Q 48: Quantum Information (Quantum Communication and Quantum Repeater) II

Time: Thursday 14:00–16:00 Location: e001

Group Report Q 48.1 Thu 14:00 e001

Quantum Readout of Physical Unclonable Keys for Authentication and Authenticated Communication — •Pepijn W. H. Pinkse — University of Twente, Enschede, The Netherlands

Authentication is essential to ensure trust in communication in modern society and will play an even more important role in automated networks. Symmetric authentication schemes rely on a shared secret, which does not scale well with the number of potential communication partners. Asymmetric authentication schemes rely on the combination of a public key and a private key. This scales better with the number of potential partners, but still requires a secret to be kept and stored in a secure way, which could be copied without the owner knowing. This is an important issue even in Quantum Key Distribution schemes that do not provide an intrinsic solution for the authentication of the communication partners.

In the past we have demonstrated the quantum-secure optical readout of a physical unclonable key (PUK) [1]. A PUK is a unique key which cannot be physically copied with existing or foreseeable technology. Recently, we have devised a communication scheme based on optical PUKs employing readout with shaped complex wavefronts of weak coherent light pulses [2].

In this talk I will give an overview of the state of the art, some insights in the hardness of copying and the possibilities to do readout over single-spatial modes.

[1] Goorden et al., Optica 1, 421 (2014). [2] Uppu et al., Quantum Sci. Tech. 4, 04501 (2019).

Q 48.2 Thu 14:30 e001

Quantum conference key agreement — •Gláucia Murta, Giacomo Carrara, Federico Grasselli, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine- Universität Düsseldorf, Universitätsstr. 1, D-40225 Düsseldorf, Germany

Conference key agreement is a cryptographic task in which several parties wish to establish a common key that is unknown to any eavesdropper. Protocols based on quantum resources allow to achieve unconditional security. Unconditionally secure conference key agreement can be established using several instances of bipartite quantum key distribution. However, multipartite quantum correlations bring the possibility of designing new protocols. In this talk we focus on conference key agreement protocols that make use of multipartite entangled states. We characterize the resources required to establish a secure conference key. We then focus on existing protocols and discuss their performance. Finally we move to a device-independent setup and discuss results towards protocols with higher rates.

Q 48.3 Thu 14:45 e001

Bell measurement using entangled telecom photons with ancilla qubits — •Nico Sieber, Matthias Bayerbach, Nico Hauser, Daniel Bhatti, and Stefanie Barz — Institute for Functional Matter and Quantum Technologies, University of Stuttgart

Photonic devices are key to a large range of quantum technologies, for example quantum communication and wider quantum networks. When transmitting quantum information over long distances, minimizing losses is crucial to any quantum protocols. Thus, the favourable wavelength is in the telecom regime 1550 nm). Many quantum protocols thus rely on pure and indistinguishable photons at this wavelength. Here we demonstrate the generation of entanglement in this wavelength regime using a parametric down-conversion photon pair source in a linear configuration which will be sent, together with anciliary states, through a network of linear elements.

Q 48.4 Thu 15:00 e001

Quantum teleportation using highly coherent emission from telecom C-band quantum dots — •Tina Mueller[1], Matthew Anderson[1,2], Joanna Skiba-Szymanska[1], Andrey Krysa[3], Jan Huwer[1], Mark Stevenson[1], Jon Heffernan[4], David Ritchie[2], and Andrew Shields[1] — [1]208 Science Park, Milton Road, Cambridge CB4 0GZ, UK — [2]Cavendish Laboratory, University of Cambridge, Cambridge CB3 0HE, UK — [3]EPSRC National Epitaxy Facility, University of Sheffield, Sheffield S1 3JD, UK — [4]Department of Electronic and Electrical Engineering, University of Sheffield, Sheffield, S1 3JD, UK

Quantum network technologies rely on interference of indistinguishable photons, demanding sources of highly coherent single photons, with ideal wavelength around 1550 nm for fibre-based applications. Recently, emission of single and entangled photons from semiconductor sources in that band has been reported, but demonstration of sufficiently long coherence times has been outstanding. We show that InAs/InP quantum dots emitting in the telecom C-band can provide photons with coherence times exceeding 1 ns. These values enable near-optimal interference of quantum dot emission with a C-band laser qubit. Using entangled photons we further demonstrate teleportation of such qubits with a fidelity reaching 83.6(2.2)%.

