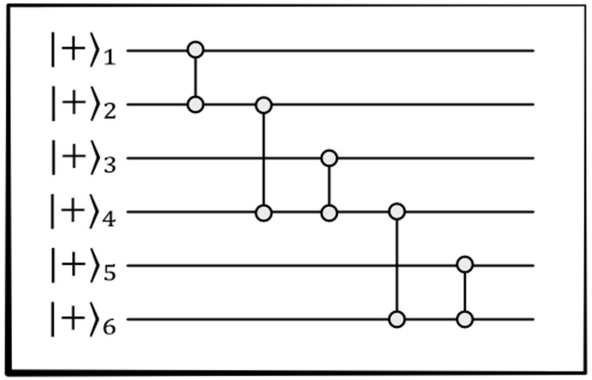
- Obtain three Bell pairs
- Measure security parameters
- AKR of each Bell pair from BB84, $r_{AB_1}, r_{B_2B_3}, r_{AB_2}$, then evaluate,

$$AKR_{2QKD} = \frac{1}{\frac{1}{r_{AB_3}} + \max\left\{\frac{1}{r_{AB_1}}, \frac{1}{r_{B_2B_3}}\right\}}$$

From Graph to Optics Circuit

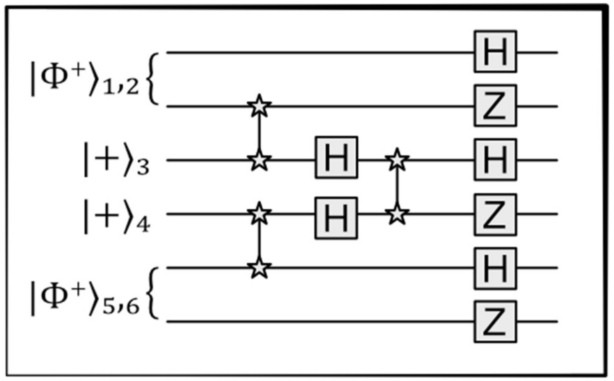


graph



equivalent circuit model

- Nodes denote qubit, $|+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$
- Edges indicate CZ gate between nodes

