

The consortium



University of Pavia and INFN: C. Macchiavello, L. Maccone, G. Chesi;



Paderborn University: C. Silberhorn, B. Brecht, L. Serino;



CNRS, Lille: M. Kolobov, D. Horoshko, S. Srivastava;

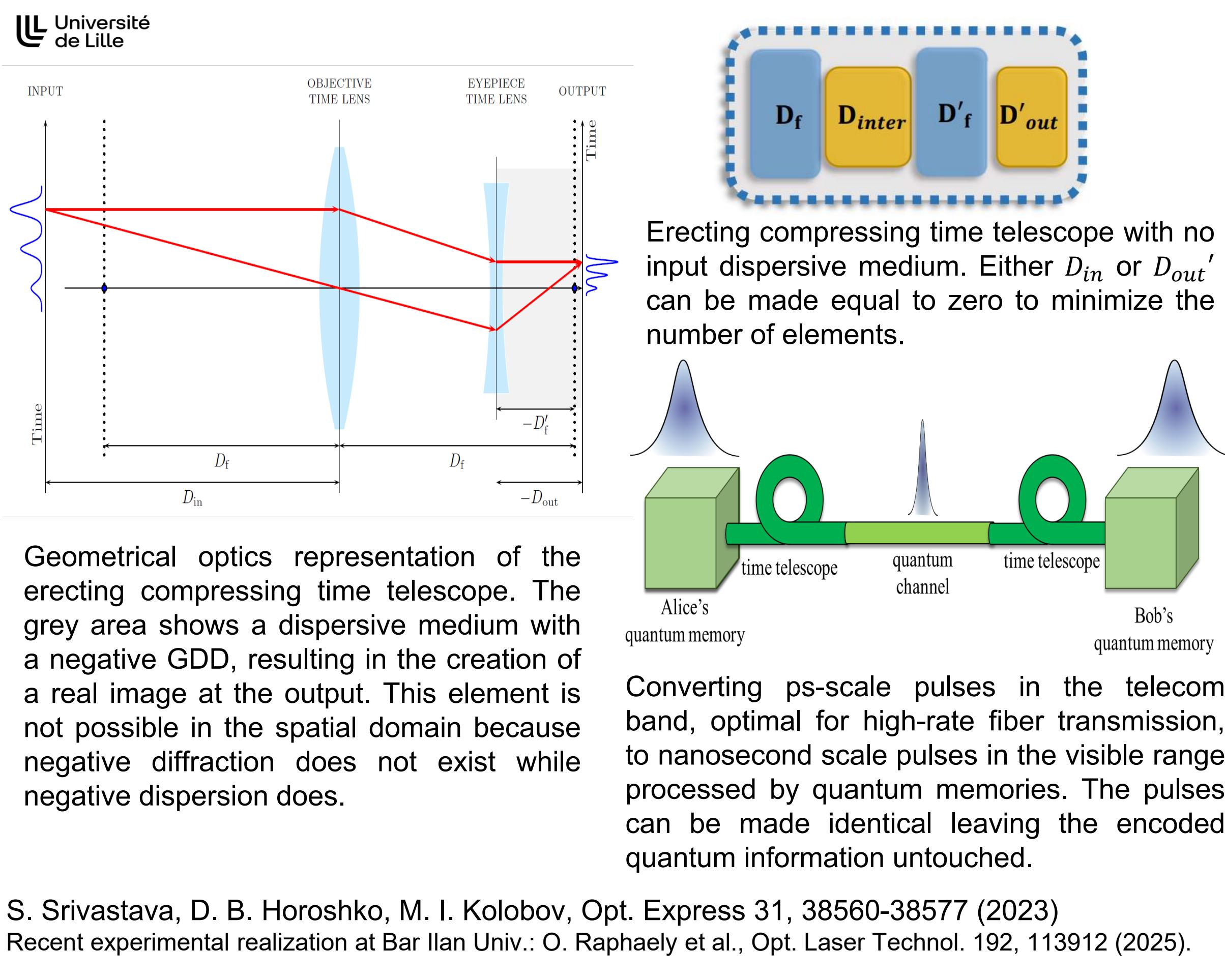


Imperial College London: I. Walmsley, S. Thomas;

