

Workshop on Entanglement-Assisted Communication Networks

Taipei, Taiwan, June 19–23, 2023

Program and Booklet of Abstracts

Organizers:

Boulat Bash
Uzi Pereg

Christian Deppe
Stefano Rini

Ray-Kuang Lee

Janis Nötzel

Technical Support:

Jin Hyeock Choi

TC Yang

Vladlen Galetsky

Simon Sekavčnik

ENTANGLEMENT-ASSISTED COMMUNICATION NETWORKS

On June 19–23, 2023, the Workshop on Entanglement Assisted Communication Networks (EACN) will take place in Taipei, Taiwan. This event is a joint workshop of the Emmy Noether Group “Theoretical Quantum System Design” and the Institute for Communications Engineering of Technical University of Munich (Germany) together with the Institute of Communications Engineering at National Chiao Tung University (Taiwan).

EACN Workshop Website: <https://mcqst.de/news-and-events/eacn-2022/>

Topics of interest

Shared entanglement is widely acknowledged as the key enabler to future quantum information processing tasks. Yet, from a technological perspective, it has remained largely unclear how exactly one should approach the transfer from ideas and laboratory experiments to actual technology. In particular this is true for the domain of quantum communication.

To find answers to multidisciplinary questions connecting theory, experiment and network design, 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 established communication models in classical networking.

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 number: 16KISK002. We further thank the MCQST for his continuous support.

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

Entanglement-Assisted Communication Networks	1
Schedule	3
Posters	8
Talks	9
Participants	26

Monday, June 19

8:30	Welcome	Technical issues and overview of the day
9:00	Lars Zimmerman	Integrated photonics in optical link technology - implementations, efficiency, bottlenecks and future trends (30' + 10')
9:40	Kai Müller	Integrated superconducting nanowire single-photon detectors for photonic quantum technologies (15' + 25')
10:20	— <i>Coffe Break</i> —	
10:40	Friedrich Sbresny	Dynamics of Deterministic Quantum-Light Generation (15' + 25')
11:20	Shahram Dehdashti	Non-Linearity and its application in Quantum Communication and Computing (15' + 25')
12:00	Xinchen Ji	Ultra Low-loss Silicon Nitride Photonic Integrated Circuits: Fabrication and Application (15' + 25')
12:40	— <i>Lunch</i> —	
14:00	Kambidz Jamshidi	Integrated Nonlinear Photonics for Photon-Pair Generation (15' + 25')
14:40	Matteo Rosati	Learning optimal decoders for fiber communication at the quantum limit (15' + 25')
15:20	You-Chia Chang	Beam shaping and steering with integrated photonics (15' + 25')
16:00	— <i>Coffe Break</i> —	
16:20	Ming Chang Lee	Integrated Photonics Applied for Quantum Optics (15' + 25')
17:00	Yen-Hung Chen	Integrated Lithium Niobate Photonic Quantum Sources (15' + 25')
17:40	— <i>Dinner</i> —	

Tuesday, June 20

8:30	Welcome	Technical issues and overview of the day
9:00	Georg Maringer	Overview on the functionality and security of lattice and code based public key encryption schemes* (60' + 20')
10:20	— <i>Coffe Break</i> —	
10:40	Marc Geitz	Quantum Secure Communication at Deutsche Telekom (15' + 25')
11:20	Anirban Patak	Quantum key distribution and beyond: Identity authentication and direct communication using entanglement and entanglement routing (15' + 25')
12:00	Adrià Sansa Perna	Integration and implementation advances in entanglement-based QKD (15' + 25')
12:40	— <i>Lunch</i> —	
14:00	Gregor Pieplow	Generating entangled photonic resource states for quantum network applications with color centers in diamond (15' + 25')
14:40	Mina Doosti	New quantum resources for quantum communication from quantum hardware security (15' + 25')
15:20	Hao-Chung Cheng	A Simple and Tighter Derivation of Achievability for Classical Communication over Quantum Channels* (15' + 25')
16:00	— <i>Coffe Break</i> —	
16:20	Jun-Yi Wu	Distributed quantum computing with entanglement-assisted gate teleportation (15' + 25')
17:00	Gelo Noel Tabia	Zero-probability constraints to the Clauser-Horne-Shimony-Holt nonlocal game* (15' + 25')
17:40	— <i>Dinner</i> —	

Wednesday, June 21

8:30	Welcome	Technical issues and overview of the day
9:00	Saikat Guha	Quantum enhancements for classical communications (30' + 10')
9:40	Peter van Loock	Quantum repeater models and protocols including or excluding quantum memories (30' + 10')
10:20	— <i>Coffe Break</i> —	
10:40	Norbert Hanik	Ultra-Broadband Optical Wavelength-Conversion in Nonlinear Multi-Modal Silicon-On-Insulator Waveguides (15' + 25')
11:20	Ashutosh Rai	Non-Local and Quantum Advantages in Network Coding for Multiple Access Channels (15' + 25')
12:00	Jiyoung Yun	Nonlocal network coding in interference channels based on Clauser-Horne-Shimony-Holt game (15' + 25')
12:40	— <i>Lunch</i> —	
14:00	Min-Hsiu Hsieh	General Distance Balancing for Quantum Locally Testable Codes. (15' + 25')
14:40	Ying-Cheng Chen	High-performance quantum memory based on electromagnetically induced transparency (30'+10')
15:20	Ku Huan-Yu	Complete classification of steerability under local filters and its relation with measurement incompatibility (30'+10')
16:00	— <i>Coffe Break</i> —	
16:20	Wang-Yau Cheng	Cs-Rb mixed-atoms for femtosecond Ti:S comb laser stabilitzation* (15' + 25')
17:00	Chih-Sung Chuu	Towards Entanglement Distribution in a Quantum Network (30'+10')
17:40	— <i>Dinner</i> —	

