

Device-Independent Quantum Key Distribution Between Two Ion Trap Nodes



David Nadlinger, Ion Trap Quantum Computing group
ECCTI 2022, June 30th, Geneva





PIs

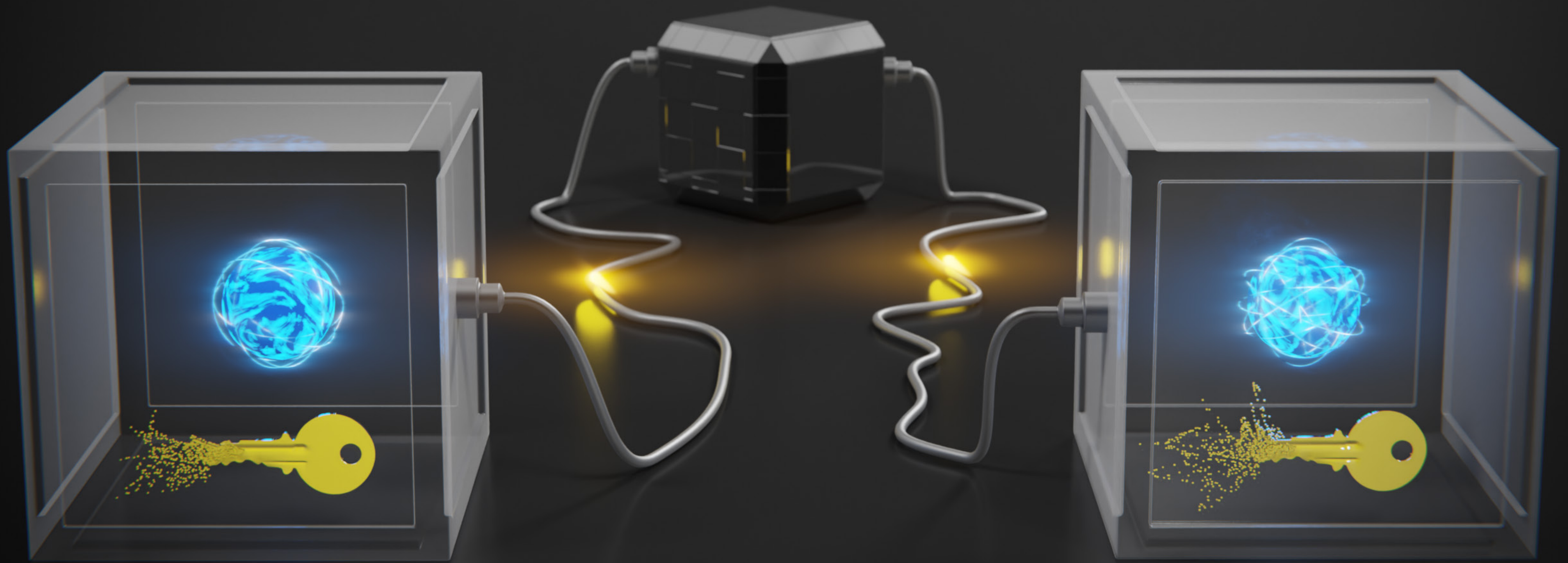
David Lucas
Chris Ballance

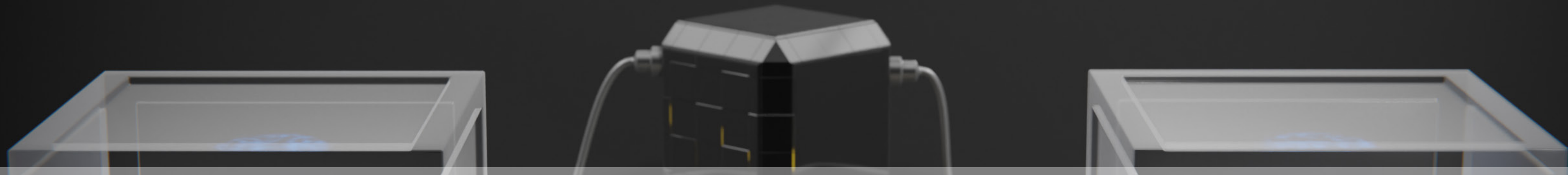
Postdocs

Joe Goodwin
Ryan Hanley
[Gabriel Araneda-Machuca](#)
Mariella Minder
Fabian Pokorny
[Raghu Srinivas](#)
Jake Blackmore
Mario Gely
Amy Hughes

Students

Clemens Löschnauer
[David Nadlinger](#)
[Beth Nichol](#)
[Peter Drmota](#)
William Hughes
Marius Weber
Oana Bazavan
Ana Sotirova
Sebastian Saner
[Dougal Main](#)
Kaitlin Gili
Jamie Leppard
Andrés Vazqu ez-Brennan



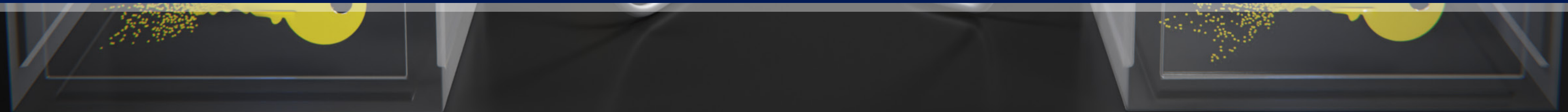


» What is DIQKD?

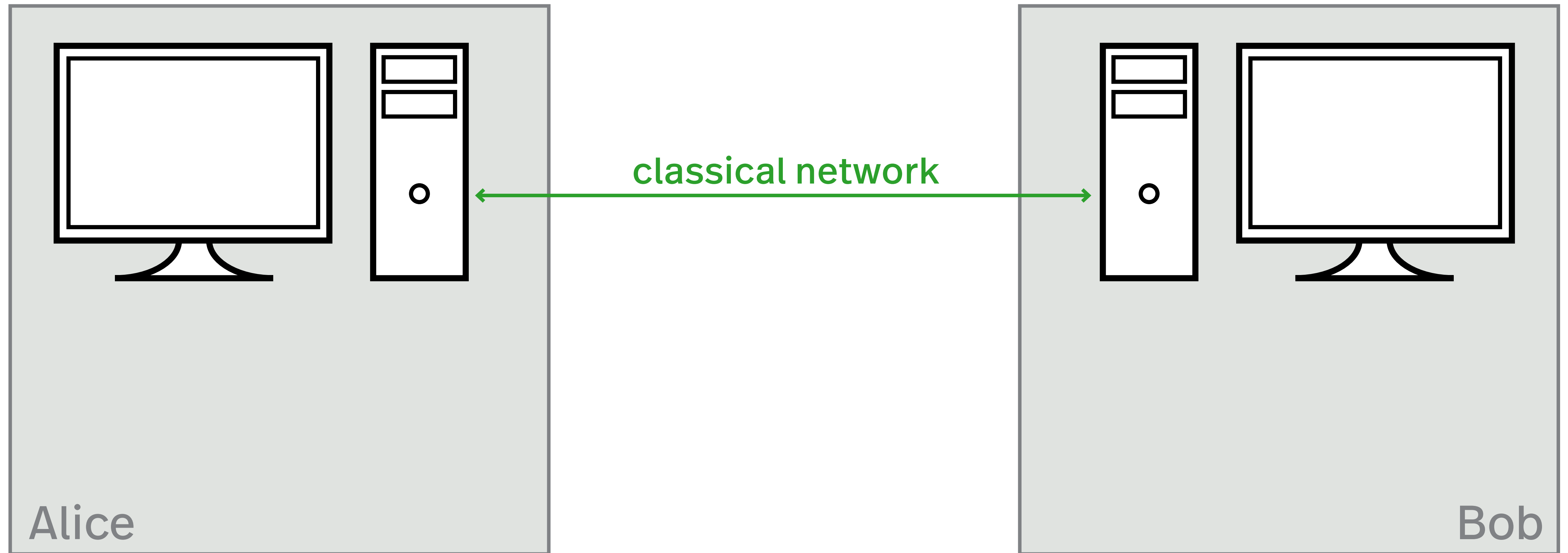
» Ion-trap network

» Micromotion
compensation

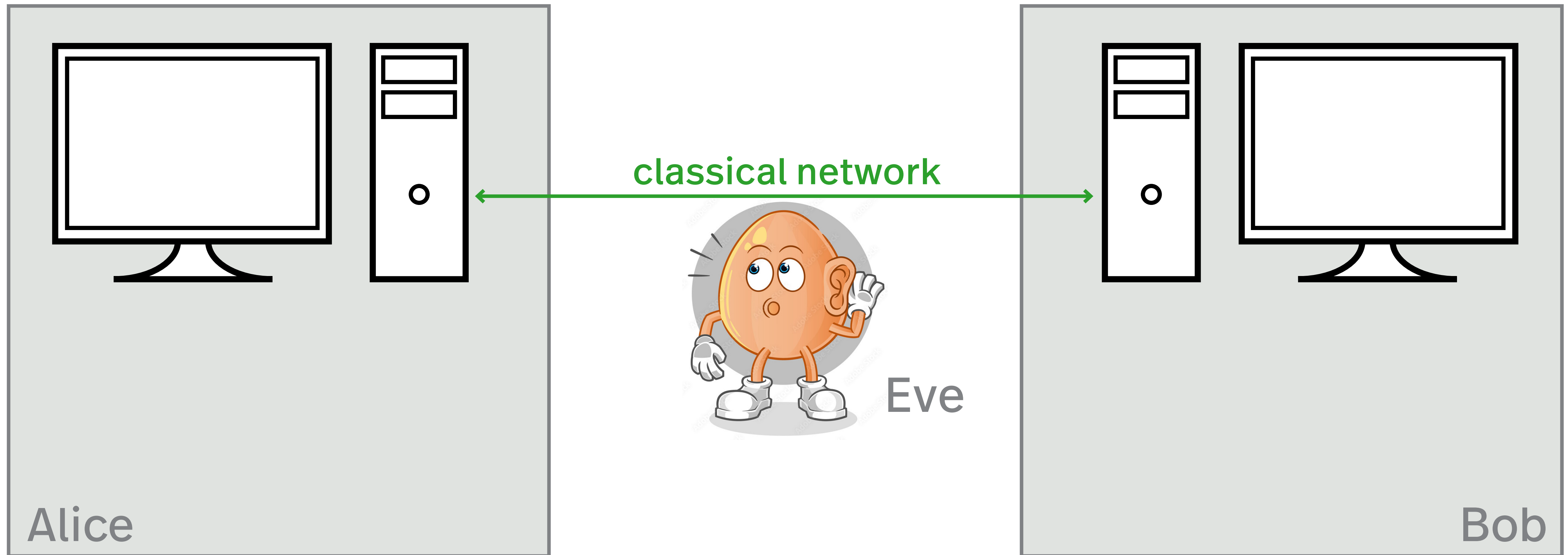
» Results



Device-Independent Quantum Cryptography

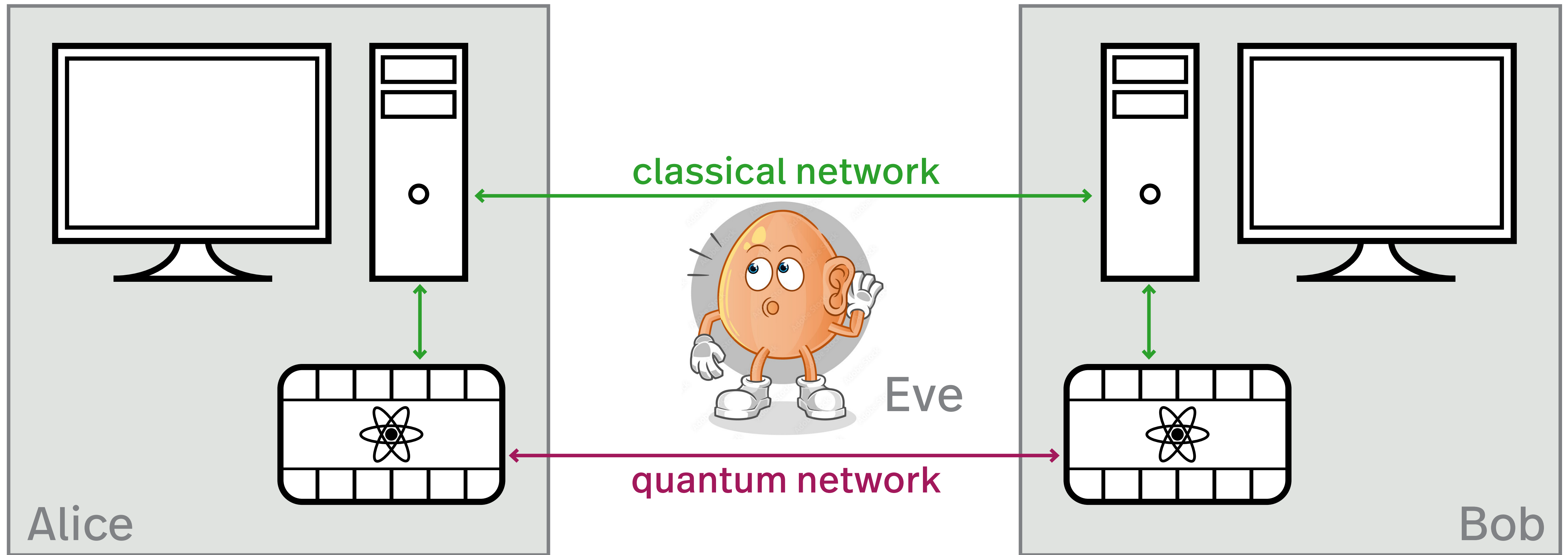


Device-Independent Quantum Cryptography



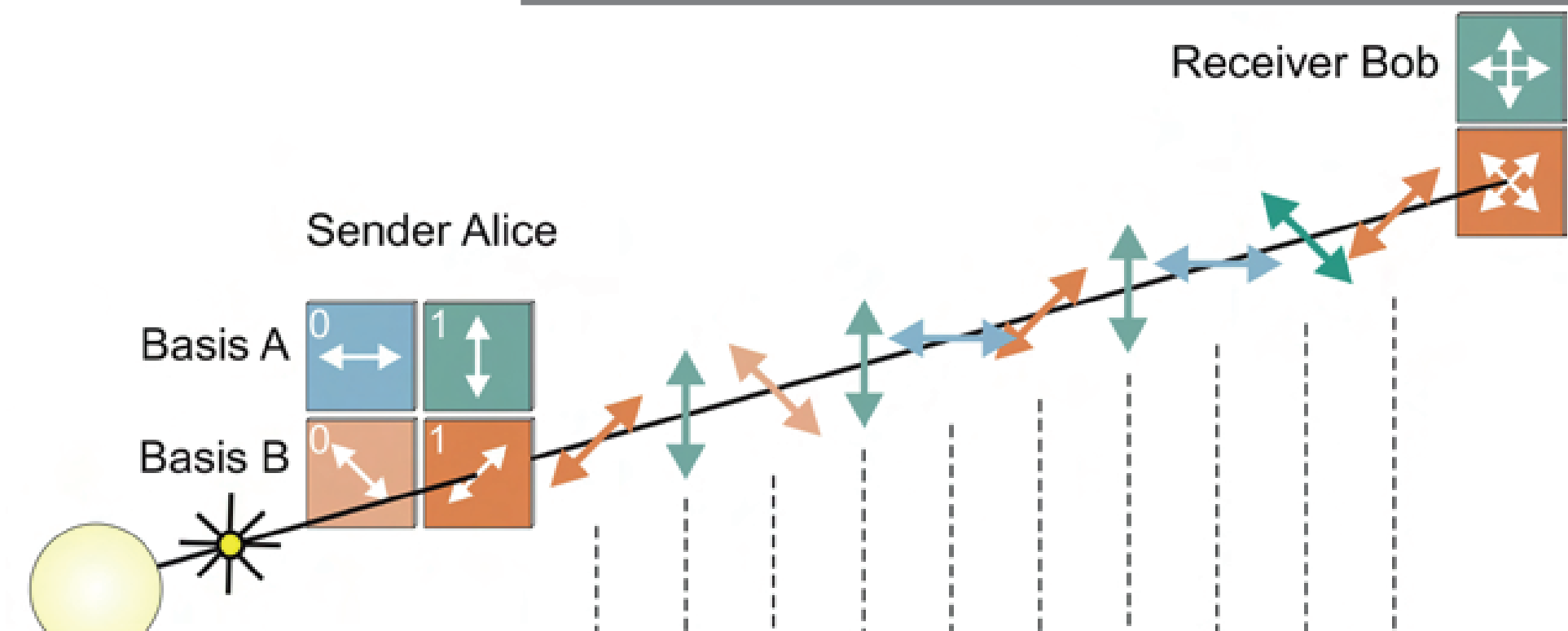
- » Only one-time pad information-theoretically secure (key length = message length)

Device-Independent Quantum Cryptography

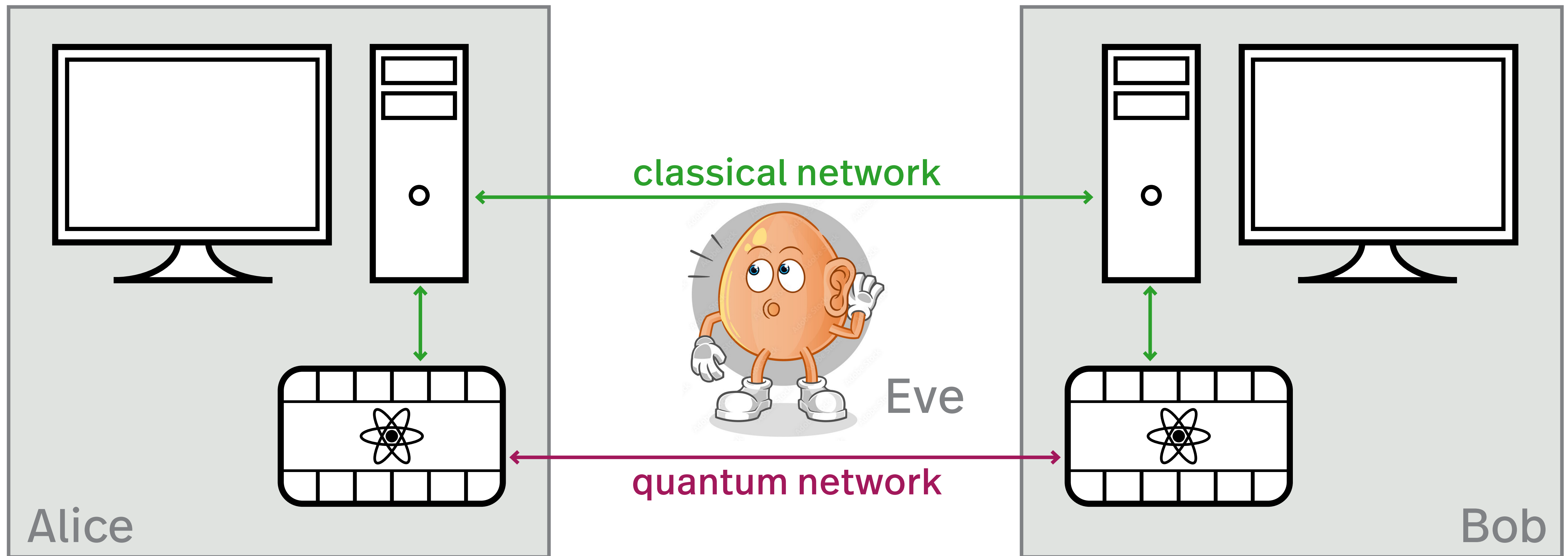


- » Established implementations (BB84, decoy states, ...)

Gisin et al. (2002), doi:10.1103/RevModPhys.74.145



Device-Independent Quantum Cryptography



- » Established implementations
(BB84, decoy states, ...)

Gisin et al. (2002), doi:10.1103/RevModPhys.74.145

- » Trusted device models
→ “quantum hacking”!

Lydersen et al. (2010), doi:10.1038/nphoton.2010.214

Garcia-Escartin et al. (2020), doi:10.1371/journal.pone.0236630

Device-Independent Quantum Cryptography



LETTERS

PUBLISHED ONLINE: 29 AUGUST 2010 | DOI: 10.1038/NPHOTON.2010.214

nature
photonics

PHYSICAL REVIEW A

Quantum hacking: Experimental demonstration against practical quantum...

Yi Zhao, Chi-Hang Fred Fung, Bing Q...
Center for Quantum Information and Quantum Control
and Computer Engineering, University of T...
(Received 8 August 2007; ...)

Quantum-key-distribution (QKD) systems can send information over optical fiber and are widely believed to be secure. However, a time-shift attack—against a popular belief, an eavesdropper, Eve, has a non-zero probability of success. Eve's success is due to the well-known Bell's inequalities. Therefore, the detection efficiency of QKD systems is also in technological applications such as...

DOI: [10.1103/PhysRevA.78.042333](https://doi.org/10.1103/PhysRevA.78.042333)

Hacking commercial quantum cryptography systems by tailored...

Lars Lydersen^{1,2*}, Carlos Wiechers^{3,4,5}, Ch...
and Vadim Makarov¹

The peculiar properties of quantum mechanics allow two remote parties to communicate a private, secret key protected from eavesdropping by the laws of physics. This is called quantum key distribution (QKD) and it is widely believed to always rely on detectors to measure the relevant quantum property of single photons⁵. Here we demonstrate that the detectors in two commercially available QKD systems can be fully remote-controlled using simple bright illumination. This makes it possible to track the full secret key; we propose an eavesdropping attack built from off-the-shelf components. The loopback attack is present in most QKD systems using avalanche photodiodes to detect single photons. We believe that this attack is crucial for strengthening the security of practical QKD systems and patching technological deficiencies.

The field of quantum key distribution has evolved over several decades. Today, quantum key distribution (QKD) laboratories can generate key over fibre channels of up to 250 km (ref. 6), and a few QKD systems are even commercially available, promising enhanced security for data communication. In all proofs for the security of QKD, assumptions are made about the devices involved. However, the component-level realization of QKD systems is often not fully understood.

RESEARCH ARTICLE

Attacking quantum key distribution by light injection via ventilation openings

Juan Carlos Garcia-Escartin^{1*}, Shihan Sajeed^{2,3,4,5}, Vadim Makarov^{4,6,7,8}

¹ Dpto. Teoría de la Señal y Comunicaciones e Ingeniería Telemática, Universidad de Valladolid, Valladolid, Spain, ² Institute for Quantum Computing, University of Waterloo, Waterloo, ON, Canada, ³ Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, ⁴ Department of Physics and Astronomy, University of Toronto, Toronto, ON, Canada, ⁵ Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada, ⁶ Russian Quantum Center, Skolkovo, Moscow, Russia, ⁷ Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information, University of Science and Technology of China, Shanghai, People's Republic of China, ⁸ NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow, Russia

* juagar@tel.uva.es

Abstract

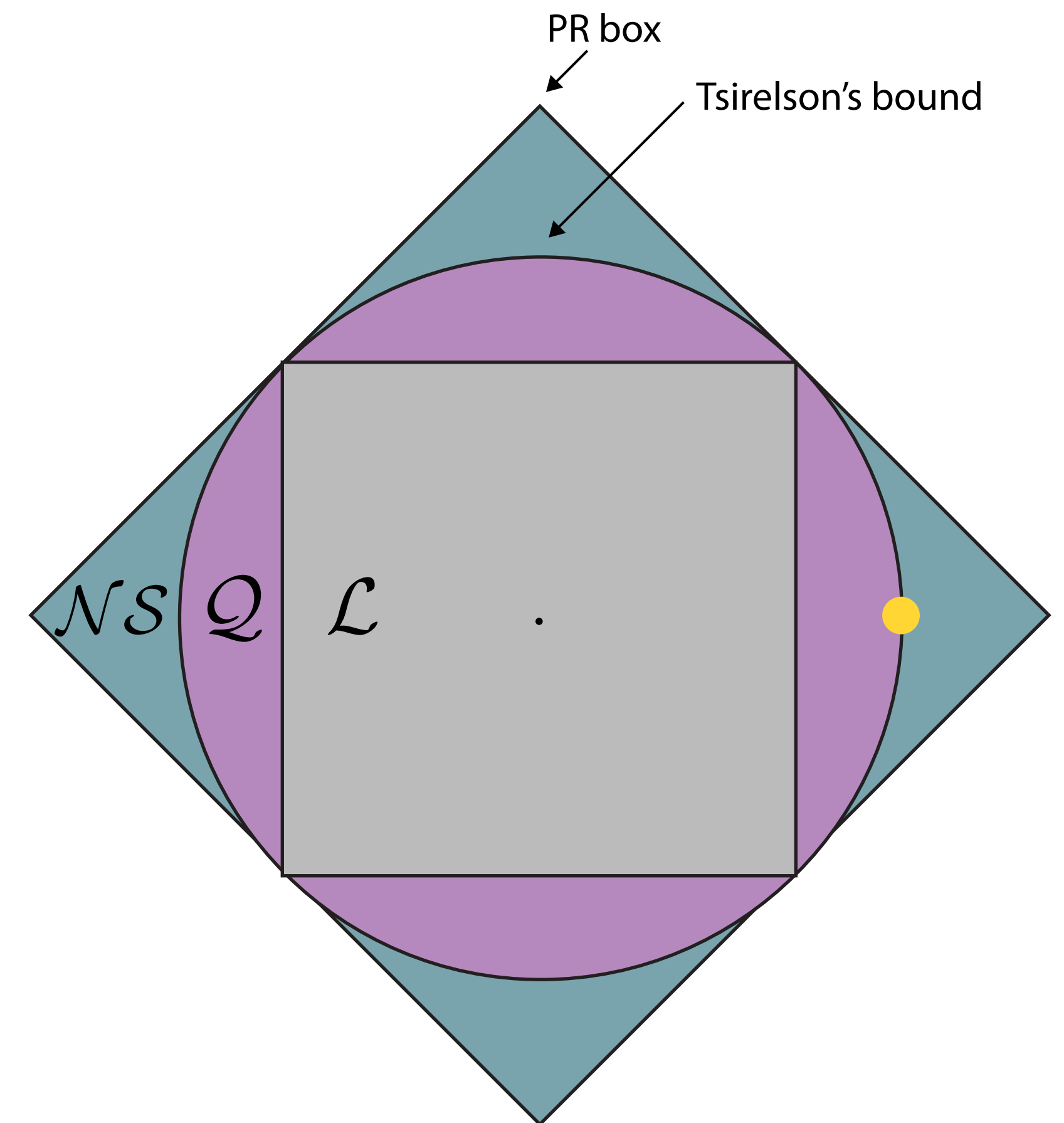
Device-Independent Quantum Cryptography

- » Quantum correlations have structure
- » Maximally-entangled states are “special”
→ monogamy of entanglement
- » With entanglement, can self-test QKD devices!

A. Ekert (1991), doi:10.1103/PhysRevLett.67.661

Mayers & Yao (2004), doi:10.5555/2011827.2011830

$$S := E(x, y) + E(x', y) + E(x, y') - E(x', y')$$

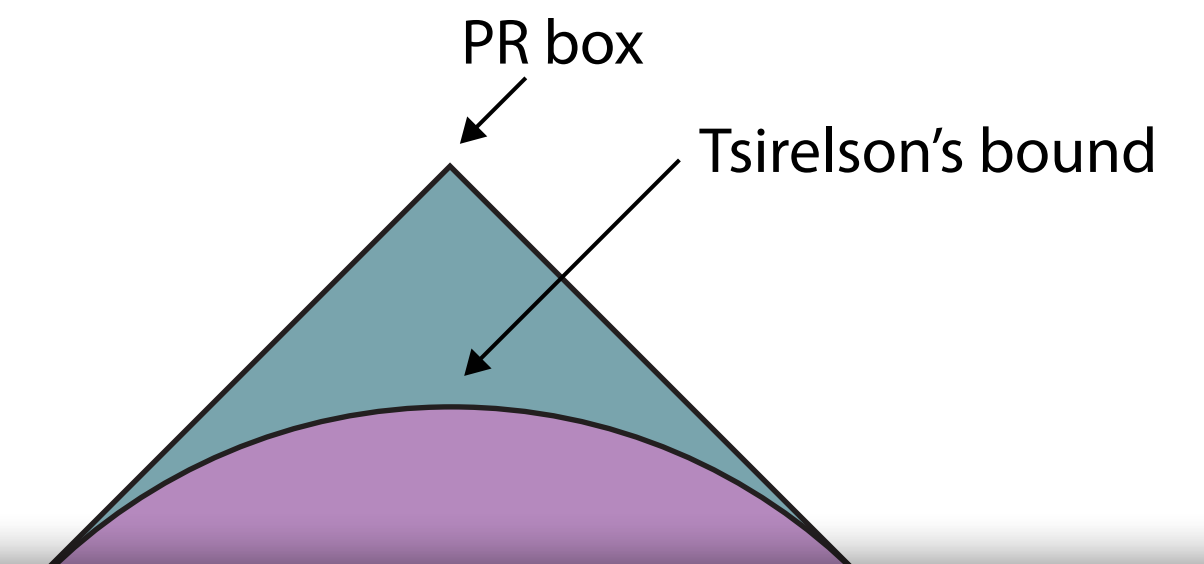


Brunner et al. (2014), doi:10.1103/RevModPhys.86.419

- » $|S| > 2$ non-classical
- » $|S| = 2\sqrt{2}$ max. entangled

Device-Independent Quantum Cryptography

- » Quantum correlations have structure
- » Maximally-entangled states are “s”
→ monogamy of entanglement
- » With entanglement, can self-test QKD devices!



VOLUME 67

5 AUGUST 1991

NUMBER 6

Quantum Cryptography Based on Bell's Theorem

Artur K. Ekert

Merton College and Physics Department, Oxford University, Oxford OX1 3PU, United Kingdom
(Received 18 April 1991)

Practical application of the generalized Bell's theorem in the so-called key distribution process in cryptography is reported. The proposed scheme is based on the Bohm's version of the Einstein-Podolsky-Rosen *gedanken experiment* and Bell's theorem is used to test for eavesdropping.

PACS numbers: 03.65.Bz, 42.80.Sa, 89.70.+c

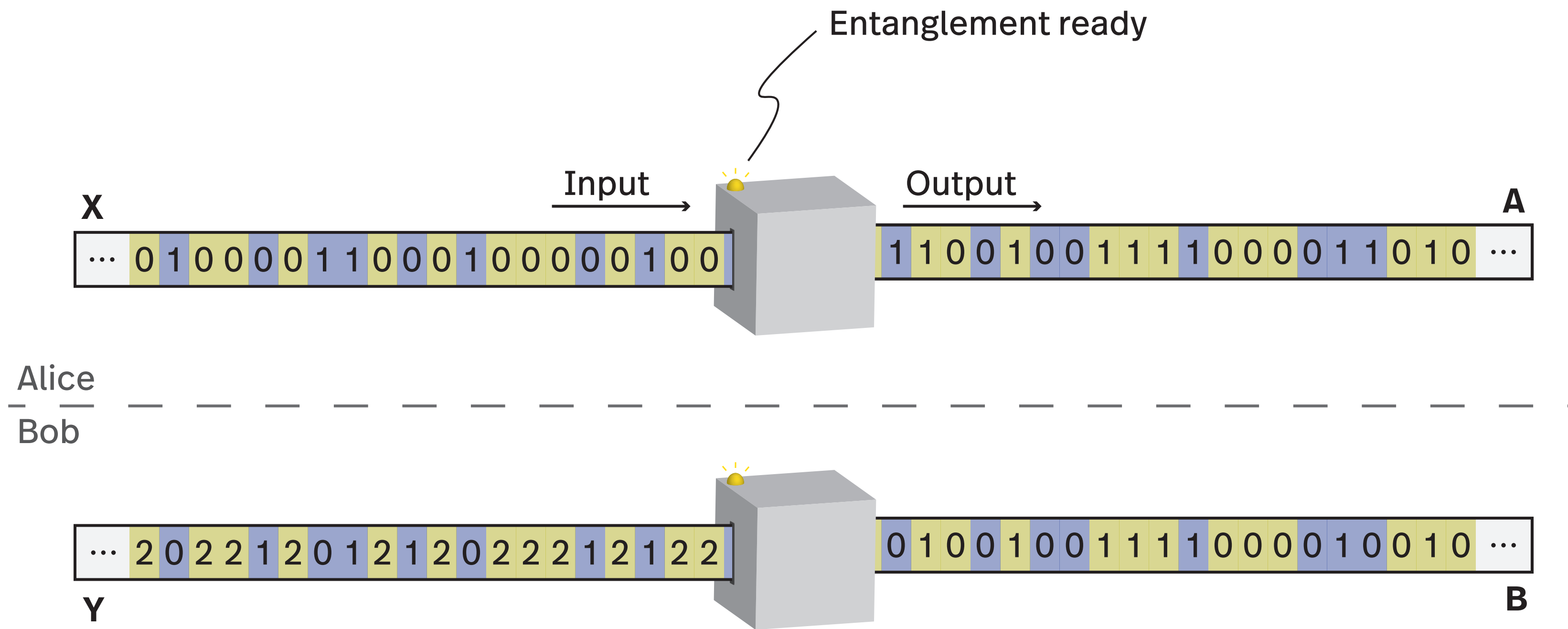
Cryptography, despite a colorful history that goes back to 400 B.C., only became part of mathematics and information theory this century, in the late 1940s, mainly due to the seminal papers of Shannon [1]. Today, one can briefly define cryptography as a mathematical system of transforming information so that it is unintelligible and therefore useless to those who are not meant to have access to it. However, as the computational process associated with transforming the information is always performed by physical means, one cannot separate the mathematical structure from the underlying laws of physics that govern the process of computation [2]. Deutsch has shown that quantum physics enriches our computational possibilities far beyond classical Turing machines [2], and current work in quantum cryptography originated by Bennett and Brassard provides a good example of this fact [3].

set up to test Bell's theorem. Before I proceed any further let me first introduce some basic notions of cryptography.

Originally the security of a cryptotext depended on the secrecy of the entire encrypting and decrypting procedures; however, today we use ciphers for which the algorithm for encrypting and decrypting could be revealed to anybody without compromising the security of a particular cryptogram. In such ciphers a set of specific parameters, called a *key*, is supplied together with the plaintext as an input to the encrypting algorithm, and together with the cryptogram as an input to the decrypting algorithm. The encrypting and decrypting algorithms are publicly announced; the security of the cryptogram depends entirely on the secrecy of the key, and this key, which is very important, may consist of any *randomly chosen, sufficiently long string of bits*. Once the key is as

$$S := E(x, y) + E(x', y) + E(x, y)$$

Device-Independent Quantum Key Distribution

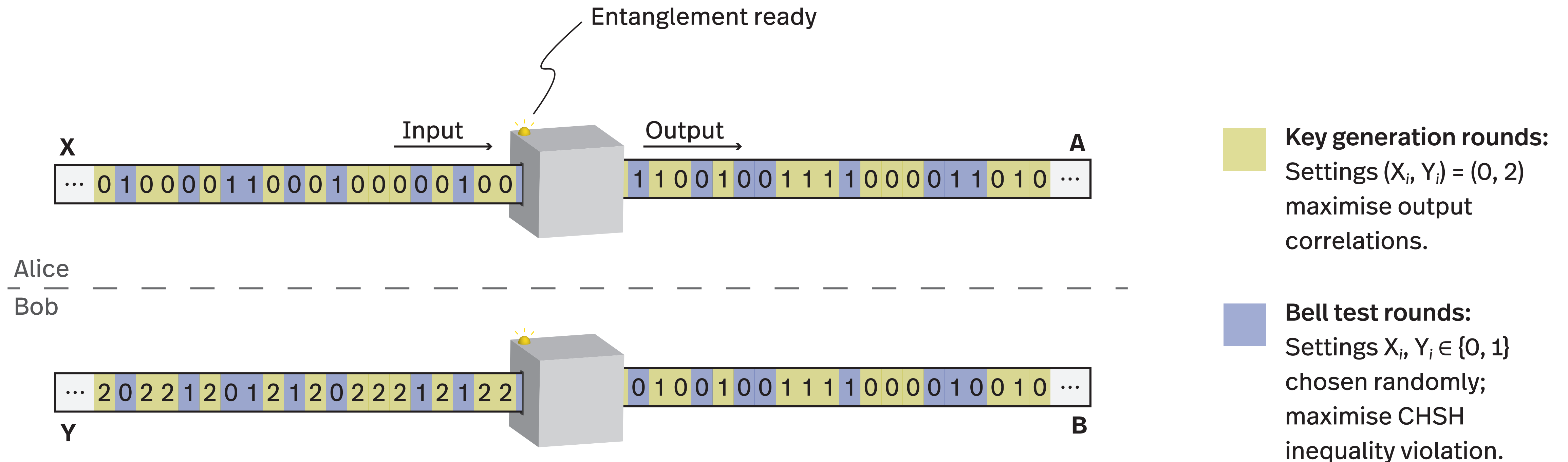


Key generation rounds:
 Settings $(X_i, Y_i) = (0, 2)$
 maximise output correlations.