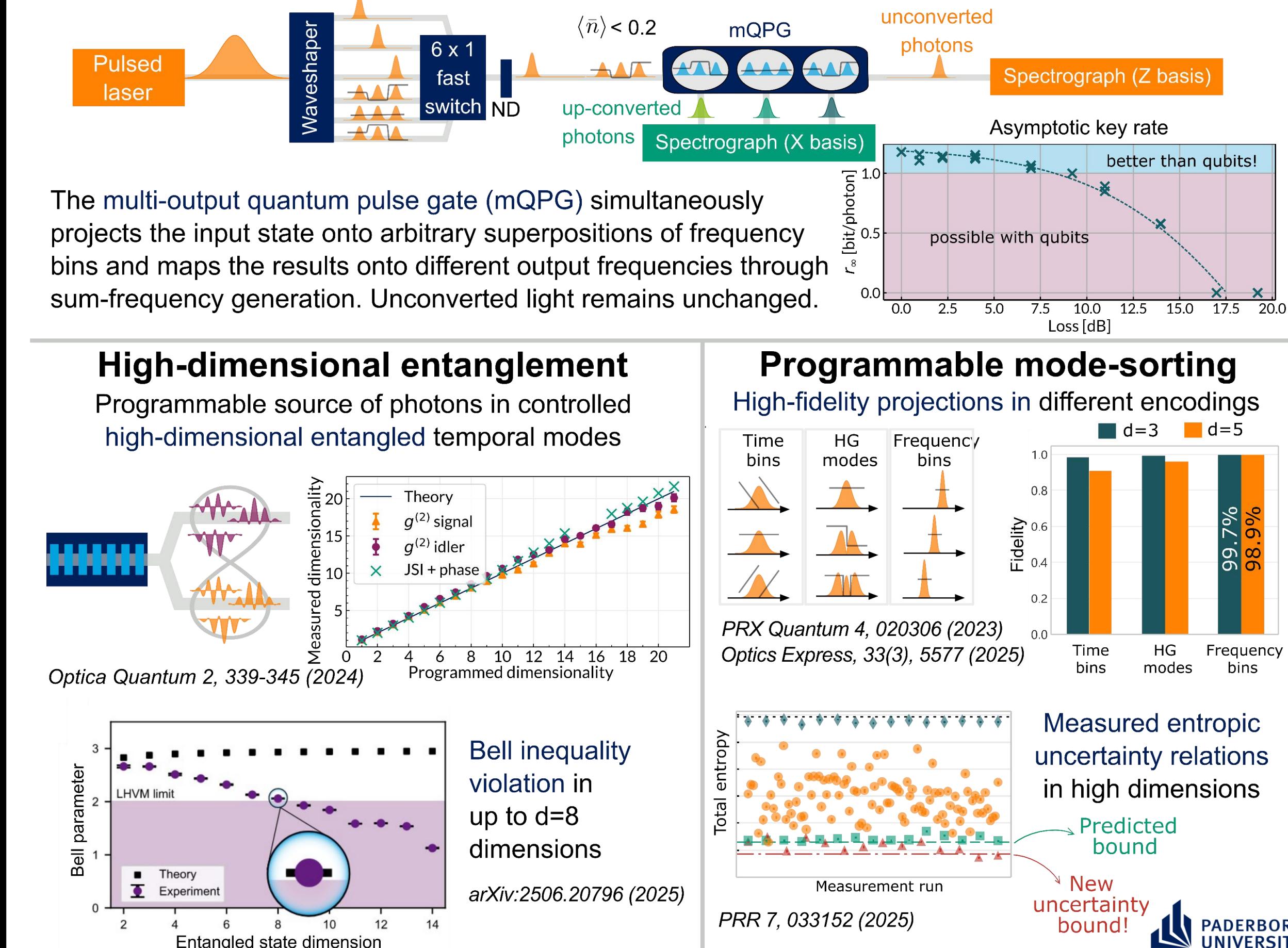


University of Warsaw: M. Karpinski, S. Kapoor, M. Ogrodnik

Quantum temporal imaging: an erecting time telescope



High-dimensional quantum key distribution with temporal modes



Construction of efficient Schmidt number witnesses



Motivation

- Modern setups (Quantum phase gate, time-frequency encoding, ...) prepare high-dimensional quantum states.
- Problem: Certify dimensionality of prepared states.