Thursday, June 22

9:00 — *Dragon Boat Celebration* —

12:40 — *Excursion: National Palace Museum* —

17:00 — *Banquet: Grand Hotel Taipei* —

Friday, June 23

- 8:30 — *Transportation to Hai Quantum Computing Research Center* —
- 9:30 Welcome Technical issues and overview of the day
- 9:40 Nithin Raveendran Exploiting Analog Information In Decoding Quantum Error Correction Codes (15' + 25')
- 10:20 — *Coffe Break* —
- 10:40 Raymond Ooi Maxwell's Demon, Information and Extracting Work from Heat (35' + 5')
- 11:20 Johannes Rosenberg Identification Over Quantum Broadcast Channels (15' + 25')
- 12:00 Pau Saus Decoupling by local random unitaries without simultaneous smoothing, and applications to multi-user quantum information tasks (35' + 5')
- 12:40 — *Lunch* —
- 14:00 Christoph Hirche Benefits and Detriments of Noise in Quantum Classification (35' + 5')
- 14:40 Filip Rozpędek All-photonic multiplexed quantum repeaters based on concatenated bosonic and discrete-variable quantum codes (15' + 25')
- 15:20 Roberto Ferrara Key Assistance, Key Agreement, and Layered Secrecy for Bosonic Broadcast Channels (15' + 25')
- 16:00 — *Coffe Break* —
- 16:20 Marco Tomamichel Entanglement monogamy via multivariate trace inequalities (15' + 25')
- 17:00 — *Travelling back to the Hotel* —
- 18:00 — *Dinner* —

POSTERS

The poster session will host the following scientific posters:

Entanglement-Assisted Covert Communication via Qubit Depolarizing Channels

Elaykim Zlotnick

Nonlocal network coding in interference channels based on the Clauser-Horne-Shimony-Holt game

Joonwoo Bae

Multipartite repeater networks with multiplexing

Julia Alina Kunzelmann

Quantum-Assisted Machine Learning for Image Processing

Kartike Pushkarna

Optimal probe states for single-mode quantum target detection

Pin Ju Tsai

Long-Distance Time-frequency Entanglement Distribution via Fiber Network

Sheng-Hung Wang

Quantum Network Simulation and Quantum Communication Protocols

Simon Sekavcnik

Polarization and phase-encoded quantum key distribution (QKD) protocols

Sumit Chaudhary

Generation and manipulation of photon pairs by a four-stage integrated optical circuit

Tien-Dat Pham

Joint Detection Receiver

Zuhra Amiri

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

TALKS

Integration and implementation advances in entanglement-based QKD <i>Adrià Sansa Perna</i>	(15' + 25')	11
Quantum key distribution and beyond: Identity authentication and direct communication using entanglement and entanglement routing <i>Anirban Pathak</i>	(15' + 25')	11
Non-Local and Quantum Advantages in Network Coding for Multiple Access Channels <i>Ashutosh Rai</i>	(15' + 25')	12
Towards Entanglement Distribution in a Quantum Network <i>Chih-Sung Chuu</i>	(30'+10')	12
Benefits and Detriments of Noise in Quantum Classification <i>Christoph Hirche</i>	(35' + 5')	12
All-photonic multiplexed quantum repeaters based on concatenated bosonic and discrete-variable quantum codes <i>Filip Rozpędek</i>	(15' + 25')	13
Dynamics of Deterministic Quantum-Light Generation <i>Friedrich Sbresny</i>	(15'+ 25)	13
Zero-probability constraints to the Clauser-Horne-Shimony-Holt nonlocal game* <i>Gelo Noel Tabia</i>	(15' + 25')	14
Overview on the functionality and security of lattice and code based public key encryption schemes* <i>Georg Maringer</i>	(60' + 20')	14
Generating entangled photonic resource states for quantum network applications with color centers in diamond <i>Gregor Pieplow</i>	(15' + 25')	15
A Simple and Tighter Derivation of Achievability for Classical Communication over Quantum Channels* <i>Hao-Chung Cheng</i>	(15' + 25')	15
Nonlocal network coding in interference channels based on Clauser-Horne-Shimony-Holt game <i>Jiyoung Yun</i>	(15' + 25')	16
Identification Over Quantum Broadcast Channels <i>Johannes Rosenberger</i>	(15' + 25')	16
Distributed quantum computing with entanglement-assisted gate teleportation <i>Jun-Yi Wu</i>	(15' + 25')	16
Integrated superconducting nanowire single-photon detectors for photonic quantum technologies <i>Kai Müller</i>	(15' + 25')	17
Integrated Nonlinear Photonics for Photon-Pair Generation <i>Kambiz Jamshidi</i>	(15' + 25')	17
Complete classification of steerability under local filters and its relation with measurement incompatibility <i>Ku Huan-Yu</i>	(30'+10')	18
Integrated photonics in optical link technology - implementations, efficiency, bottlenecks and future trends <i>Lars Zimmermann</i>	(30' + 10')	18
Quantum Secure Communication at Deutsche Telekom <i>Marc Geitz</i>	(15' + 25')	18
Entanglement monogamy via multivariate trace inequalities <i>Marco Tomamichel</i>	(15' + 25')	19
Learning optimal decoders for fiber communication at the quantum limit <i>Matteo Rosati</i>	(15' + 25')	19
New quantum resources for quantum communication from quantum hardware security <i>Mina Doosti</i>	(15' + 25')	19