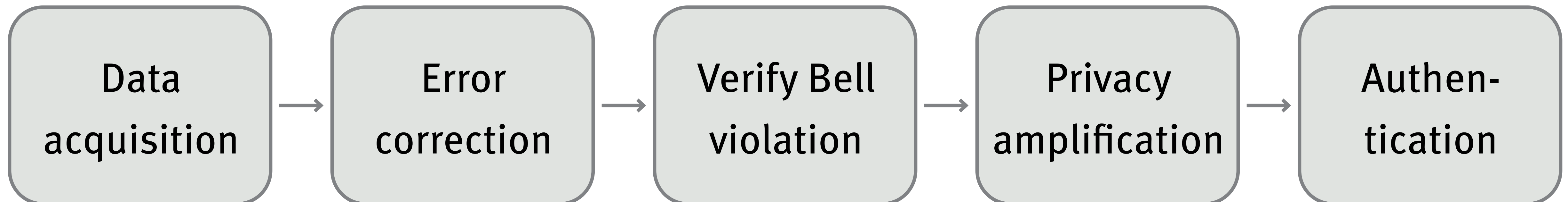
Bell test rounds:
 Settings $X_i, Y_i \in \{0, 1\}$
 chosen randomly;
 maximise CHSH inequality violation.

DPN et al. (2021), arXiv:2109.14600

Device-Independent Quantum Key Distribution



DPN et al. (2021), arXiv:2109.14600



Number of key bits is a balance of entropies

positive: private randomness in outputs

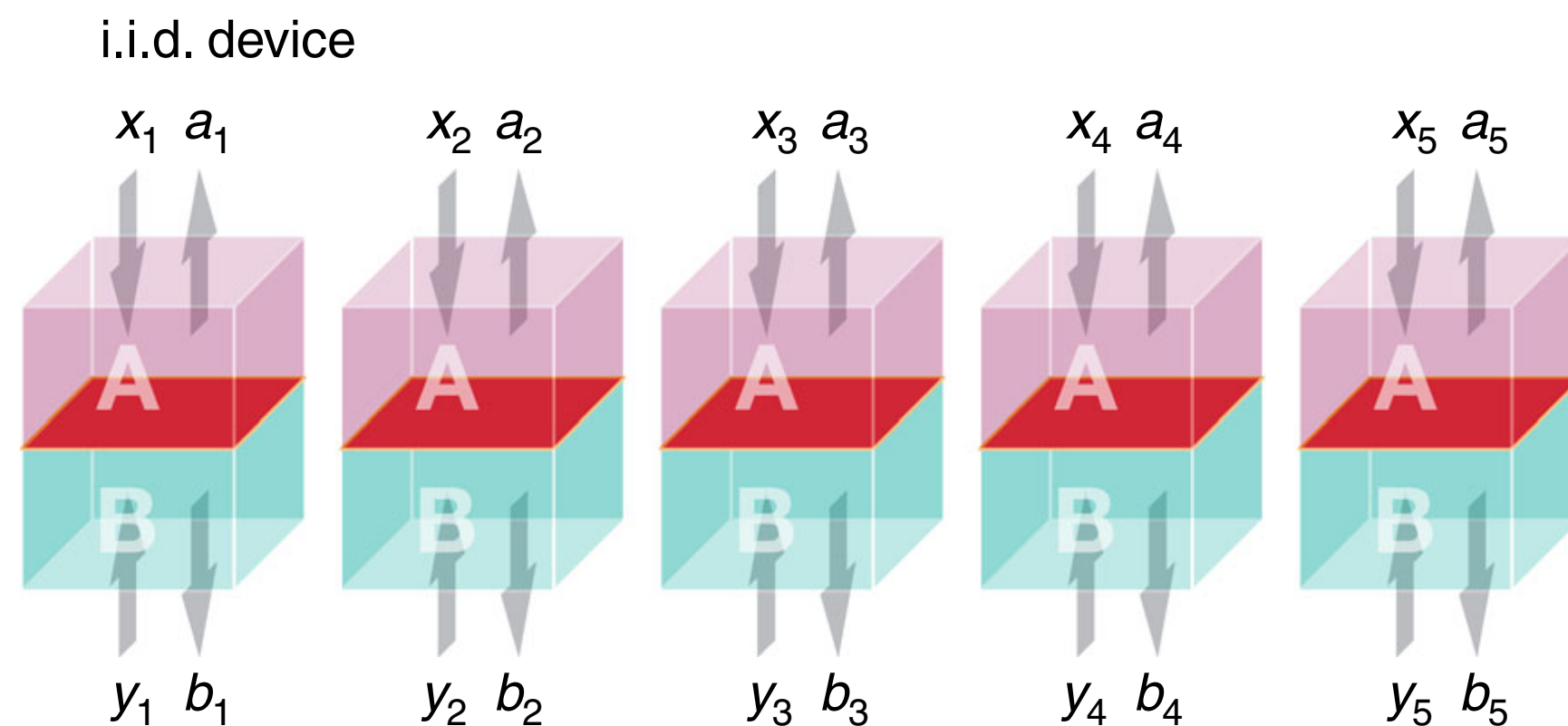
» key length

$l \approx$

$$\boxed{H(A|EXY)} - \boxed{H(A|BXY)}$$

negative: error correction cost

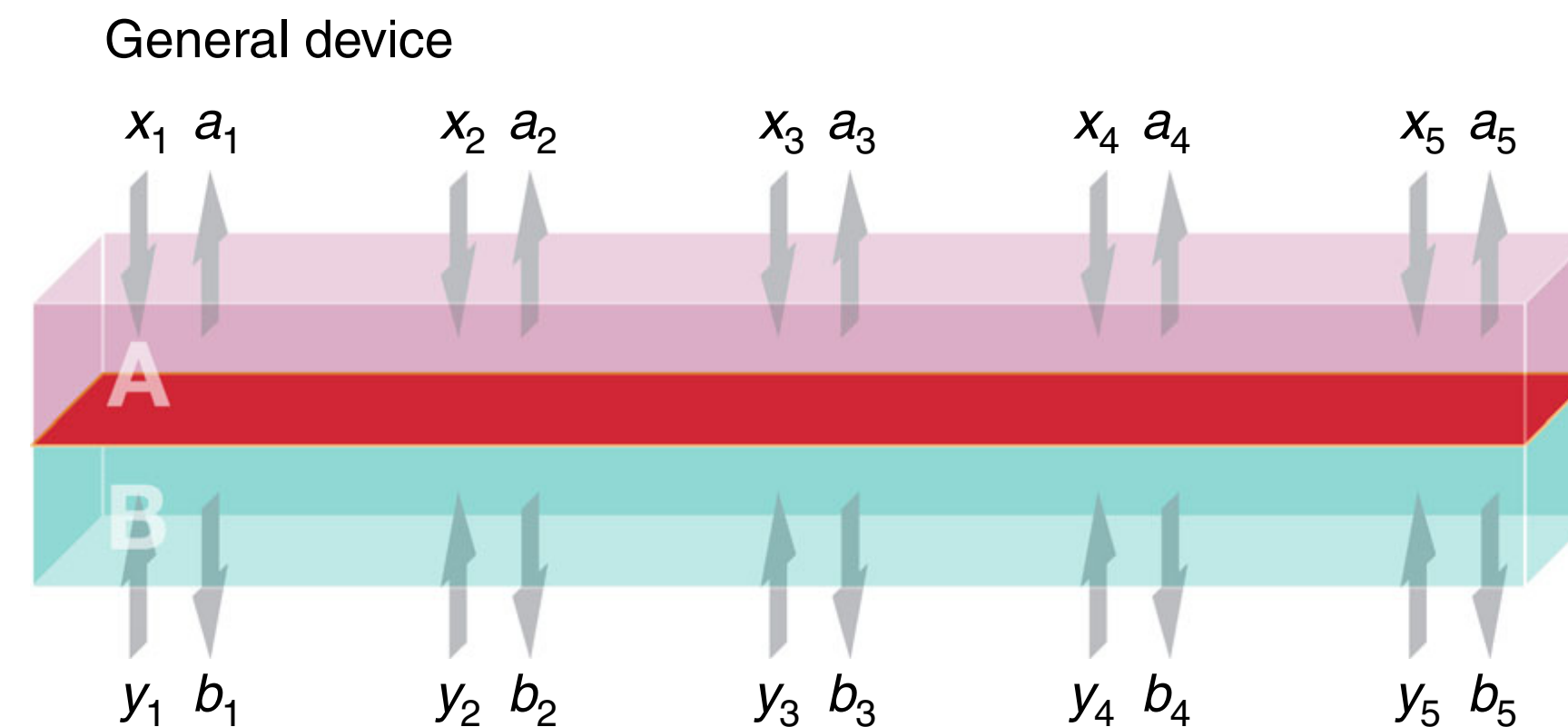
» Entropy accumulation theorem: i.i.d. behaviour to general security



Independent and identical behaviour

Arnon-Friedman et al. (2018), doi:10.1038/s41467-017-02307-4

General device

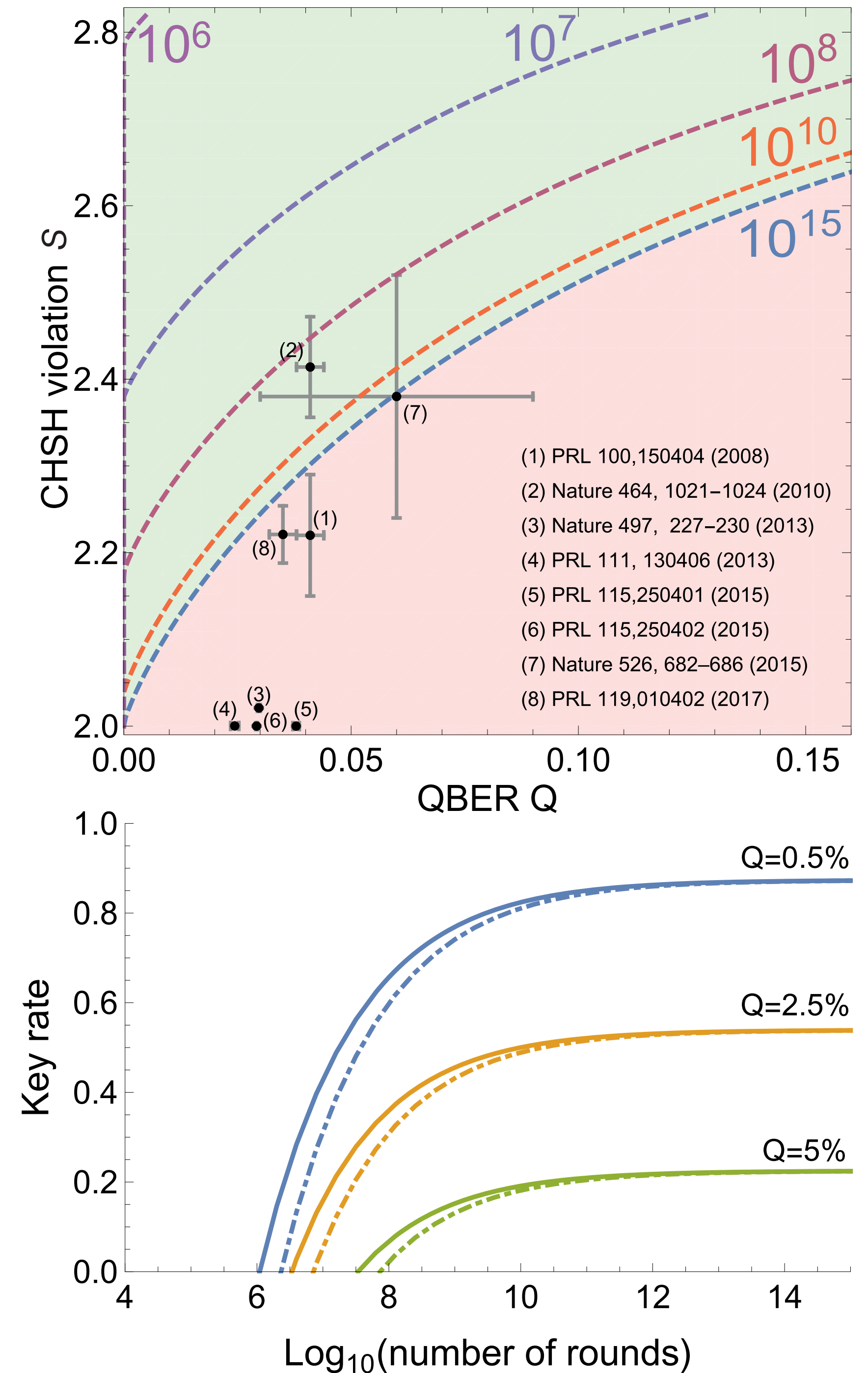


..... Sequential interaction>

» $H(A|EXY) \geq n h(S) - C\sqrt{n}$

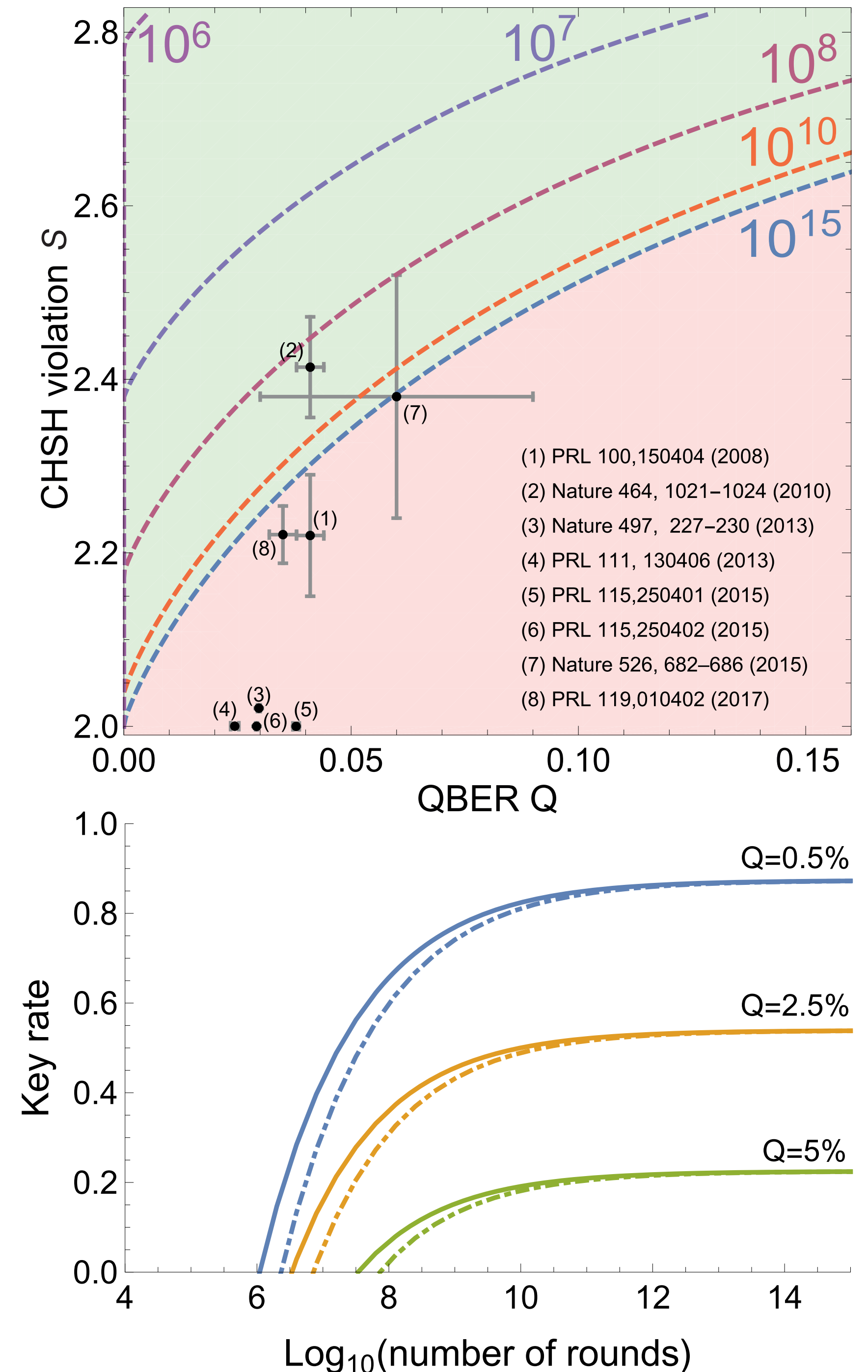
Requirements

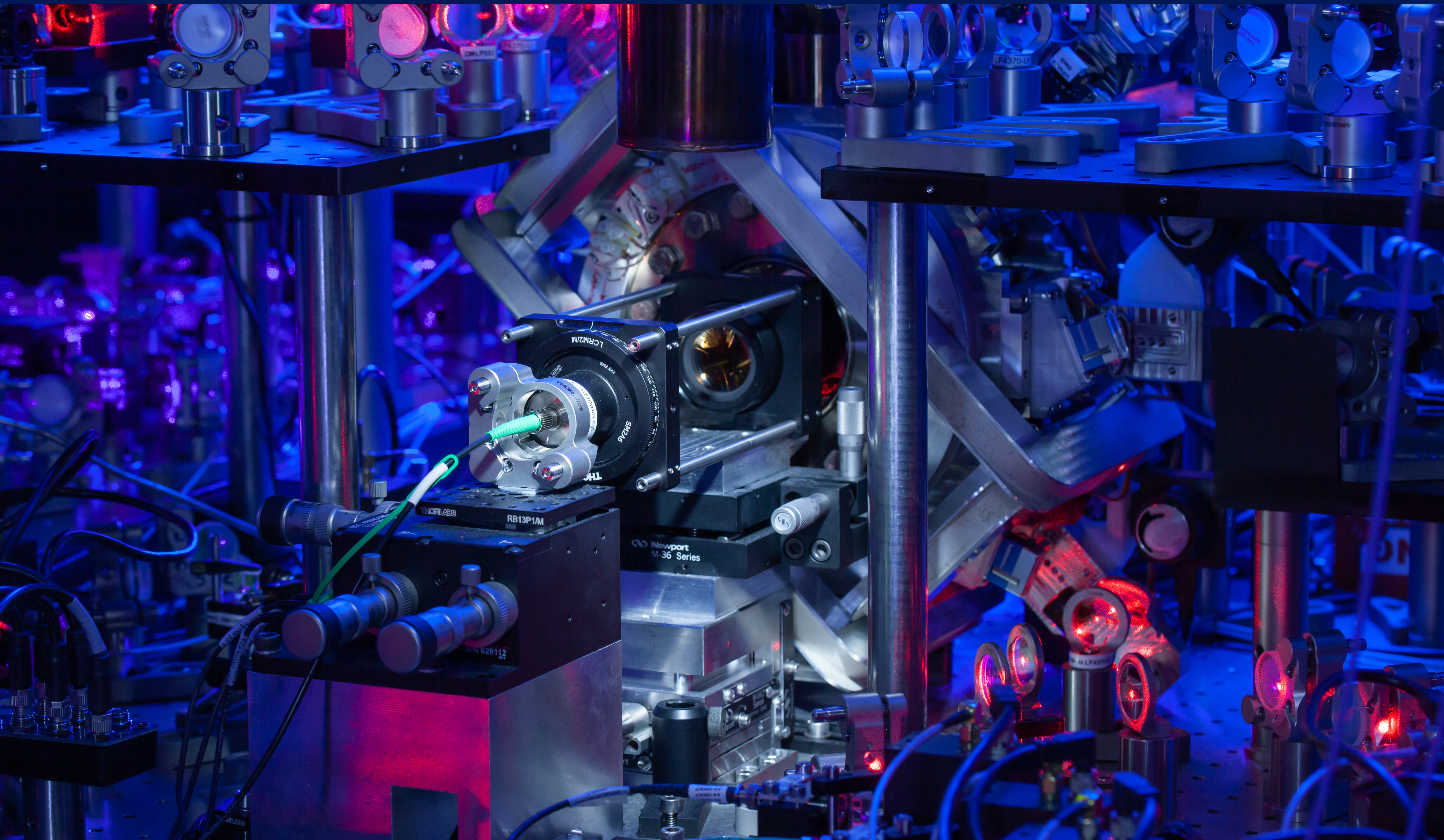
- » Bell test bounds Eve's information
→ $S \gg 2$, detection-loop-hole-free
- » Wrong correlations increase EC overhead
→ Q small
- » Finite statistics overhead
→ fast data acquisition



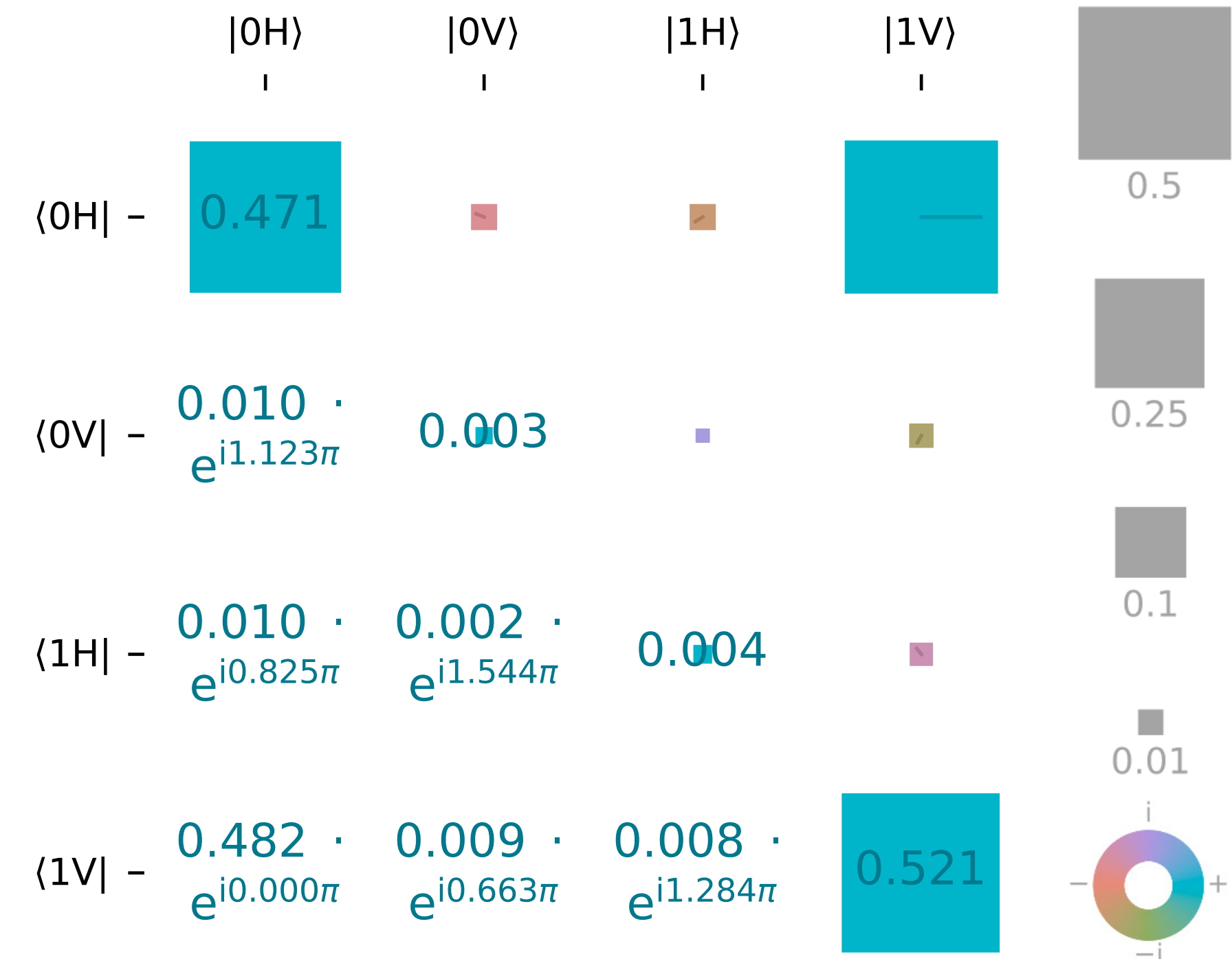
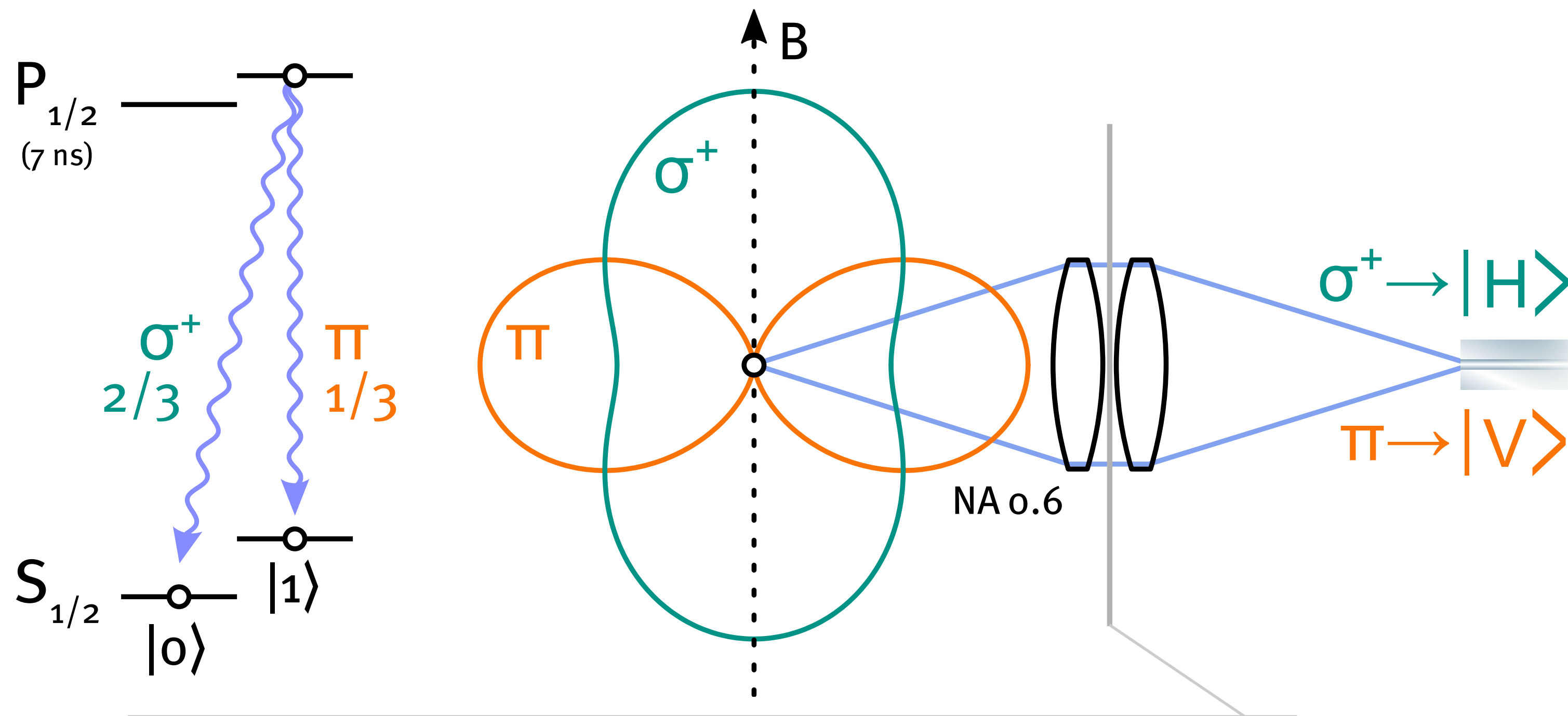
Requirements

- » Bell test bounds Eve's information
→ $S \gg 2$, detection-loop-hole-free
- » Wrong correlations increase EC overhead
→ Q small
- » Finite statistics overhead
→ fast data acquisition
- » Outcomes must not leak to Eve
→ isolation after entanglement established

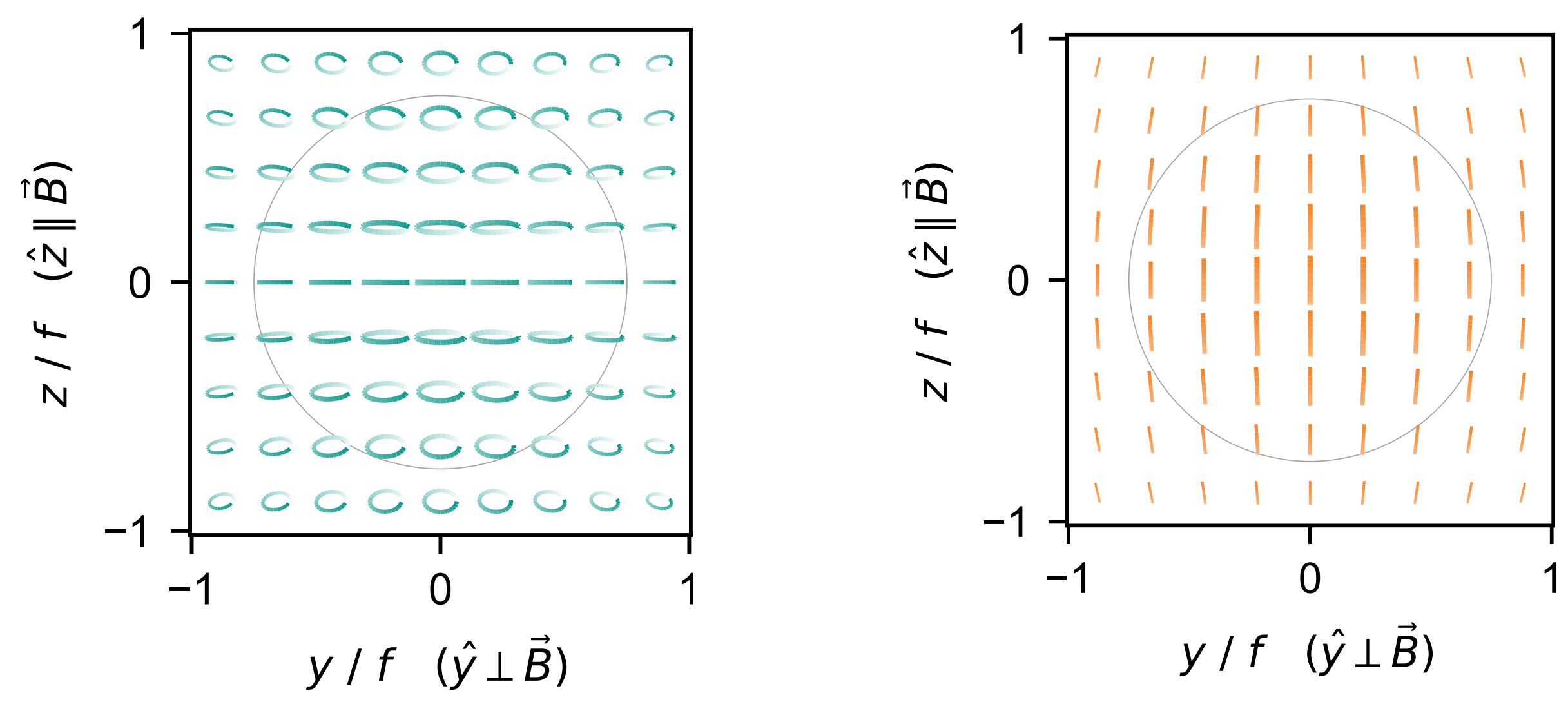




Free-space entanglement of $^{88}\text{Sr}^+$ ion and photon polarisation

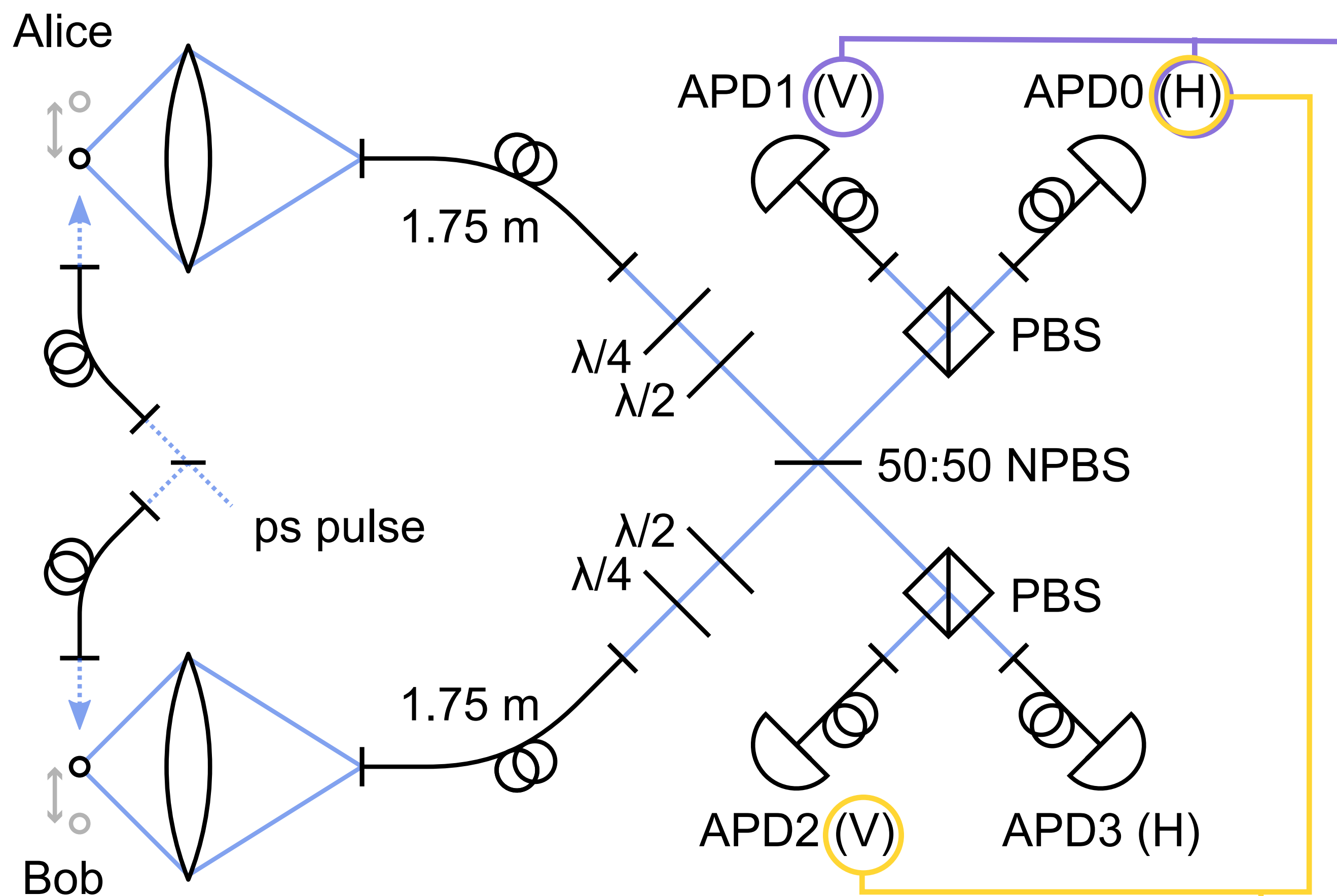


Stephenson, DPN et al. (2020), [10.1103/PhysRevLett.124.110501](https://doi.org/10.1103/PhysRevLett.124.110501)