Schmidt number

- Decompose pure state: $|\psi\rangle = \sum_{i=0}^{k-1} \sqrt{\lambda_i} |i\rangle_A |i\rangle_B$

- k is called **Schmidt rank**, measures dimension of state.

- For mixed states: convex roof yields Schmidt number

$$SN(\rho) = \min_{\rho = \sum p_i |\psi_i\rangle\langle\psi_i|} \max_i \text{SR}(|\psi_i\rangle)$$

- Detect using Schmidt number witness W :

$$\text{Tr}(W\rho) \geq 0 \quad \forall \rho \in S_k,$$

$$\text{Tr}(W\rho) < 0 \quad \text{for some } \rho.$$

- Simple witness:

$$W = 1 - \frac{d}{k} |\phi^+\rangle\langle\phi^+|$$

$$\text{with } |\phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle$$

The algorithm

- Problem: requires $O(d^2)$ measurements in standard basis.
- Construct witness that uses measurements M with $|M| =$

- Choose k , subset M and some constant $C \in (-1, 1)$.
- Run semidefinite program

$$\text{find } \tilde{W}^{(1)}$$

$$\text{s.t. } \langle \phi^+ | \tilde{W}^{(1)} | \phi^+ \rangle = -1,$$

$$-1 \leq \tilde{W}^{(1)} \leq 1.$$
- Find $\min_{|\phi_k^{(1)}\rangle} \langle \phi_k^{(1)} | \tilde{W}^{(1)} | \phi_k^{(1)} \rangle$.
- Go back to 2., add constraint

$$\langle \phi_k^{(1)} | \tilde{W}^{(2)} | \phi_k^{(1)} \rangle \geq C.$$
- Stop if infeasible (decrease C) or converged (increase C) and repeat.

Result

- Measuring $\text{Tr}(\tilde{W}) < -\sqrt{\frac{d^2 - 4d + 4k}{d^2}}$ with

$$\tilde{W} = \left(1 - \frac{2}{d}\right) |00\rangle\langle 00| - \frac{2}{d} \sum_{i=1}^{d-1} (|00\rangle\langle ii| + |ii\rangle\langle 00|) - \left(1 - \frac{2}{d}\right) \sum_{i=1}^{d-1} |ii\rangle\langle ii|$$
- certifies Schmidt rank $k + 1$.