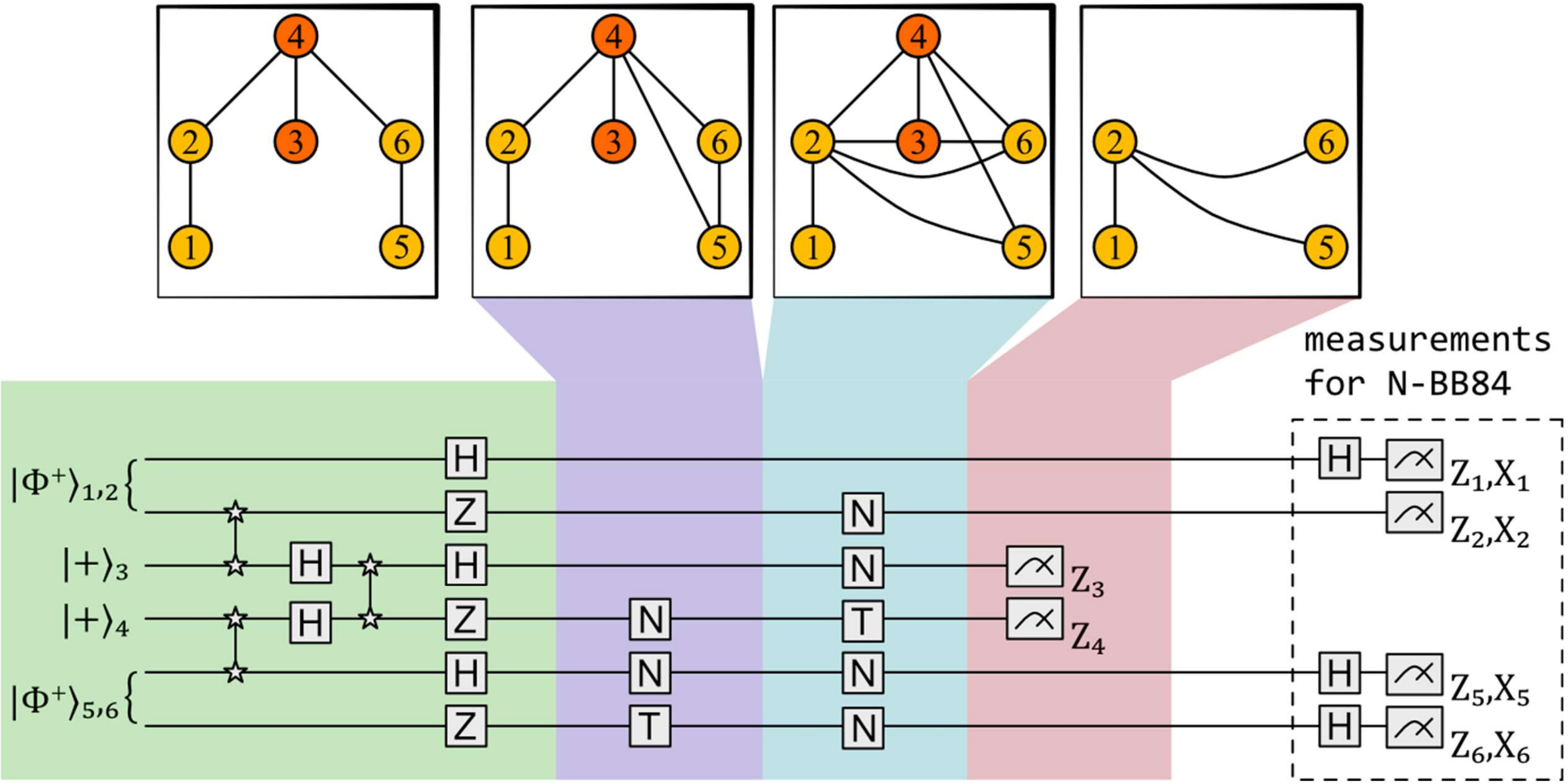


circuit optimisation

<u>Optimum linear optics circuit exploiting:</u>

- Offline entanglement
- Fusion gates
- Local unitaries

