A Quantum Key Distribution Testbed using a Plug&Play Telecom-Wavelength Single-Photon Source

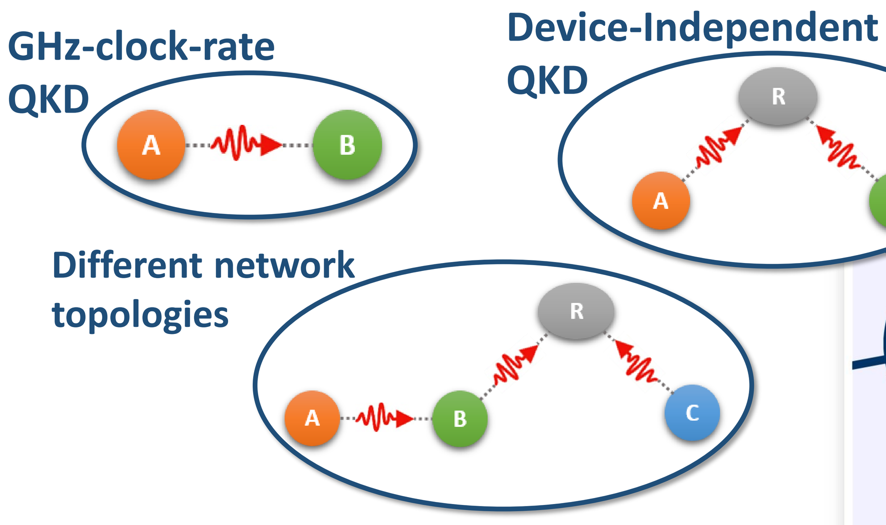
Group Website

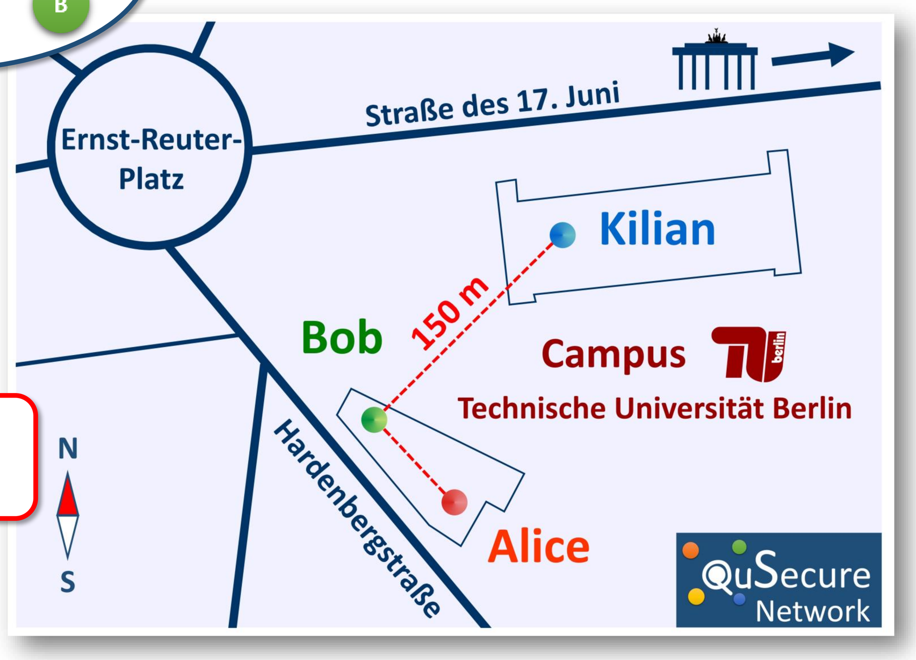
Timm Gao[1,*], Lucas Rickert[1], Felix Urban[1], Jan Große[1], Nicole Srocka[1], Sven Rodt[1], Anna Musiał[2], Kinga Żołnacz[3], Paweł Mergo[4], Kamil Dybka[5], Wacław Urbańczyk[3], Grzegorz Sęk[2], Sven Burger[6], Stephan Reitzenstein[1], and **Tobias Heindel**[1,*]