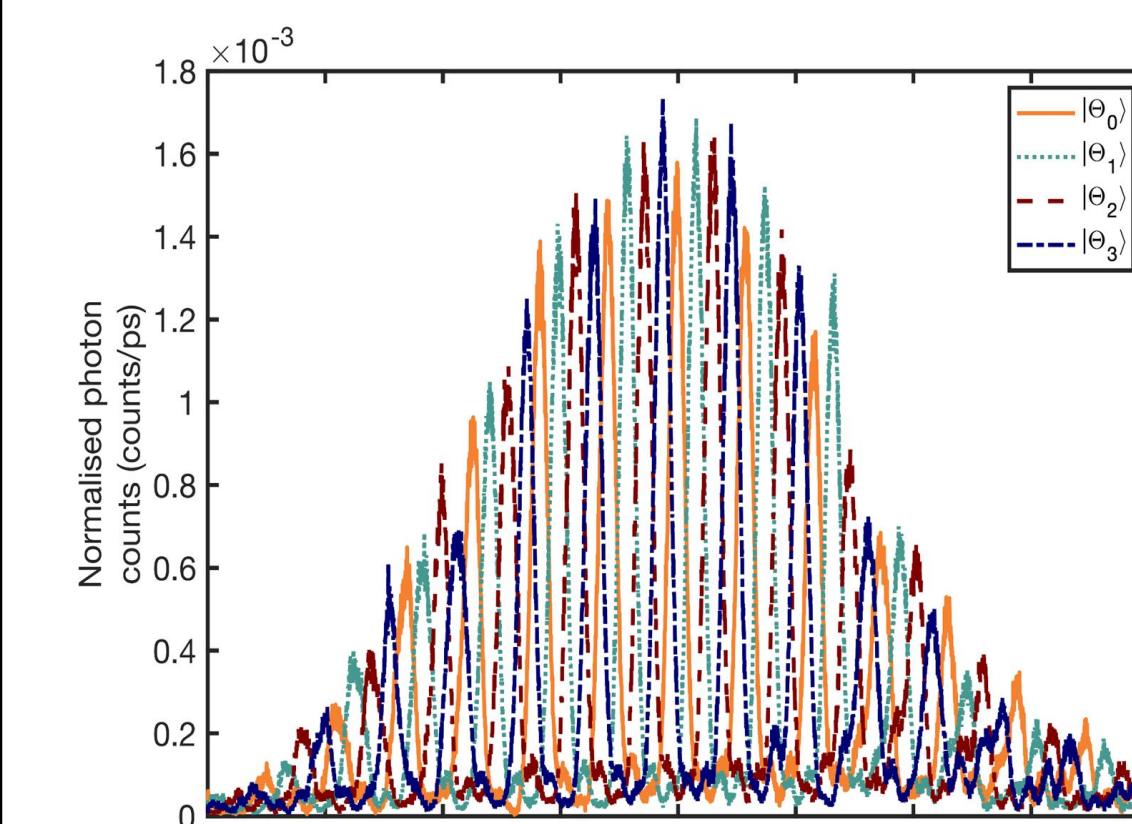
N. Wyderka, G. Chesi, H. Kampermann, C. Miacchiavello, D. Bruß, Phys. Rev. A 107, 022431 (2023)

Efficient detection of multidimensional single-photon time-bin superpositions



photon.fuw.edu.pl

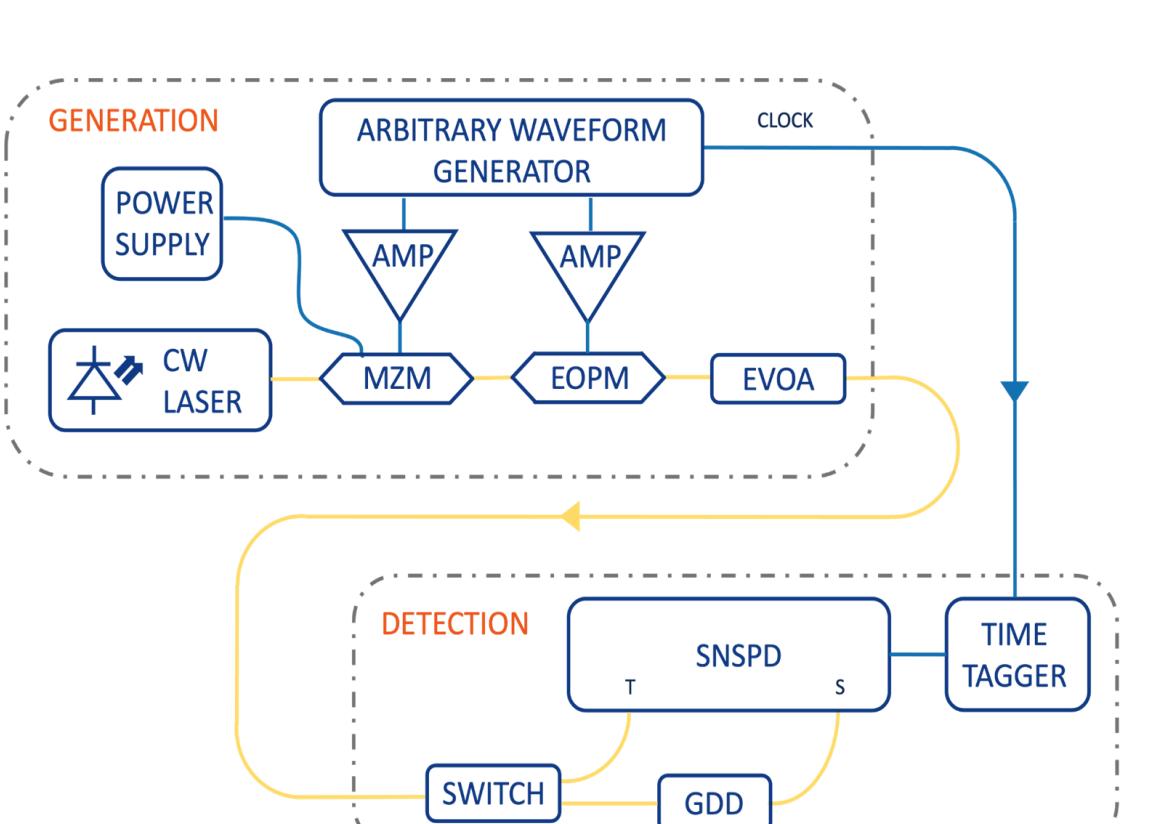
With dispersive medium we can detect time-bin superpositions in the single-photon-counting regime in an all-fiber setup without the use of interferometers. We showed that we can do that efficiently thanks to the temporal Talbot effect. Currently we are working on using this method for high-dimensional quantum key distribution.