Implementing Local Complementation

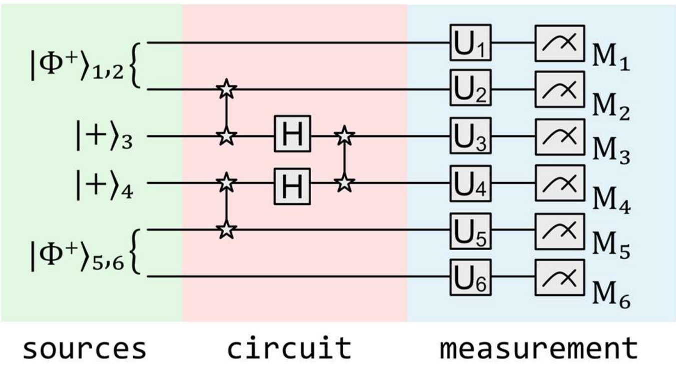


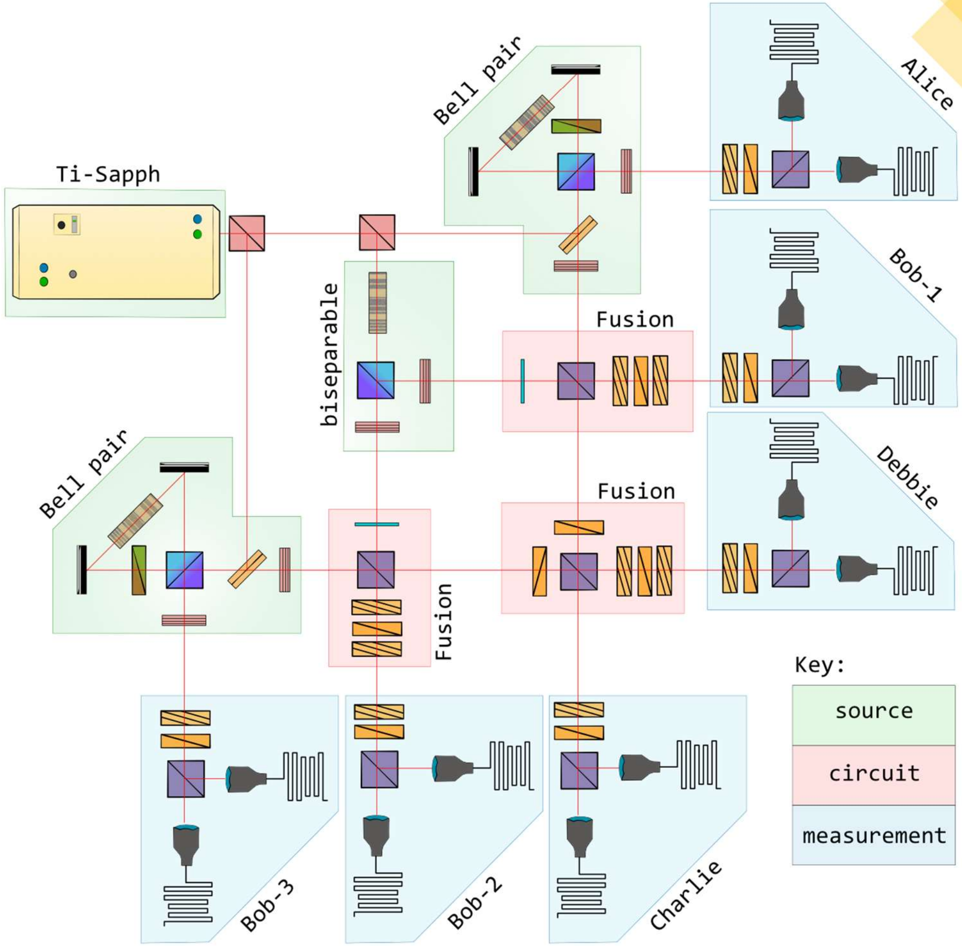
$\boxed{N} = \sqrt{-iX}$ $\boxed{T} = \sqrt{iZ}$