- » Single-mode fibre avoids polarisation mixing
- » Measured fidelity: 97.90(12)%
- » Overall efficiency: 2.4(1)% (attempt rate: 1 MHz)

Heralded remote ion-ion entanglement



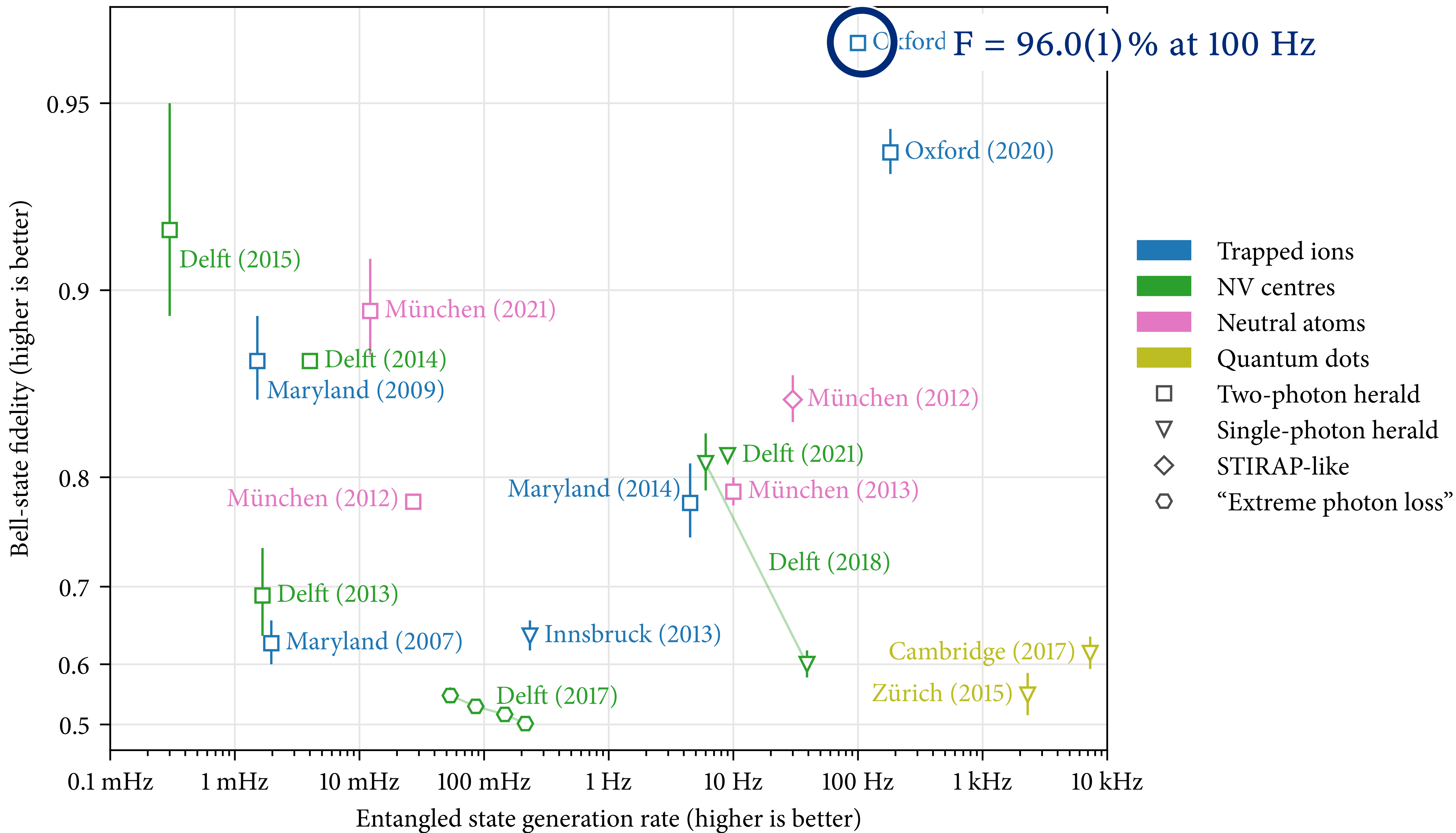
- » Measure 2 of 4 photon Bell states
→ swap entanglement onto ion pair
- » Move ions from focus to disconnect link

	$\langle 00 $ 	$\langle 10 $ 	$\langle 01 $ 	$\langle 11 $
$ 00\rangle -$	0.010			
$ 10\rangle -$	$0.049 \cdot e^{i1.859\pi}$	0.505		
$ 01\rangle -$	$0.043 \cdot e^{i1.363\pi}$	$0.468 \cdot e^{i1.532\pi}$	0.481	
$ 11\rangle -$	$0.003 \cdot e^{i0.931\pi}$	$0.021 \cdot e^{i0.749\pi}$	$0.028 \cdot e^{i1.158\pi}$	0.005

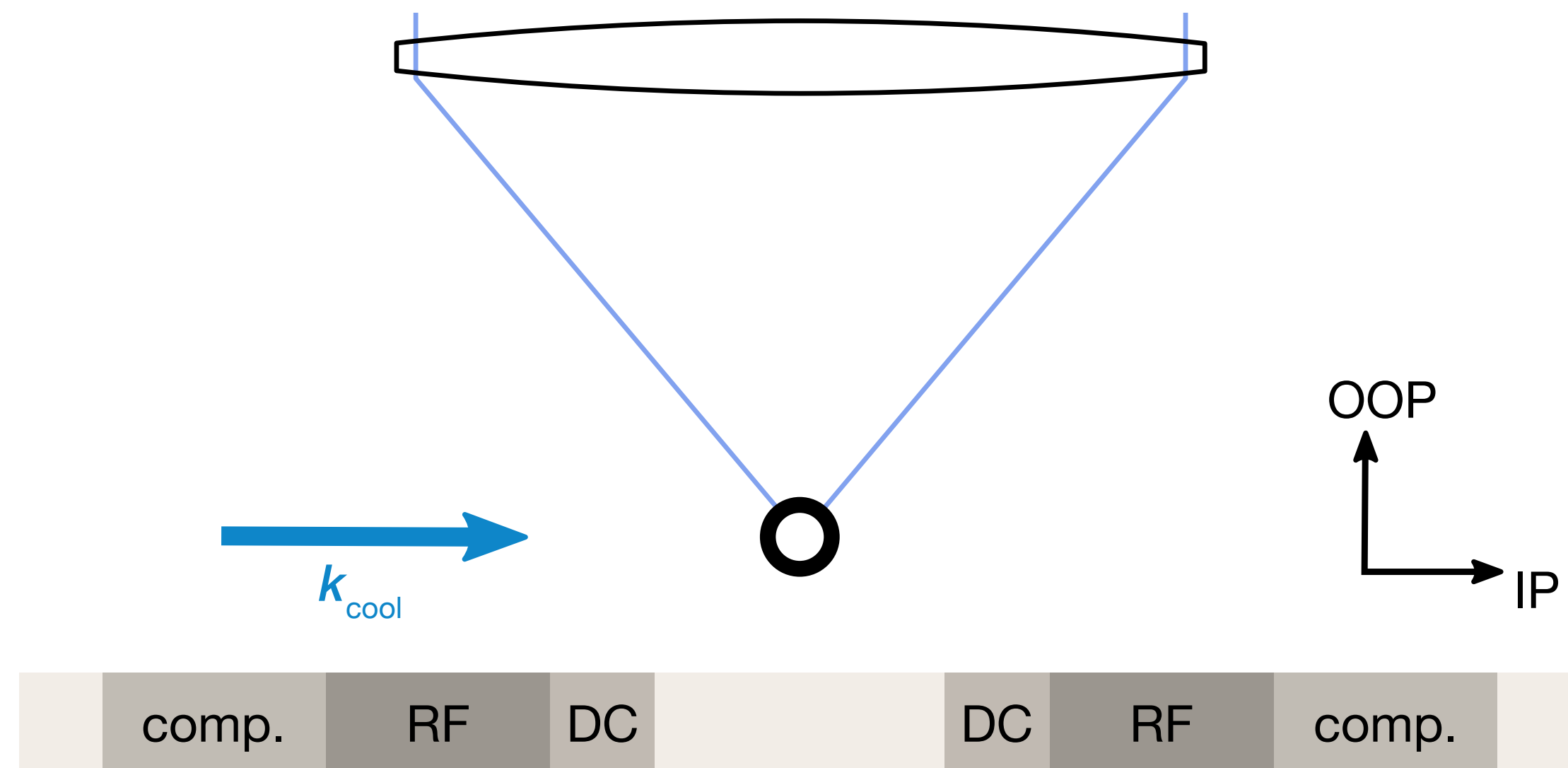
Stephenson, DPN et al. (2020), 10.1103/PhysRevLett.124.110501

$$|\psi\rangle_{AB} = \sqrt{\frac{1}{2}} (|\uparrow\rangle_A |\downarrow\rangle_B + e^{i\varphi} |\downarrow\rangle_A |\uparrow\rangle_B)$$

$$|\psi\rangle_{AB} = \sqrt{\frac{1}{2}} (|\uparrow\rangle_A |\downarrow\rangle_B + e^{i(\varphi+\pi)} |\downarrow\rangle_A |\uparrow\rangle_B)$$

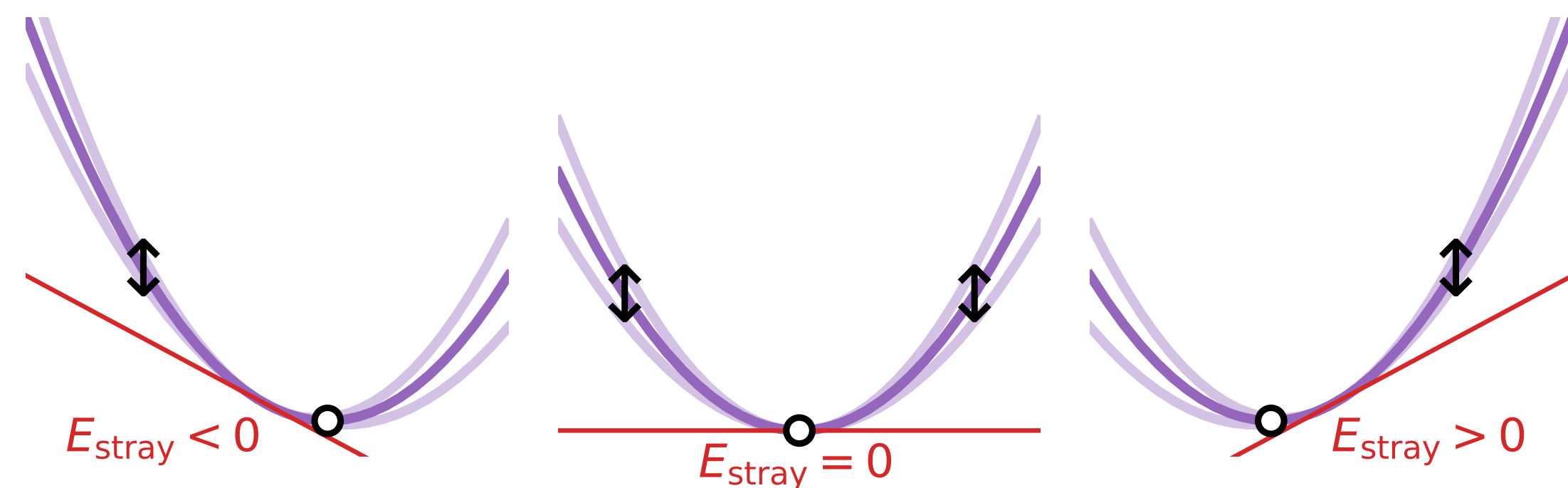
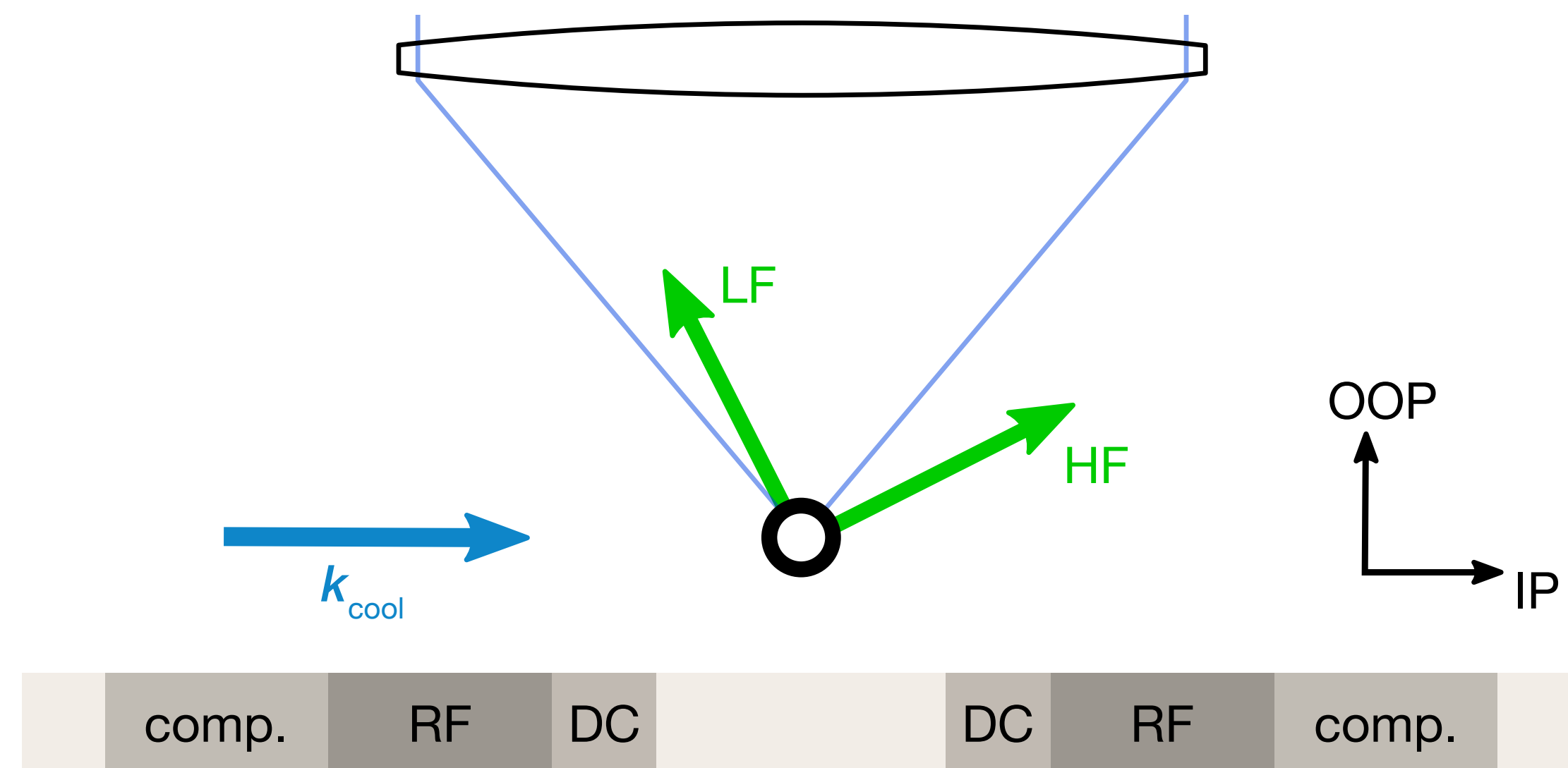


Micromotion compensation by parametric excitation



- » Challenge: Detect stray E field (displacement from RF null) normal to trap surface

Micromotion compensation by parametric excitation

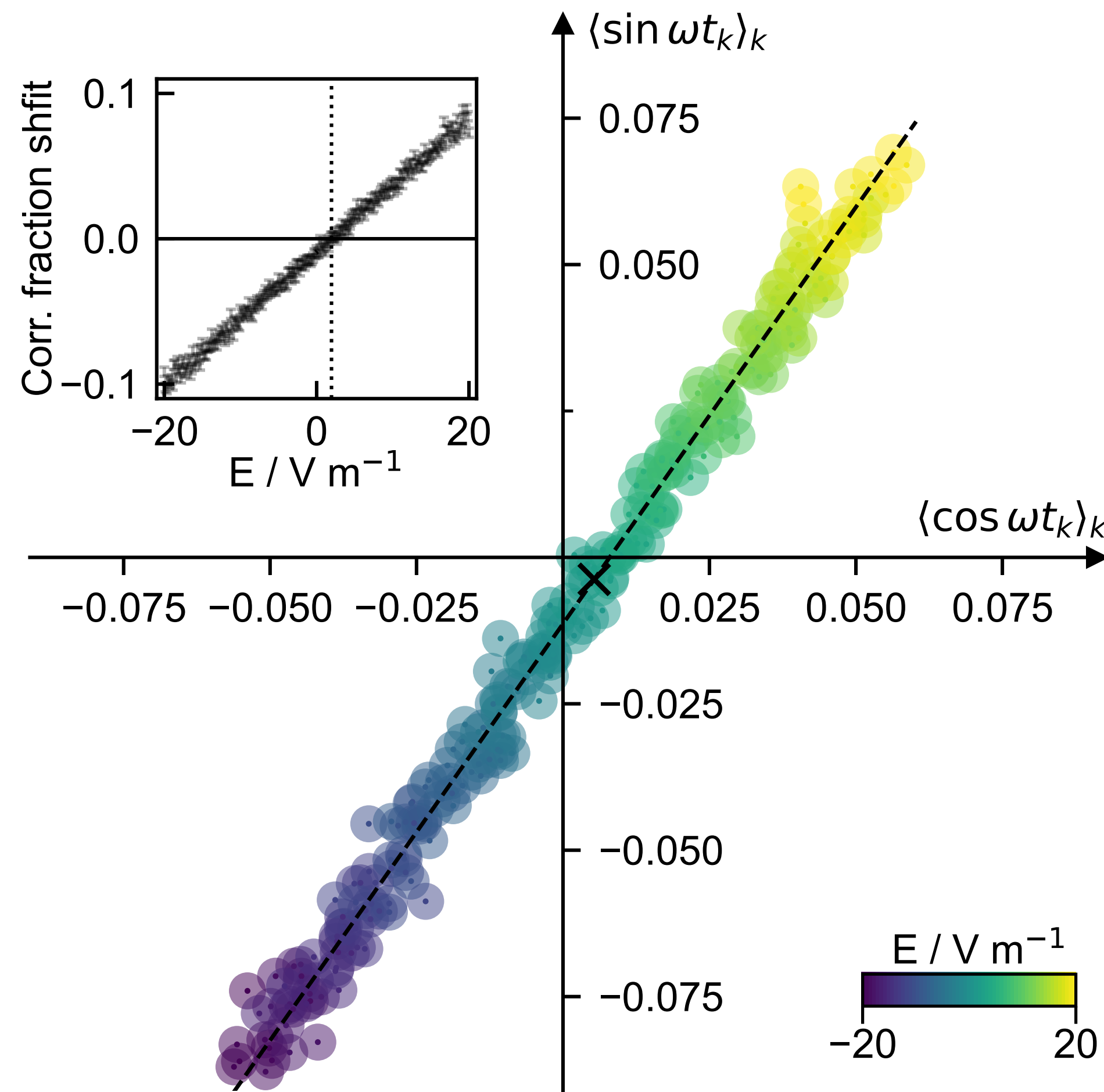


- » Challenge: Detect stray E field (displacement from RF null) normal to trap surface
- » Amplitude-modulate trap RF to map stray field to motion
- » Demodulate photon arrival times to detect motion

DPN et al., arXiv: 2107.00056

Micromotion compensation by parametric excitation

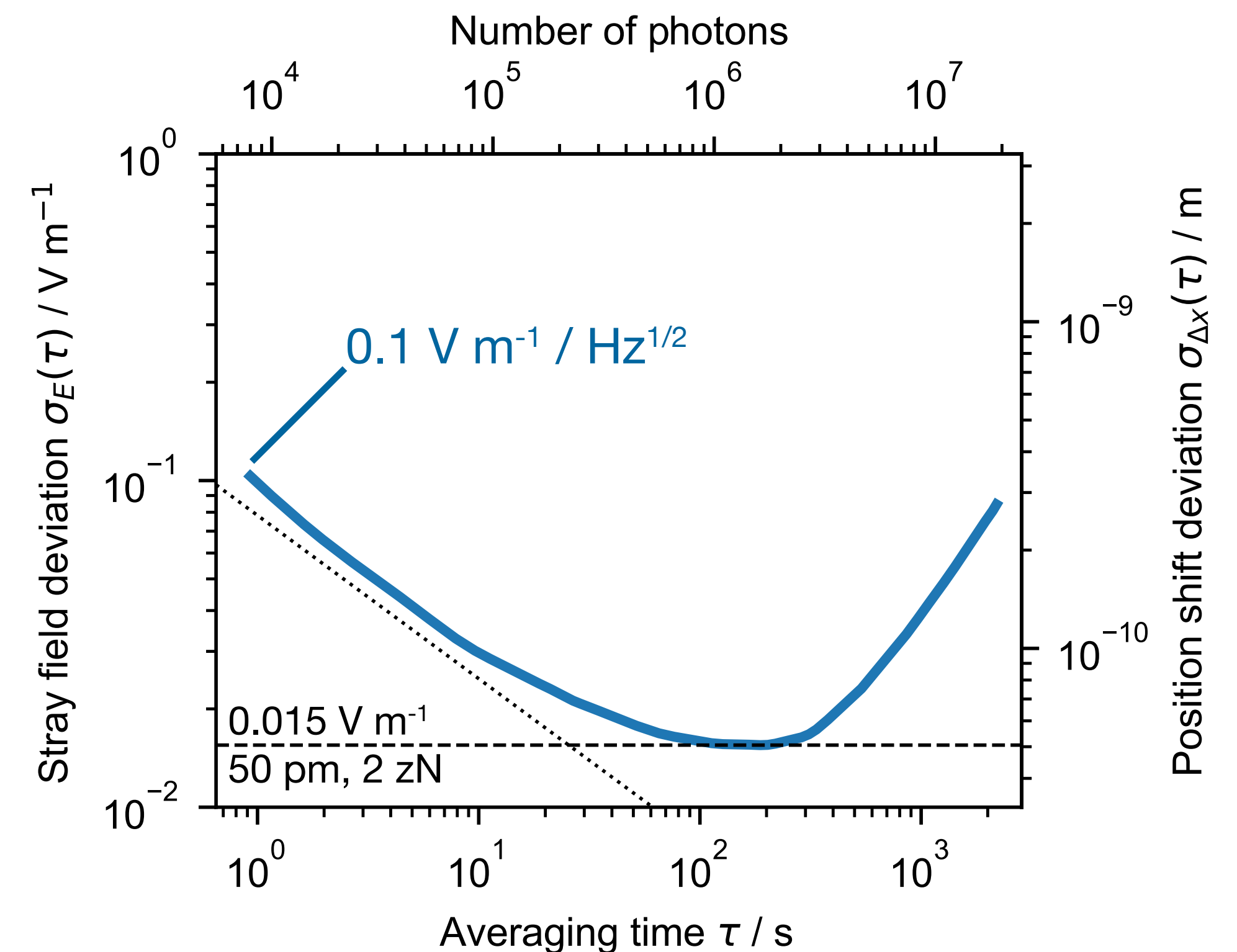
- » Linear dependence of correlated photon fraction on compensation field



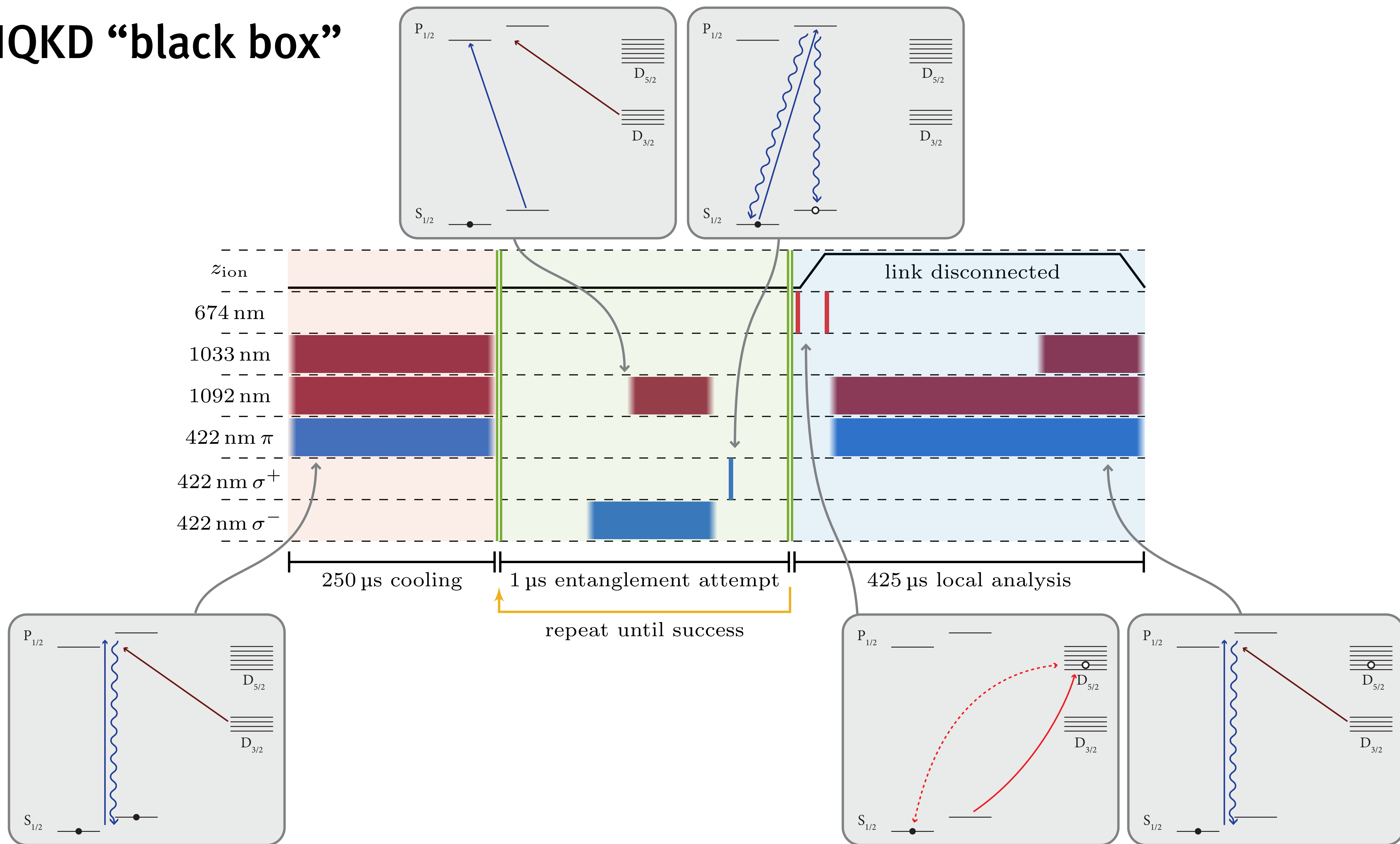
DPN et al., arXiv: 2107.00056

- » One beam yields 3D information
- » No narrow transitions needed
- » Modest time resolution req.
- » “State-of-the-art” sensitivity

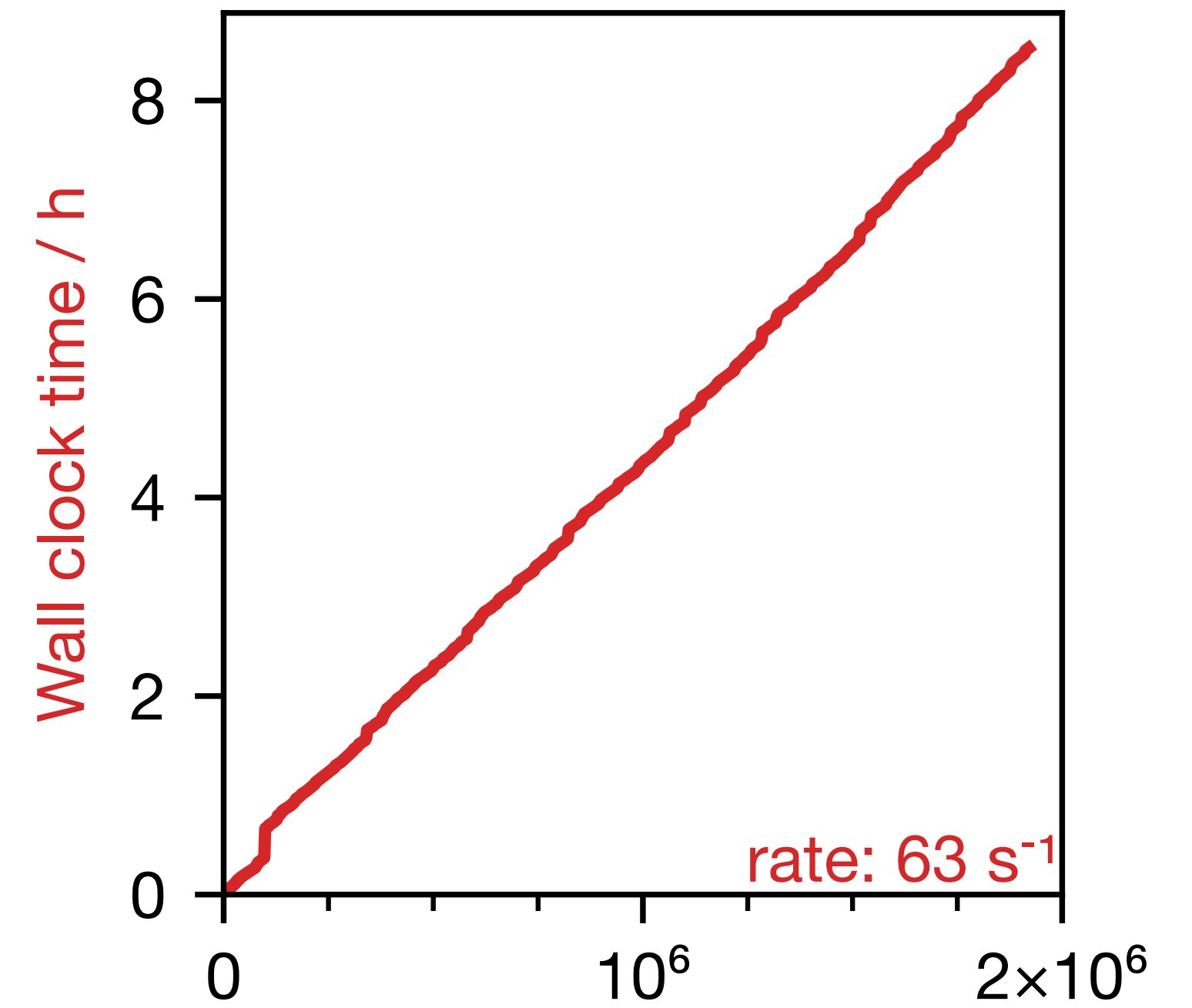
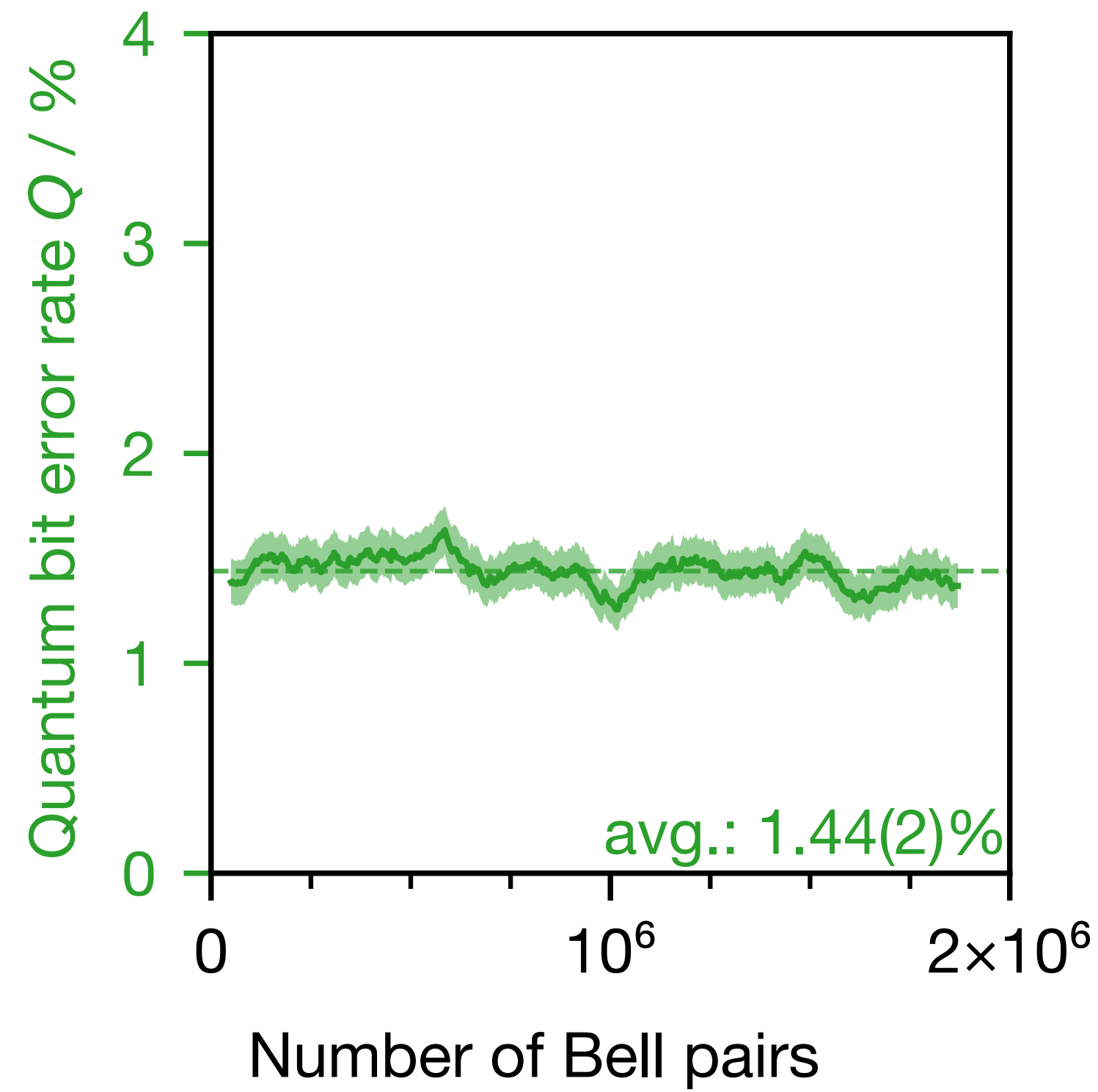
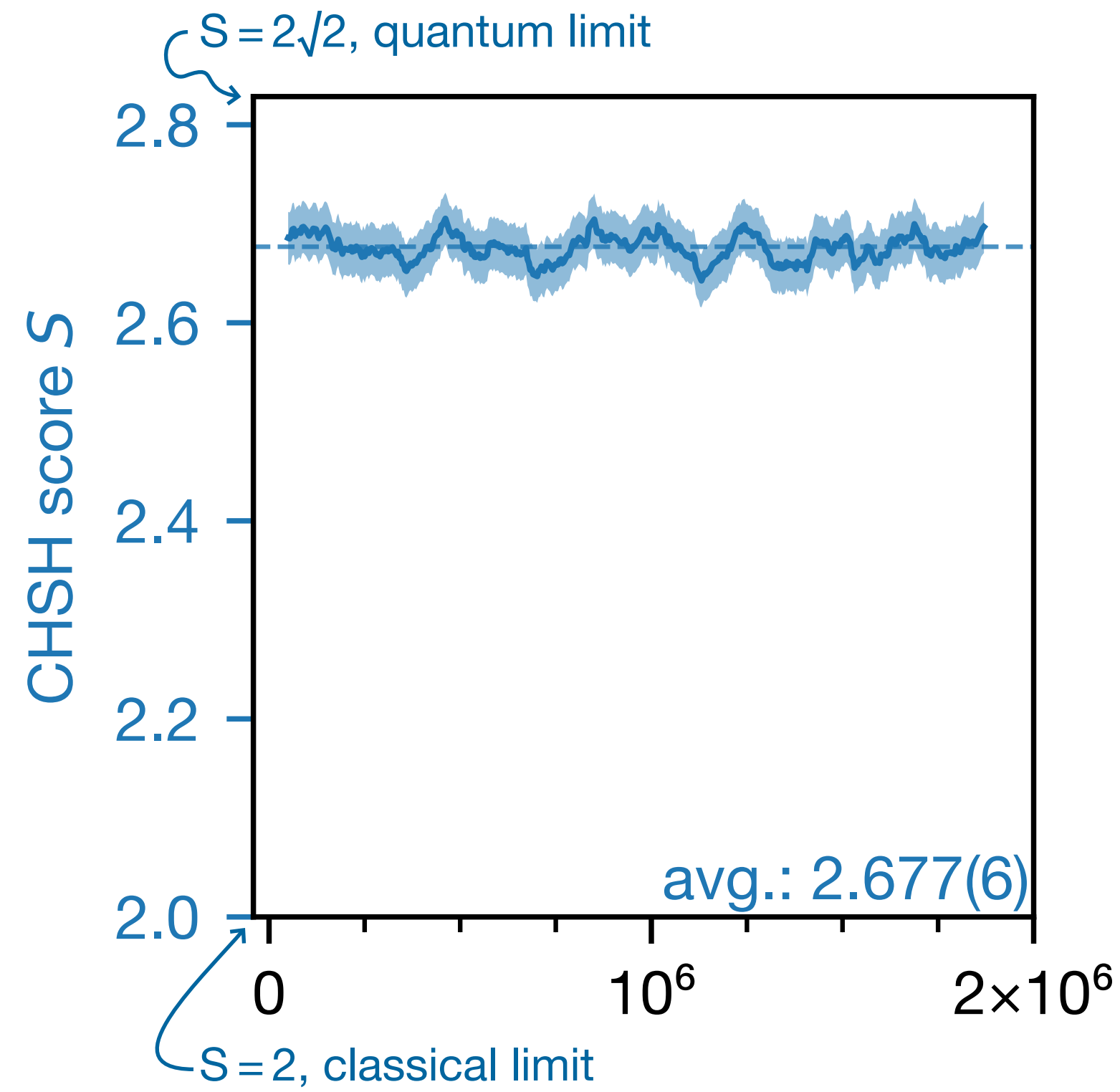
coherent: Higgins et al. (2021), doi:10.1088/1367-2630/ac3db6