[1]Institute of Solid-State Physics, Technische Universität Berlin, Berlin, Germany
[2]Department of Experimental Physics, Wroclaw University of Science and Technology, Wroclaw, Poland
[3]Department of Optics and Photonics, Wroclaw University of Science and Technology, Wroclaw, Poland
[4]Institute of Chemical Sciences, Maria Curie Sklodowska University, Lublin, Poland
[5]Fibrain Sp. z o.o., Zaczernie, Poland
[6]Zuse Institute Berlin, Berlin, Germany

*E-Mail: **t.kupko@tu-berlin.de, tobias.heindel@tu-berlin.de**

Motivation — Quantum-secured Networks





Background — Single-Photon QKD Performance

Secret Key Rate (asymptotic)

$$S_\infty = S_{\mathrm{sift}}\left[A\left(1-h(e/A)\right)-f_{\mathrm{EC}}h(e)\right]$$ [2], [3]

QBER

$$\mathrm{QBER} = \mathrm{QBER}_{\mathrm{prep}} + \mathrm{QBER}_{\mathrm{Ch}} + \mathrm{QBER}_{\mathrm{Bob}}$$

Sifting

$$p_{\mathrm{sifted}} = \frac{p_{\mathrm{click}}}{2}$$

Multiphoton-Probability [4]

$$p_{\mathrm{m}} \leq \frac{\mu^2 g^{(2)}(0)}{2}$$

$$A = (p_{\mathrm{click}} - p_{\mathrm{m}})/p_{\mathrm{click}}$$

Secret Key Rate (finite)

$$S_{\mathrm{finite}}(N) = nA\left(1-h(\tilde{e}/A)\right) - nf_{\mathrm{EC}}h(e) - \Delta(n))$$ [5]