Integrated Photonics Applied for Quantum Optics <i>Ming Chang Lee</i>	(15' + 25')	20
General Distance Balancing for Quantum Locally Testable Codes. <i>Min-Hsiu Hsieh</i>	(15' + 25')	20
Exploiting Analog Information In Decoding Quantum Error Correction Codes <i>Nithin Raveendran</i>	(15' + 25')	21
Ultra-Broadband Optical Wavelength-Conversion in Nonlinear Multi-Modal Silicon-On-Insulator Waveguides 22 <i>Norbert Hanik</i>	(15' + 25')	22
Decoupling by local random unitaries without simultaneous smoothing, and applications to multi-user quantum information tasks <i>Pau Saus</i>	(35' + 5')	22
Quantum repeater models and protocols including or excluding quantum memories <i>Peter van Loock</i>	(30' + 10')	22
Maxwell's Demon, Information and Extracting Work from Heat <i>Raymond Ooi</i>	(35' + 5')	22
Key Assistance, Key Agreement, and Layered Secrecy for Bosonic Broadcast Channels <i>Roberto Ferrara</i>	(15' + 25')	23
Quantum enhancements for classical communications <i>Saikat Guha</i>	(30' + 10')	23
Non-Linearity and its application in Quantum Communication and Computing <i>Shahram Dehdashti</i>	(15' + 25')	23
Cs-Rb mixed-atoms for femtosecond Ti:S comb laser stabilization* <i>Wang-Yau Cheng</i>	(15' + 25')	24
Ultra Low-loss Silicon Nitride Photonic Integrated Circuits: Fabrication and Application <i>Xinchen Ji</i>	(15' + 25')	24
Integrated Lithium Niobate Photonic Quantum Sources <i>Yen-Hung Chen</i>	(15' + 25')	24
High-performance quantum memory based on electromagnetically induced transparency <i>Ying-Cheng Chen</i>	(30'+10')	25
Beam shaping and steering with integrated photonics <i>You-Chia Chang</i>	(15' + 25')	25

Integration and implementation advances in entanglement-based QKD

Adrià Sansa Perna

Tuesday, June 20, 12:00, 15' + 25'

Since the foundation of our company in 2020, our vision was to create a fully automatized, entanglement-based QKD system. This year we present the development of our products, including entangled photon sources, receivers and protocol, which are miniaturized, automated with polarization compensation modules and plug-and-play based on Si- and InGaAs SPADs or nanowire detectors for high efficiencies. The QKD systems at 800 nm and the hybrid 800/1550 nm systems are different from the rest of commercially available QKD systems in that they are based on the polarization entanglement of single photons, and thus constitute a further step towards the integration with quantum memories and quantum repeaters and a future quantum internet. We report on the miniaturization of the polarization entangled photon source (EPS) for use in space using a photonics micro-assembly machine. The EPS is highly integrated, having a footprint of 80x128x26 mm and is capable of generating up to 800 bps secure key rate using photons at 810 nm. The current parameters of the EPS are reported as well as long-term measurements and the variability between different produced EPSs. Future iterations to optimize the performance of the source for use on QKD, especially focused on the increase of the produced photon pairs per second, which is currently the bottleneck for the key rate are explored. We also present our plans for integration of the polarization analysis modules using the micro-assembly machine. In both cases, the miniaturization brings better performance as well as stability to the system. Finally, we report on the whole envisioned architecture of the system involving networks in which a single EPS is sharing keys to several different parties. To complete the protocol, the security of the system is proven by a general security proof for our particular polarization-entanglement QKD implementation, showing the resistance against the most general coherent attacks.

Quantum key distribution and beyond: Identity authentication and direct communication using entanglement and entanglement routing

Anirban Pathak

Tuesday, June 20, 11:20, 15' + 25'

Applications of entangled states will be described in the context of quantum key distribution, quantum secure direct communications, quantum dialogue, etc. with specific attention to the schemes for quantum identity authentication. Specifically, in the commercial quantum key distribution system, classical identity authentication schemes are used, but it's possible to modify the existing schemes for secure quantum communication to design new protocols for quantum identity authentication. Entangled state-based identity authentication schemes will be described. Further, the relevance of entanglement routing for the realization of quantum internet and distributed quantum algorithms will be briefly described, and a generalized algorithm for multipartite entanglement routing over a grid network will be presented. Majority of the talk will be based on Refs. [1-4].

- [1] R. Van Meter and S. J. Devitt, "The Path to Scalable Distributed Quantum Computing," *Computer*, vol. 49, pp. 31-42, 2016.
- [2] Entanglement Routing and Bottlenecks in Grid Networks, V. Mannalath and A. Pathak, arXiv: 2211.12535.
- [3] Multiparty Entanglement Routing in Quantum Networks, V. Mannalath and A. Pathak, arXiv: 2211.06690.
- [4] Controlled secure direct quantum communication inspired scheme for quantum identity authentication, A. Dutta and A. Pathak, *Quant. Infor. Proc.* 22 (2023) 13.
- [5] A short review on quantum identity authentication protocols: How would Bob know that he is talking with Alice? A. Dutta and A. Pathak, *Quant. Infor. Proc.* 21 (2022) 369.

Non-Local and Quantum Advantages in Network Coding for Multiple Access Channels

Ashutosh Rai

Wednesday, June 21, 11:20, 15' + 25'

Devising efficient communication in a network consisting of multiple transmitters and receivers is a problem of immense importance in communication theory. Interestingly, resources in the quantum world have been shown to be very effective in enhancing the performance of communication networks. In this work, we study entanglement-assisted communication over classical network channels. We consider multiple access channels, an essential building block for many complex networks, and develop an extensive framework for n -senders and 1-receiver multiple access channels based on nonlocal games. We obtain generic results for computing correlation assisted sum-capacities of these channels. The considered channels introduce less noise on winning and more noise on losing the game, and the correlation assistance is classified as local (L), quantum (Q), or no-signaling (NS). Furthermore, we consider a broad class of multiple access channels such as depolarizing ones that admix a uniform noise with some probability and prove general results on their sum-capacities. Finally, we apply our analysis to three specific depolarizing multiple access channels based on Clauser-Horne-Shimony-Holt, magic square, and Mermin-GHZ nonlocal games. In all three cases we find significant enhancements in sum-capacities on using nonlocal correlations. We obtain either exact expressions for sum-capacities or suitable upper and lower bounds on them

Towards Entanglement Distribution in a Quantum Network

Chih-Sung Chuu

Wednesday, June 21, 17:00, 30' + 10'

Entanglement distribution allows novel technologies such as the entanglement-based quantum key distribution, distributed quantum computing, and longer-baseline telescopes. As a key step towards the entanglement distribution in the quantum network recently set up in Taiwan, we demonstrated the Hong-Ou-Mandel interference between independent single photons heralded from two types of continuous-wave narrowband biphoton source located in two laboratories. By exploiting the long coherence time of the biphotons, we also observed the entanglement swapping by the time measurements.