DIQKD “black box”



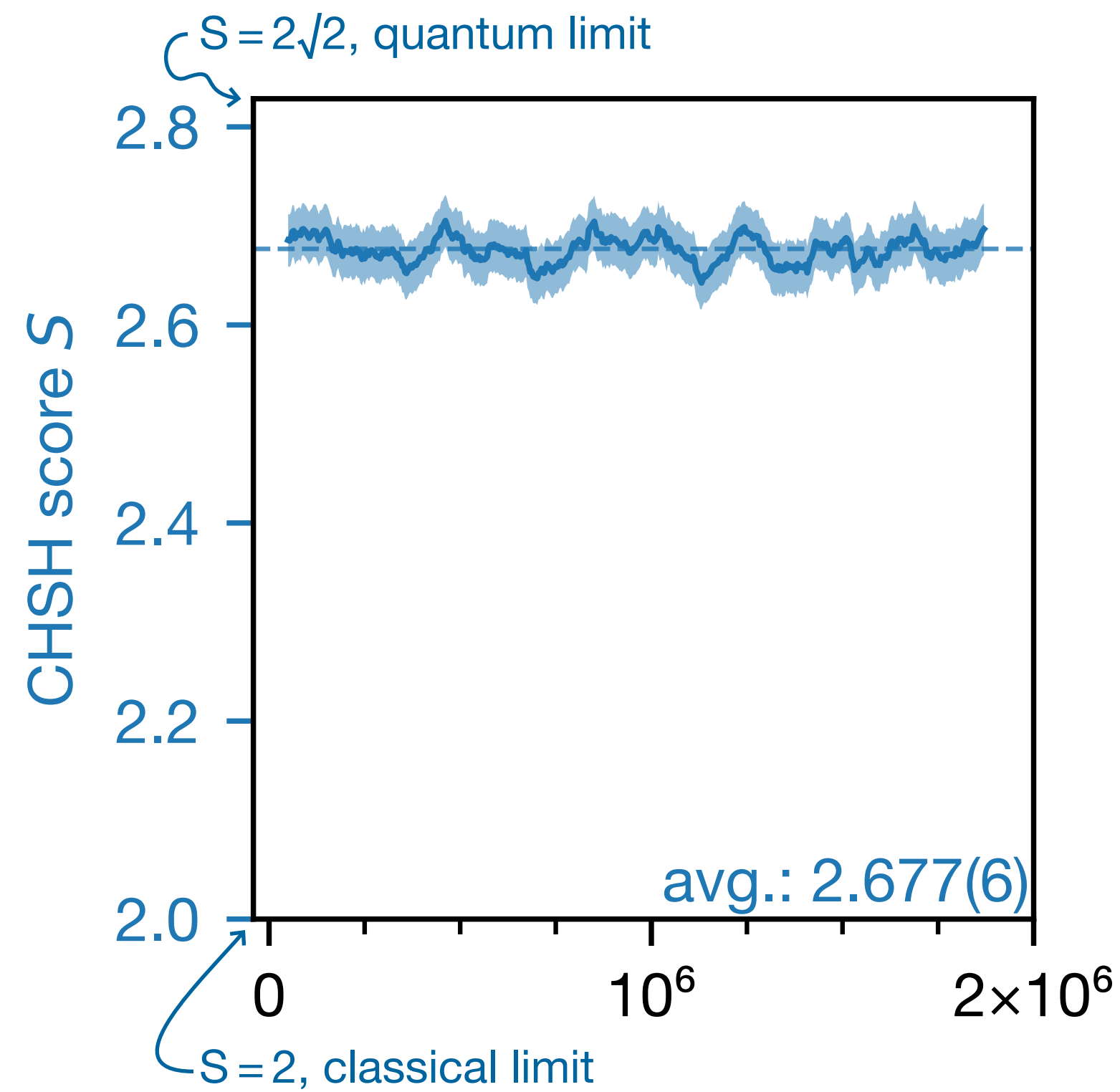
Link stability



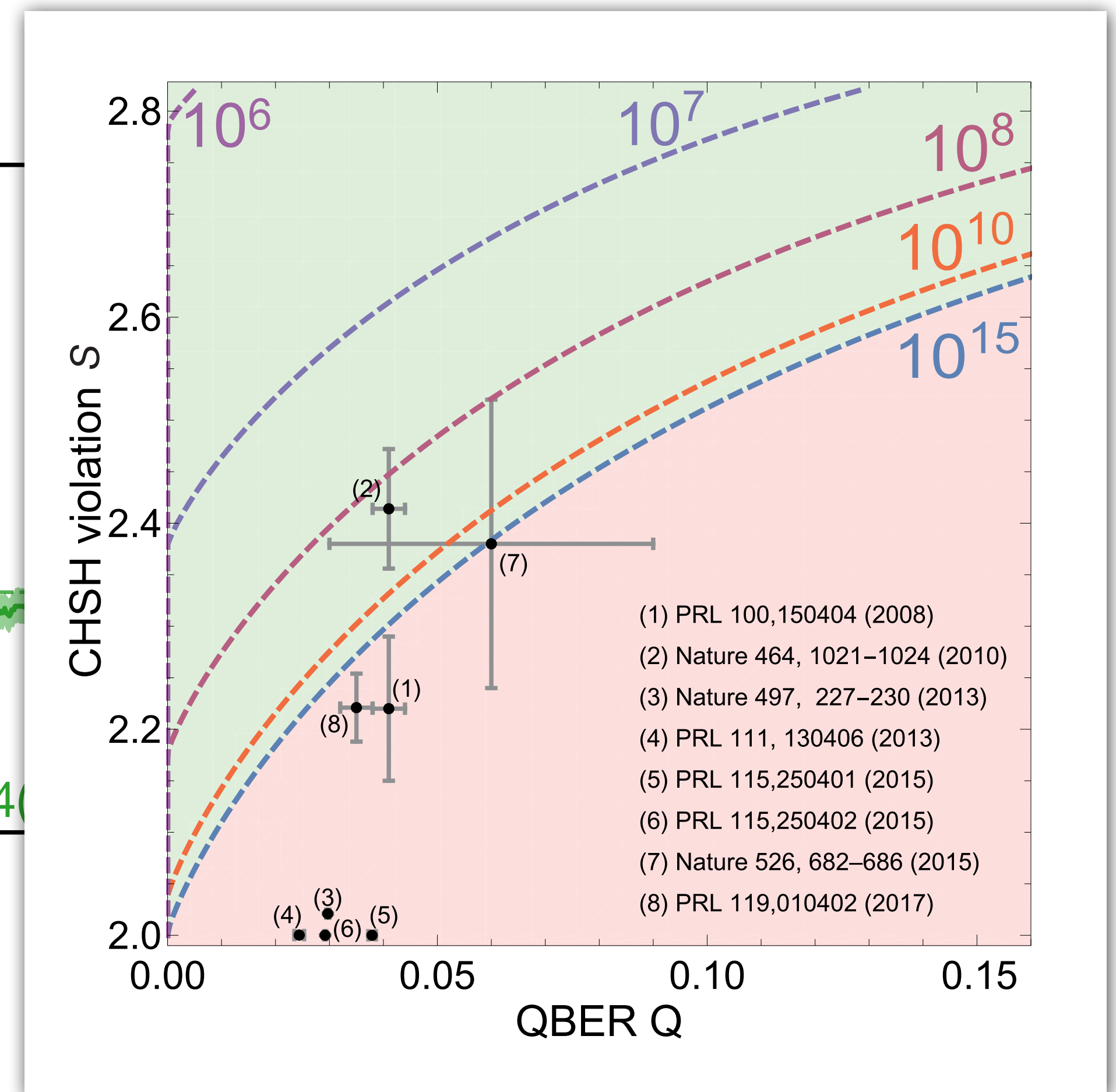
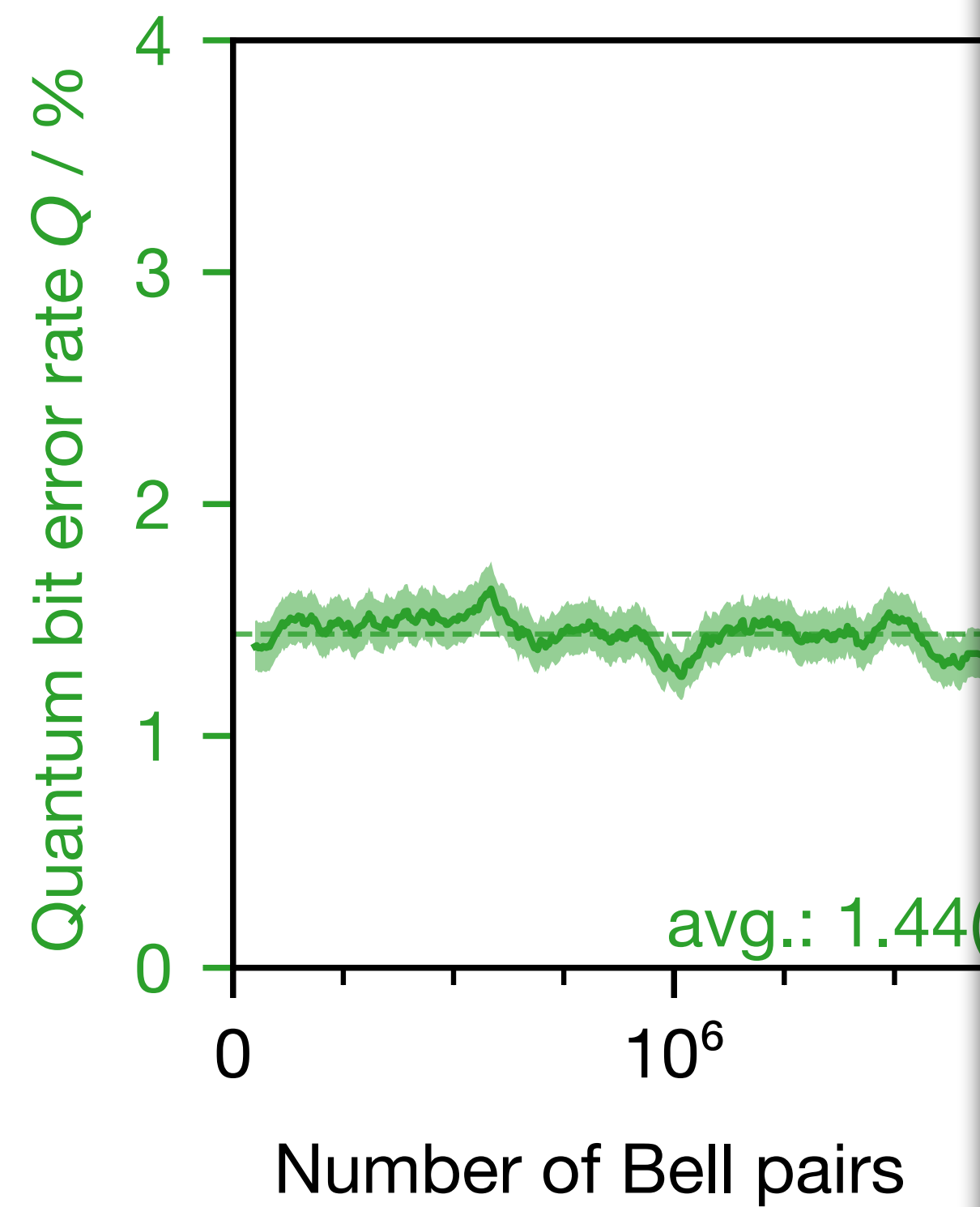
(no post-selection/...)

DPN et al. (2021), arXiv:2109.14600

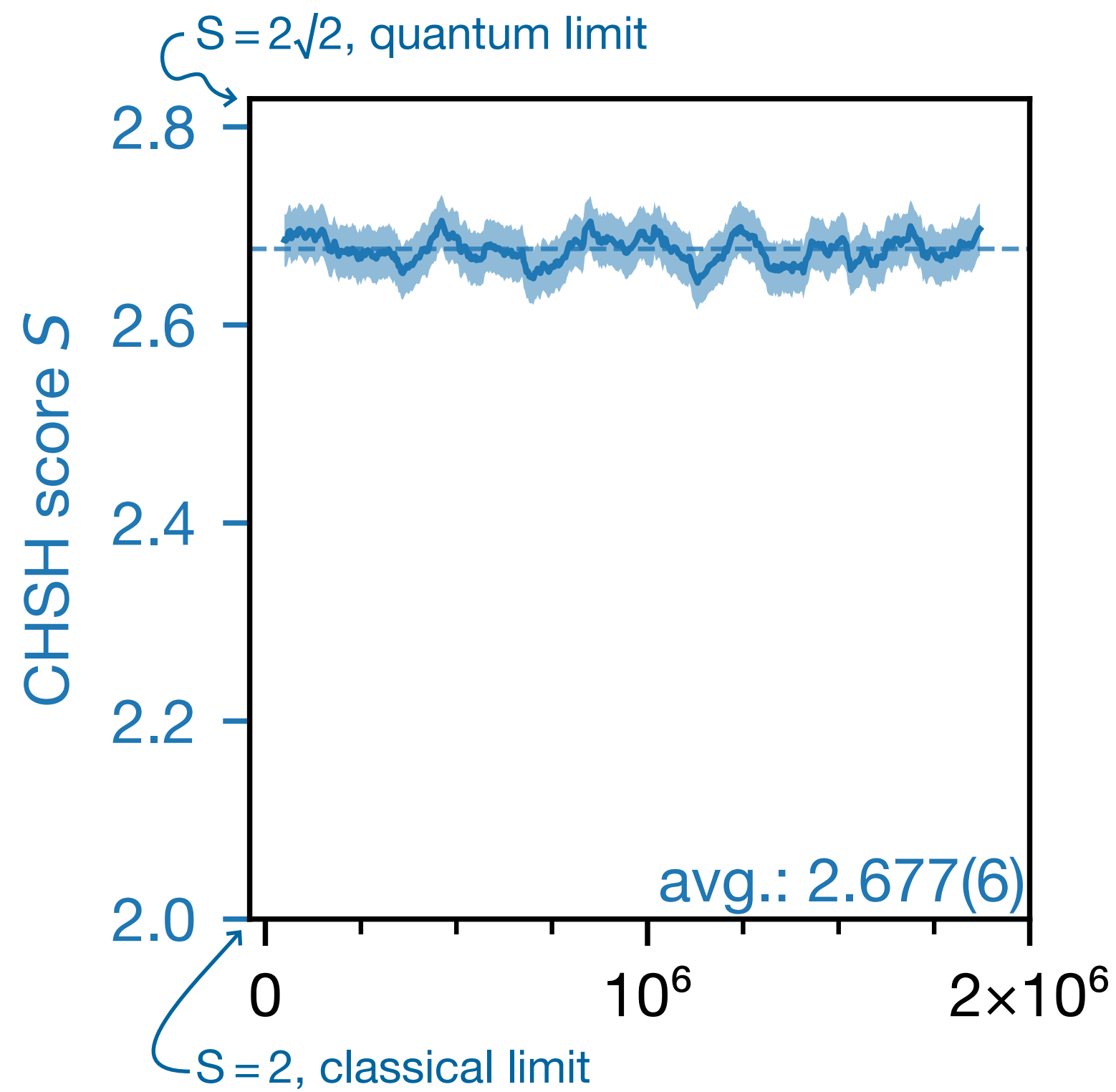
Link stability



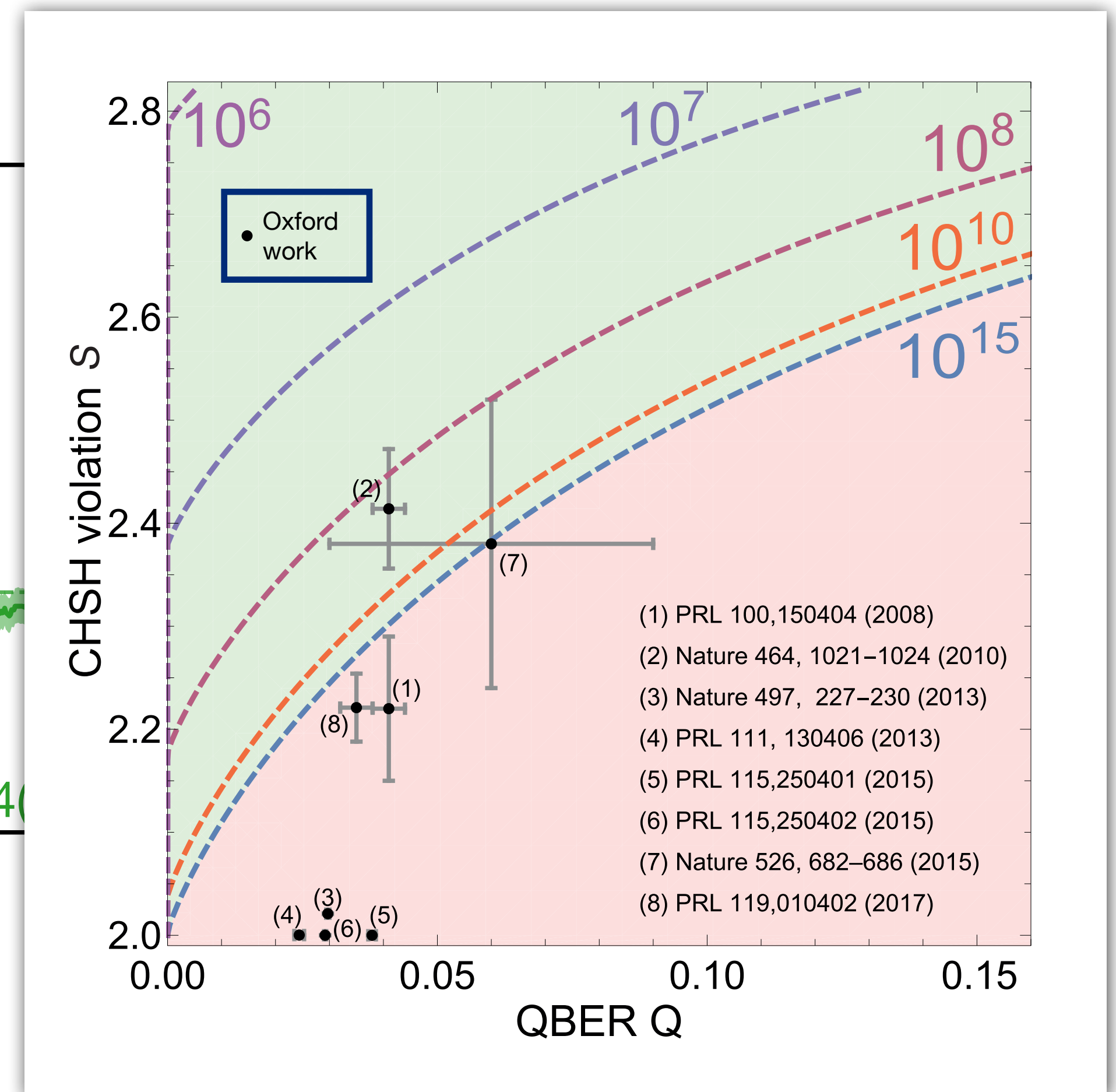
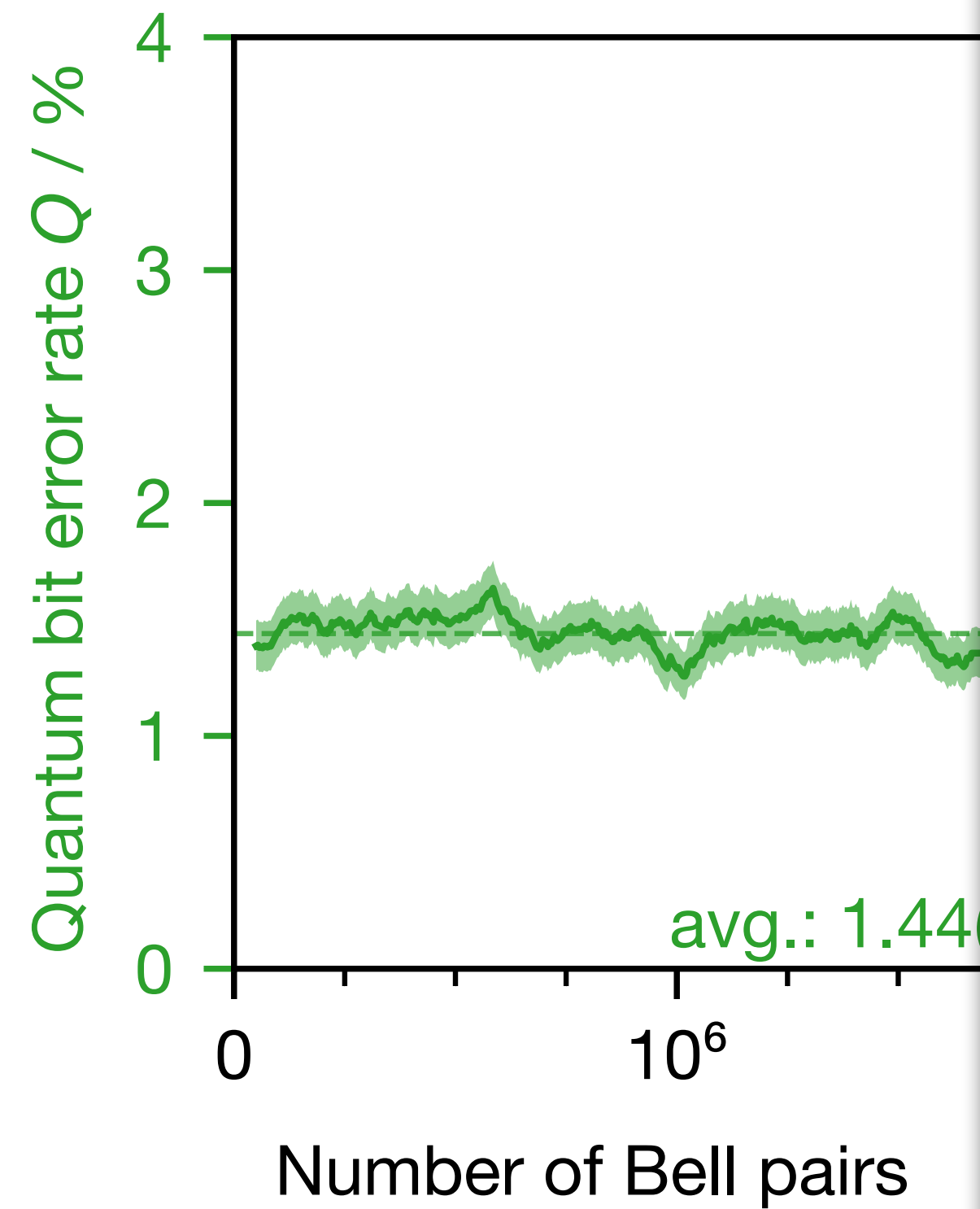
(no post-selection/...)



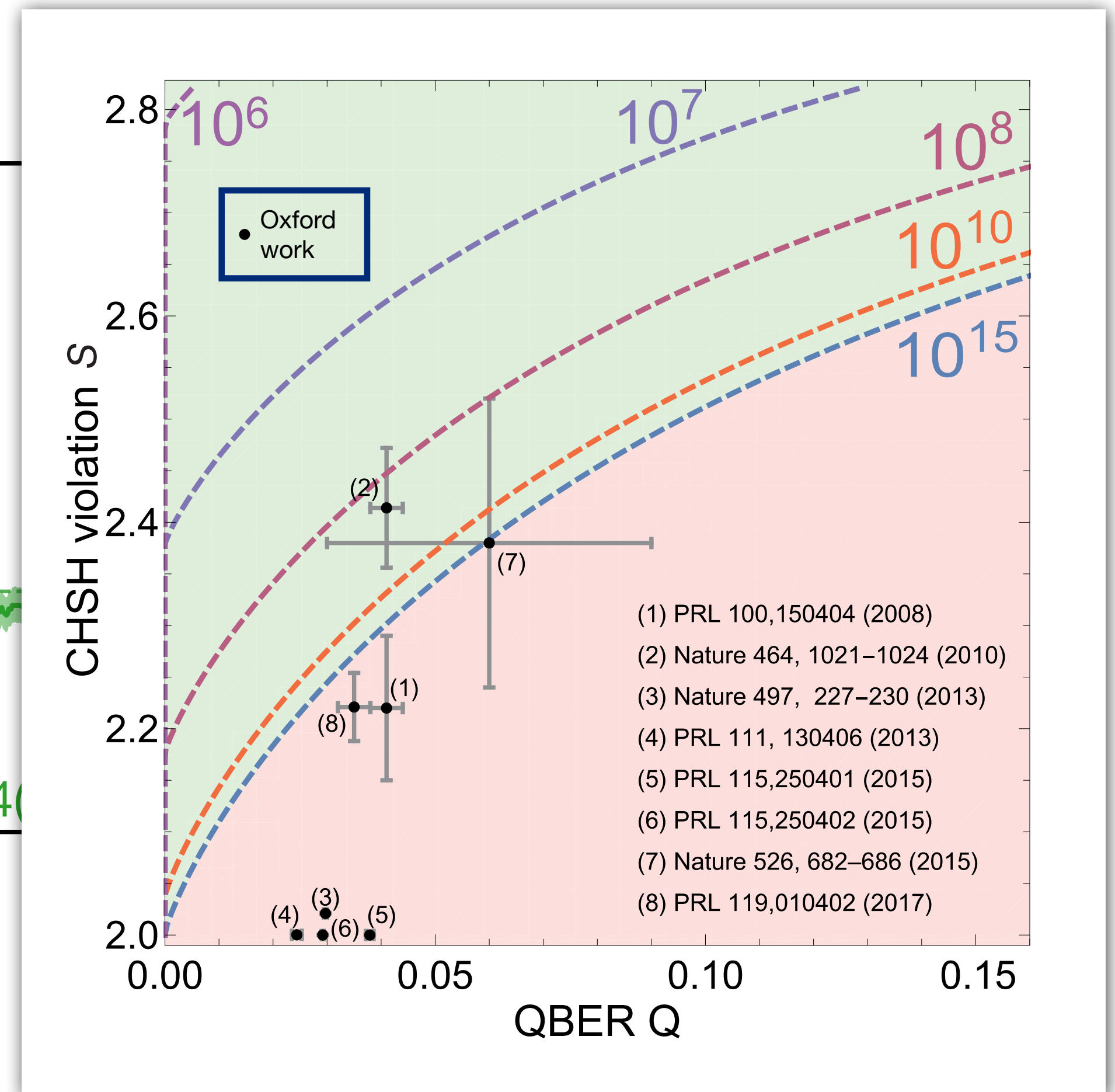
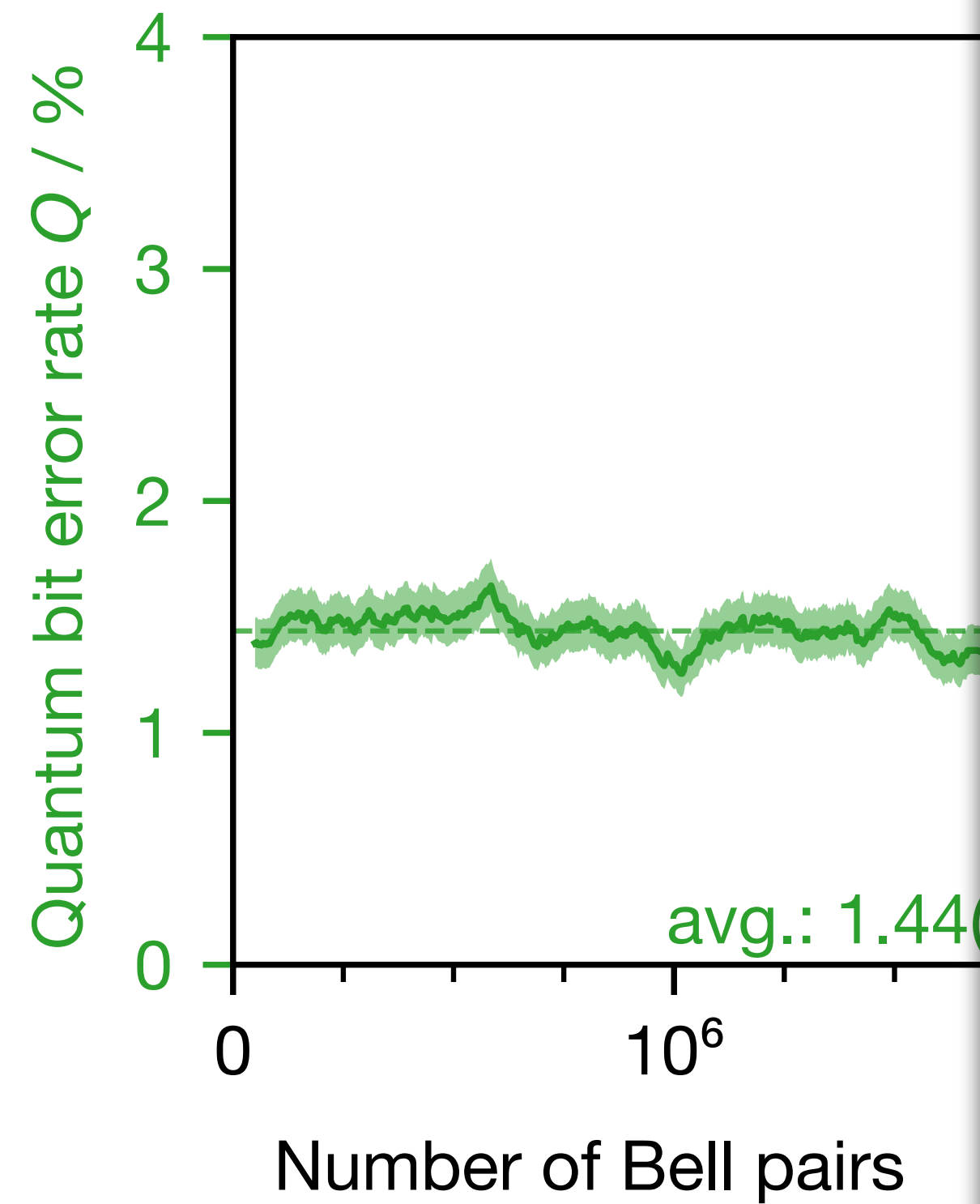
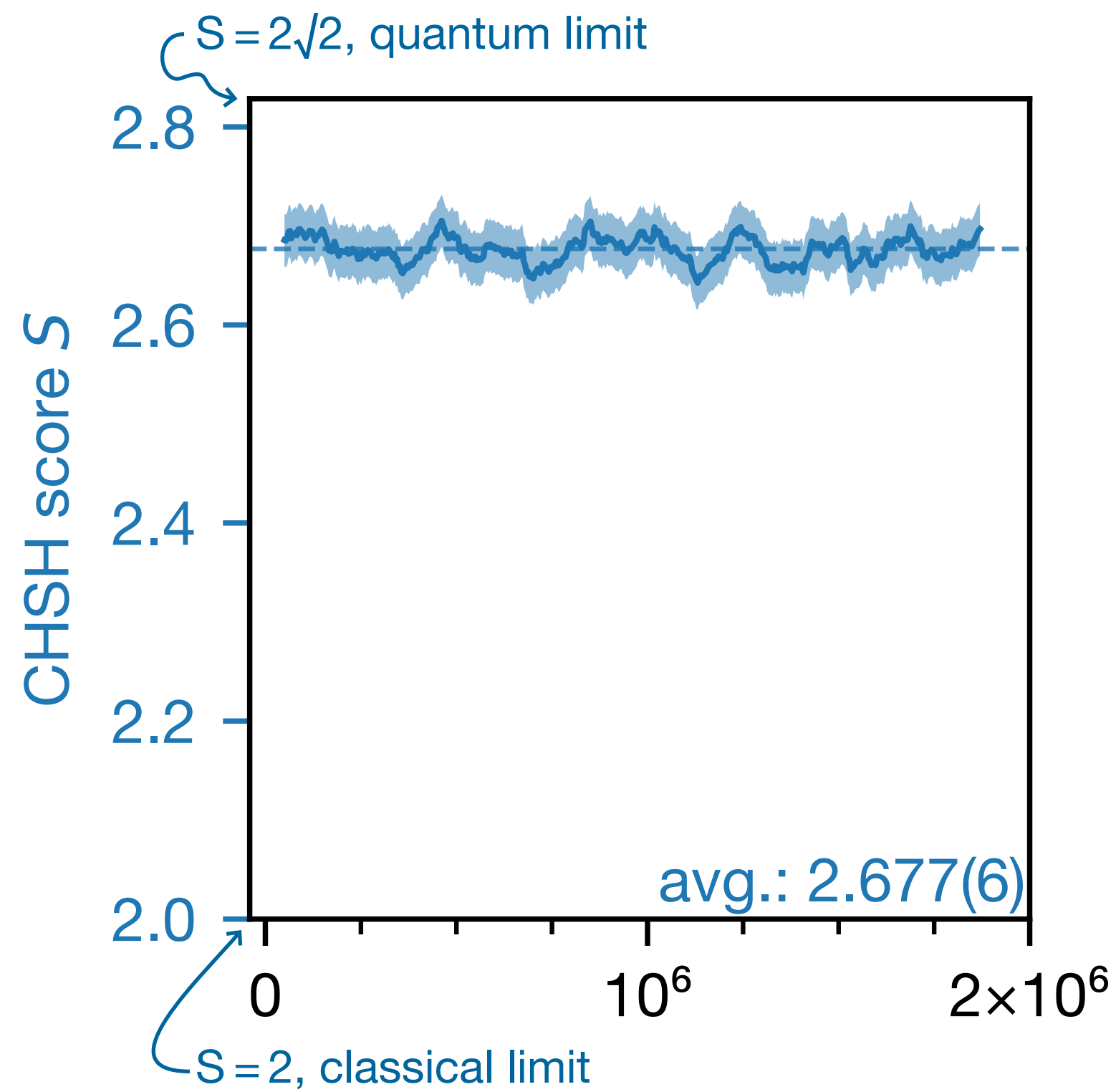
Link stability



(no post-selection/...)