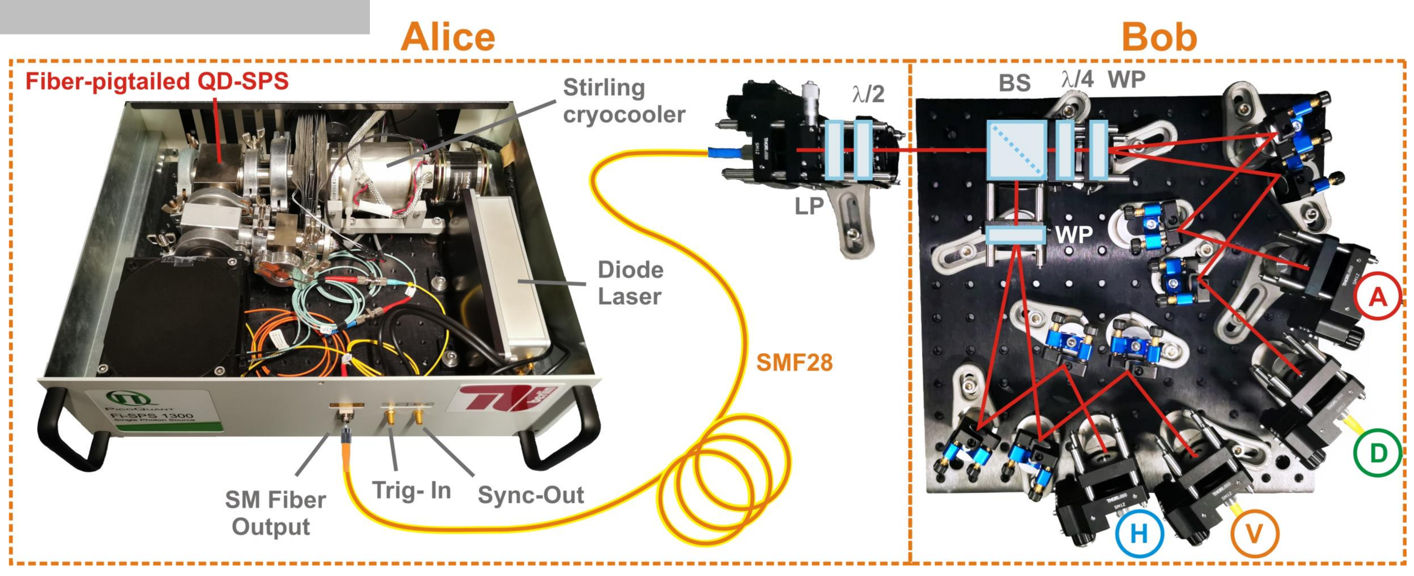
Finite Corrections

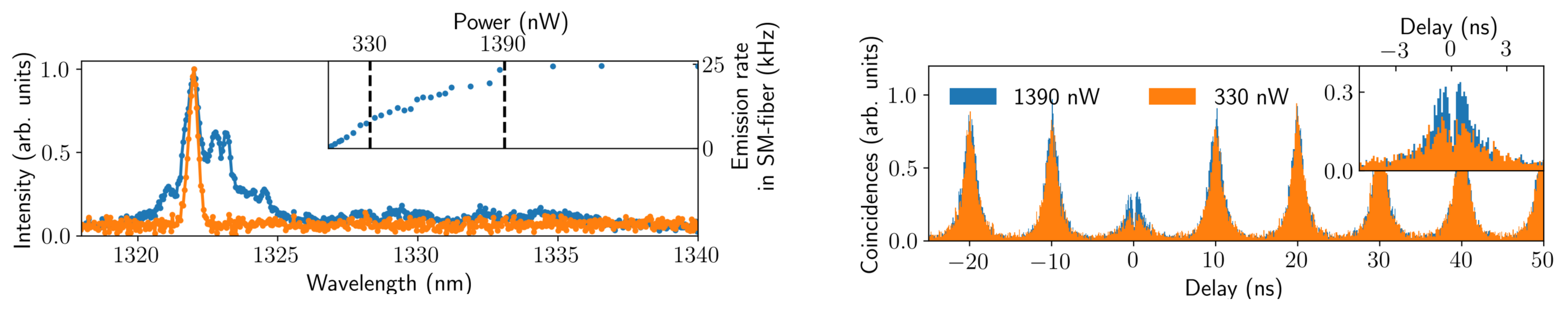
$$\Delta(n) = 7n\sqrt{\frac{1}{n}\log_2\frac{2}{\tilde{\epsilon}}} + 2\log_2\frac{1}{\epsilon_{\mathrm{PA}}} + \log_2\frac{2}{\epsilon_{\mathrm{EC}}}$$

$$\tilde{e} = e + \sqrt{(\ln(1/\epsilon_{\mathrm{PE}}) + 2\ln(m+1))/2m}$$

[2] D. Gottesman et al., *Quantum Info. Comput.* **4**, 325-360 (2004) [3] P. Chaiwongkhot et al., *Quantum Sci. Technol.* **2**, 044003 (2017))
[4] E. Waks et al., *Phys. Rev. A* **66**, 042315 (2002) [5] R. Y. Cai & V. Scarani, *New J. Phys.* **11**, 045024 (2009)