Benefits and Detriments of Noise in Quantum Classification

Christoph Hirche

Friday, June 23, 14:00, 35' + 5' Classification

of data is a fundamental task in machine learning. While high accuracy is generally the main goal in classification, also other properties, such as good robustness, are often required. Intuitively, adding noise may sound like a questionable idea whenever one aims for high accuracy, but it was also shown that, in the classical case, it can lead to provable robustness guarantees at a manageable cost. In particular, adding any differentially private preprocessing can give such results. This approach has subsequently also been transferred to quantum classification, i.e. the task of classifying quantum states. Here, the depolarizing channel, as an ϵ -differentially private channel, was shown to give provable robustness guarantees. In this work, we revisit the question by significantly extending the previous results and also by discussing their limitations. Concretely, we give robustness bounds in terms of the Hockey-Stick divergence and Renyi divergences. These imply robustness against several types of adversarial noise and give rise to robustness guarantees when applying general (ϵ, δ) -differentially private or (ϵ, α) -Renyi differentially private noise. We then discuss the particular case of depolarizing noise and show that the robustness guarantees that can be given provide generally no improvement over the noiseless setting. However, such noise can still be used to improve the robustness of particular data subsets, which we call targeted smoothing. Additionally we discuss robust encoding of classical data. Finally, we discuss the effect of noise on the training process. In particular, we show that stable channels, a special case of differential privacy, show good generalization properties.

All-photonic multiplexed quantum repeaters based on concatenated bosonic and discrete-variable quantum codes

Filip Rozpedek

Friday, June 23, 14:40, 15' + 25'

Long distance quantum communication will require the use of quantum repeaters to overcome the exponential attenuation of signal with distance. One class of such repeaters utilizes quantum error correction to overcome losses in the communication channel. Here we propose a novel strategy of using the bosonic Gottesman-Kitaev-Preskill (GKP) code in a two-way repeater architecture with multiplexing. The crucial feature of the GKP code that we make use of is the fact that GKP qubits easily admit deterministic two-qubit gates, hence allowing for multiplexing without the need for generating large cluster states as required in previous all-photonic architectures based on discrete variable codes. Moreover, alleviating the need for such clique-clusters entails that we are no longer limited to extraction of at most one end-to-end entangled pair from a single protocol run. In fact, thanks to the availability of the analog information generated during the measurements of the GKP qubits, we can design better entanglement swapping procedures in which we connect links based on their estimated quality. This enables us to use all the multiplexed links so that large number of links from a single protocol run can contribute to the generation of the end-to-end entanglement. We find that our architecture allows for high-rate end-to-end entanglement generation and is resilient to imperfections arising from finite squeezing in the GKP state preparation and homodyne detection inefficiency. In particular we show that long-distance quantum communication over more than 1000 km is possible even with less than 13 dB of GKP squeezing. We also quantify the number of GKP qubits needed for the implementation of our scheme and find that for good hardware parameters our scheme requires around 103 - 104 GKP qubits per repeater per protocol run.

This work is available on arxiv at arXiv:2303.14923

Dynamics of Deterministic Quantum-Light Generation

Friedrich Sbresny

Monday, June 19, 10:40, 15' + 25'

For real-world implementations of quantum communication networks deterministic quantum light sources are a pivotal building block. Semiconductor quantum dots are one of the most promising material platforms for this task. This stems from their excellent optical properties, such as almost-exclusive emission into the zero-phonon line, near transform-limited linewidth, high emission rates and their integrability into nanophotonic structures. A level scheme of particular interest for quantum light generation is the biexciton-exciton cascade, which originates from two excited electron-hole pairs in the lowest energy levels of the quantum dot. The subsequent relaxation of each electron-hole pair results in the emission of a single photon where both individual photons carry a different photon energy and thus are separable. Due to the spin selection rules, the biexciton can decay via two independent branches, which form a quantum four-level system, where the emitted photon pair is polarization entangled [1]. One advantage of employing this level scheme for the generation of single photons or entangled photon pairs is that the ground state biexciton state can be directly excited via a virtual state, that is spectrally detuned from the optical transitions of interest. It has been shown that while the photons generated by this excitation scheme have excellent single-photon purity [2,3], their indistinguishability is intrinsically limited by the timing jitter of the cascaded decay [4]. Removing this timing jitter e.g. via the stimulation of the biexciton-exciton decay employing a second precisely timed laser pulse results in a restoration of the indistinguishability while simultaneously inheriting the ultra-low multiphoton error of the biexciton cascade [5]. Exploring the intrinsic physical limitations of photons emitted by such a four-level system in combination with the limitations induced by the excitation method is of fundamental interest to enable the development of deterministic quantum light sources

- [1] O. Benson et al. Phys. Rev. Lett. 84, 2513 (2000).
- [2] L. Schweickert et al. Appl. Phys. Lett. 112, 093106 (2018).
- [3] L. Hanschke et al. npj Quantum Inf. 4, 43 (2018)
- [4] E. Schöll et al. Phys. Rev. Lett. 125, 233605 (2020)
- [5] F. Sbresny, L. Hanschke et al. Phys. Rev. Lett. 128, 093603 (2022)

Zero-probability constraints to the Clauser-Horne-Shimony-Holt nonlocal game*

Gelo Noel Tabia

Tuesday, June 20, 17:00, 15' + 25'