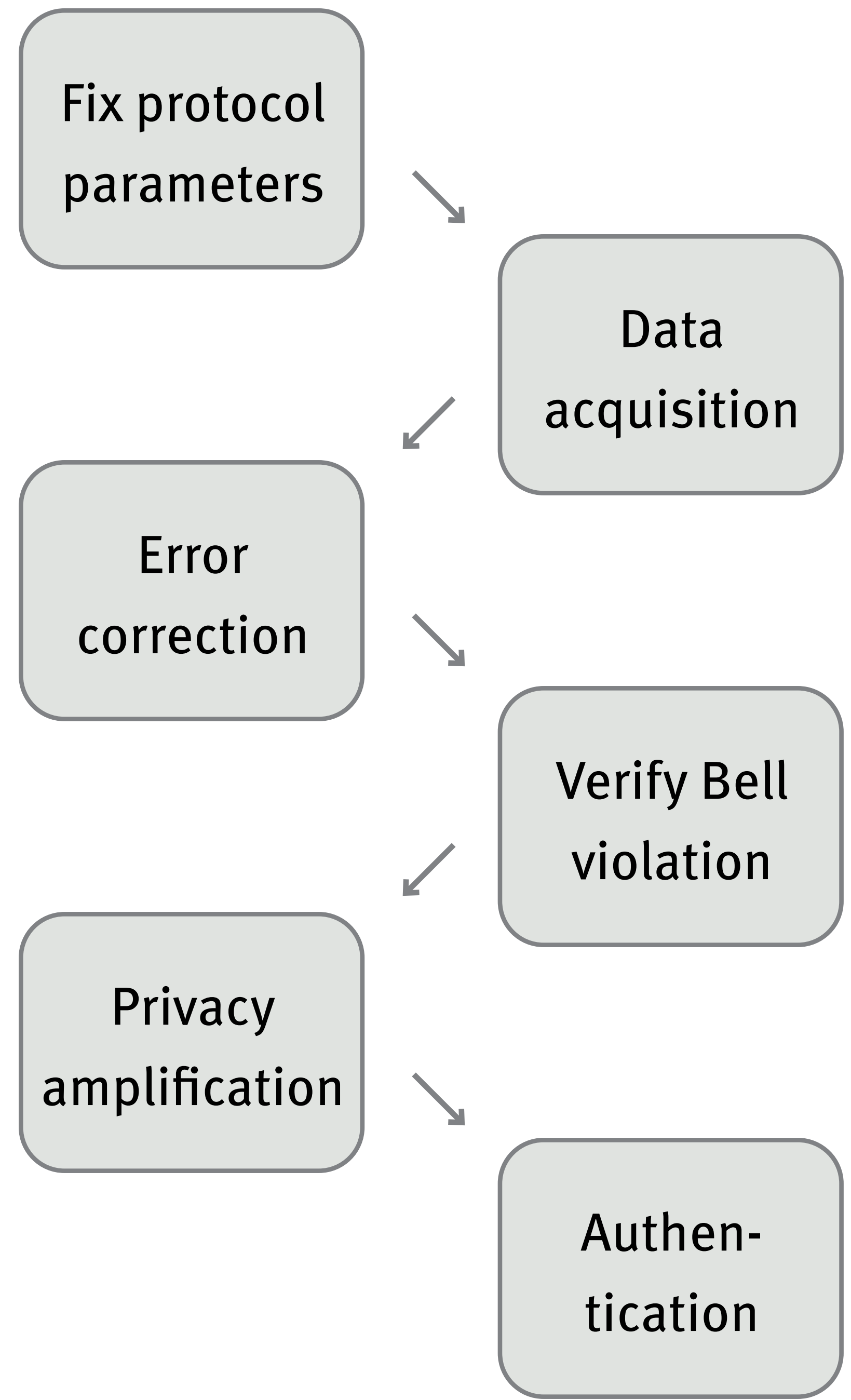
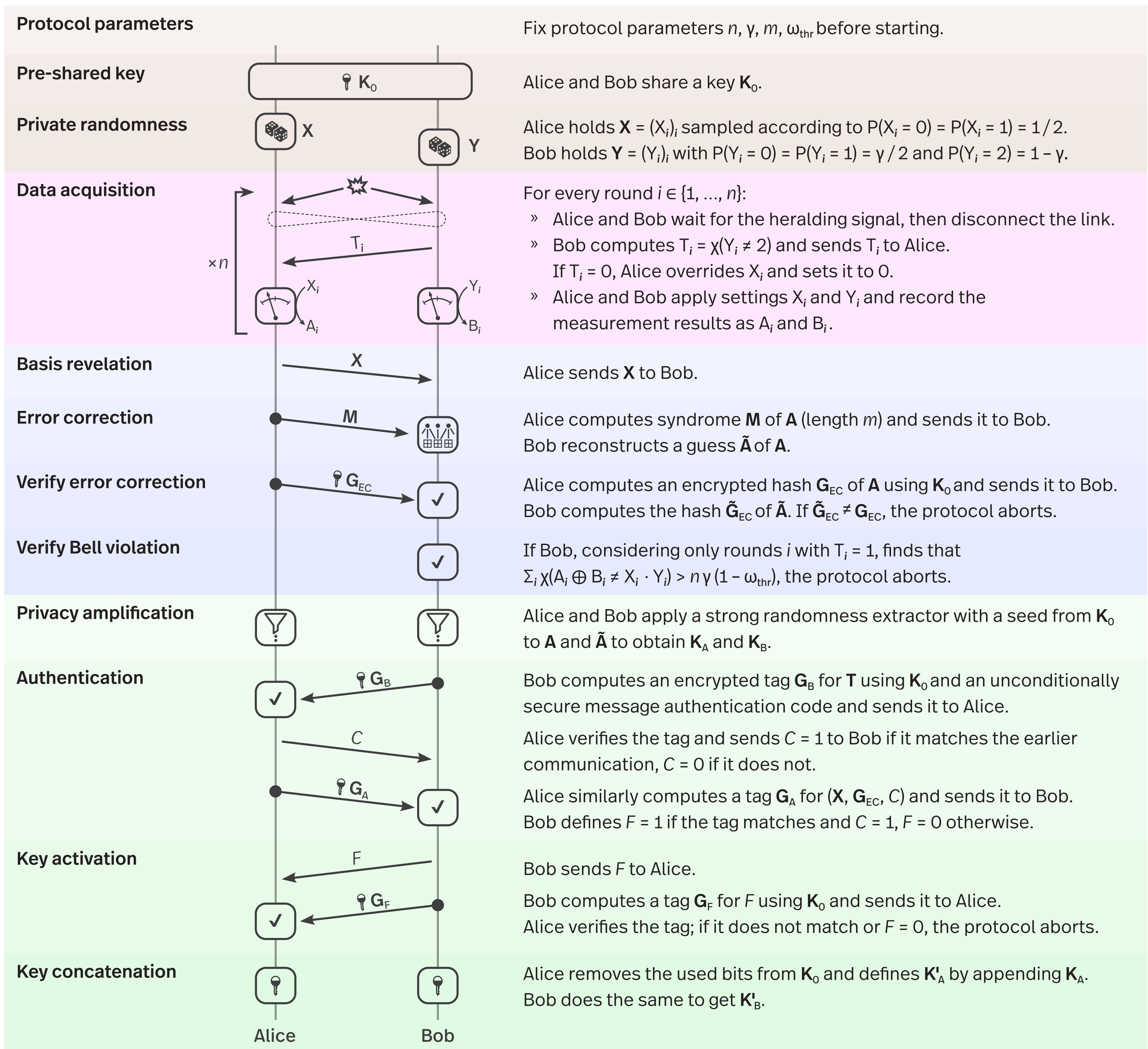


Link stability



(no post-selection/...)

- » Autonomous operation over ~days
- » Two separate control nodes, coordination over Ethernet



Device-Independent Quantum Key Distribution

D. P. Nadlinger,¹ P. Drmota,¹ B. C. Nichol,¹ G. Araneda,¹ D. Main,¹ R. Srinivas,¹ D. M. Lucas,¹ C. J. Ballance,¹ K. Ivanov,² E. Y-Z. Tan,³ P. Sekatski,⁴ R. L. Urbanke,² R. Renner,³ N. Sangouard,⁵ and J-D. Bancal⁵

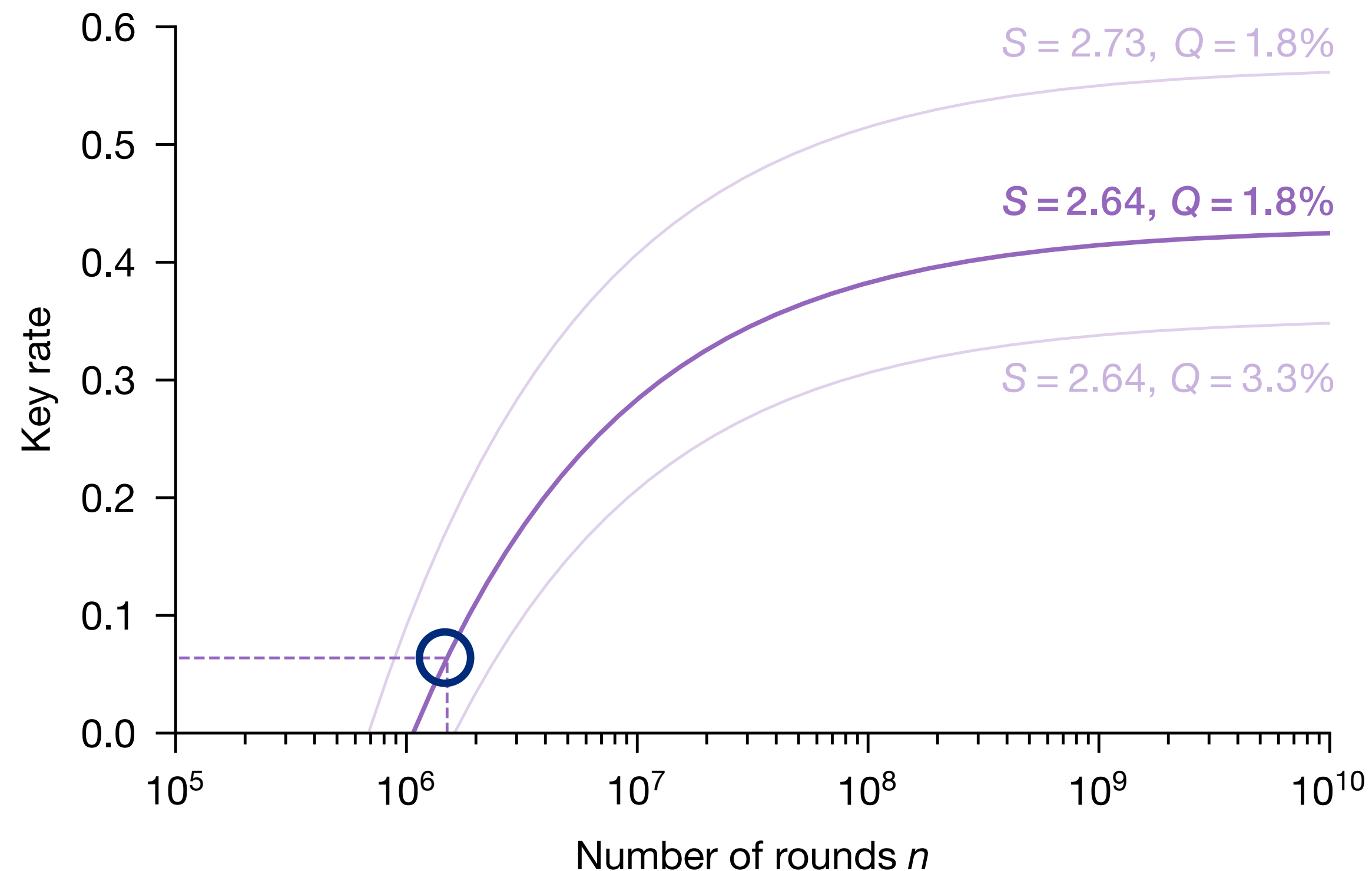
¹*Department of Physics, University of Oxford, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, U.K.*

²*School of Computer and Communication Sciences, EPFL, 1015 Lausanne, Switzerland*

³*Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland*

⁴*Department of Applied Physics, University of Geneva,
Rue de l'École-de-Médecine, 1211 Geneva, Switzerland*

⁵*Université Paris-Saclay, CEA, CNRS, Institut de physique théorique, 91191, Gif-sur-Yvette, France*



DPN et al. (2021), arXiv:2109.14600

- » Raw data:
1.5 million Bell pairs, 8 hours
- » Derived key: 95 884 bits
(\gg 256 bits consumed for auth.)

Experimental quantum key distribution certified by Bell's theorem

~~Device-Independent Quantum Key Distribution~~

D. P. Nadlinger,¹ P. Drmota,¹ B. C. Nichol,¹ G. Araneda,¹ D. Main,¹ R. Srinivas,¹ D. M. Lucas,¹ C. J. Ballance,¹ K. Ivanov,² E. Y-Z. Tan,³ P. Sekatski,⁴ R. L. Urbanke,² R. Renner,³ N. Sangouard,⁵ and J-D. Bancal⁵

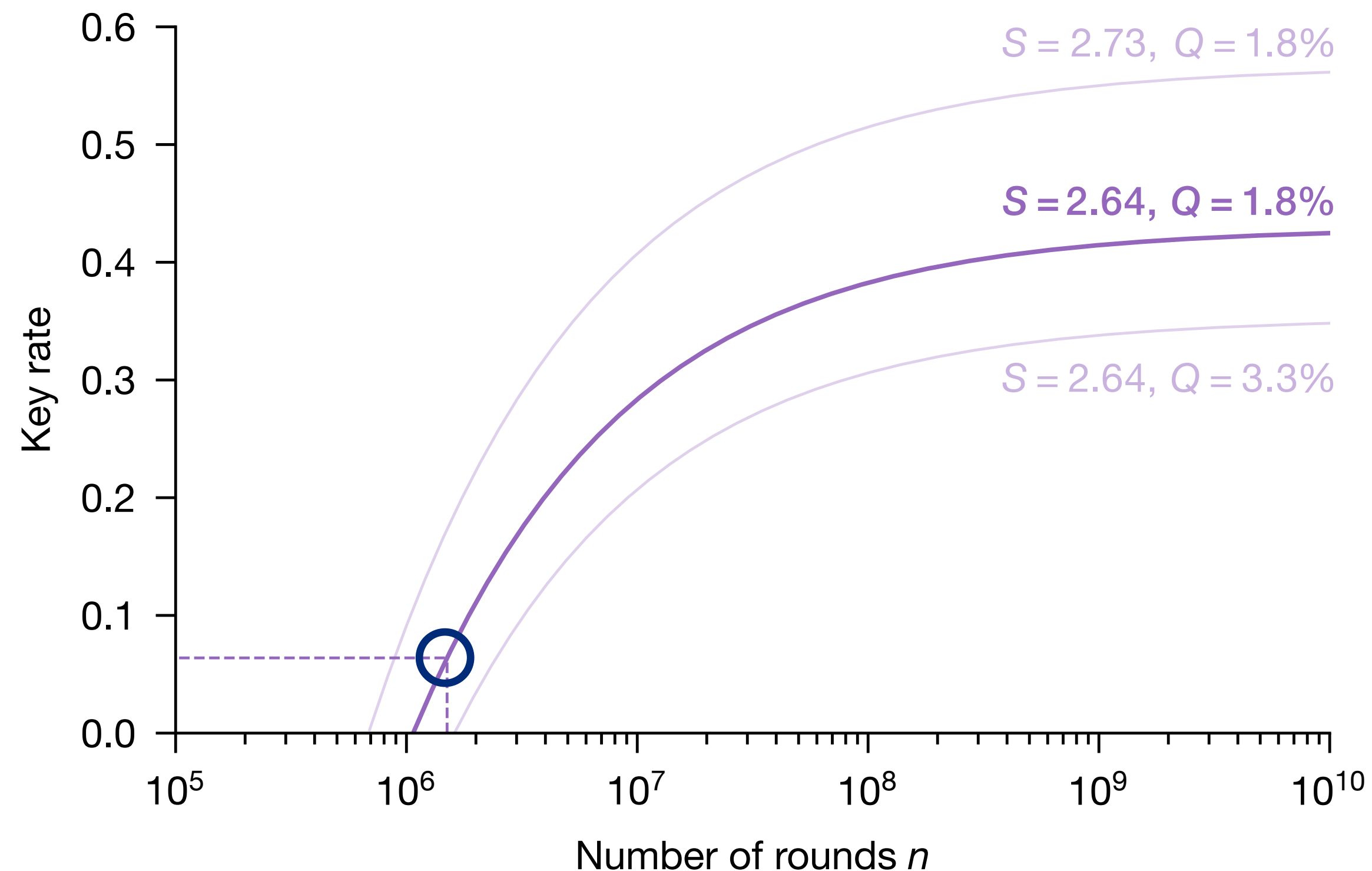
¹*Department of Physics, University of Oxford, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, U.K.*

²*School of Computer and Communication Sciences, EPFL, 1015 Lausanne, Switzerland*

³*Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland*

⁴*Department of Applied Physics, University of Geneva,
Rue de l'École-de-Médecine, 1211 Geneva, Switzerland*

⁵*Université Paris-Saclay, CEA, CNRS, Institut de physique théorique, 91191, Gif-sur-Yvette, France*

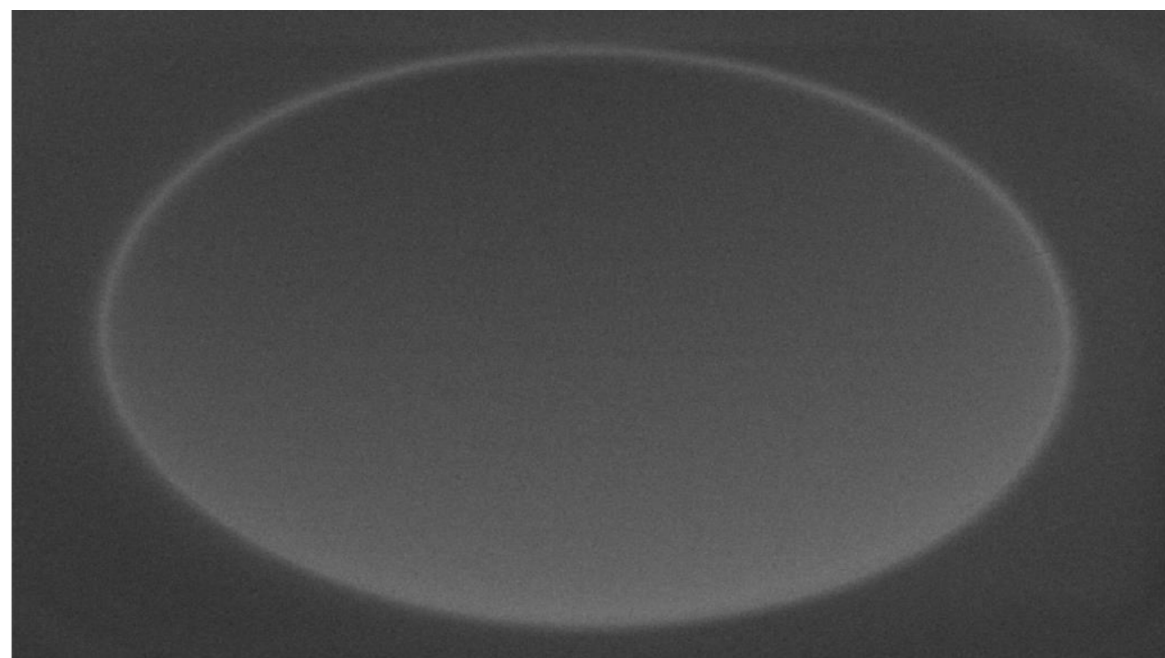


- » Raw data:
1.5 million Bell pairs, 8 hours
- » Derived key: 95 884 bits
(\gg 256 bits consumed for auth.)

DPN et al. (2021), arXiv:2109.14600

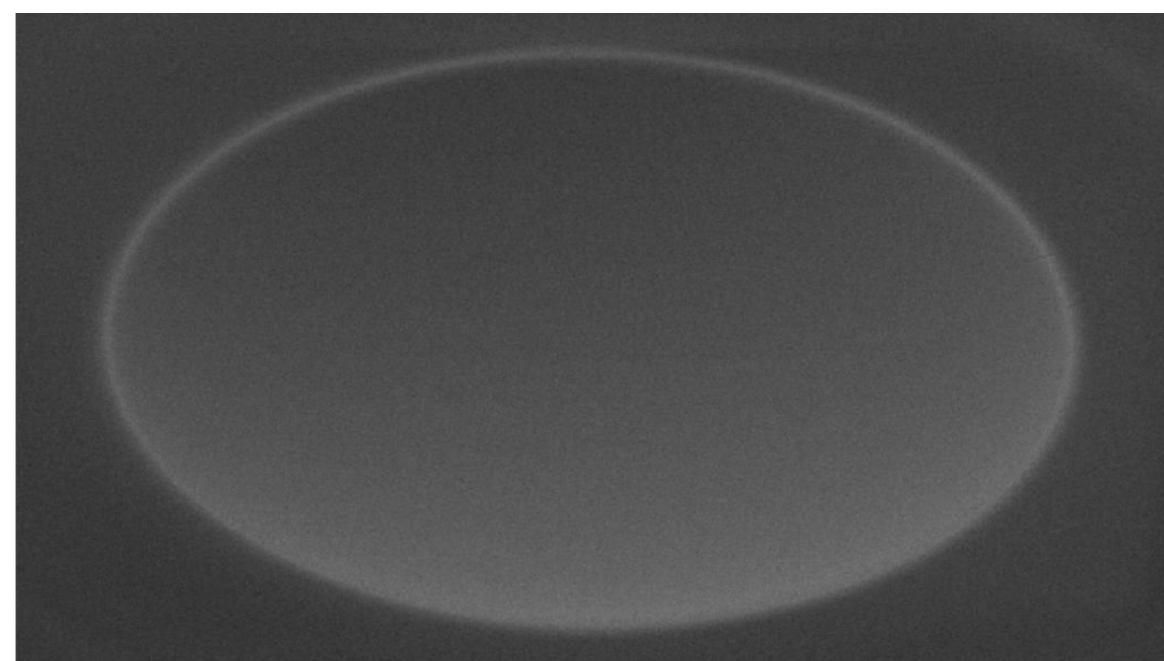
Outlook

- » Long-distance entanglement
 - » 422 nm: $\frac{1}{2}$ rate every ~ 100 m
 - » Quantum frequency conversion to telecommunication wavelengths
[Wright et al. \(2018\), doi:10.1103/PhysRevApplied.10.044012](#)
 - » Cavities
[Schrupp et al. \(2021\), doi:10.1103/PRXQuantum.2.020331](#)
- » Larger entanglement rate

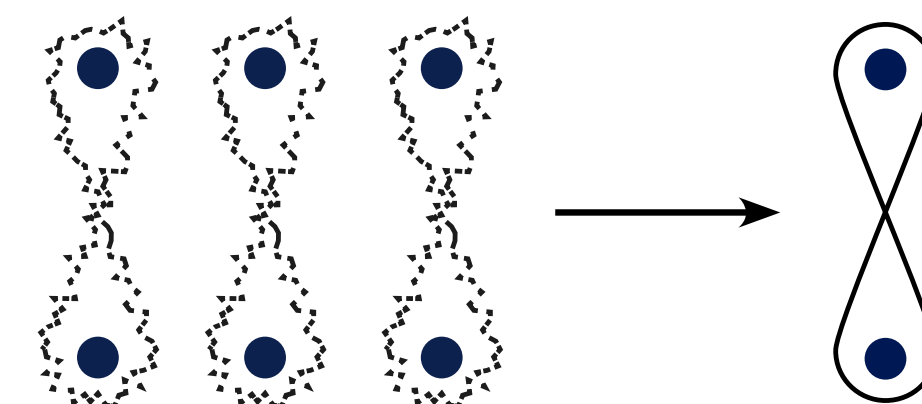
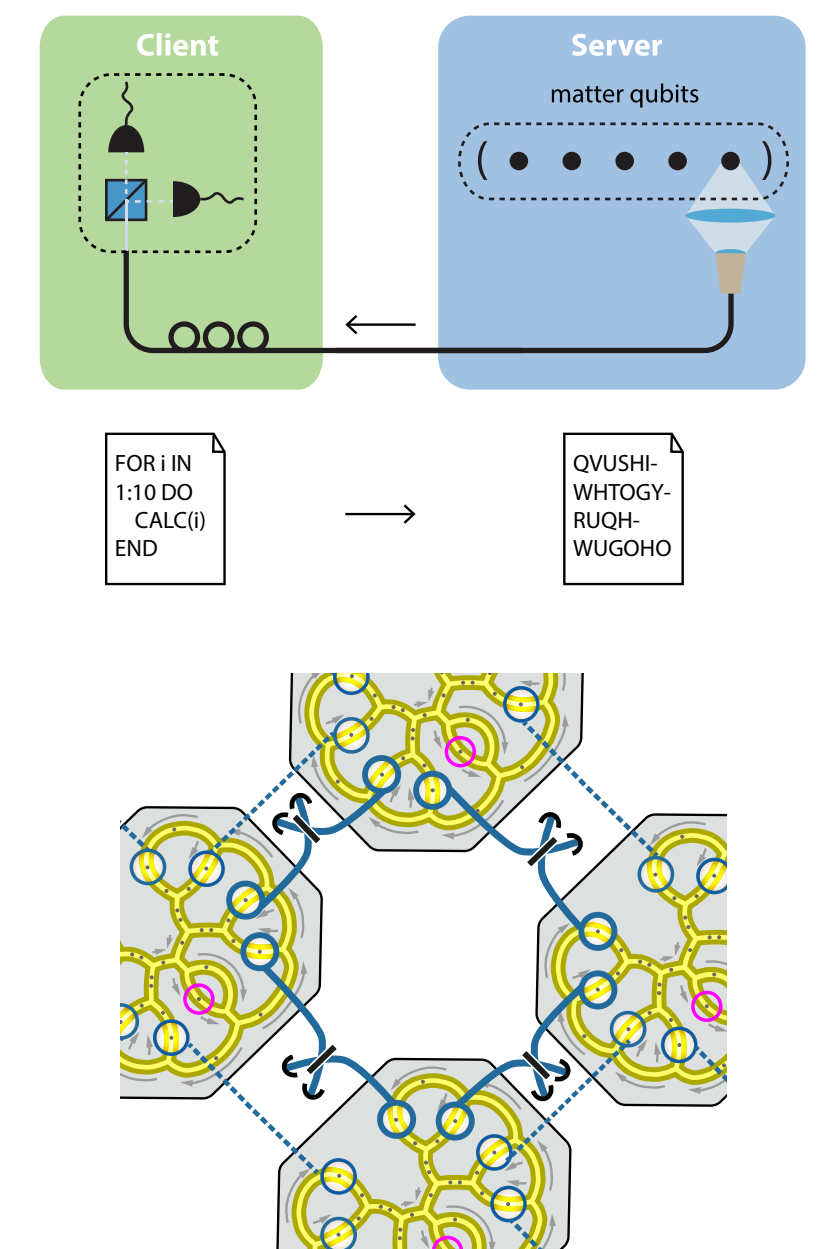
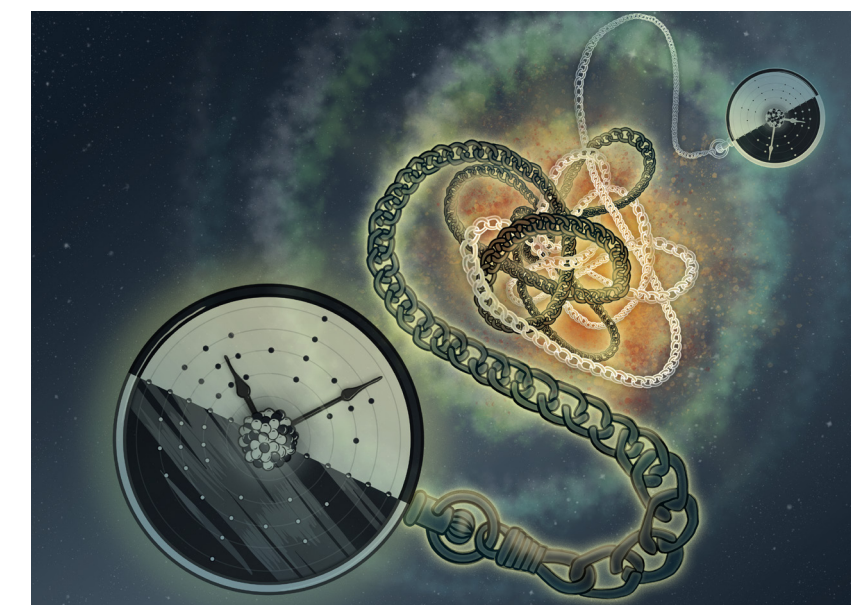


Outlook

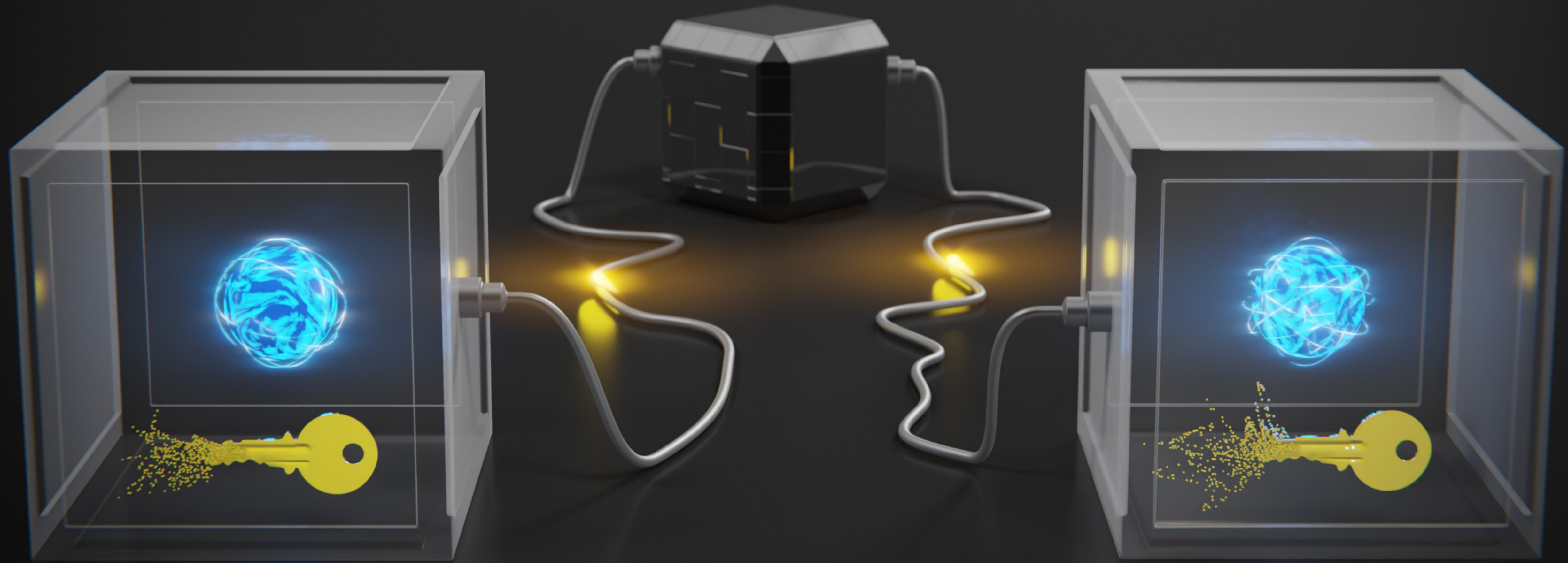
- » Long-distance entanglement
 - » 422 nm: $\frac{1}{2}$ rate every ~ 100 m
 - » Quantum frequency conversion to telecommunication wavelengths
[Wright et al. \(2018\), doi:10.1103/PhysRevApplied.10.044012](#)
 - » Cavities
[Schrupp et al. \(2021\), doi:10.1103/PRXQuantum.2.020331](#)
- » Larger entanglement rate



- » Complete, end-to-end DIQKD demonstration
incomplete (very slow), but 400 m distance:
[Zhang et al. \(2021\), arXiv:2110.00575 \(München\)](#)
- » Robust building block for other applications



Oxford: D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance.
Zurich: E. Y-Z. Tan, R. Renner. **Lausanne:** K. Ivanov, R. L. Urbanke. **Geneva:** P. Sekatski. **Paris:** N. Sangouard, J.-D. Bancal.



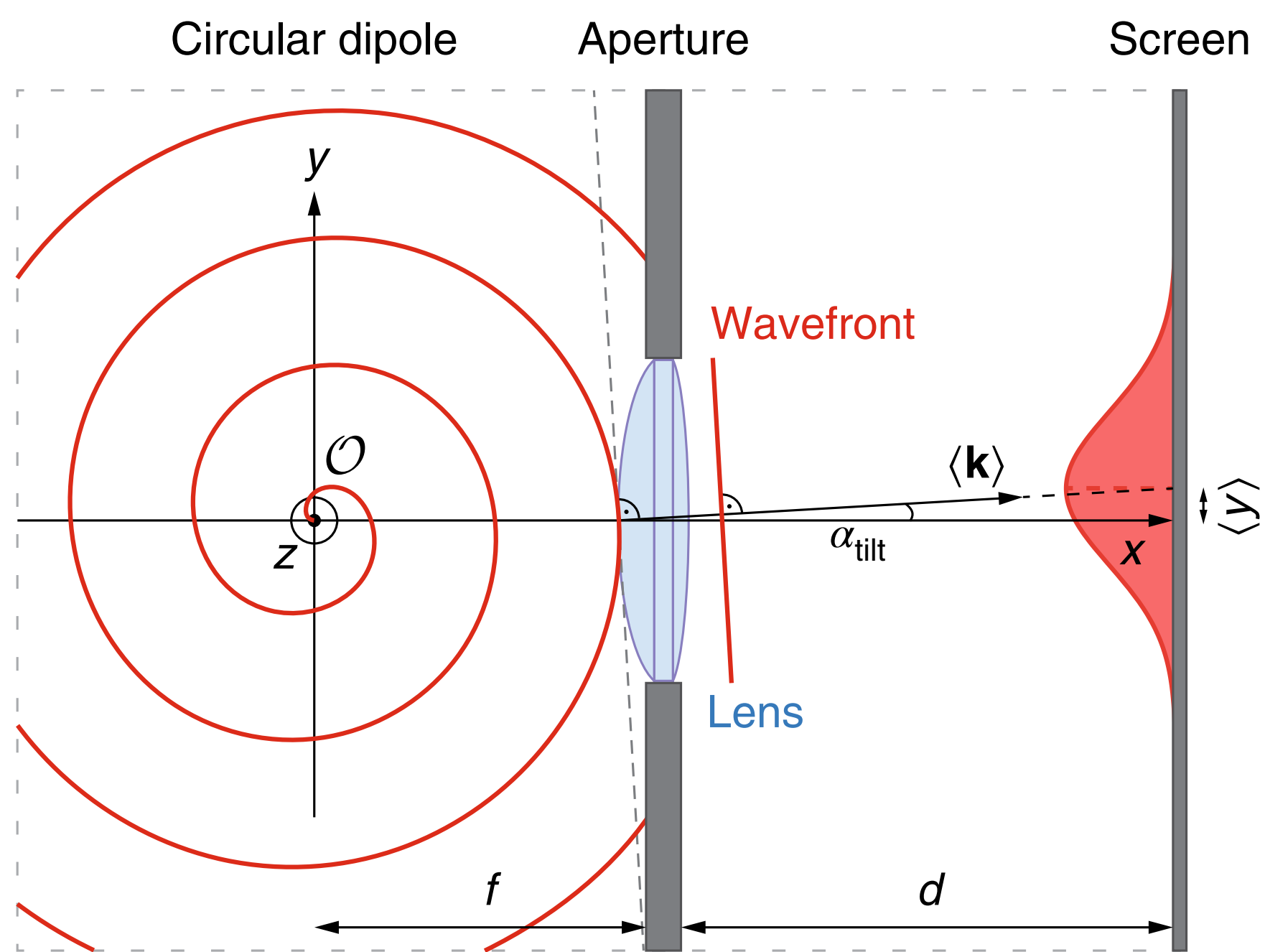
Questions?

