Workshop on Entanglement-Assisted Communication Networks

Braunschweig, Germany, September 18–20, 2024

Program and Booklet of Abstracts

Organizers:

Boulat Bash Christian Deppe Janis Nötzel Uzi Pereg

Local Organization:

Pol Julià Farré Athin Mohan Yaning Zhao Ines Richlick

ENTANGLEMENT-ASSISTED COMMUNICATION NETWORKS

On September 18–20, 2024, the Workshop on Entanglement Assisted Communication Networks (EACN) will take place at the TU Braunschweig.

EACN Workshop Website: `http://www.eacn.eu`

Topics of interest

Will quantum communication reshape classical network design? What will be the next technological breakthrough in quantum communication? This interdisciplinary workshop focusses on entanglement as a resource assisting classical communication systems. We welcome participants from academic institutions, research labs and industry. Selected approaches to entanglement-assisted communication will be presented, along with insights into the status of repeater technology, sensing, quantum networks, technical advancements in entanglement-based Quantum Key Distribution and theoretical insights.

Thanks

The organizers acknowledge funding by the DFG via grants NO 1129/2-1 and NO 1129/4-1 and the NSTC as well as by the Bundesministerium für Bildung und Forschung in the programme of “Souverän. Digital. Vernetzt.”. Joint project 6G-life, project identification numbers: 16KISK002 and 16KISK001K, and via the q-net-q project (16KISK168).

About this booklet

This booklet contains hyperlinks to help you navigate:

- Clicking the talk title in the schedule will take you to the talk abstract
- Clicking the talk date/time in the abstract will take you to the schedule
- Clicking the name of a chair will open their email address

CONTENTS

Wednesday, September 18

09:00	Fei Ding Chair: Christian Deppe	Niedersachsen Quantum Link: Towards a large-scale quantum network with deterministic quantum light sources (45’ + 15’)
10:00	*— Coffee —*	
10:30	Julian Struck Chair: Riccardo Bassoli	Satellite-Based Quantum Communication: The Long Road From Fundamental Research To Commercial Application (25’ + 5’)
11:15	Gregor Pieplow Chair: Riccardo Bassoli	Creating spin-photon entanglement with group four color centers in diamond (25’ + 5’)
12:00	Karol Łukanowski Chair: Riccardo Bassoli	DIQKD vs OKD: The many flavors of physical layer security (25’ + 5’)
12:30	*— Lunch —*	
14:00	Christian Bertoni Chair: Pau Colomer	**??**
14:30	*— Lightening talks for Posters and Demos (90 seconds) —*	
15:00	*— Coffee Break —*	
15:20	*— Group Photo —*	
15:30	*— Poster Session with BBQ(starting around 19:00) —*	

Thursday, September 19

09:00	Andreas Winter Chair: Janis Nötzel	Entanglement-Assisted Communication (45’ + 15’)
10:00	*— Coffee —*	
10:30	Meir Lederman Chair: Johannes Rosenberger	Secure Communication with Unreliable Entanglement Assistance (25’ + 5’)
11:00	Johannes Moerland Chair: Johannes Rosenberger	Bound entangled Bell diagonal states of unequal local dimensions, and their witnesses (25’ + 5’)
11:30	Arun Padakandla Chair: Johannes Rosenberger	Simulation of Separable Measurements on Distributed Bipartite States via Likelihood POVMs (25’ + 5’)
12:00	*— Lunch —*	
13:20	*— Walk from Mensa to Bus —*	
14:00	*— PTB lab Tour —*	

Friday, September 20

09:00	Moritz Wiese Chair: Hadi Aghaee	Discussion of Security Metrics & Implementation (25' + 5')
09:45	Karolin Varner Chair: Hadi Aghaee	Computational Authenticated Key Distribution - Encryption, the Old-Fashioned Way (25' + 5')
10:15	Nilesh Kumar Chair: Hadi Aghaee	Discussion on QKD (25' + 5')
10:45	*— Coffee —*	
11:15	Paul Spooren Chair: Hadi Aghaee	QKD with PQC - harder, simpler, faster, cheaper (10' + 20')
11:45	Marc Geitz Chair: Hadi Aghaee	Update on Quantum Security at Deutsche Telekom (25' + 5')
12:15	*— Lunch —*	
13:30	Ángeles Vazquez-Castro Chair: Boulat Bash	Integrating Crypto-Agility with Physical Layer Security (10' + 5')
14:00	Nilesh Kumar Chair: Boulat Bash	Quantum PUF: Unlocking Security Through Information-Theoretic Insights (25' + 5')
14:30	Dan Kilper Chair: Boulat Bash	QKD Networks in the CoQREATE Project (25' + 5')
15:00	*— Podiums Discusssion: Quantum Security (all speakers of Friday) —*	
16:00	*— Good Bye —*	