The security of virtually all cryptographic protocols relies on the ability to produce randomness that is unknown to external parties. Device-independent randomness generation is based on the observation that the violation of a Bell inequality can be used to certify that the outputs of a nonlocal game are truly random, even without trusting the devices employed. In this talk, we will consider local randomness expansion protocols, where local refers to the notion that the extracted bits are random even with respect to the other participants of the nonlocal game. We illustrate that by adding zero-probability constraints to the Clauser-Horne-Shimony-Holt (CHSH) nonlocal game, one can significantly improve the extractable rate of local randomness in both the asymptotic and finite-size regimes. The corresponding modified local randomness expansion protocols are based on the existence of nonlocal quantum correlations with a few vanishing joint conditional probabilities. Using the generalized entropy accumulation theorem and some refinement of the bound on its second-order correction terms, we show that a local randomness of up to 0.9 bit per round can be achieved asymptotically with one of the modified protocols, compared to the maximum of 0.55 bit achievable with a protocol based on the standard CHSH game. We also demonstrate that the results exhibit some tolerance to experimental noise, that is, they remain valid even when we allow small deviations for the zero-probability constraints.

Overview on the functionality and security of lattice and code based public key encryption schemes*

Georg Maringer

Tuesday, June 20, 9:00, 60' + 20'

In 1994 Shor introduced an algorithm that efficiently solves the integer factorization problem as well as the discrete logarithm problem on a quantum computer. Meanwhile the security of currently deployed asymmetric cryptography (public key encryption and digital signatures) is mostly still based on the hardness of these two problems. Therefore, in 2016 the NIST announced a standardization competition in order to find viable solutions to replace the currently used cryptosystems with alternatives based on mathematical problems that are conjectured to be hard even if the attacker is granted access to a large scale quantum computer. Schemes that fulfill this kind of security are referred to as being post-quantum secure. Two prominent problem classes that meet those requirements are lattice based and code based constructions. This talk shall give an overview on the functionality and security of both classes using Kyber and McEliece as examples for lattice and code based public key encryption schemes, respectively. Furthermore, we give an overview on post-quantum secure digital signatures and introduce the notion of fully homomorphic encryption which enables to perform computations on an external server without giving the server access to any plaintext information.

Generating entangled photonic resource states for quantum network applications with color centers in diamond

Gregor Pieplow

Tuesday, June 20, 14:00, 15' + 25'

Two key quantum technologies, measurement-based quantum computing [1] and one-way quantum repeaters [2], require the generation of highly entangled photonic states such as Greenberger-Horne-Zeilinger (GHZ) states or cluster states. To enable fault tolerant quantum computations, GHZ states and linear cluster states can be used to build up larger photonic cluster states by performing fusion operations using Bell-state-measurements (BSMs) [3]. In particular, GHZ states can be used to improve on the 50% success rate of a BSM with linear optical elements.

In this work, we theoretically analyze aspects of entangled resource state generation for quantum network applications using group-IV color centers in diamond that contain an intrinsic electron spin. Generation of these states requires the repeated application of single and two-qubit gates on the color center. However, even small imperfections in these operations can significantly degrade the state's quality, which diminishes exponentially as the state size increases. We provide a detailed analysis of single-qubit gates used for the deterministic generation of highly entangled states through emission [4] or scattering-based schemes [5]. Both schemes utilize a solid-state spin system coupled to a well-confined cavity mode. The central focus of our work is a coherent control scheme based on an all-optical off-resonant Raman scheme. For implementing single-qubit gates, this scheme employs two laser pulses that couple non-degenerate spin states with an excited state. By operating in the off-resonant regime, only a minimal population is transferred to the excited states. Minimizing the population of the excited state during the control sequence helps reduce dephasing of the spin qubit caused by optical relaxation processes. Importantly, this control scheme enables ultrafast gates of tens of picoseconds, in contrast to microwave control limited to tens of nanoseconds. The rapid subsequent emission of multiple coherent entangled photons is particularly valuable when considering photon loss in optical elements like waveguides and fibers used as delay lines, optical phase gates, or for guiding and confining a mode for detection. Our work also investigates the role of the magnetic field in spin gate design, optimizing the spin gates in the presence of a magnetic field and highlighting the importance of field orientation for moderate magnetic field strengths up to 1 T. Additionally, we introduce an original quality measure for GHZ states and cluster states, emphasizing the significance of ultrafast and high-fidelity control techniques in producing large time-bin entangled photonic qubit states with a solid-state emitter.

[1] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* 86, 5188–5191 (2001).

[2] J. Borregaard, H. Pichler, T. Schroder, M. D. Lukin, P. Lodahl, and A. S. Sørensen, *Phys. Rev. X* 10, 021071 (2020).

[3] Srikrishna Omkar, Seok-Hyung Lee, Yong Siah Teo, Seung-Woo Lee, and Hyunseok Jeong, *PRX Quantum*, 3, 030309 (2022).

[4] J. P. Lee, B. Villa, et al., *Quantum Sci. Technol.* 4, 025011 (2019).

[5] Yu Shi and Edo Waks, *Phys. Rev. A*, 104 1, 013703 (2021).

A Simple and Tighter Derivation of Achievability for Classical Communication over Quantum Channels*

Hao-Chung Cheng

Tuesday, June 20, 15:20, 15' + 25'

In this talk, we will first introduce the concept of the one-shot channel capacity of transmitting classical information over quantum channels with entanglement assistance. Second, we will show that using the position-based encoding with the pretty-good measurements as decoding can achieve the state-of-the-art one-shot entanglement-assisted classical capacity. Lastly, we will discuss the potential open problems. This talk is based on arXiv:2208.02132.