<http://photonic.link>

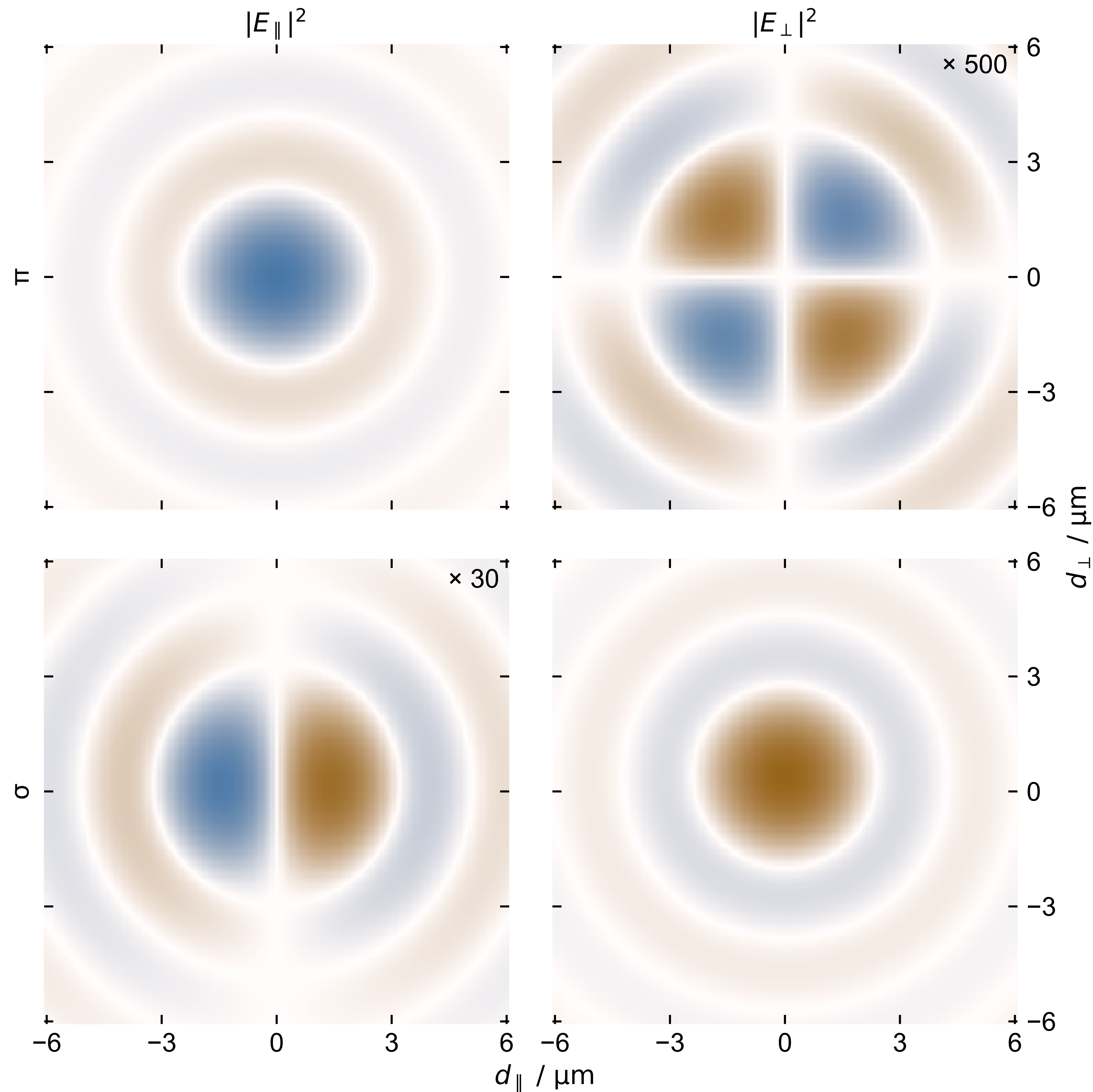
david.nadlinger@physics.ox.ac.uk

Come find me to chat about: Experimental control software & hardware, ARTIQ (+ndscan), open-source collaborations, programming languages, photographing single atoms, ... And where did the angular momentum go in σ perp. to the B field anyway?

Additional material



G. Araneda et al. (2018), 10.1038/s41567-018-0301-y



Aside: Microwave photons



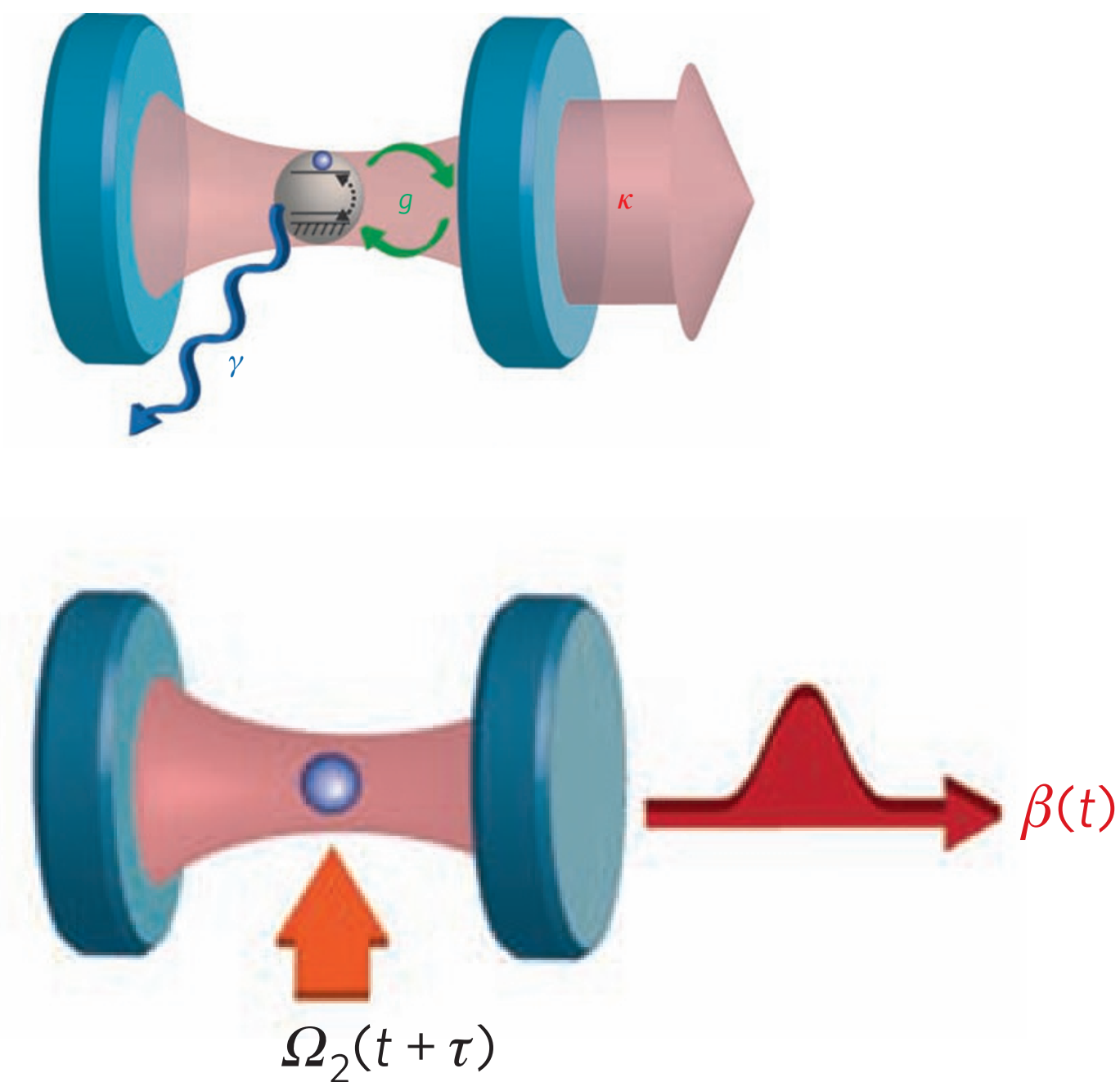
Wallraff group, ETH Zürich

» 5 GHz (~ 0.24 K) vs. 500 THz ($\sim 2.4 \times 10^4$ K)

Convert entanglement onto photon and back?

Deterministic reabsorption of single photon is tricky:

- » Light-matter interactions are weak
→ cavities
- » Temporal mode matching
→ e.g. stimulated Raman adiabatic passage
- » Link loss
→ ?

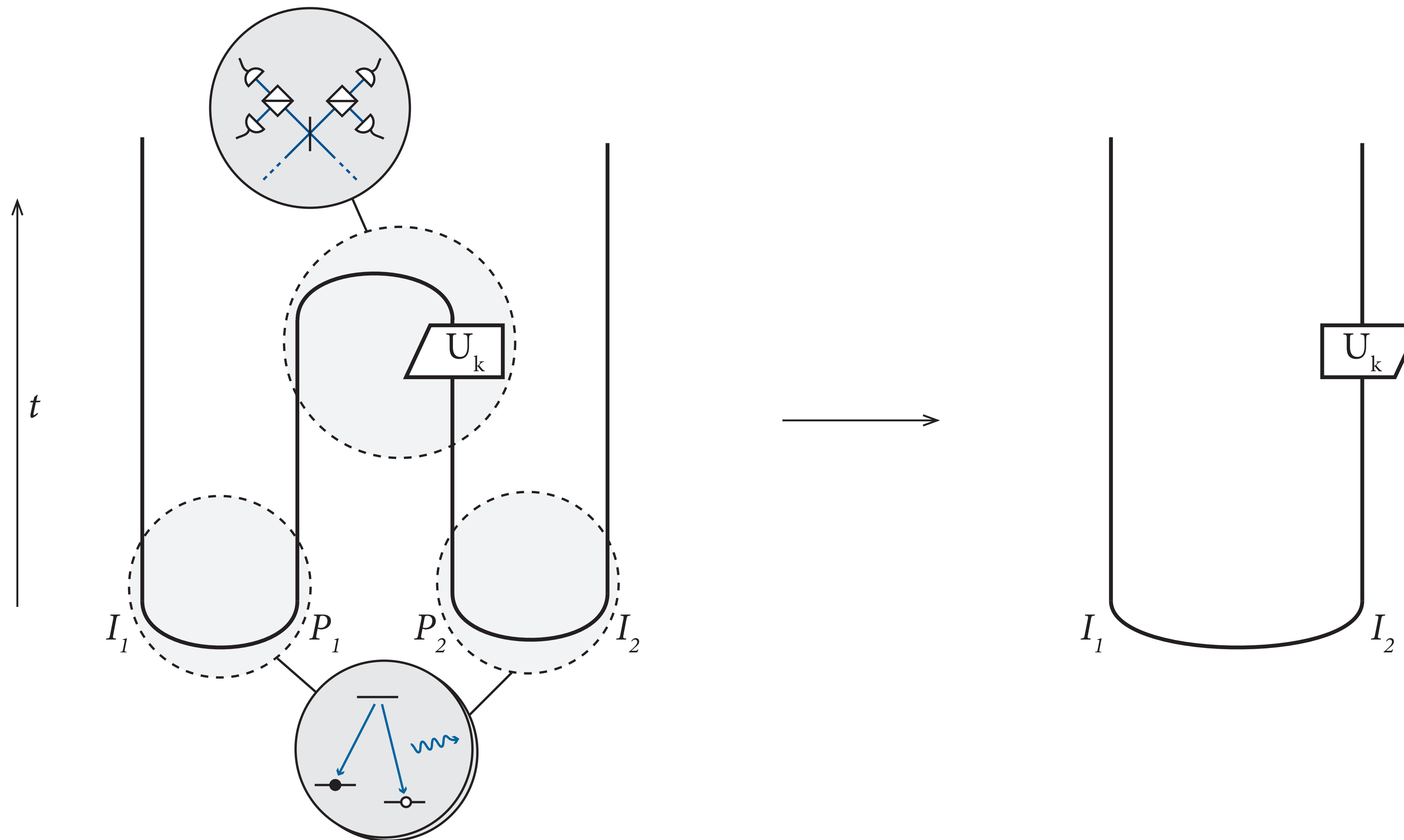


H. J. Kimble (2008), doi:10.1038/nature07127

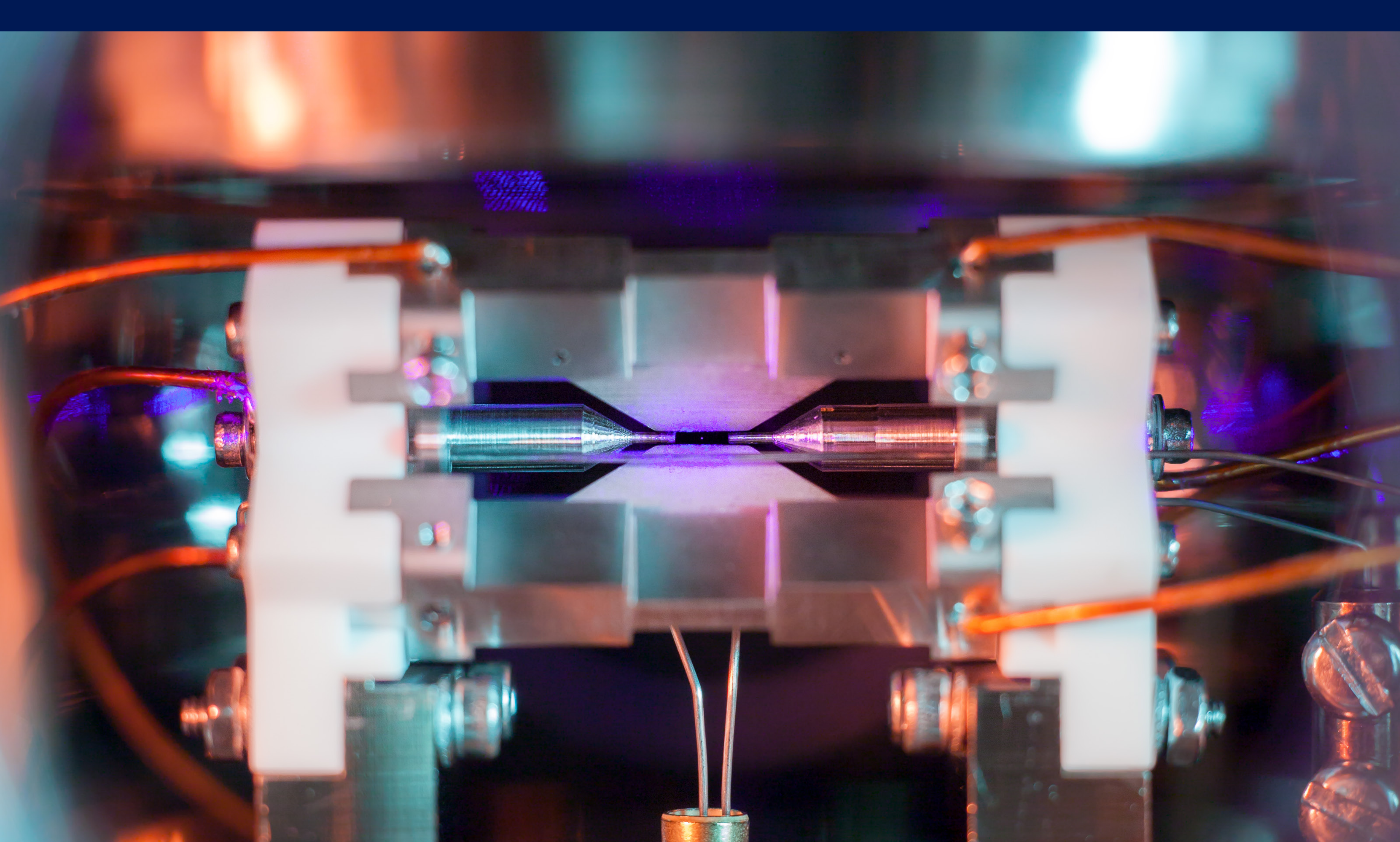


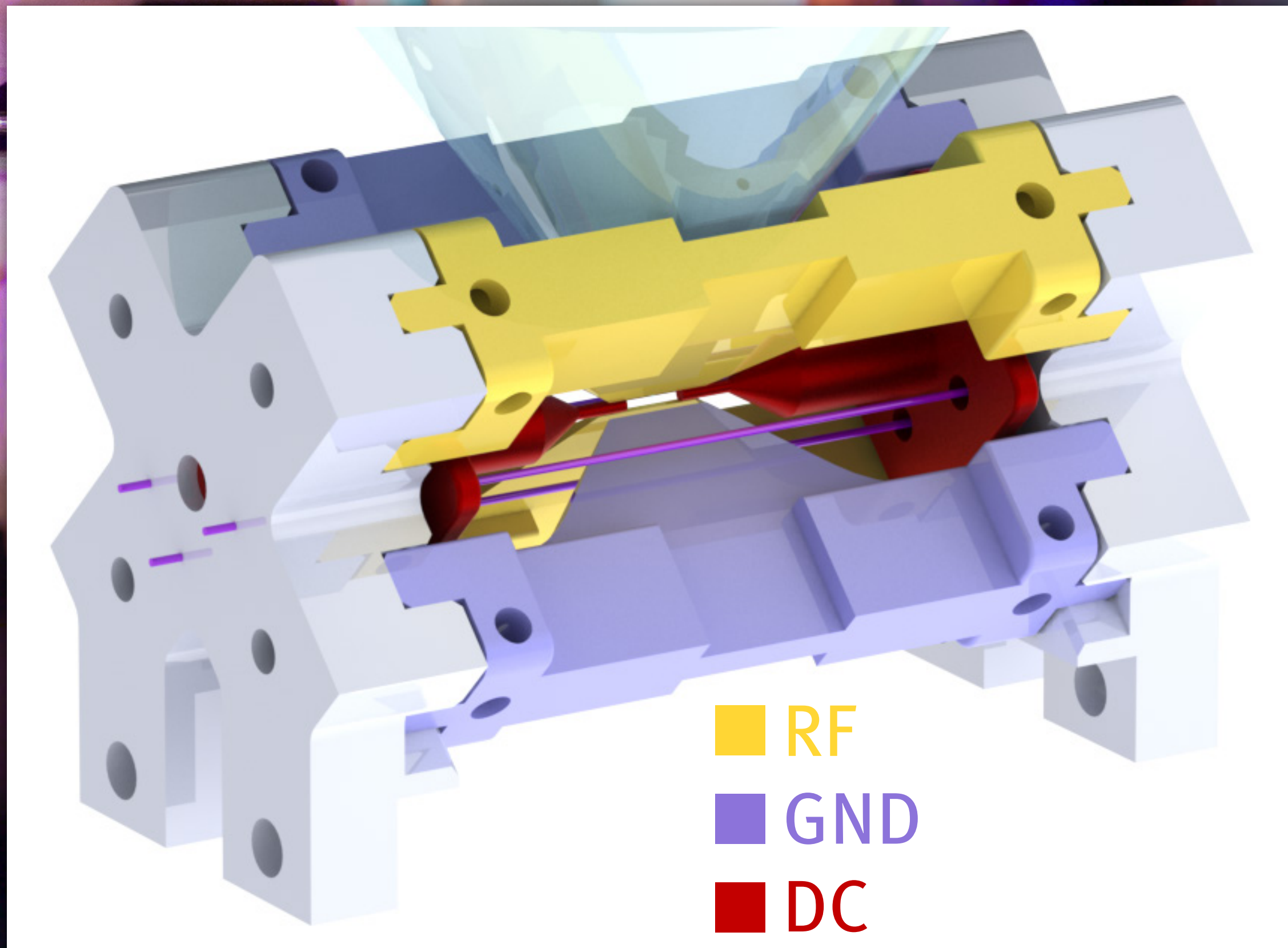
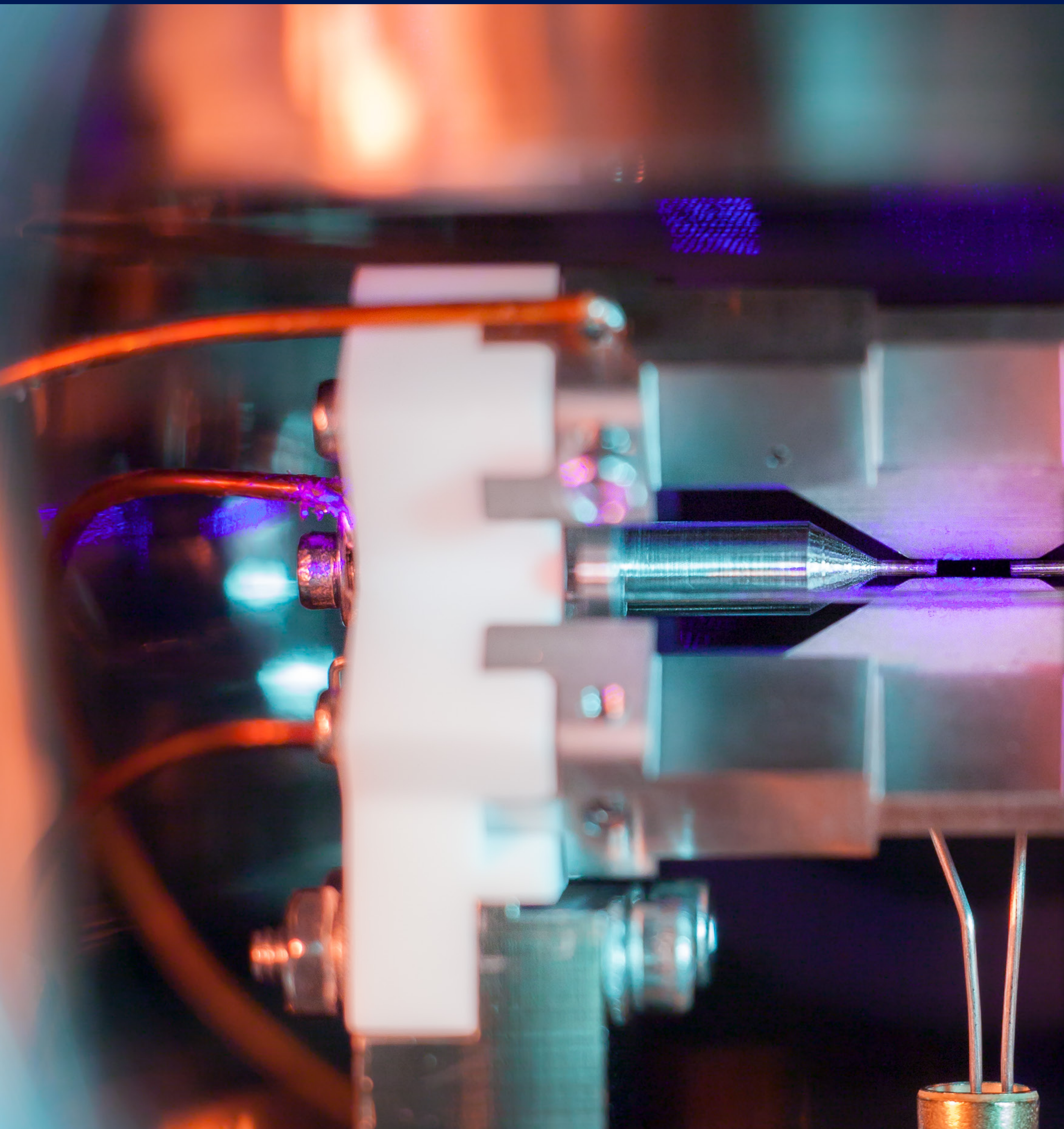
Niemietz et al., *Nondestructive detection of photonic qubits* (2021), doi:10.1038/s41586-021-03290-z

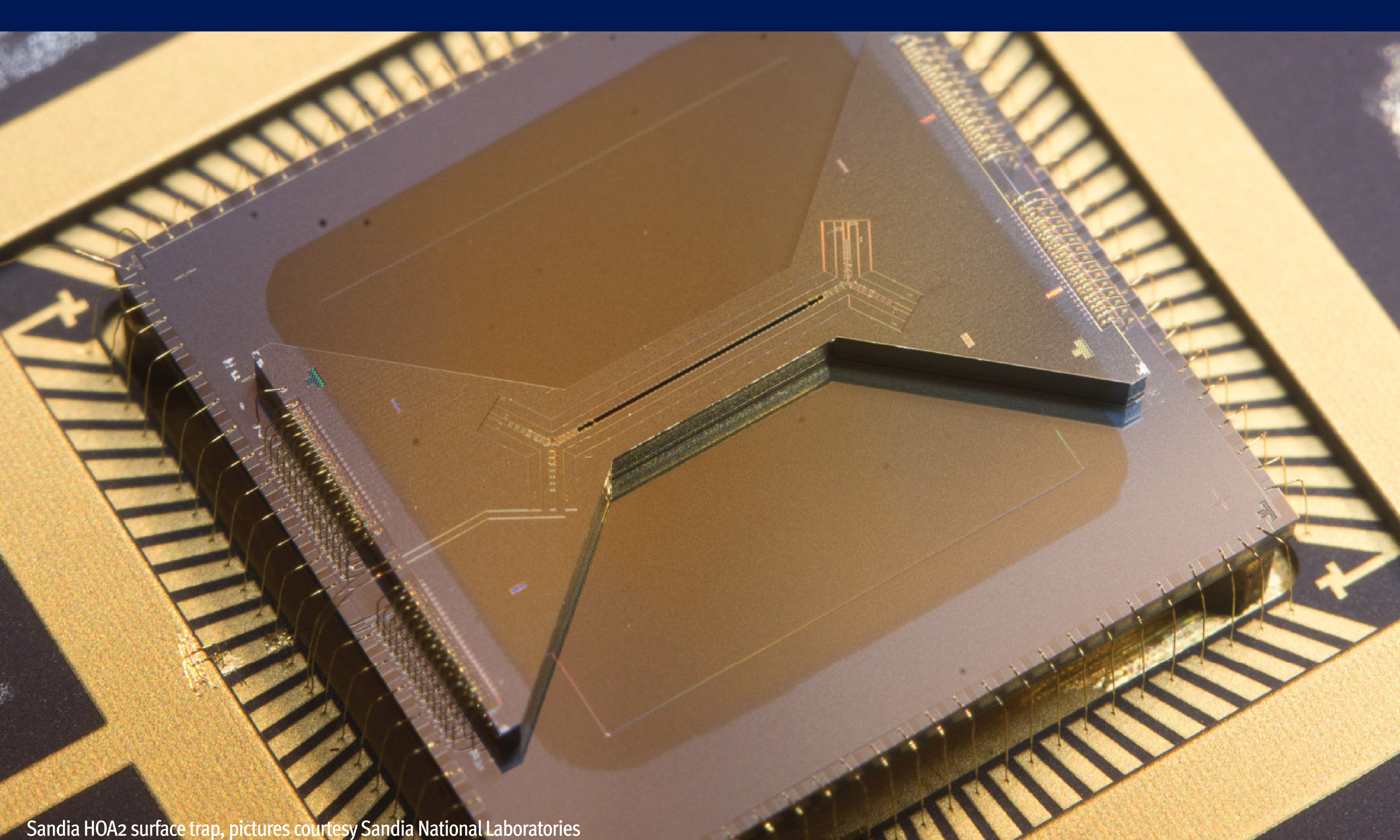
Heralded entanglement swapping



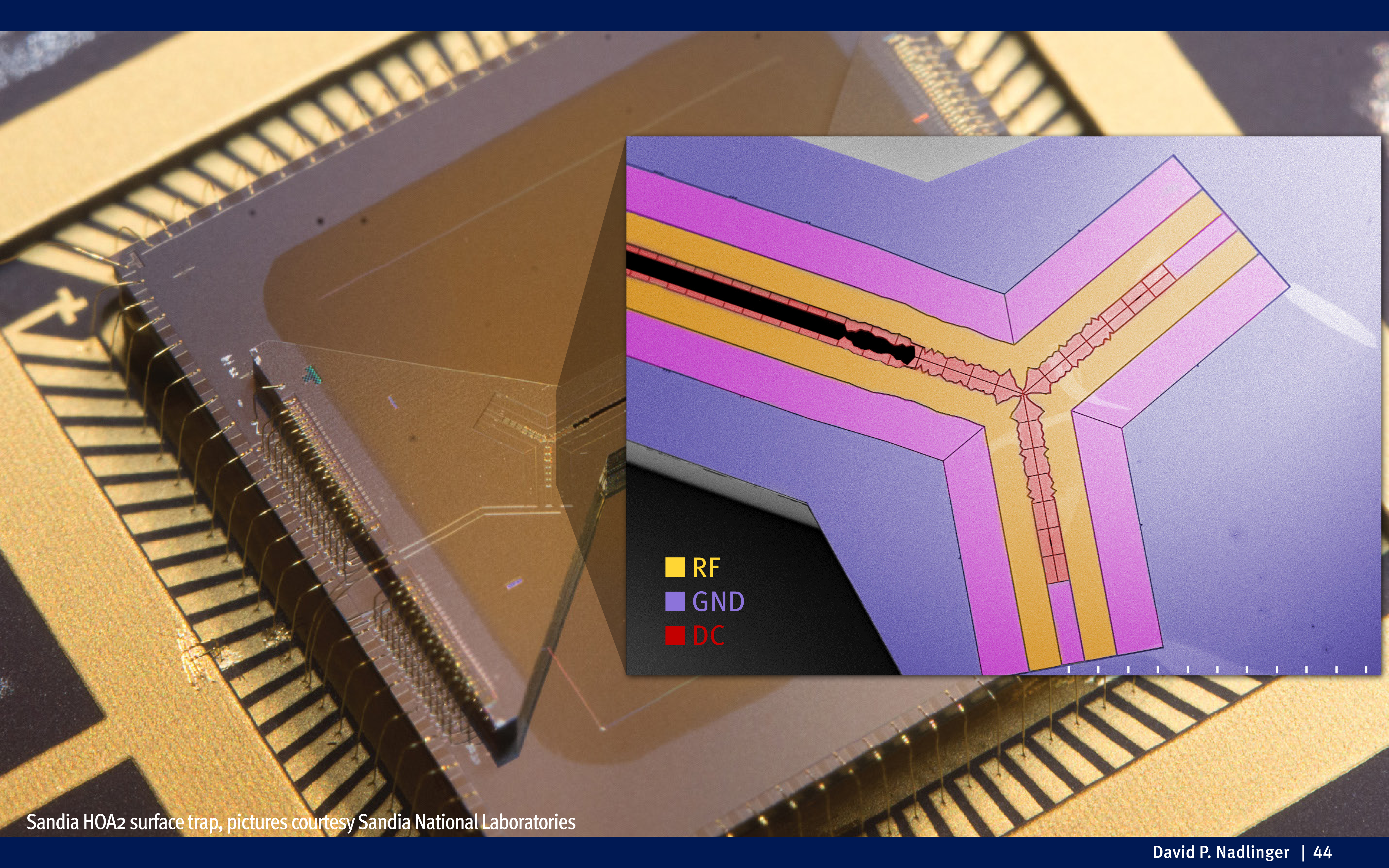
Coecke & Kissinger, *Picturing Quantum Processes*, Cambridge University Press (2017).
Coecke et al. (2022), doi:10.1016/j.tcs.2021.07.024