Adcock et al., Quantum Sci. Tech. 4, 015010 (2019)

Experimental QCKA Using Photonic Graph

- Ti-sapph laser: 80 MHz @ 774.9 nm, 1.3 ps
- 30 mm aperiodically-poled KTP crystal[1] for Type-II SPDC, 1550 nm photon pairs
- Non-deterministic Fusion gates, $P_{suc} = \frac{1}{8}$

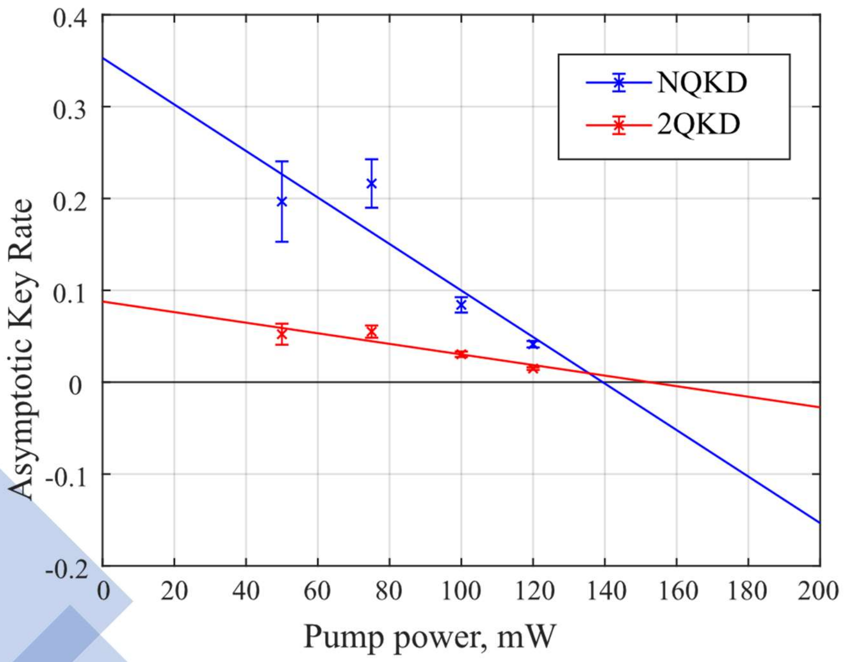


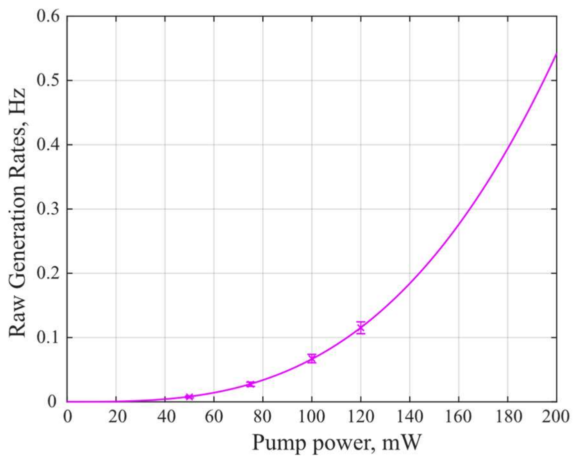


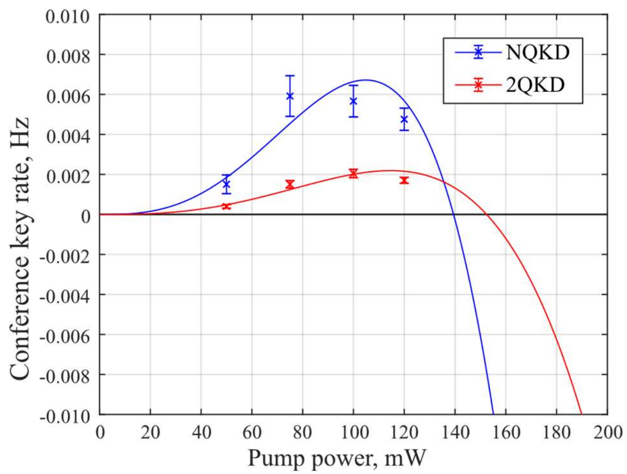
[1]Pickston et al., Opt. Express 29, 6991-7002 (2021)

Experimental QCKA Using Photonic Graph - Results

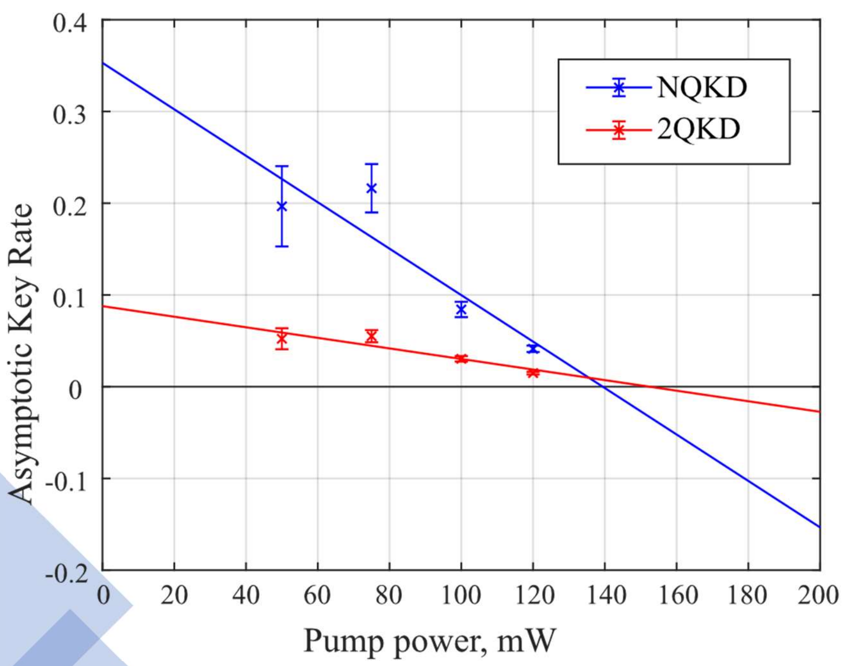
- Measured noise parameters, QBER and QX, to evaluate AKR when using N-BB84 for NQKD and 2QKD
- Increasing source brightness led to reduction in fractional key rates owing to added noise