Nonlocal network coding in interference channels based on Clauser-Horne-Shimony-Holt game

Jiyoung Yun

Wednesday, June 21, 12:00, 15' + 25'

In this work, we consider two-sender and two-receiver interference channels where noise occurs via a non-local game: a malicious third party introduces two distinct channels depending on whether messages by senders win the game, such as the Clauser-Horne-Shimony-Holt (CHSH) game, or not. We show that network coding realized by quantum correlations can achieve a higher channel capacity over classical ones. Namely, a hierarchy in channel sum-capacities according to non-signaling, quantum, and local resources is presented. We also discuss optimal encoding strategies with quantum resources.

Identification Over Quantum Broadcast Channels

Johannes Rosenberger

Friday, June 23, 11:20, 15' + 25'

The talk will present results on identification of classical messages over quantum broadcast channels. As opposed to the information transmission task, where the messages should be exactly reproduced after a channel, the receiver only identifies whether a message of his choice was sent or not. This relaxation allows for a code size that is double-exponential in the number of channel uses. We derive an achievable identification rate region for a quantum broadcast channel, and a full characterization for the class of classical-quantum broadcast channels. As a consequence, we obtain the identification capacity region of the single-mode pure-loss bosonic broadcast channel. In contrast to the single-user case, the capacity region for identification can be significantly larger than for transmission. We demonstrate that for the quantum erasure broadcast channel and the pure-loss bosonic broadcast channel, the achievable identification rate region is even rectangular.

Distributed quantum computing with entanglement-assisted gate teleportation

Jun-Yi Wu

Tuesday, June 20, 16:20, 15' + 25'

In noisy intermediate-scale (NIS) quantum computing, the scalability of a quantum processor unit (QPU) is limited by the connectivity of qubits. The connectivity of qubits in a QPU is intrinsically limited by the topology of a physical system. One can extend the connectivity of a local QPU by distributed quantum computing (DQC), in which one can harness the connectivity of a quantum internet to implement entanglement-assisted local operations and classical communication (LOCC). Teleportation and EJPP protocol [Eisert et.al., PRA, 62:052317, (2000)] are two types of entanglement-assisted LOCCs that can be employed for DQC. The EJPP protocol is optimum for control-unitary gates, but not for general circuits. To make DQC feasible in experiments, we need a more entanglement-efficient protocol. To this end, we introduce a notion of embedding and develop an entanglement-efficient DQC protocol based on "distributing enhanced by embedding". We show that the structure of distributability and embeddability of a circuit can be represented by two types of graphs, namely the packing graphs and conflict graphs. Based on these graphs, we derive heuristic algorithms for finding an entanglement-efficient packing of distributing processes. These algorithms can determine the required entanglement cost and the number of local ancillary qubits in the DQC. One can also set an upper limit on the local ancillary qubits with these algorithms. We apply these algorithms for bipartite DQC of UCC circuits and find a significant entanglement reduction through embeddings. This method can be employed to determine a constructive upper bound on entanglement cost for a circuit that approaches its lower bound.

Integrated superconducting nanowire single-photon detectors for photonic quantum technologies

Kai Müller

Monday, June 19, 9:40, 15' + 25'

Quantum technologies are enabled by the principles of superposition and entanglement and rely on the ability to prepare, manipulate and read-out quantum states. For photonic quantum technologies, such as quantum communication or photonic quantum computation, the ability to detect single photons and read out quantum states encoded e.g. in their polarization, time bins or number basis is a key ingredient. Therefore, in recent years, there has been tremendous progress in the development of highly efficient single-photon detectors and their implementation in demonstrator experiments. Among all possible single-photon detection technologies superconducting nanowire single photon detectors (SNSPDs) are particularly promising for photonic quantum technologies, as they simultaneously enable near-unity detection efficiencies, low timing jitter, low dark counts and low dead times (high count rates). Moreover, their integration into photonic circuits allows for on-chip quantum state analysis and on-chip quantum information processing, with promising potential for fast feed-forward operation. In this talk, we will review their fundamental working principle, the engineering of highly performant detectors, and their integration into photonic integrated circuits and quantum devices [1-5]. Moreover, we will discuss their application in quantum communication and photonic quantum computing.

- [1] G. Raithmaier Nano letters 15 (8), 5208-5213 (2015)
- [2] F. Flassig et al., Quantum Sensing and Nano Electronics and Photonics XVIII, 120090F (2022)
- [3] J.R. Flaschmann et al., Nanoscale 15, 1086-1091 (2022)
- [4] S. Majety et al., Mater. Quantum. Technol. 3, 015004 (2023)
- [5] J.R. Flaschmann et al., under review at Mater. Quantum. Technol. (2023)
- [6] S. Strothauer et al. in submission (2023).

Integrated Nonlinear Photonics for Photon-Pair Generation

Kambiz Jamshidi

Monday, June 19, 14:00, 15' + 25'

In this paper, we will review our recent research in the field of integrated nonlinear photonics to generate photon pairs. Two platforms are considered in this regard based on silicon and silicon nitride materials. We will investigate the conditions for dual pump parametric amplification in silicon nitride for photon pair generation [1]. In addition, electric field-induced second harmonic generation in silicon will also be discussed for this purpose [2, 3].

- [1] He, Menglong, and Kambiz Jamshidi. "Conditions for Dual-pumped Optical Parametric Oscillation in Silicon Nitride Ring Cavities." 2022 IEEE Photonics Conference (IPC). IEEE, 2022.
- [2] Heydari, David, et al. "Degenerate optical parametric amplification in CMOS silicon." Optica 10.4 (2023): 430-437.
- [3] Heydari, David, et al. "Second-order nonlinear optics in CMOS silicon." 2022 Conference on Lasers and Electro-Optics (CLEO). IEEE, 2022.

Complete classification of steerability under local filters and its relation with measurement incompatibility

Ku Huan-Yu

Wednesday, June 21, 15:20, 30' + 10'

Quantum steering is a central resource for one-sided device-independent quantum information. It is manipulated via one-way local operations and classical communication, such as local filtering on the trusted party. In this talk, I will show a necessary and sufficient condition for a steering assemblage to be transformable into another via local filtering. We characterize the equivalence classes with respect to filters in terms of the steering equivalent observables (SEO), first proposed to connect the problem of steerability and measurement incompatibility. We provide an efficient method to compute the extractable steerability that is maximal via local filters and show that it coincides with the incompatibility of the SEO. Moreover, we show that there always exists a bipartite state that provides an assemblage with steerability equal to the incompatibility of the measurements on the untrusted party.