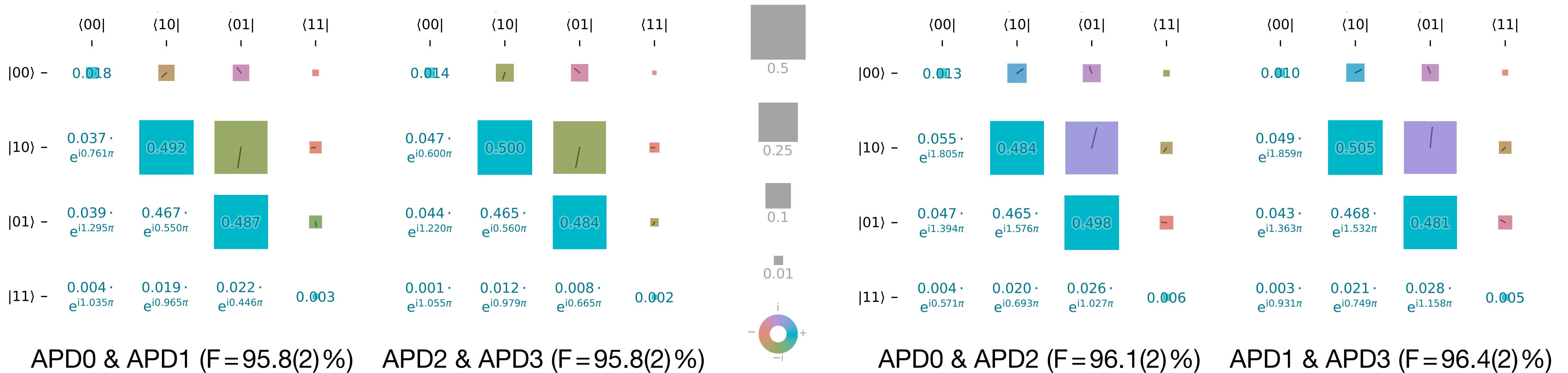


Sandia HOA2 surface trap, pictures courtesy Sandia National Laboratories



Sandia HOA2 surface trap, pictures courtesy Sandia National Laboratories

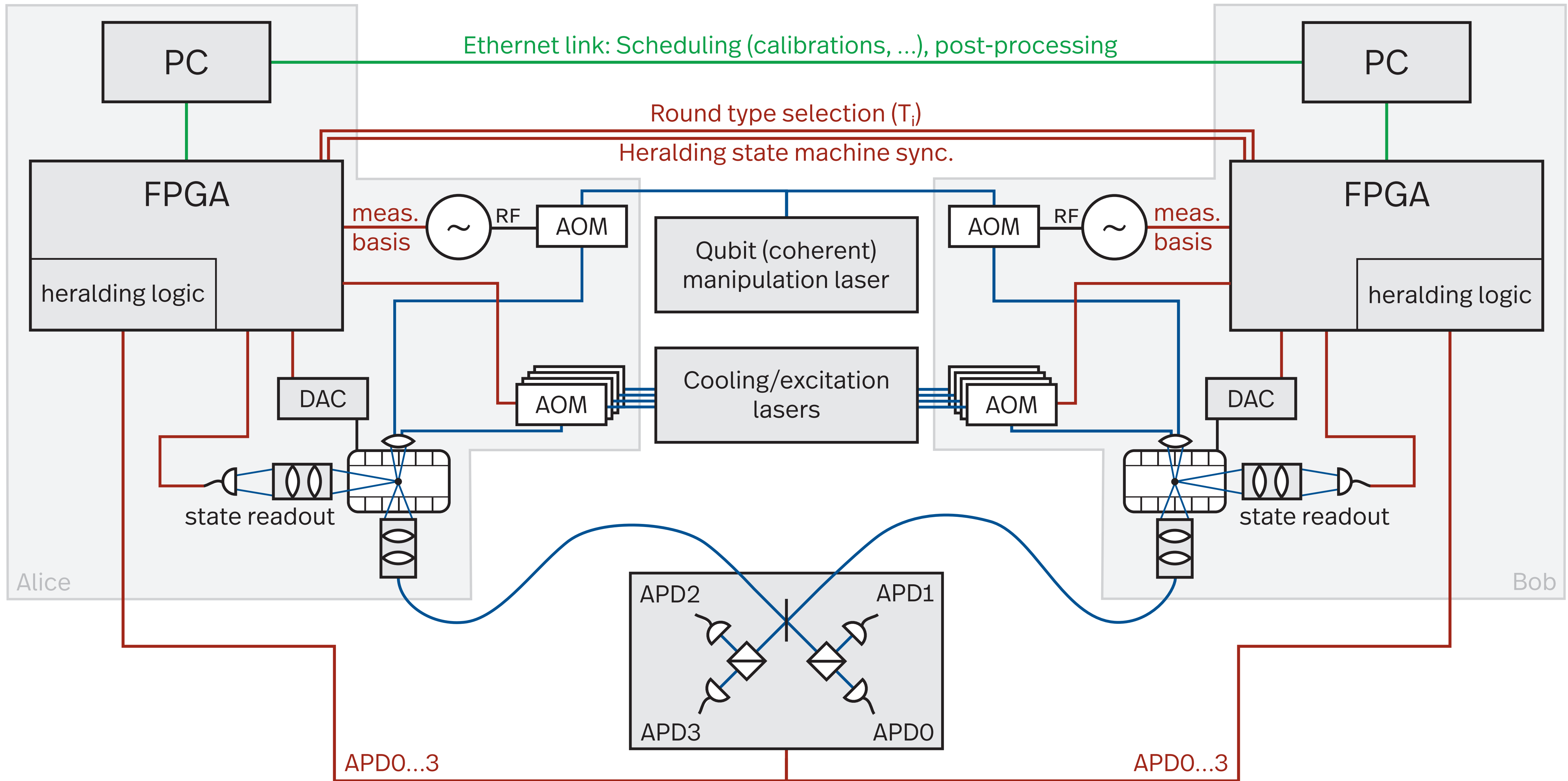
Heralded remote ion-ion entanglement

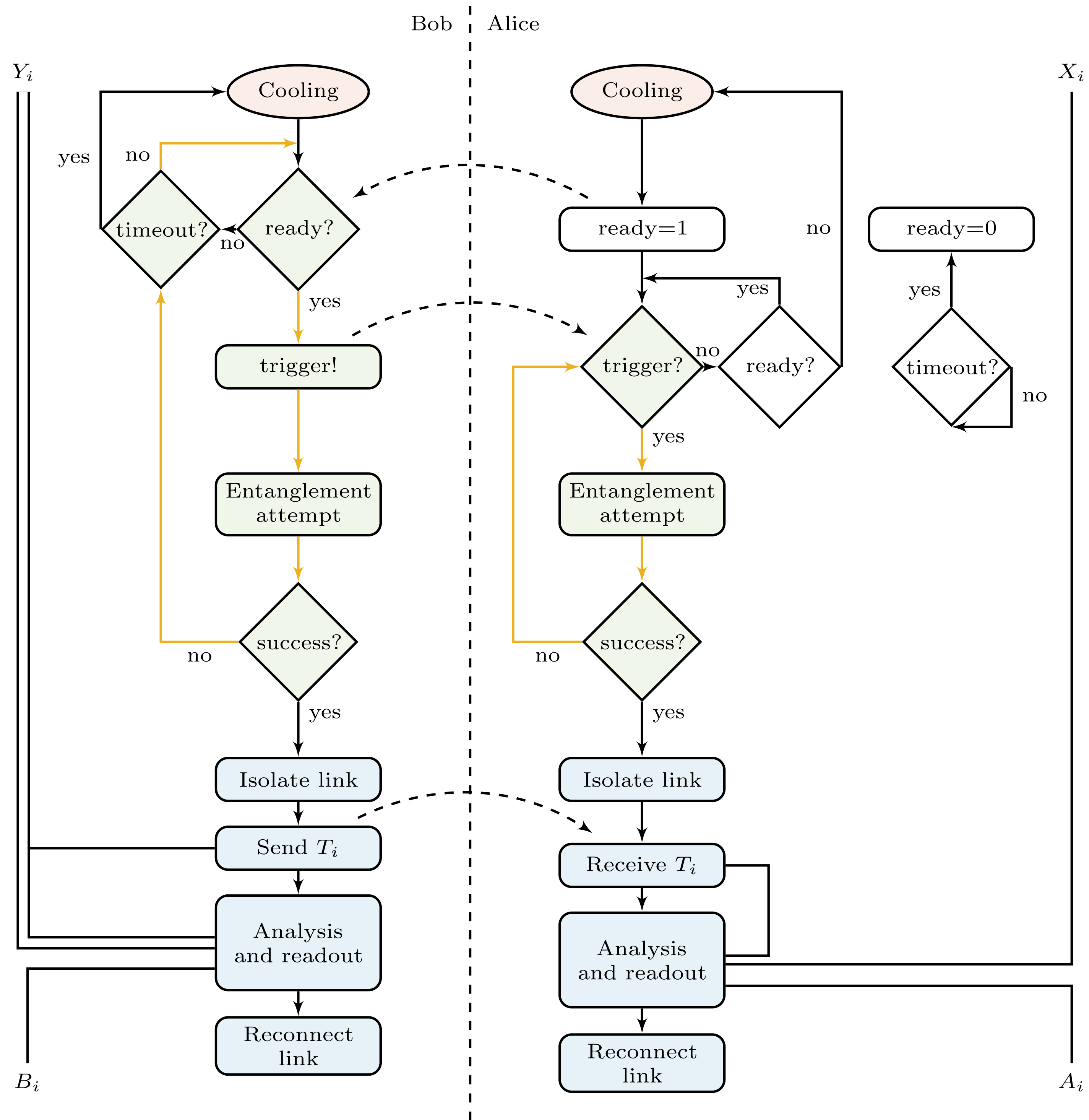


Stephenson, DPN et al. (2020),
10.1103/PhysRevLett.124.110501

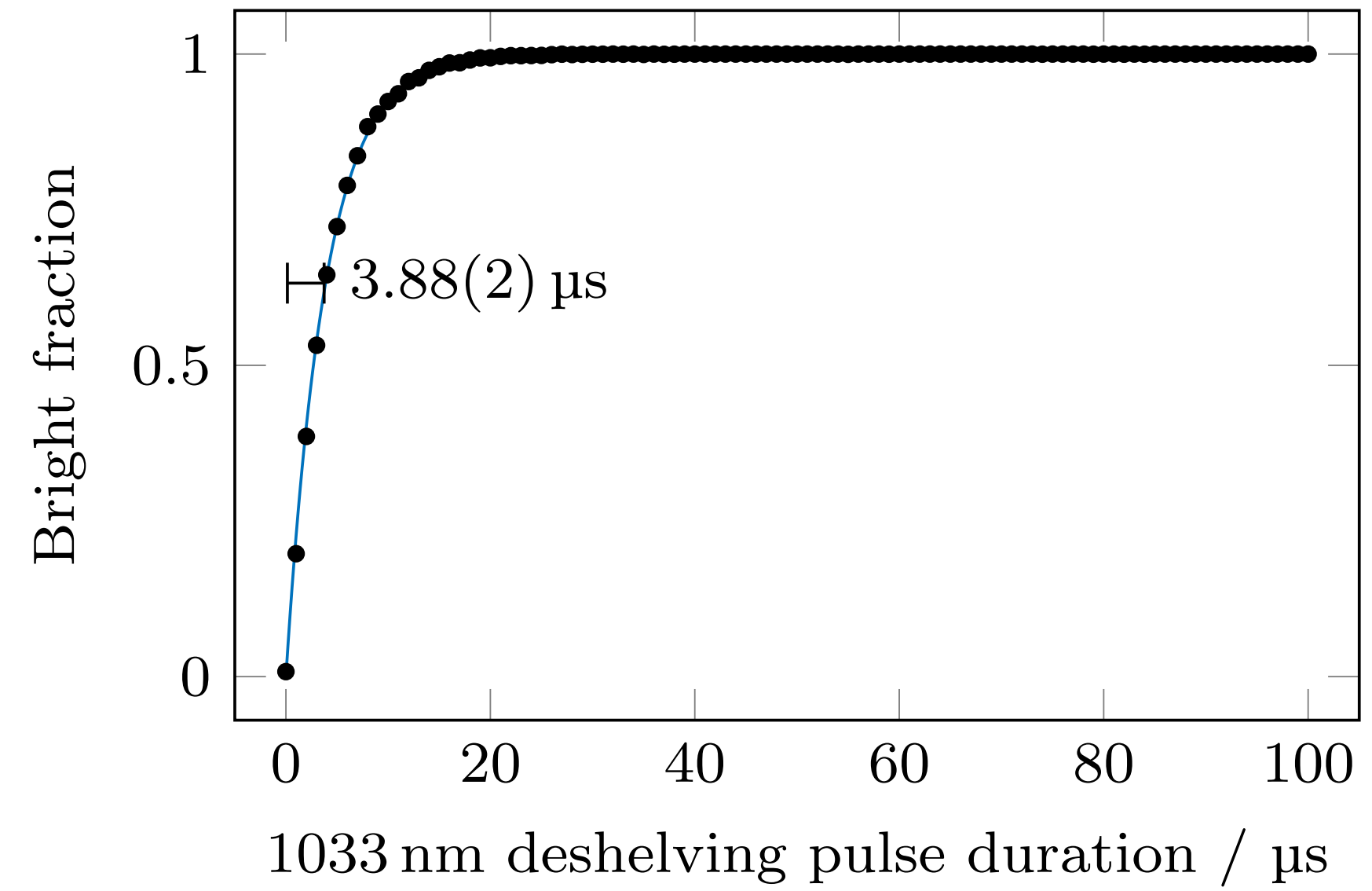
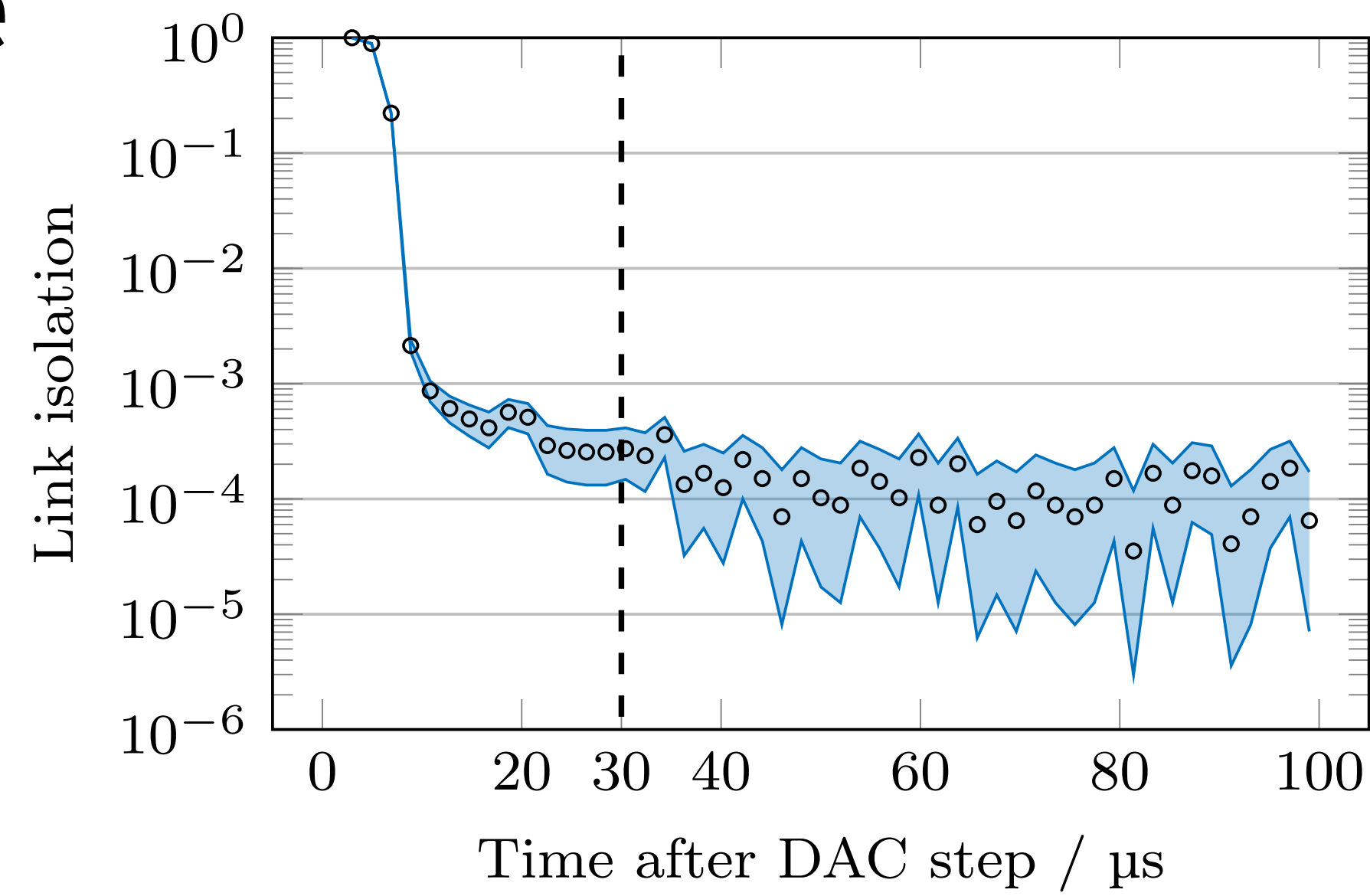
- » Fidelity: 96.0(1)%
- » Entanglement of formation: 0.890(3)

- » Overall rate (incl. cooling):
 - » Best observed: 182 s^{-1}
 - » This data: 100 s^{-1}
 - » Optimistic: $\sim 10^3 \text{ s}^{-1}$

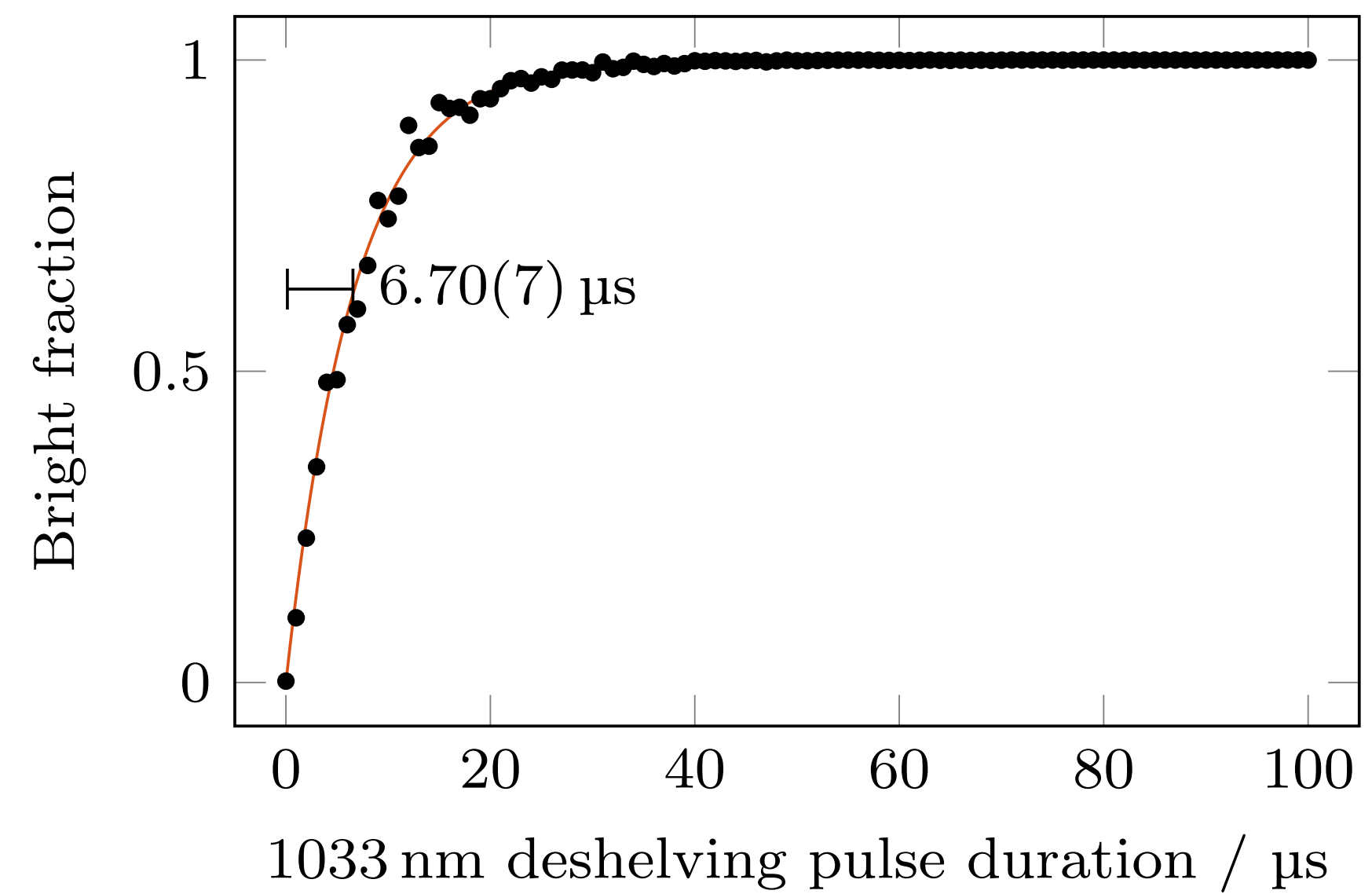
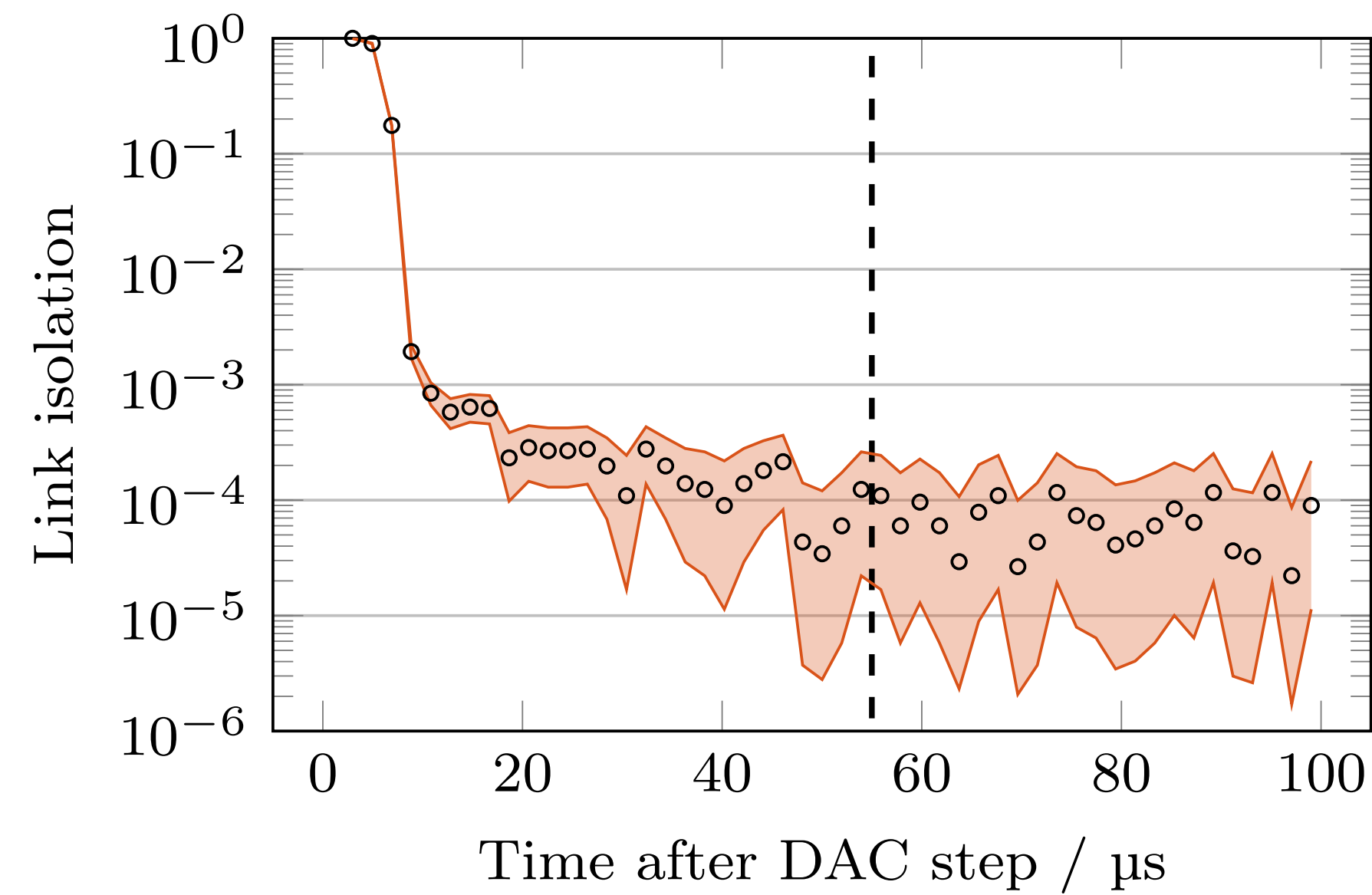




Alice



Bob

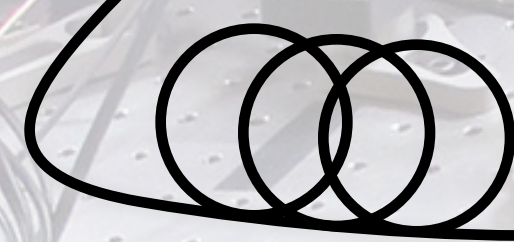
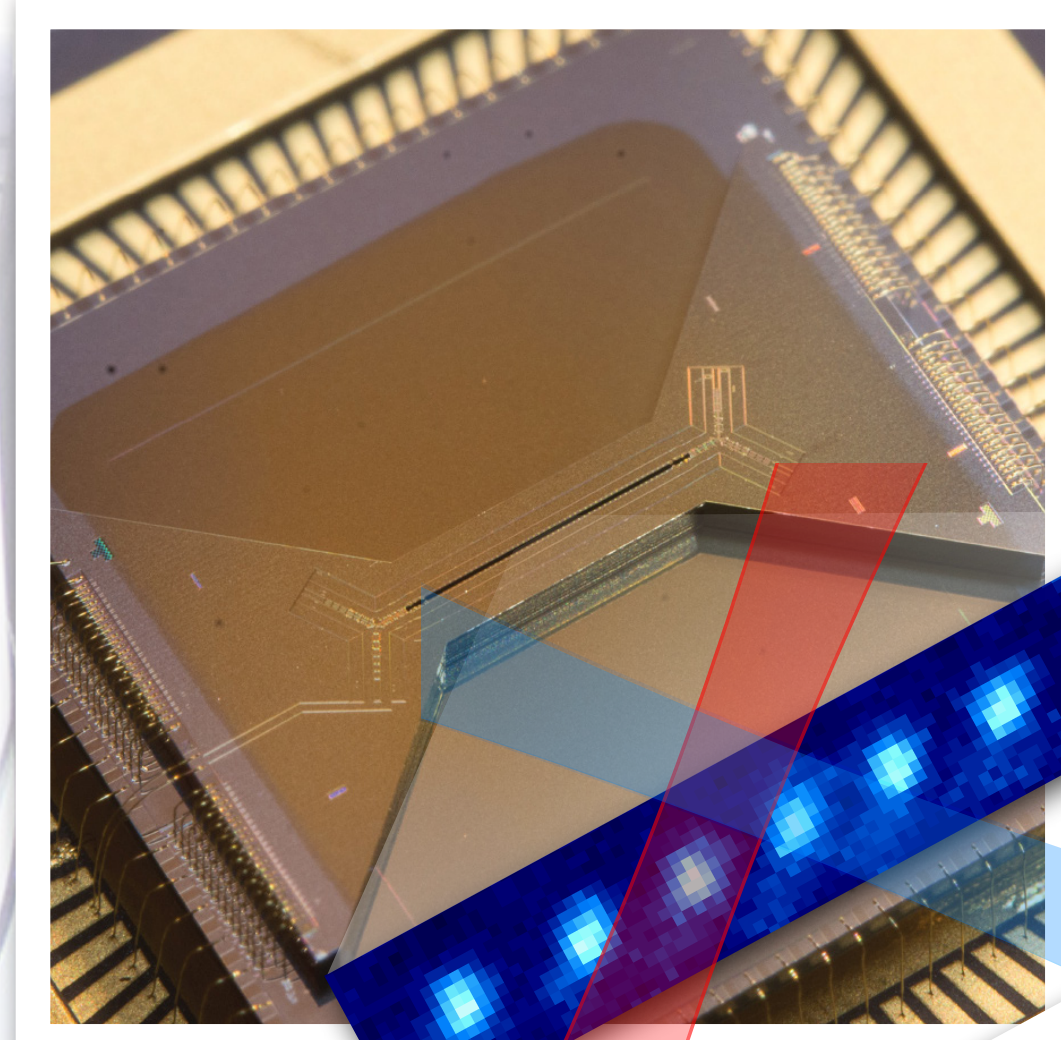


Lower qubit state	Transition magnetic field sensitivity	Coherence time	
		Alice	Bob
$ S_{1/2}, m_J = -1/2\rangle$	-11.2 MHz/mT	4.2 ms	7.5 ms
$ S_{1/2}, m_J = +1/2\rangle$	-39.2 MHz/mT	1.0 ms	1.7 ms

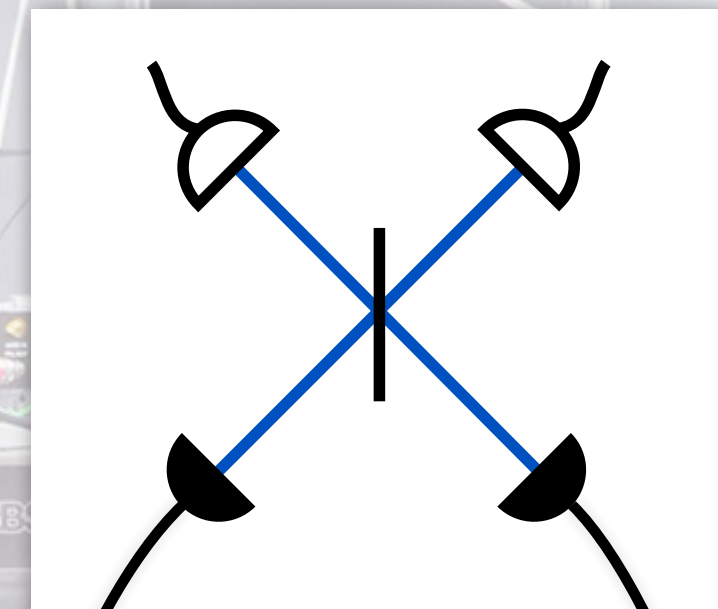
Table S3: Measured $1/e$ coherence times on optical transitions with $|D_{5/2}, m_J = -3/2\rangle$ as the upper qubit state, extracted from a Gaussian fit to the contrast decay in a Ramsey experiment with varying wait duration, without any dynamical decoupling pulses. The $|S_{1/2}, m_J = -1/2\rangle \leftrightarrow |D_{5/2}, m_J = -3/2\rangle$ qubit is used to store the remote entanglement between heralding and measurement basis choice.



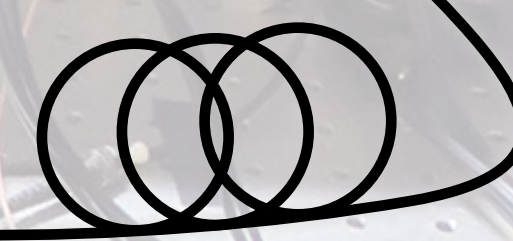
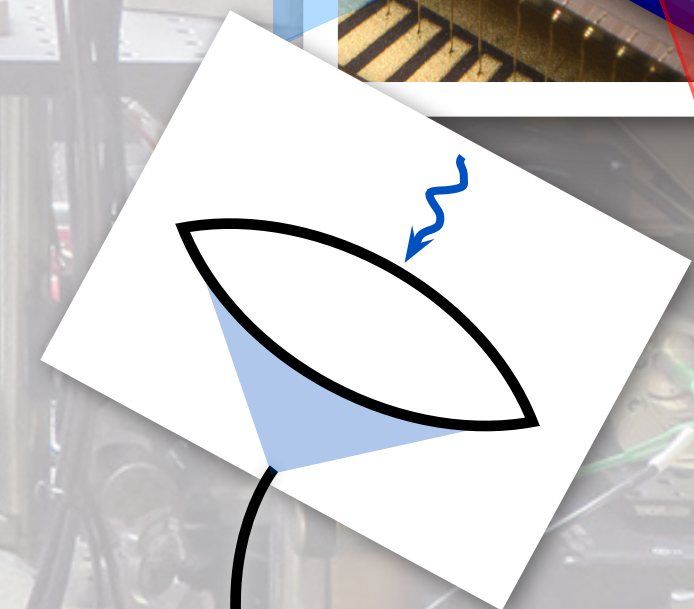
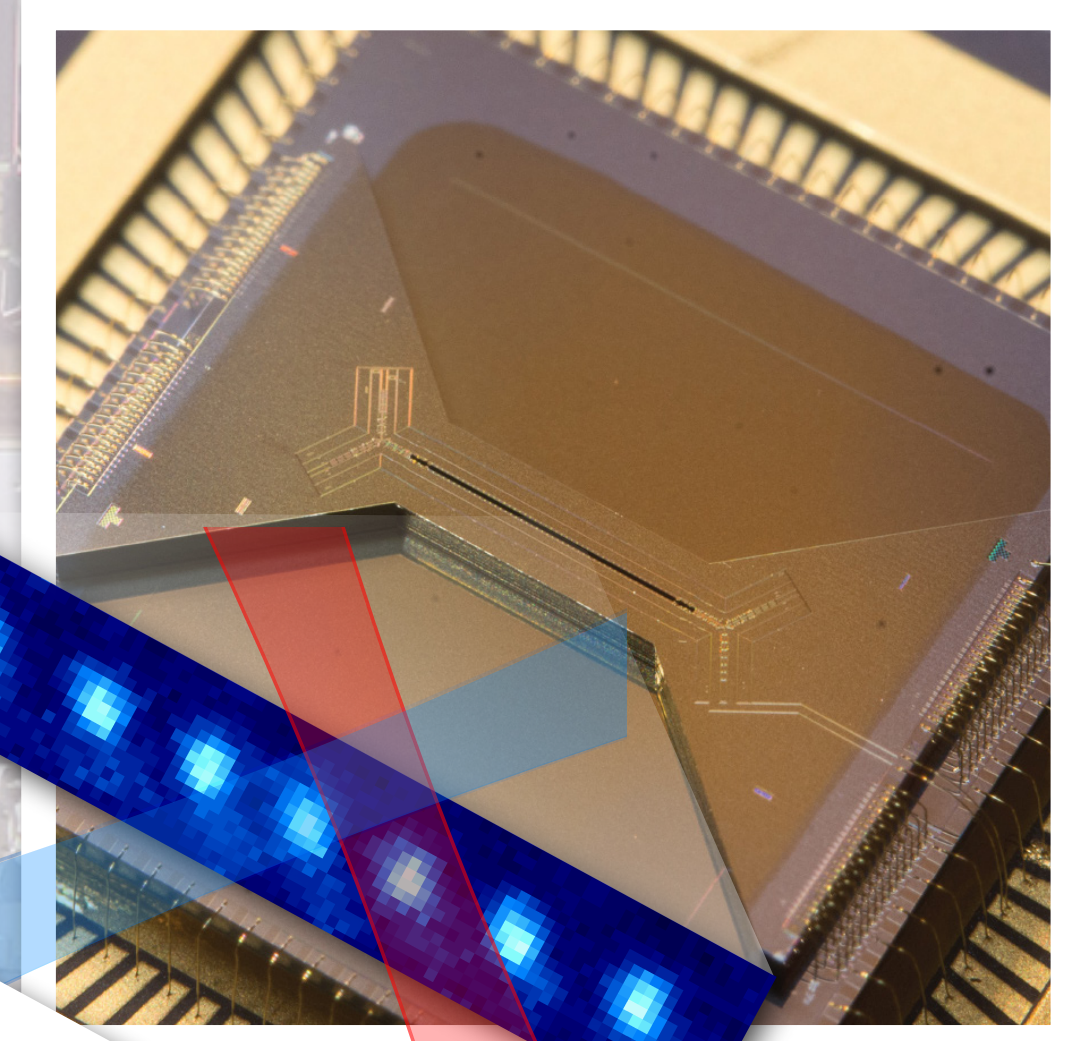
Alice