Measured time of arrival histograms for superpositions of four pulses with equal time separation.

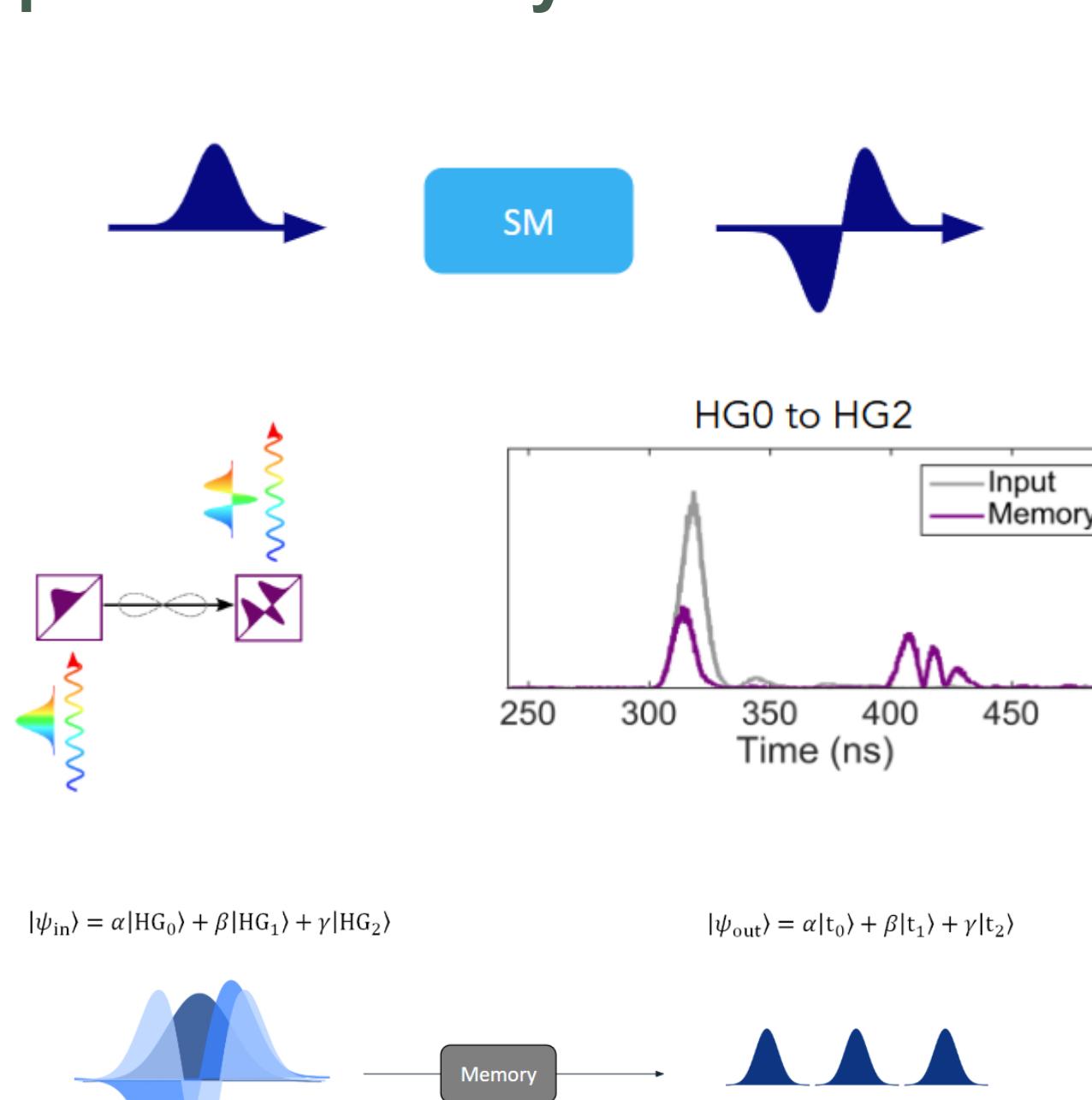
$$|\Theta_n\rangle = \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} e^{-2\pi i m n / d} |t_m\rangle$$