POSTERS AND DEMOS

The poster and demo session will host the following scientific posters and demos:

Low Photon Advantages in Quantum Optical Communication
Aakash Warke

Quantum Communication System with Entanglement Budget
Athin Mohan

Combined Physical and Link Layer Protocols for Quantum Networks
Benedikt Baier

The Limits of Oblivious Transfer
Hadi Aghaee

Demo: Quantum Simulator
Janis Nötzel

Comparative System Metrics for Quantum Key Distribution Networks
Jerry Horgan

Identification over quantum broadcast channels
Johannes Rosenberger

Entanglement-Assisted Communication via the Interference Channel
Jonas Hawellek

New results in Identification via Quantum Channels
Pau Colomer

Entanglement-Assisted Authenticated BB84 Protocol
Pol Julià Farré

Entanglement-assisted decision making for VNF migration in 6G Communication Networks
Shivam Maheshwari

Quantum Repeater of the Second Generation
Suraj Vishwanath

Demo: QuantumVR
Tobias Voss

“QUANTista” a board game about quantum technologies
Tobias Voss

Furthermore, posters about various research projects connected to this workshop will be presented.

TALKS

Niedersachsen Quantum Link: Towards a large-scale quantum network with deterministic quantum light sources

Fei Ding Wednesday, September 18, 09:00, 45' + 15'

Hundreds and thousands of fireflies synchronize their dazzling light on summer nights – one of nature's most beautiful demonstrations of the importance of synchronization and scalability in a network. Inspired by this, we can ask such a question: is it possible to synchronize many devices in a future quantum internet? This is an important fundamental question that emerged during the development of quantum information science in the past decades. Recently we have successfully realized the first entanglement swapping experiment with a deterministic quantum light source based on semiconductor quantum dots. It opens the possibility of connecting many devices in an entanglement-based quantum network. Now we aim to test this type of source in a real-world quantum optical network. In the short term, the idea is to demonstrate a time and frequency synchronized quantum communication link by using only one segment of the fiber network. In the middle term, the two-node link shall be extended to multipartite links by using (hybrid) quantum repeaters. Thus, large-scale multipartite entanglement can be created on this link, which forms the experimental testbeds for several exciting experiments.

[1] M. Zopf, R. Keil, Y. Chen, J. Yang, D. Chen, F. Ding and O. G. Schmidt, "Entanglement Swapping with Semiconductor-Generated Photons Violates Bell's Inequality," Phys. Rev. Lett., vol. 123, no. 16, p. 160502, 10 2019.

[2] Yang, Jingzhong, et al., "High-rate intercity quantum key distribution with a semiconductor single-photon source," Light: Science & Applications, vol. 13, no. 1, p. 150, 2024.

Creating spin-photon entanglement with group four color centers in diamond

Gregor Pieplow Wednesday, September 18, 11:15, 25' + 5'

We present a theoretical analysis of generating entangled resource states for quantum network applications using group-IV color centers in diamond, which feature an intrinsic electron spin. Creating these states necessitates the repeated application of both single and two-qubit gates on the color centers. However, even minor imperfections in these operations can lead to a significant degradation in the quality of the generated states. We offer a comprehensive analysis of single-qubit gates employed in the deterministic generation of highly entangled states, utilizing either emission-based or scattering-based approaches. Both methods leverage a solid-state spin system that is coupled to a well-confined cavity mode.

DIQKD vs OKD: The many flavors of physical layer security

Karol Łukanowski Wednesday, September 18, 12:00, 25' + 5'

Physical layer security techniques protect communication channels at the practical implementation level. On one end of the spectrum there's the paranoid device-independent paradigm of quantum cryptography, on the other - the carefree optical key distribution, not even „quantum" anymore. Which is the better approach?

Entanglement-Assisted Communication

Andreas Winter Thursday, September 19, 09:00, 45' + 15'

Survey the benefits and limitations of entanglement in communication networks of all sorts, mostly in the sense of providing an advantage on the rate(s) of transmission. The plan is to start from the basics (dense coding) and proceed to more recent and more complex examples.