QKD Testbed — Alice & Bob



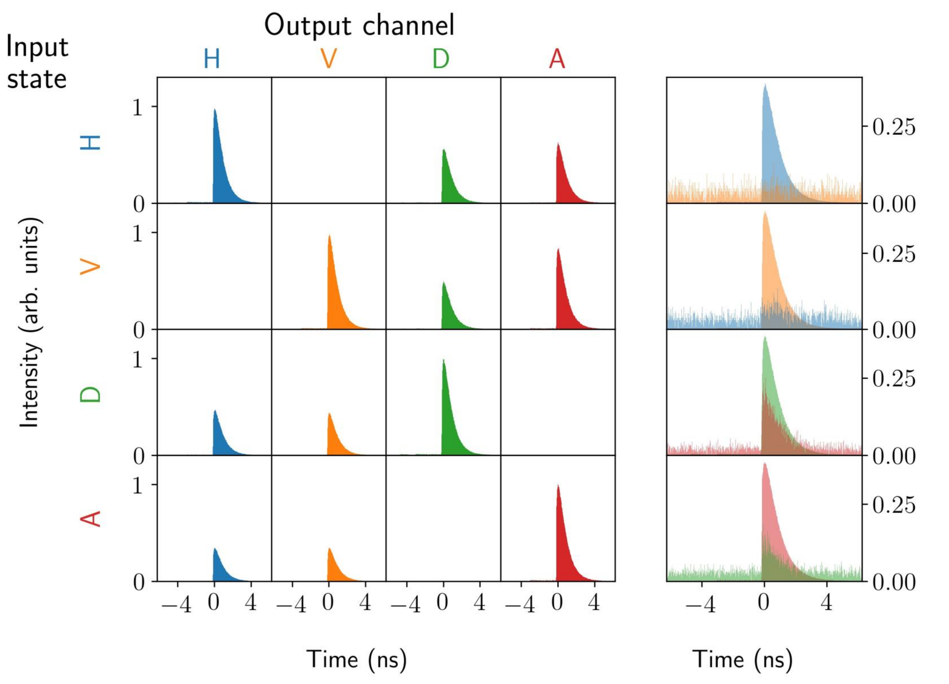


- Deterministically fabricated singe-photon source permanently **fiber-coupled** [1]
- Stirling cryocooler (40K base-temperature) cryogen-free, **stand-alone operation**
- Internal or external laser for triggering of emission
- Static polarization preparation at "Alice" (Back-to-Back configuration)
- 4-state polarization analyzer for BB84 QKD "Bob": Standard optical components + SNSPDs + quTAG (TDC electronics)

[1] A. Musial et al., *Adv. Quantum Technol.* **3**, 2000018 (2020)

Kupko et al., arXiv:2105.03473

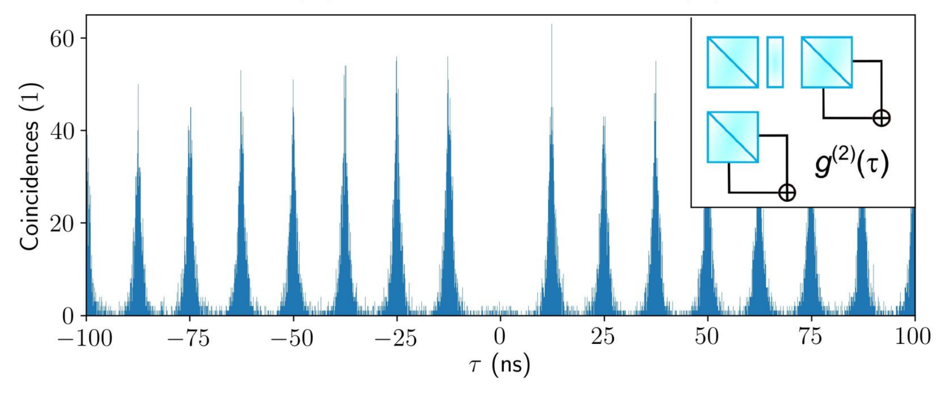
Basic Characterization — QBER, $g^{(2)}(0)$ etc.



Counts & QBER

$$\mathrm{QBER}_{\mathrm{Bob}} = \underbrace{\frac{q p_{\mathrm{signal}}}{p_{\mathrm{click}}}}_{\text{optical}} + \underbrace{\frac{p_{\mathrm{dc}}/2}{p_{\mathrm{click}}}}_{\text{Noise}}$$