A. Widomski, M. Ogrodnik, M. Karpiński, Optica 11, 926 (2024).

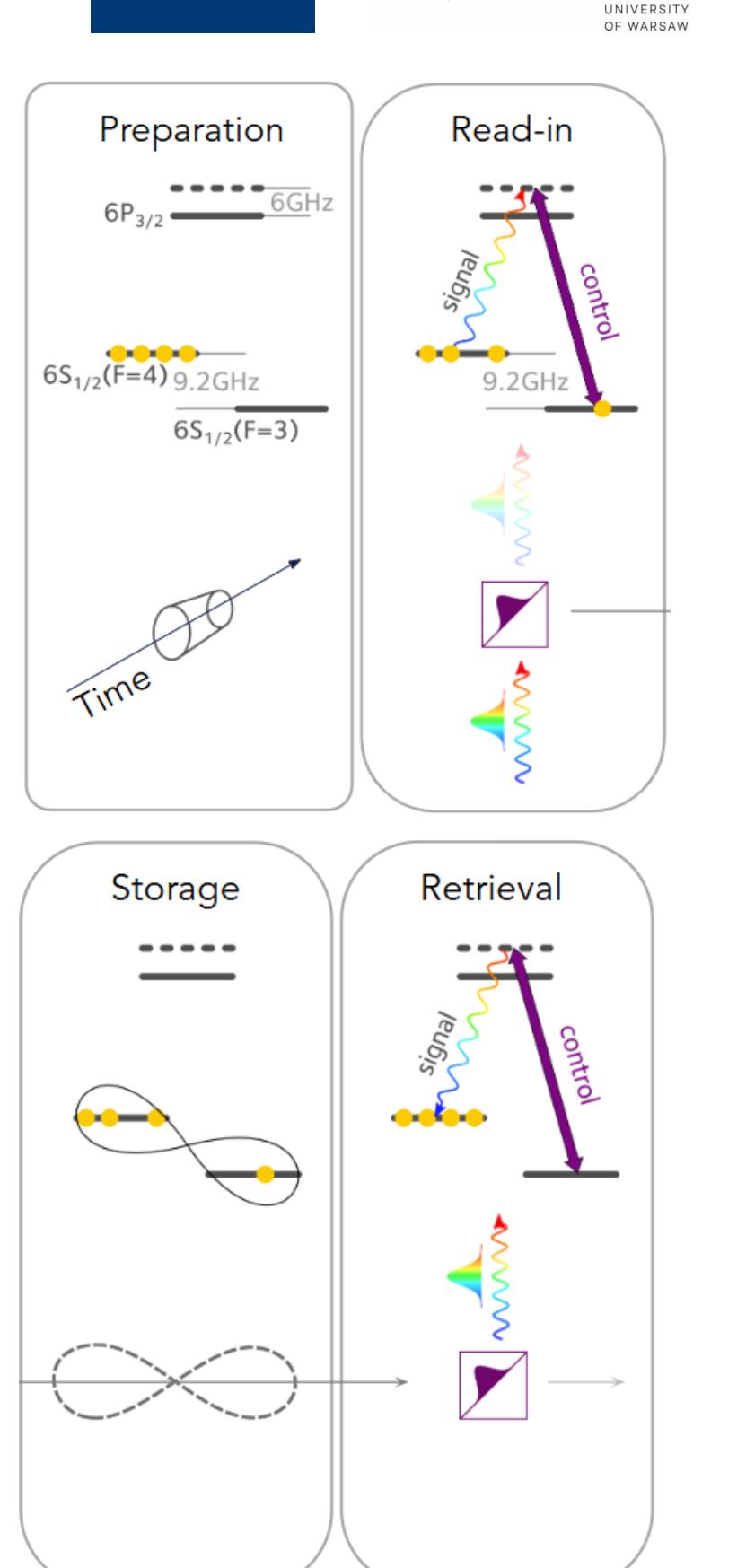


Pulses in time-bins are carved with Mach-Zehnder modulator (MZM) and phases are given by electro-optic phase modulator (EOPM). To detect superpositions pulses are