Q 48.5 Thu 15:15 e001

A high bandwidth quantum network node with a single trapped ion in an ultraviolet fiber cavity — •Pascal Kobel[1], Moritz Breyer[1], Ralf Berner[1], Vidhya Sasidharan Nair[1], Konstantin Ott[2], Jakob Reichel[2], and Michael Köhl[1] — [1]Physikalisches Institut, Universität Bonn, Wegelerstraße 8, D-53115 Bonn, Germany — [2]Laboratoire Kastler-Brossel, ENS/UPMC-Paris 6/CNRS, F-75005 Paris, France

We investigate the integration of fiber cavities into ion traps for use in quantum networks. Since ions typically have their strongest dipole transition in the ultraviolet (UV), the extension of fiber cavities to work in the UV is important for high bandwidth networks. We present coupling of a single Ytterbium ion to a 260 μm long fiber cavity, which is resonant with the electric dipole transition at 370 nm. We achieve a coherent coupling rate of a single ion to the cavity of about $g/2\pi = 60$ MHz, which exceeds previous realizations by more than one order of magnitude. Using the Purcell effect, we demonstrate single photon generation and efficient extraction by pulsed ion excitation. Coherent manipulation of the hyperfine qubit enables us to investigate entanglement between the photon polarization and the spin state of the ion.

Q 48.6 Thu 15:30 e001

Performance Optimization Tools for Single-Photon Quantum Key Distribution — •Timm Kupko[1], Martin v. Helversen[1], Lucas Rickert[1], Jan-Hindrik Schulze[1], André Strittmatter[1,2], Manuel Gschrey[1], Sven Rodt[1], Stephan Reitzenstein[1], and Tobias Heindel[1] — [1]Institut für Festkörperphysik, Technische Universität Berlin, 10623 Berlin, Germany — [2]Institut für Experimentelle Physik, Otto-von-Guericke Universität Magdeburg, 39106 Magdeburg, Germany

Solid-state quantum light sources have the potential to boost quantum communication [1,2]. Here, we report on tools to optimize the performance of quantum key distribution (QKD) implemented with single-photon sources (SPSs). We analyze the performance of a receiver module designed for polarization encoded QKD using deterministically-fabricated quantum dot SPSs. Exploiting two-dimensional temporal filtering and real-time security monitoring, we analyze the sifted key fraction, the quantum bit error ratio, and $g^{(2)}(0)$ expected in full implementations of the BB84 protocol as a function of the acceptance time-window. This routine enables us to choose optimal filter settings depending on the losses of the quantum channel [3]. Our findings are relevant for the development of QKD-secured communication networks based on quantum-light sources.

[1] T. Heindel et al., New J. Phys. 14, 083001 (2012)
[2] E. Waks et al., Phys. Rev. A **66**, 042315 (2002)
[3] T. Kupko et al., arXiv:1908.02672 (2019)

Q 48.7 Thu 15:45 e001

Storing single photons in a room temperature vapor cell — •Roberto Mottola[1], Gianni Buser[1], Chris Müller[2], Tim Kroh[2], Sven Ramelow[2], Oliver Benson[2], Philipp Treutlein[1], and Janik Wolters[1,3] — [1]Universität Basel, Schweiz — [2]HU Berlin — [3]DLR Institut für optische Sensorsysteme Berlin

Quantum memories are a key ingredient for the realization of quantum networks [1]. Furthermore, they allow the synchronization of probabilistic single photon sources significantly enhancing the generation rates of multiphoton states [2].

We implemented a broadband, optical quantum memory in hot Rb vapor with on-demand storage and retrieval [3]. With a bandwidth matched spontaneous parametric downconversion (SPDC) source, we can generate heralded single photons suited for storage with a heralding efficiency ≈ 50 % [4]. We report on our recent achievements in storing SPDC single photons with a linewidth of 230 MHz with an end-to-end efficiency $\eta_{e2e} = 1.3(1)$ % for a storage time of $T = 50$ ns. A signal to noise ratio of 1.9(2) and a memory lifetime $\tau = 380$ ns are achieved. The measurement of the second order autocorrelation of retrieved single photons results in $g^{(2)} = 0.91(3)$, showing that the non-classical properties of the stored light are maintained.

[1] N. Sangouard et al., *Rev. Mod. Phys.* **83**, 33 (2011).
[2] J. Nunn et al., *Phys. Rev. Lett.* **110**, 133601 (2013).
[3] J. Wolters, et al., *Phys. Rev. Lett.* **119**, 060502 (2017).
[4] R. Mottola et al., arXiv:1908.00590v2 (2019).