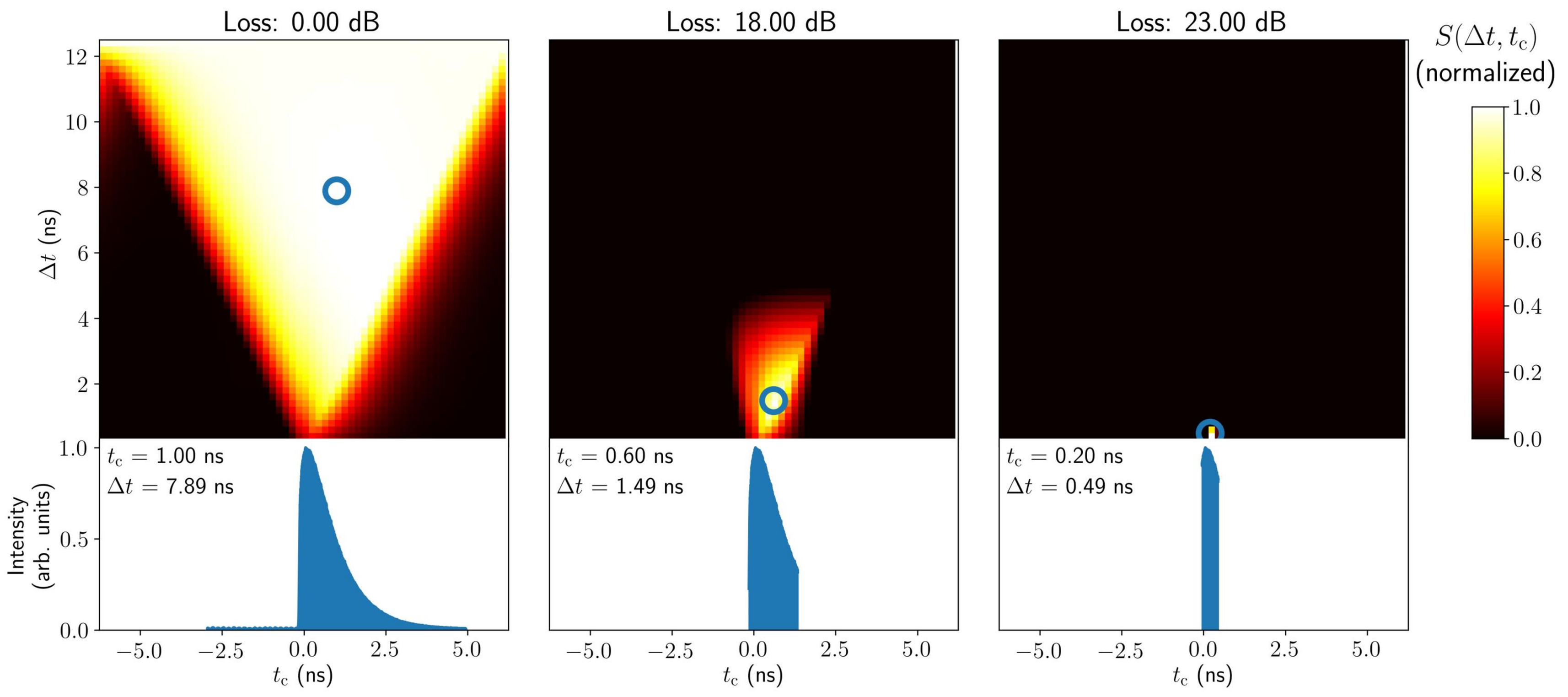
- 42 Hz Dark Count Rate
- QBER 0.35 % to 0.82 %
- Mean photon number into quantum channel µ = 0.0002
- Raw key rate 4.72 kHz