transmitted through group delay dispersion medium (GDD).

Temporal mode manipulation using a quantum memory



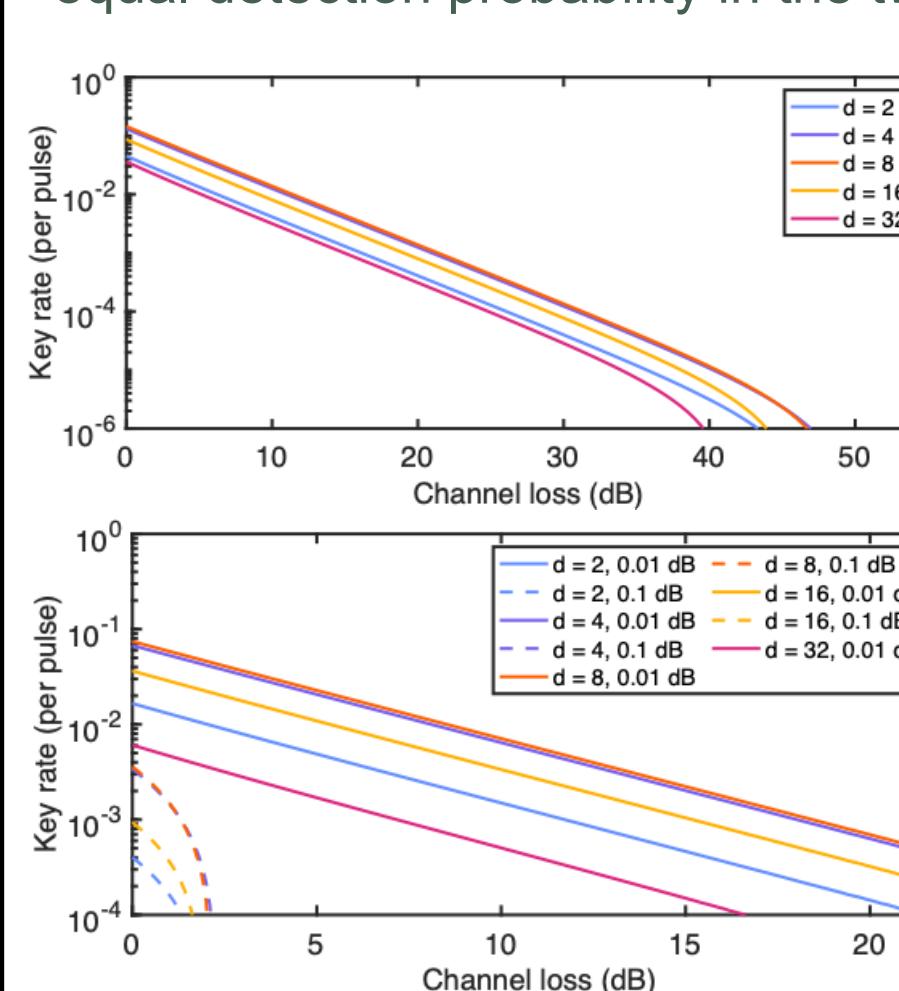
Multipass quantum memory approach was used to convert between overlapping temporal modes and nonoverlapping time bins.