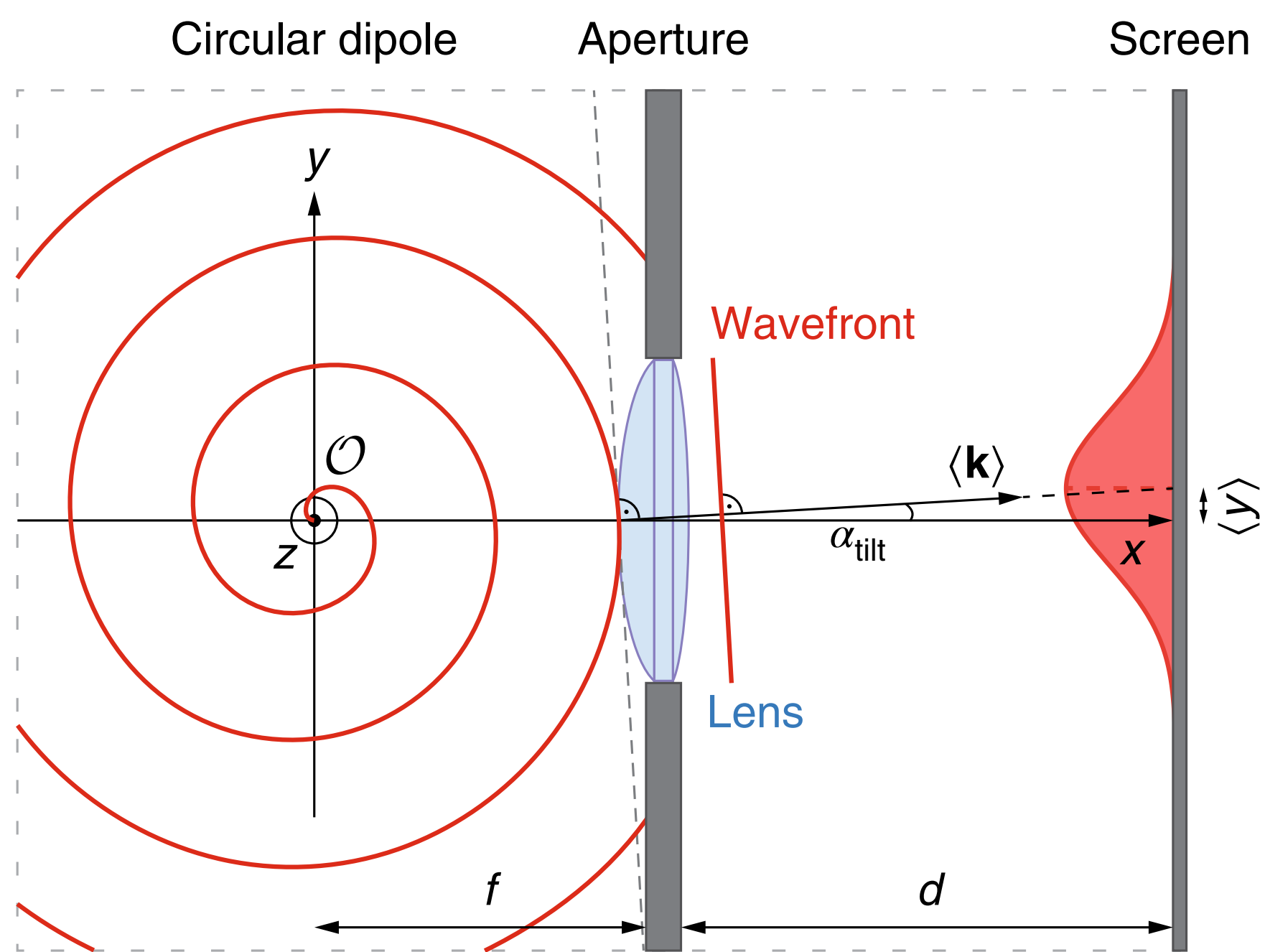


Entangler

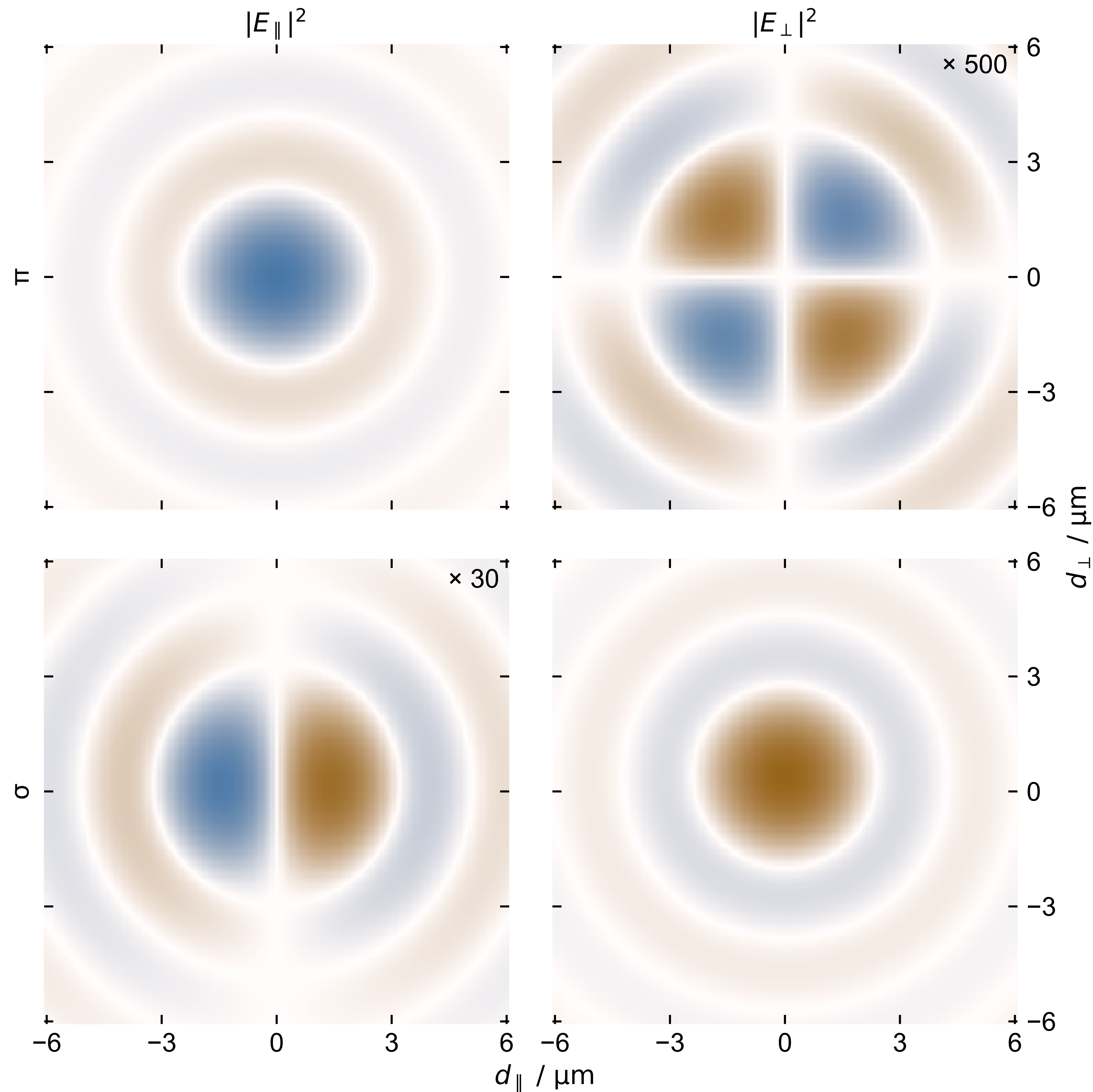


Bob

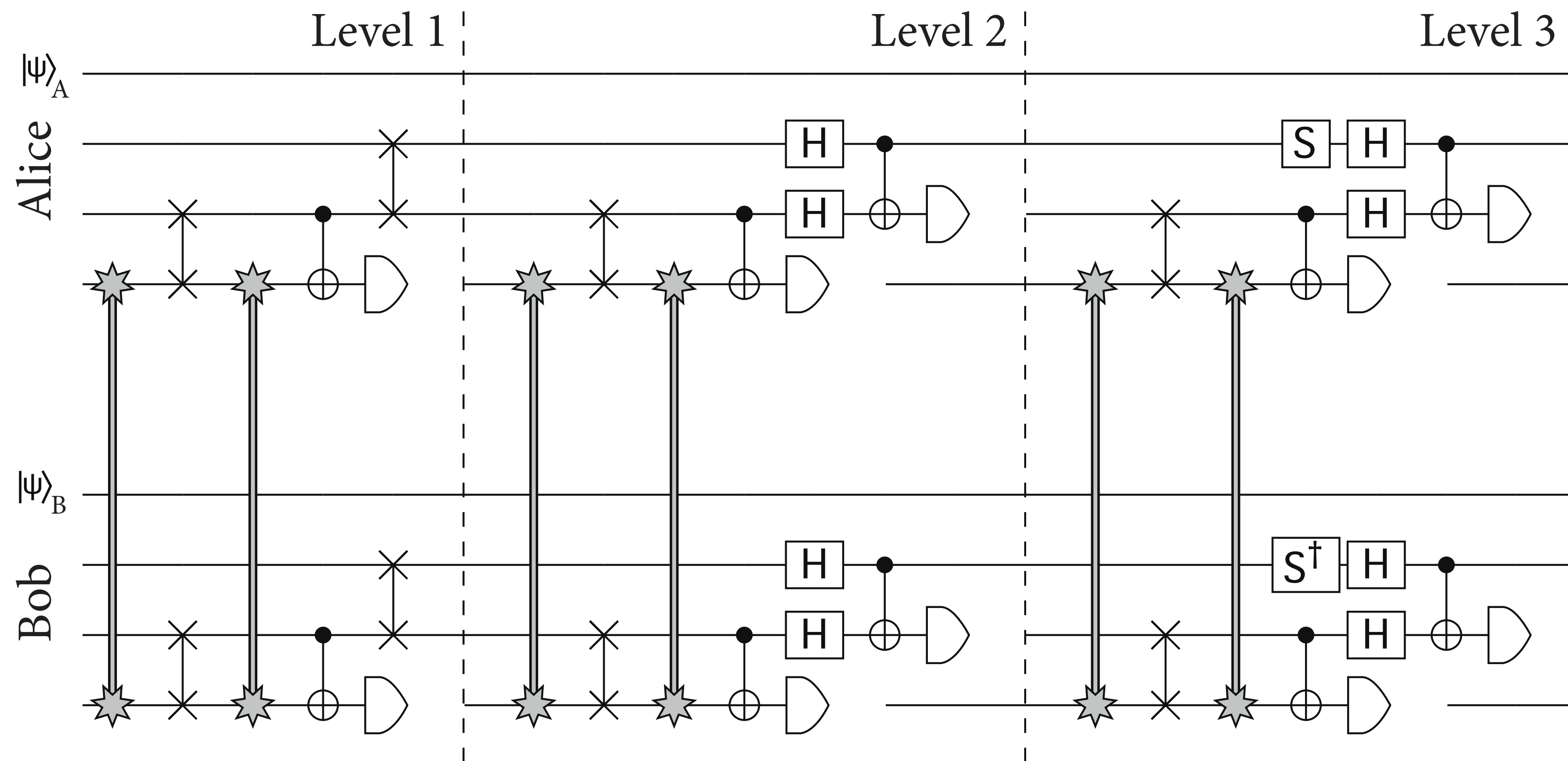




G. Araneda et al. (2018), 10.1038/s41567-018-0301-y



Outlook: Entanglement distillation



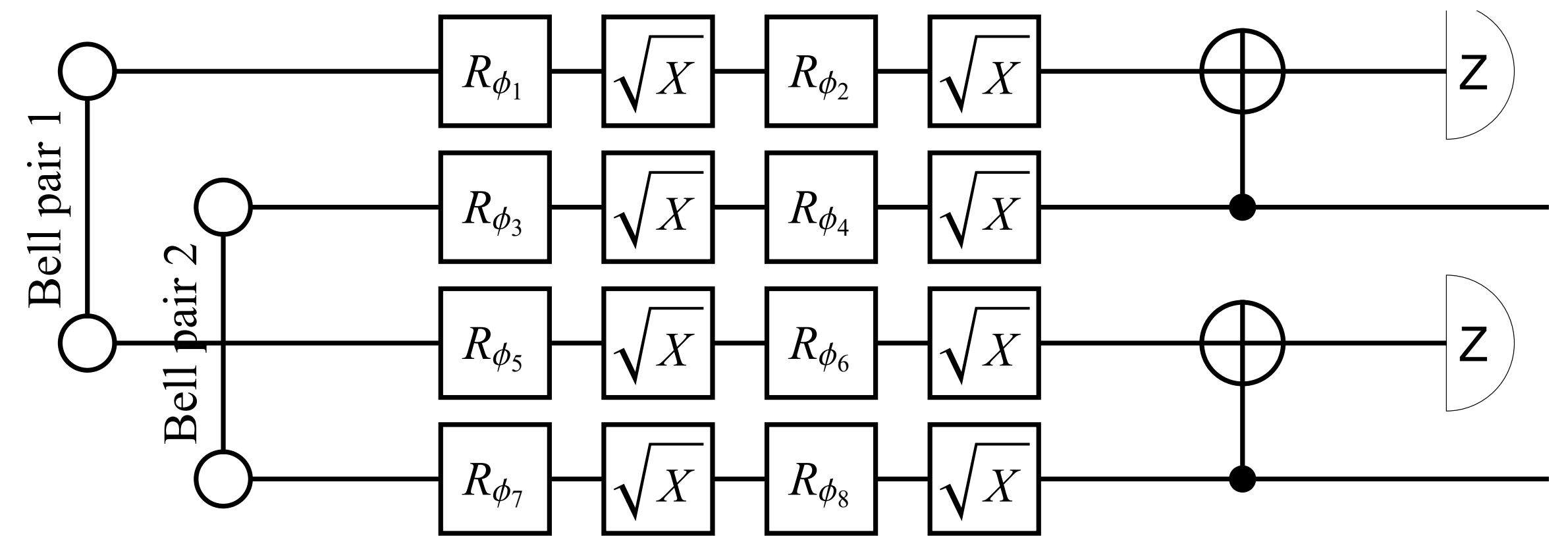
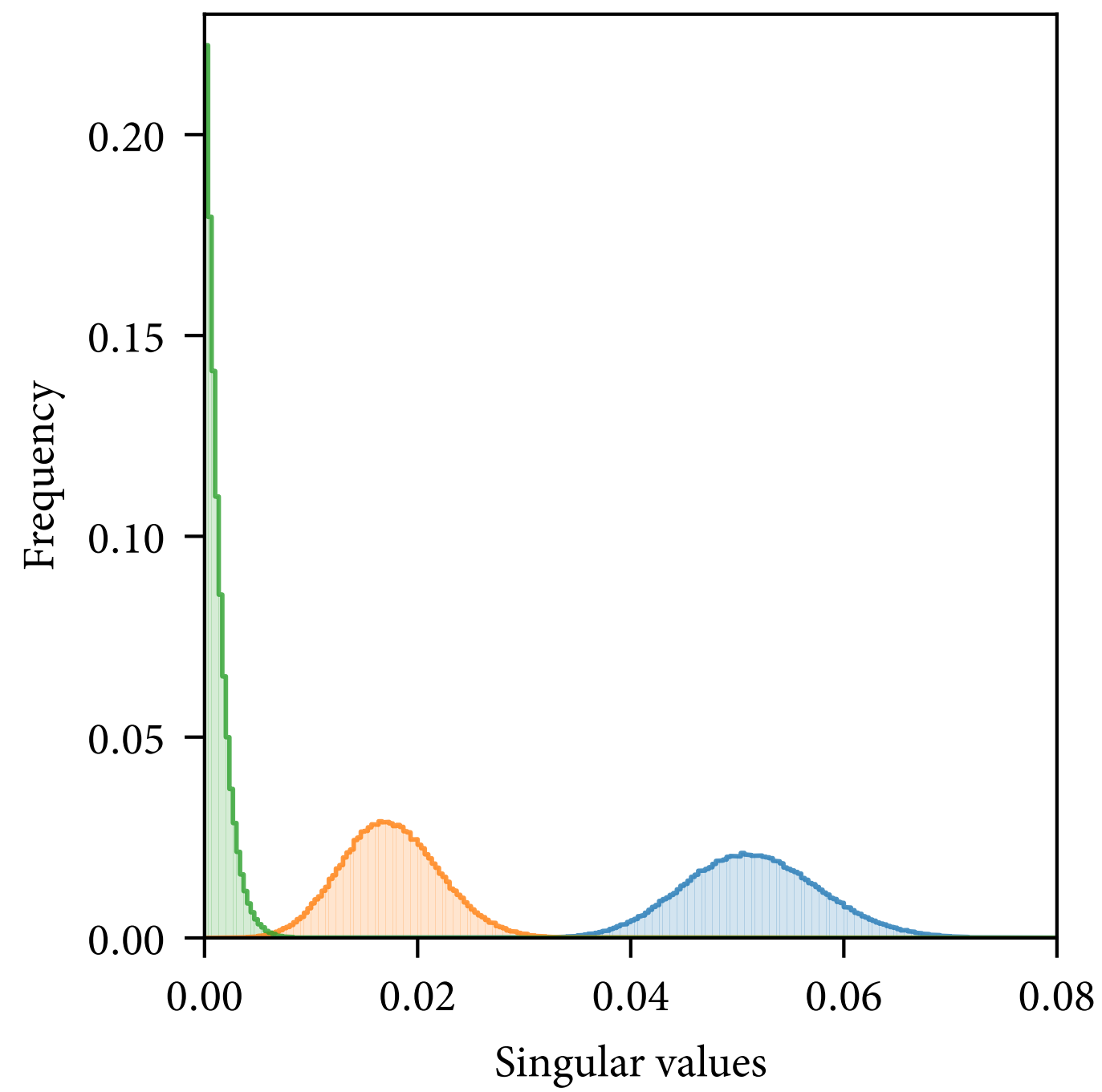
Nigmatullin et al. (2016), doi: 10.1088/1367-2630/18/10/103028

- » Exploit high-fidelity local operations, long coherence times
- » 99.7 % Bell state fidelity using 6 “raw” pairs
- » 2 traps, 5 ions each ($2 \times {}^{88}\text{Sr}^+$, $3 \times {}^{43}\text{Ca}^+$)

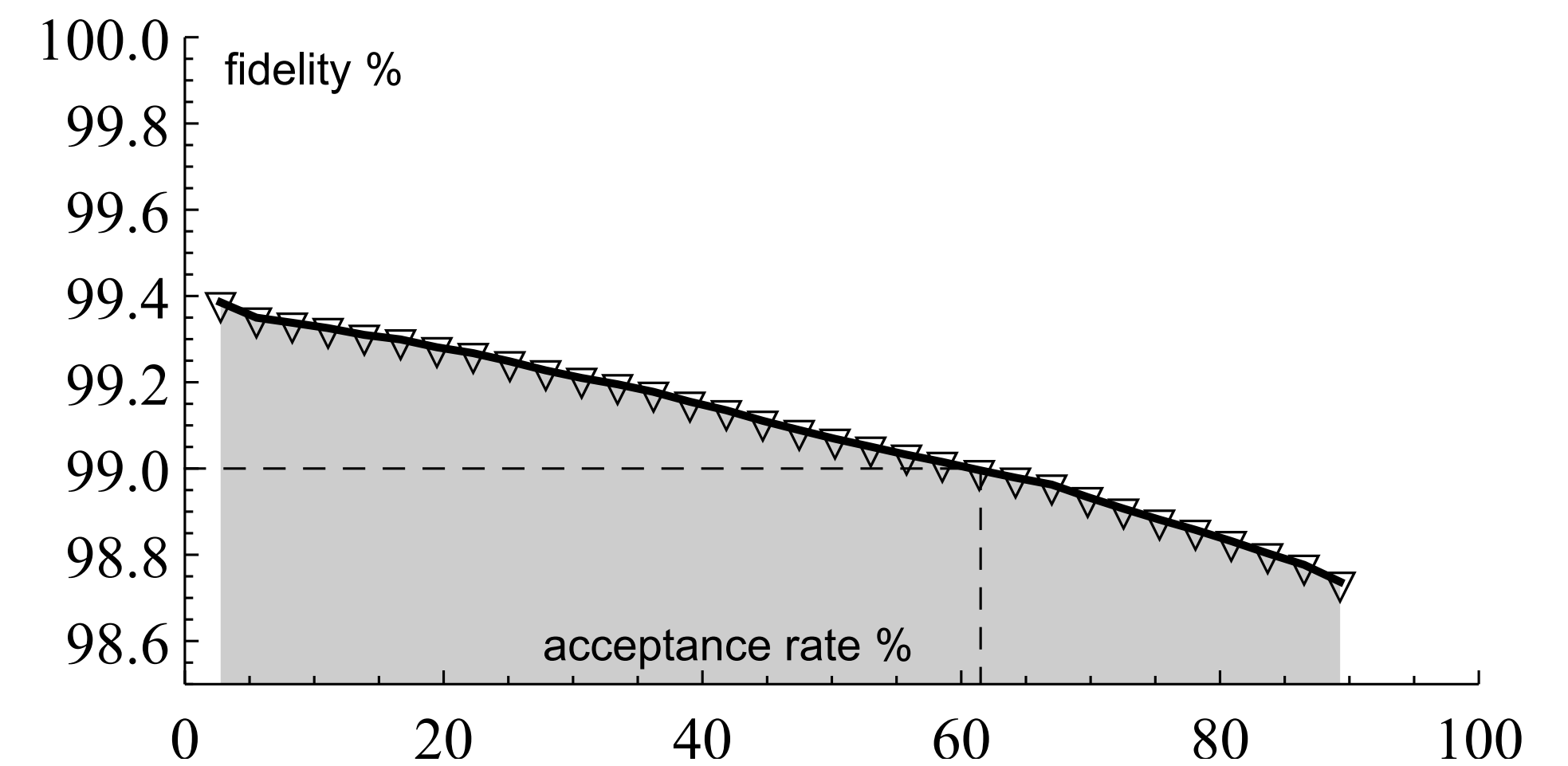
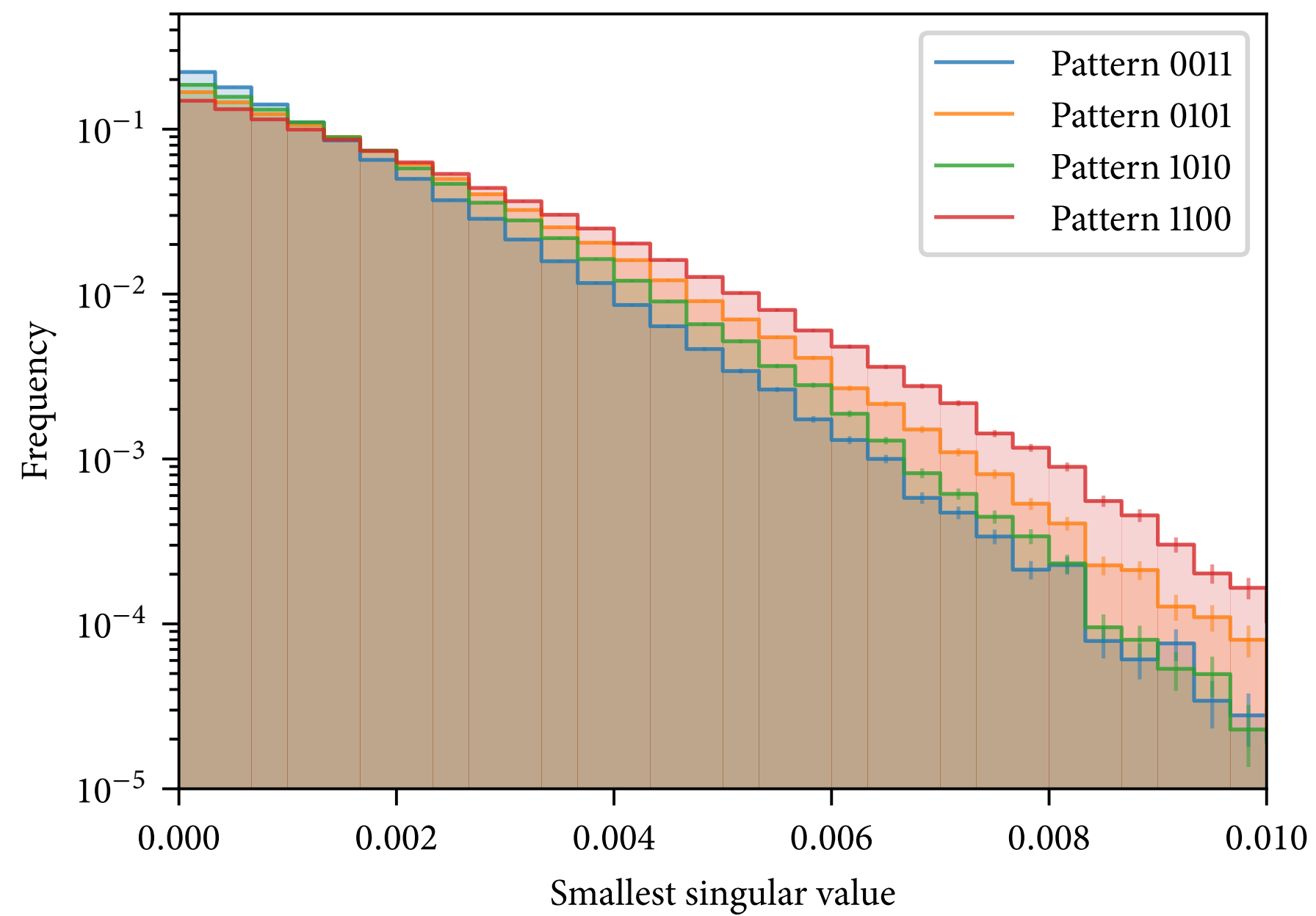
$$\rho_\epsilon = (1 - \epsilon)\Phi^+ + \frac{\epsilon}{3}\Phi^- + \frac{\epsilon}{3}\Psi^+ + \frac{\epsilon}{3}\Psi^-$$

$$\tilde{\rho}_\epsilon^{(1)} \equiv F[\rho_\epsilon, \rho_\epsilon] = \left(1 - \frac{2}{3}\epsilon - \frac{2}{3}\epsilon^2\right)\Phi^+ + \left(\frac{2}{3}\epsilon + \frac{2}{9}\epsilon^2\right)\Phi^- + \frac{2}{9}\epsilon^2\Psi^+ + \frac{2}{9}\epsilon^2\Psi^- + O(\epsilon^3)$$

$$\tilde{\rho}_\epsilon^{(3)} \sim \left(\frac{2}{9}\epsilon^2, \frac{8}{27}\epsilon^3, \frac{8}{27}\epsilon^3\right)$$

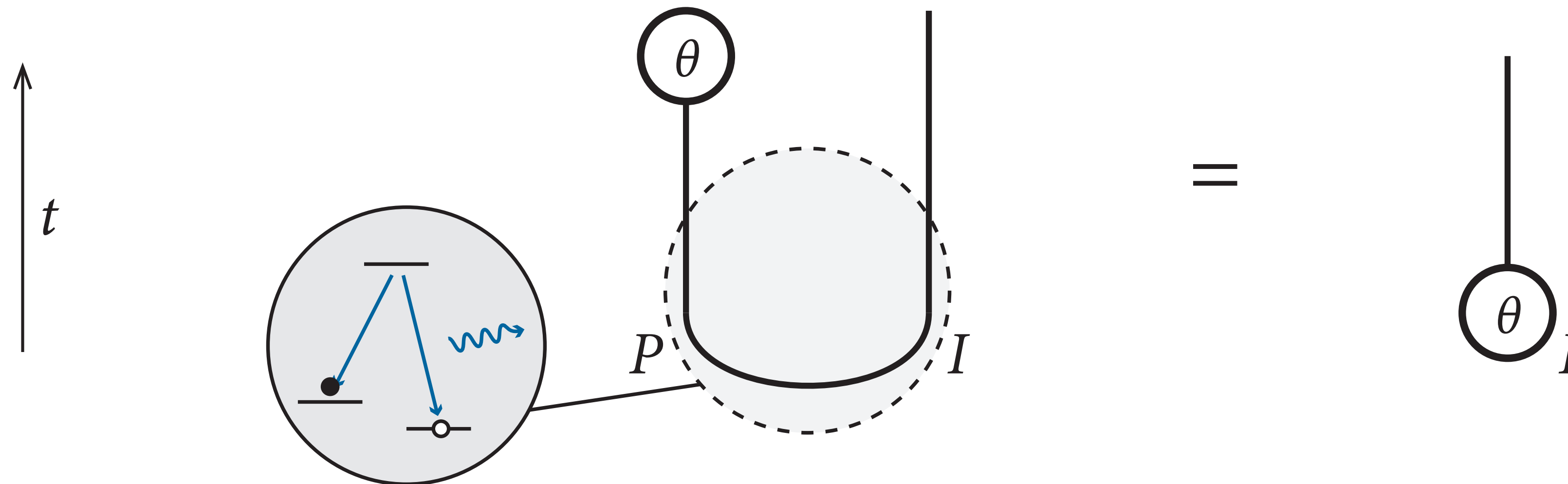


32 outcomes – 99% fidelity with 60% acceptance rate

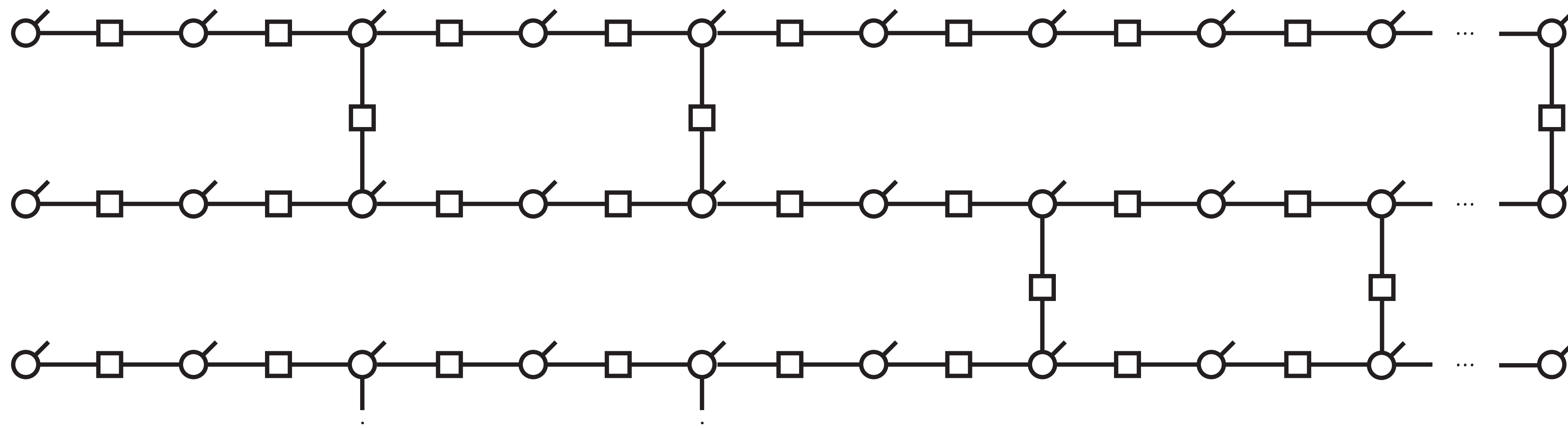


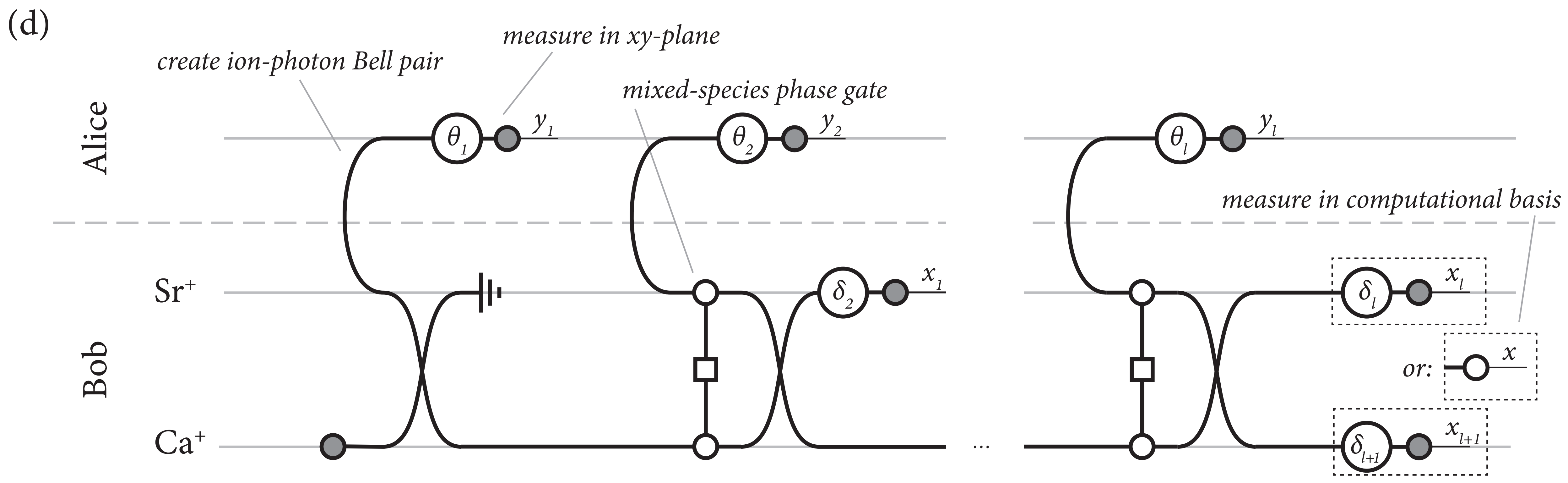
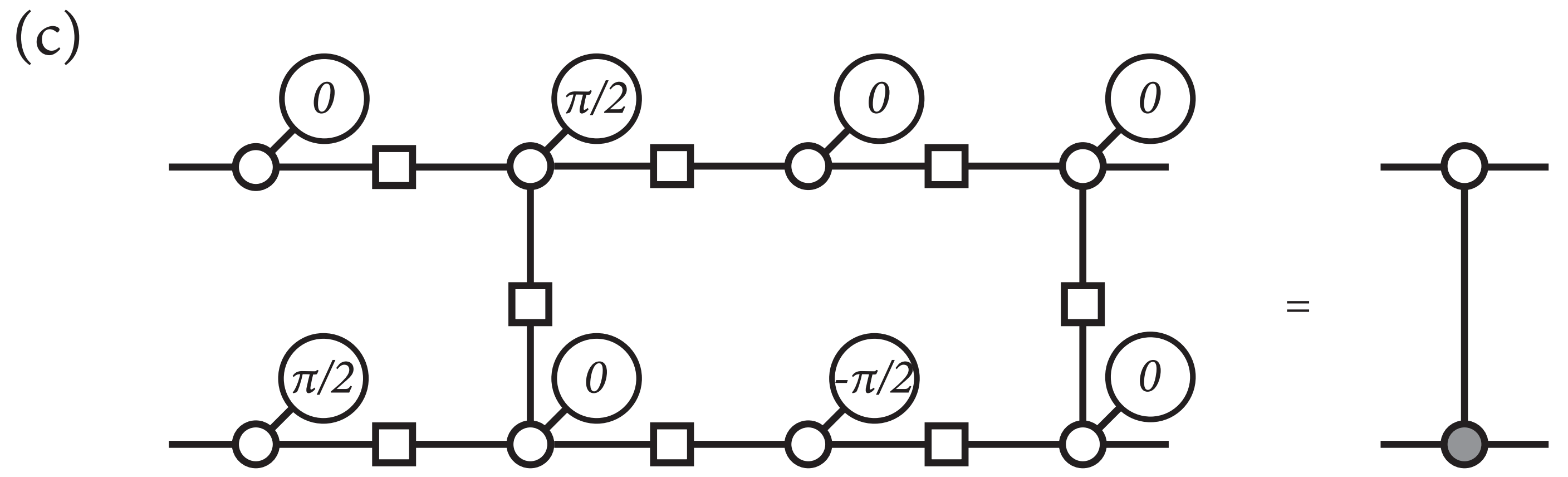
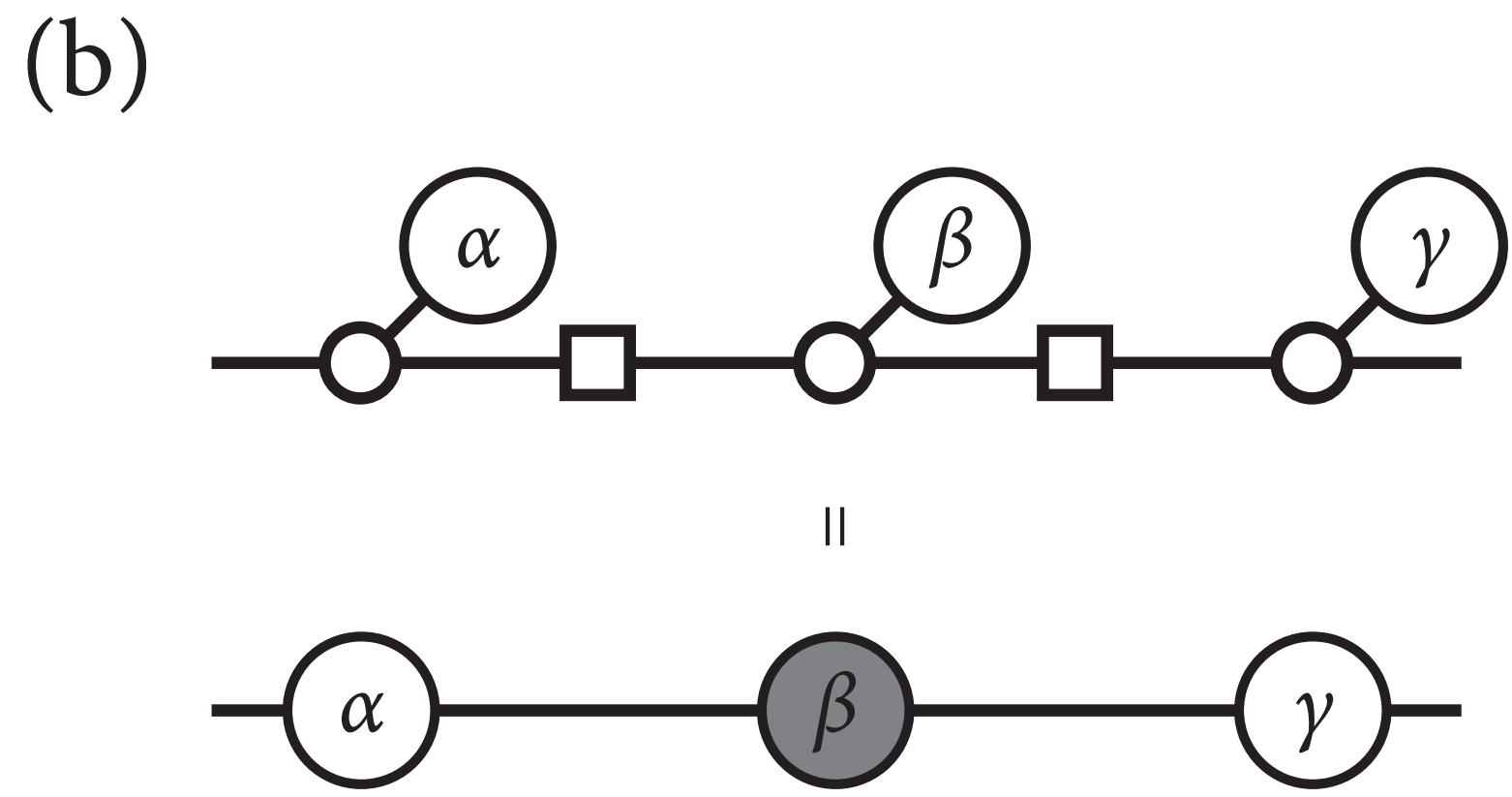
Outlook: Blind quantum computing

- » Idea: Client can outsource computation to server, without the server learning about algorithm or input/output data



- » Basis: Measurement-based QC, teleport phases into brickwork state





End of additional material