Integrated photonics in optical link technology - implementations, efficiency, bottlenecks and future trends

Lars Zimmermann

Monday, June 19, 9:00, 30' + 10'

Optical link technology is of high relevance for data transport in various network domains. Fiber optical communication is the pre-dominant optical link technology, covering core or transport networks, networks in datacenters and for super-computers, optical access, and support of wireless networks. Central to optical networks are optical subsystems for transmission and switching. These subsystems rely more and more on photonic integration, photonic integrated circuits (PICs) and photonic-electronic integration. The advance of such subsystems is closely related to the development of high-speed optical communication chip sets that are deployed in opto-electronic transceivers. Transceivers are core-enablers of optical point-to-point networks, comprising in one module optical transmit and receive functions and electric interfaces for high-speed digital data. Currently, data center applications are a major driver of photonic integrated circuit technology. State-of-the-art datacenter transceivers provide data rates of 800Gbps and beyond. The progress of transceiver technology has been enabling for the setup of large scale data-centers, but the ability to continue past capacity growth is crucial to meet future demands in big data processing. There are two main semiconductor technologies for integrated photonics, III-V and silicon photonics. Both technology families are used for the manufacturing of photonic integrated circuits. III-V material based platforms inherit the superior opto-electronic properties that made these materials very successful in discrete photonic device applications. Silicon integrated circuit technology on the other hand, matured over more than 50 years and is an established basis for rapid development cycles common in microelectronics industry. Major advantages of silicon photonics are therefore related to meeting the need of scalable fabrication. Starting from the prerequisite that future trends will rely on integrated photonics implementations, especially on silicon, the talk will attempt to identify bottlenecks in optical link technology that might require entirely new approaches such as entanglement-assisted communication

Quantum Secure Communication at Deutsche Telekom

Marc Geitz

Tuesday, June 20, 10:40, 15' + 25'

Telecommunication providers, being major disseminators of quantum secure communication technologies, closely observe the technology development of Quantum Key Distribution, Post-Quantum Cryptography and Physical Layer Encoding. This talk gives an overview about quantum secure technology from the customer's point of view and presents technology demonstrators set up by T-Labs, the applied research and development organization of Deutsche Telekom, to obtain hands-on experience.

Entanglement monogamy via multivariate trace inequalities

Marco Tomamichel

Friday, June 23, 16:20, 15' + 25'

Entropy is a fundamental concept in quantum information theory that allows to quantify entanglement and investigate its properties, for example, its monogamy over multipartite systems. Here, we derive variational formulas for relative entropies based on restricted measurements of multipartite quantum systems. By combining these with multivariate matrix trace inequalities, we recover and sometimes strengthen various existing entanglement monogamy inequalities. In particular, we give direct, matrix-analysis-based proofs for the faithfulness of squashed entanglement by relating it to the relative entropy of entanglement measured with one-way local operations and classical communication, as well as for the faithfulness of conditional entanglement of mutual information by relating it to the separably measured relative entropy of entanglement. We discuss variations of these results using the relative entropy to states with positive partial transpose, and multipartite setups. Our results simplify and generalize the previous derivations in the literature that employed operational arguments about the asymptotic achievability of information-theoretic tasks.

Learning optimal decoders for fiber communication at the quantum limit

Matteo Rosati

Monday, June 19, 14:40, 15' + 25'

We introduce a set of methods to optimize bosonic circuits comprising Gaussian operations and photodetection with the aim of minimizing the average error probability in recovering a message encoded in coherent states of the field. We apply our methods to perform a comprehensive study of optimal decoders for various families of codes: random, linear and polar. We find circuit setups that offer up to a 3-fold enhancement in the success probability with respect to the optimal single-mode decoder and less than 7% away from the optimal decoder, which is not known to be implementable with this class of circuits to date.

New quantum resources for quantum communication from quantum hardware security

Mina Doosti

Tuesday, June 20, 14:40, 15' + 25' Quantum hardware security is a

growing field that offers novel solutions for quantum protocols and subroutines, leveraging the unique properties of quantum and classical devices to unlock new functionalities. Quantum Physical Unclonable Functions (QPUFs) are a prime example, relying on the physical properties of quantum systems to create unclonable hardware tokens that have many existing and potential applications in quantum cryptography and distributed quantum computing. This talk will introduce new resources from the quantum hardware security field that offer a range of applications for quantum communication infrastructure, specifically, protocols for quantum-secure authentication and identification based on quantum and hybrid hardware designs that can be implemented with existing quantum technology. These protocols combine hardware security and quantum communication, providing strong security guarantees and demonstrating useful properties achievable only with quantum communication. Furthermore, we discuss the potential future applications of these new quantum resources for distributed quantum computing.

Integrated Photonics Applied for Quantum Optics

Ming Chang Lee

Monday, June 19, 16:20, 15' + 25'

Integrated optoelectronics and photonics are the key technology platform for developing large-scale optical systems for various optical applications. For example, multi-channel integrated transceivers based on Si photonics are recently demonstrated for over 800 Gbps data transmission aiming at data centers, high-performance cluster computers, and cloud servers. Meanwhile, these technologies are also exploited for implementing large-scale quantum photonics circuits. Several key players of quantum optics companies, like PsiQuantum and Xanadu, are developing their owned integrated quantum photonic chips by leveraging advanced CMOS technologies. In this talk, I will introduce a new integrated photonic platform and show the opportunities and challenges in the applications of quantum optics

General Distance Balancing for Quantum Locally Testable Codes.