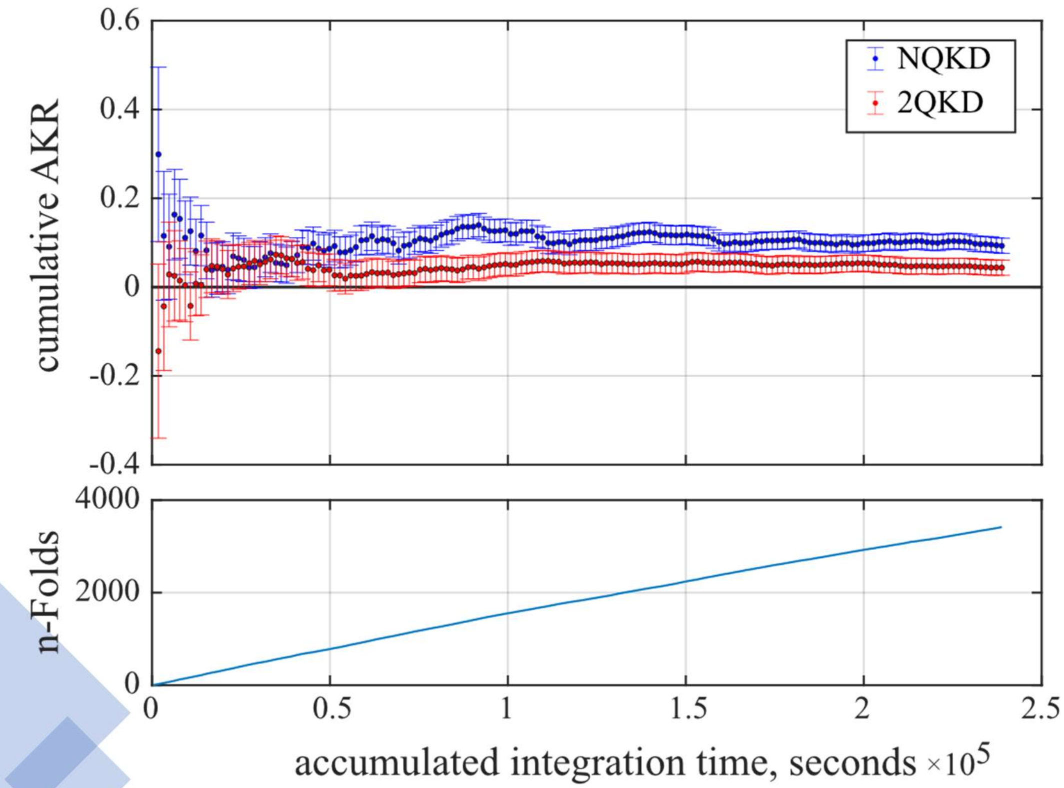
Experimental QCKA Using Photonic Graph - Results



- Measured noise parameters, QBER and QX, to evaluate AKR when using N-BB84 for NQKD and 2QKD
- Increasing source brightness led to reduction in fractional key rates owing to added noise
- NQKD outperforms 2QKD by a factor greater than 2 in our measurement regime

Pump power	AKR – NQKD	AKR – 2QKD	Ratio
50 mW	0.19 ± 0.02	0.052 ± 0.004	3.8 ± 0.4
75 mW	0.216 ± 0.009	0.055 ± 0.003	3.9 ± 0.3
100 mW	0.084 ± 0.003	0.030 ± 0.001	2.8 ± 0.2
120 mW	0.041 ± 0.002	0.0148 ± 0.0005	2.8 ± 0.2

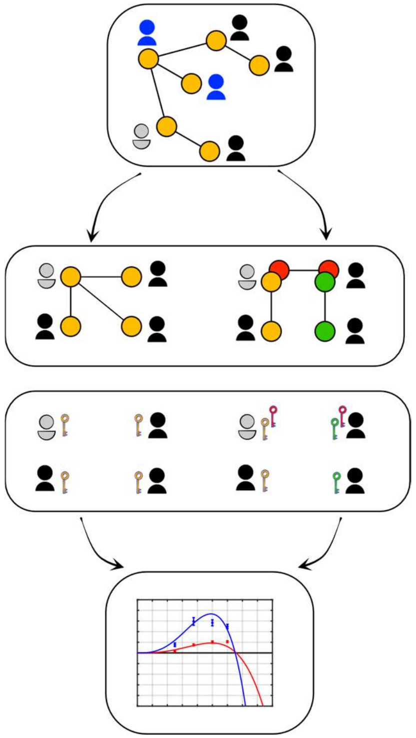
Experimental QCKA Using Photonic Graph - Results



- Repeated measurement of noise terms for each protocol to assess long-term performance
- Measurement over 17 days without stabilisation or re-optimisation of state preparation
- Mean ratio of NQKD vs 2QKD rates of complete dataset,

$$AKR_{NQKD}:AKR_{2QKD} = 2.13 \pm 0.06$$

Summary



- Experimentally implemented a 6-photon graph suitable for quantum conference key agreement
- We used local operations to distil resource states for NQKD and 2QKD (GHZ states and Bell pairs respectively)
- For a range of source brightness we observed the key rate advantage for NQKD over 2QKD
- In extended measurement run we measured a key rate advantage of NQKD:2QKD = 2.13 ± 0.06

<u>Outlook:</u>

- Improve 6-photon rates for other tasks
- Robustness of graph states to noise, e.g., photon loss, gate errors, channel dephasing