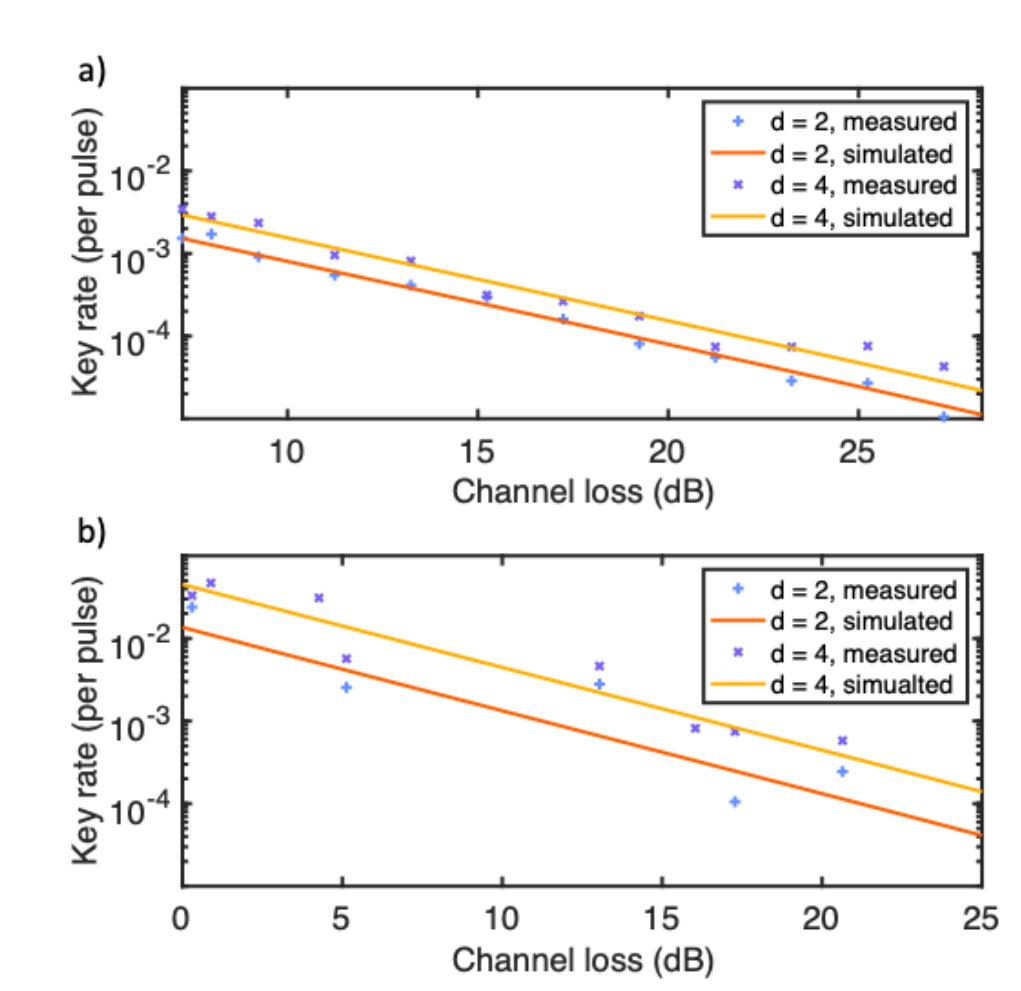
High-dimensional quantum key distribution with resource-efficient detection



By employing a detection scheme based on the temporal Talbot effect, we can perform QKD experiments using only a single detector per measurement, irrespective of the encoding dimension. We present experimentally-obtained secret key rates for both two-dimensional and four-dimensional scenarios, showing that a 4-dimensional encoding offers higher resistance to noise and information entropy than a qubit-based scheme. We show key rates according to two different security proofs – a standard BB84 protocol and a new tunable beam splitter (TBS) protocol [Grasselli2025], developed within QuICHE, which allows dropping assumption about equal detection probability in the two bases.



Ogrodnik et.al. Optica Quantum (2025),
Grasselli et.al., Phys. Rev. Applied 23, 044011 (2025)



Measured BB84 key rates: a) in-lab
b) over urban dark fibers in Warsaw