Bound entangled Bell diagonal states of unequal local dimensions, and their witnesses

Johannes Moerland Thursday, September 19, 11:00, 25' + 5'

Bell diagonal states constitute a well-studied family of bipartite quantum states that arise naturally in various contexts in quantum information. We generalize the notion of Bell diagonal states to the case of unequal local dimensions and investigate their entanglement properties. To that end, we extend the family of entanglement criteria of Sarbicki et al. [Phys. Rev. A 101, 012341 (2020)] to determine suitable entanglement witnesses. We show how to optimize these witnesses for maximal noise robustness, both analytically and numerically. Finally, we construct bound entangled states that are detected by these witnesses, but not by the usual computable cross norm or realignment and de Vicente criteria.

Update on Quantum Security at Deutsche Telekom

Marc Geitz Friday, September 20, 11:45, 25' + 5'

Telecommunication providers diligently monitor the advancement of quantum technologies, encompassing quantum computing, cryptography, and sensing. This presentation provides an update of T-Labs' initiatives and technology showcases, offering practical insights into the implementation of use cases within the telecommunications industry.

QKD with PQC - harder, simpler, faster, cheaper

Paul Spooren Friday, September 20, 11:15, 10' + 20'

This presentation introduces a hybrid approach that integrates cutting-edge post-quantum cryptography (PQC) with quantum key distribution (QKD) to create a multi-layered key exchange system. This system facilitates the formation of secure tunnels for any type of application data. Built on a foundation of established tools commonly utilized in Unix operating systems, this approach minimizes the need to reinvent processes and maximizes the ability to audit security measures. Consequently, the setup effectively secures data transmission between two end nodes across multiple trusted nodes, while maintaining the security assumptions inherent in both the PQC and QKD methodologies.

Quantum PUF: Unlocking Security Through Information-Theoretic Insights

Nilesh Kumar Friday, September 20, 14:00, 25' + 5'

In this talk, we delve into the evolving landscape of Physical Unclonable Functions (PUFs) and their role in bolstering IoT security. While classical PUFs have shown promise, they face significant challenges, such as susceptibility to machine learning attacks and limited defenses against quantum threats. To overcome these issues, we explore Quantum PUFs (QPUFs), which leverage quantum mechanical principles to enhance security. This presentation provides a thorough survey of various QPUF architectures and their security features. We also discuss the information-theoretic applications of QPUFs in IoT, including secret key generation, secure storage, authentication, and identification. Our findings suggest that many classical results are effectively applicable in the quantum realm, with QPUFs offering larger capacity regions than their classical counterparts.

QKD Networks in the CoQREATE Project

Dan Kilper Friday, September 20, 14:30, 25' + 5'

CoQREATE is a US-Ireland project that brings together the Center for Quantum Networks in the US with the CONNECT Centre and QTEQ in the island of Ireland to advance research on quantum communication networks. This talk will describe recent activities in this initiative including research to progress the engineering of QKD systems into networks and the challenges this entails.

Secure Communication with Unreliable Entanglement Assistance

Meir Lederman Thursday, September 19, 10:30, 25' + 5'

Secure communication is considered with unreliable entanglement assistance, due to one of two reasons: Interception or loss. We consider two corresponding models. In the first model, Eve may intercept the entanglement resource. In the second model, Eve is passive, and the resource may dissipate to the environment beyond her reach. The operational principle of communication with unreliable entanglement assistance is to adapt the transmission rate to the availability of entanglement assistance, without resorting to feedback and repetition. We derive achievable transmission rates for both models, and a multi-letter formula for degraded channels. As an example, we consider the erasure channel and the amplitude damping channel. In the erasure channel, time division is optimal and we derive single-letter formulas for both models. In the amplitude damping channel, under interception, time division is not necessarily possible, and the boundary of our achievable region is disconnected. In the passive model, our rate region outperforms time division.

Satellite-Based Quantum Communication: The Long Road From Fundamental Research To Commercial Application

Julian Struck Wednesday, September 18, 10:30, 25' + 5'

In recent years, quantum communication and in particular quantum key distribution has significantly matured and is now transitioning from basic research to commercial application. While the focus of this transition has been on terrestrial systems and networks, the space-segment is the key to bride pan- and inter-continental long-range distances. Here, I will present a brief overview of the achievements, current state and open challenges of space borne quantum key distribution. In particular, I will discuss TESATs interest in this field, our on-going programs and collaborations with research institutes and academic partners.