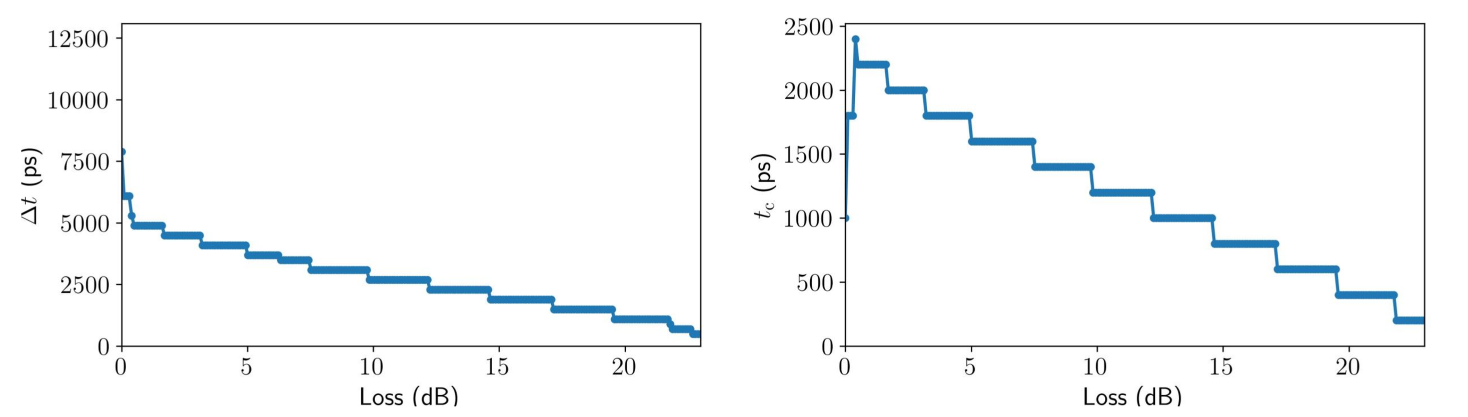
Photon statistics

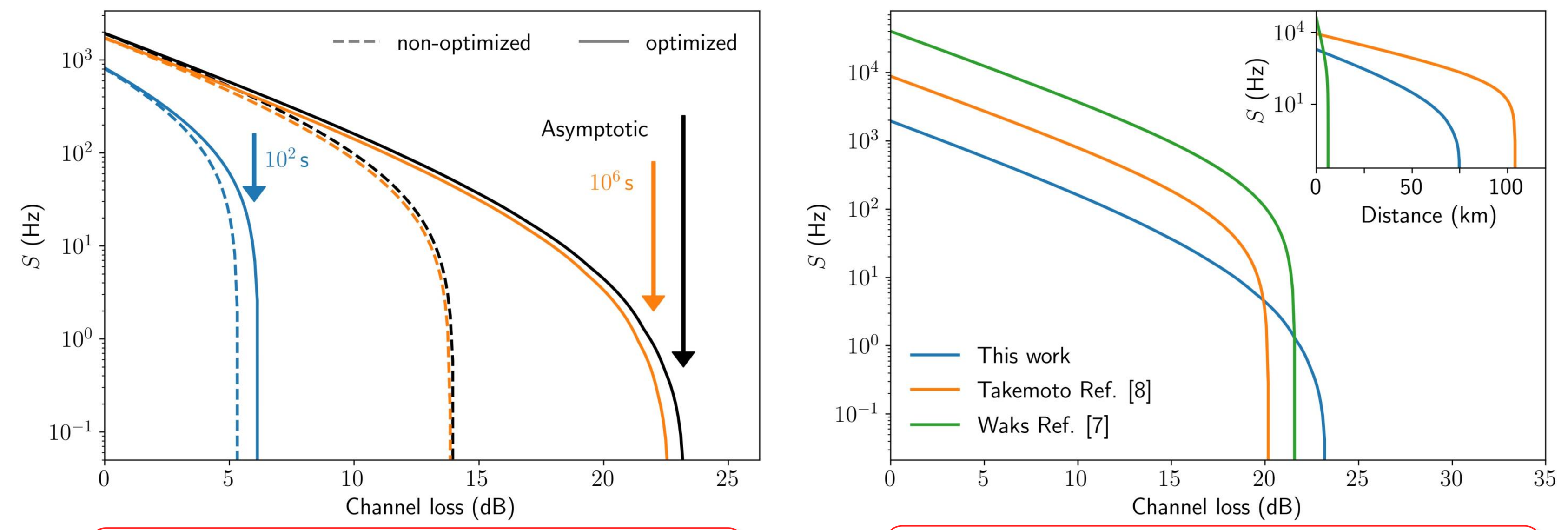
- $g^{(2)}(0)$ via HBT-measurement
- Channels of each bases combined
- Timestamp evaluation
- $g^{(2)}(0)$ = 0.10+/-0.01

Temporal Filtering — Parameter Optimization [6]



- Optimize Width Δt and Center t_c of acceptance time window
- Trade-Off between raw/sifted key and QBER





Large improvement in range with temporal filtering.

Comparable tolerable losses to laboratory scale SPS.

[6] T. Kupko et al., *npj Quantum Inf.* **6**, 29 (2020) [7] Waks et al., *Nature* **420**, 762 (2002) [8] Takemoto et al., *Sci. Rep.* **5**, 14383 (2015)

Outlook — BQN – The Berlin Quantum Network

Next Steps

Single Photon Source

- Telecom O-band CBG SPSs
- Source with electrically triggered SPS

QKD Implementation

- Modulation of Signal with fast EOM
- Investigation of sender side Alice
- Full implementation in laboratory and in field

We acknowledge funding via the "Quantum Futur" project 'QuSecure' (Code: 13N14876)
BMBF-Program Photonic Research Germany
Federal Ministry of Education and Research (BMBF)

Dr. Tobias Heindel
BMBF Junior Research Group Leader

QuSecure
SPONSORED BY THE
Federal Ministry of Education and Research