Integrating Crypto-Agility with Physical Layer Security

Ángeles Vazquez-Castro Friday, September 20, 13:30, 10' + 5'

Integrating crypto-agility with physical layer security involves designing secure communication systems that leverage physical layer properties and adapt cryptographic strategies at software, hardware, or both levels. Such integration not only dynamically guards against traditional and emerging threats but also ensures adherence to evolving security standards and seamless operability across existing networks.

Computational Authenticated Key Distribution - Encryption, the Old-Fashioned Way

Karolin Varner Friday, September 20, 09:45, 25' + 5'

I am the main researcher behind Rosenpass, the only actively used post-quantum secure protocol with post-quantum authentication. Rosenpass can be used together with WireGuard and QKD to create hybrid setups, which is what my colleague Paul Spooren will focus on in a later talk. As the cryptographer of the group, I will instead attempt to lay a theoretical foundation, explaining the goals and constraints of such a system from a cryptographic perspective.

Together, we will try to get an overview of the many disciplines involved in the construction of secure cryptographic systems and discuss how many different approaches need to be used together to secure real-world systems step by step. We will explore the yardsticks by which high-quality encryption systems are measured and contrast security properties provided by computational encryption systems QKD.

I cannot hide the fact that, to many cryptographers, QKD is an inferior technology. Even fully realized, QKD boasts one security property, information theoretic secrecy, but lacks other crucial features such as authentication.

Despite this, proponents of QKD should not be discouraged: Hybrid systems can improve the security of real-world encryption right now. We will explore this and discuss how including QKD in systems of computational encryption can provide extra redundancy, even without practical information-theoretic security.

Discussion of Security Metrics & Implementation

Moritz Wiese Friday, September 20, 09:00, 25' + 5'

Simulation of Separable Measurements on Distributed Bipartite States via Likelihood POVMs

Arun Padakandla Thursday, September 19, 11:30, 25' + 5'

Discussion on QKD

Nilesh Kumar Friday, September 20, 10:15, 25' + 5'

PARTICIPANTS

Aakash Warke	*Johannes Gutenberg Universität Mainz*
Albert Rico	*Jagiellonian University*
Andreas Winter	*Universitat Autònoma de Barcelona*
Ángeles Vazquez-Castro	*Universitat Autònoma de Barcelona*
Anshul Singhal	*TU Munich*
Arun Padakandla	*Eurecom*
Athin Mohan	*TU Braunschweig*
Benedikt Baier	*TU Munich*
Chris Aaron Schneider	*Porsche Leipzig GmbH*
Christian Bertoni	*Freie Universität Berlin*
Christian Deppe	*TU Braunschweig*
Dan Kilper	*Trinity College Dublin*
Davide Li Calsi (online)	*TU Munich*
Eduard Jorswieck	*TU Braunschweig*
Fei Ding	*Leibniz University Hannover*
Florian Seitz	*TU Munich*
Gilad Gour	*University of Calgary*
Gregor Pieplow	*Humboldt University of Berlin*
Hadi Aghaee	*TU Braunschweig*
Janis Nötzel	*TU Munich*
Jerry Horgan	*Walton Institute Ireland*
JinHyeock Choi	*TU Munich*
Johannes Moerland	*Georg-August-Universität Göttingen*
Johannes Rosenberger	*TU Munich*
Jonas Hawellek	*TU Braunschweig*
Joy Halder	*TU Dresden*
Juan Cabrera (online)	*TU Dresden*
Julia Kunzelmann (online)	*Heinrich Heine University Düsseldorf*
Julian Struck	*Tesat-Spacecom*
Karol Łukanowski	*University of Warsaw*
Karolin Varner	*Max Planck Institute for Security and Privacy*
Kumar Nilesh	*TU Munich*
Linus Krieg (online)	*PTB*
Marc Geitz	*Deutsche Telekom*
Meir Lederman	*Technion - Israel Institute of Technology*
Moritz Wiese	*TU Munich*
Pau Colomer	*TU Munich*
Paul Spooren	*Hochschule Nordhausen University of Applied Sciences*
Pol Julià Farré	*TU Braunschweig*
Rafael Schaefer (online)	*TU Dresden*
Rathinamala Vijay (online)	*TU Berlin*
Riccardo Bassoli	*TU Dresden*
Roland Thomas (online)	
Shivam Maheshwari	*TU Dresden*
Stefan de Boer	
Sumit Chaudhary (online)	*TU Munich*
Suraj Vishwanath	*TU Braunschweig, IISER Mohali*
Tobias Voss	*TU Braunschweig*

Uzi Pereg *Technion - Israel Institute of Technology*
Xi Ding *TU Braunschweig*