Min-Hsiu Hsieh

Wednesday, June 21, 14:00, 15' + 25'

In this paper [arXiv:2305.00689], we prove a lower bound on the soundness of quantum locally testable codes under the distance balancing construction of Evra et al. arXiv:2004.07935 [quant-ph]. Our technical contribution is that the new soundness of the quantum code is at least the old soundness divided by the classical code length (up to a constant factor). This allows us to use any classical code with independent checks when distance balancing, where previously only the repetition code had been considered for qLTCs. By using a good classical LDPC code, we are able to grow the dimension of the hypersphere product codes arXiv:1608.05089 [quant-ph] and the hemicubic codes arXiv:1911.03069 [quant-ph] while maintaining their distance and locality, but at the expense of soundness. From this, and also by distance balancing a chain complex of Cross et al. arXiv:2209.11405 [cs.IT], we obtain quantum locally testable codes of new parameters.

Exploiting Analog Information In Decoding Quantum Error Correction Codes

Nithin Raveendran

Friday, June 23, 9:40, 15' + 25'

Quantum error correction (QEC) has recently been shown to benefit greatly from specific physical encodings of the code qubits as well as characteristics of the noise and their biases. Unlike classical error correction where we have access to the channel information, QEC relies on stabilizer measurements to obtain a syndrome that enables us to decode by identifying the most probable error that could have occurred (given the details of the noise model). However, since all components of a quantum processor are unreliable, so are the stabilizer measurements. This leads to the realistic scenario of a noisy syndrome which could potentially confuse the decoder and mislead it toward an incorrect error pattern. In this talk, We will discuss two scenarios wherein analog/soft information can aid in this strategic decoding process. The first scenario is in a code concatenation setting where the decoder for an outer code can appropriately leverage the analog information from the inner error correction code to improve decoding performance [1]. The case we use is wherein the individual code qubits are encoded with the continuous variable Gottesman-Kitaev Preskill (GKP) code and then encoded into an outer discrete-variable code such as a generic quantum low-density parity-check (QLDPC) code. In this work, we demonstrate a natural way to exploit the GKP analog information in iterative decoding algorithms. While traditional iterative decoders typically suffer from a flooring effect in the logical error rate curves in the low noise regime, we show that the GKP analog information seems to significantly lower the error floor or potentially eliminate it completely. The other scenario is where we explore the soft information in the syndromes [2] to consider the noisy ancilla cases as well. For this, we need a decoder that can naturally exploit soft syndromes. Several research groups have investigated repeating syndrome measurements for topological codes in order to overcome this noisy syndrome issue. However, this leads to additional latency and complexity in the decoder. The idea of single-shot decoding is to devise a decoder for a given code such that even with one round of noisy measurements it can correct errors very well. We will discuss a modified iterative decoder that performs almost as well as the standard decoder with noiseless syndromes. The key idea is to introduce “virtual variable nodes” of degree 1 at each check node in the Tanner graph of the stabilizer code; these input the noisy syndrome to the check node. While many works in the literature simply assume that the noisy syndrome is the ideal binary syndrome with an additional probabilistic flip, we consider a more realistic model of the ideal binary syndrome being corrupted by a continuous-valued additive white Gaussian noise, i.e., a soft syndrome. Since several hardware platforms can produce much more information at the output of measurements, this model for the noisy syndrome is widely applicable. The key modification is that, during the check node update of the modified min-sum decoder, we also update the syndrome by sending an update to the virtual variable node. By identifying a suitable threshold value for the reliability of messages, we determine when it is better to rely on the inputs from other variables rather than the soft syndrome itself. Since the syndrome itself is noisy, the stopping criterion of an iterative decoder in the presence of measurement errors is ambiguous. Even in the presence of noisy syndrome, the ‘Soft Syndrome’ decoder is able to correct the syndrome and data errors quickly to converge to the true error pattern. Hence, under a reasonable amount of syndrome noise, besides avoiding repeated syndrome measurements and single-shot property, the modified MSA also does not suffer from a penalty in decoding latency. We also implemented the ‘Soft Syndrome’ decoder on FPGA device with the appropriate hardware optimizations to keep latency and complexity almost minimal. Developing fast and scalable decoders is of strategic importance and we must exploit every bit of ‘soft’ information into such novel algorithms.

- [1] N. Raveendran, N. Rengaswamy, F. Rozpedek, A. Raina, L. Jiang, and B. Vasic, “Finite rate QLDPC-GKP coding scheme that ϵ surpasses the CSS Hamming bound,” *Quantum*, vol. 6, p. 767, Jul. 2022. [Online]. Available: <https://arxiv.org/abs/2111.07029>
- [2] N. Raveendran, N. Rengaswamy, A. K. Pradhan, and B. Vasic, “Soft syndrome decoding of quantum LDPC codes to correct of data ϵ and syndrome errors,” in *IEEE Intl. Conf. on Quantum Computing and Engineering*, Sep. 2022

Ultra-Broadband Optical Wavelength-Conversion in Nonlinear Multi-Modal Silicon-On-Insulator Waveguides

Norbert Hanik

Wednesday, June 21, 10:40, 15' + 25'

Ultra-Broadband Wavelength Conversion is identified as one of the key issues in future high capacity, flexible optical networks. In this contribution, methods to optimize the design of Multi-Modal high-nonlinear SOI-Waveguides to achieve broadband wavelength conversion between dedicated optical wavelength-bands are presented. Finally, numerical optimization examples and experimental results are discussed that prove ultra-broadband conversion of data signals between different λ -bands

Decoupling by local random unitaries without simultaneous smoothing, and applications to multi-user quantum information tasks

Pau Saus

Friday, June 23, 12:00, 35' + 5' We show

that a simple telescoping sum trick, together with the triangle inequality and a tensorisation property of expected-contractive coefficients of random channels, allow us to achieve general simultaneous decoupling for multiple users via local actions. Employing both old [Dupuis et al. Commun. Math. Phys. 328:251-284 (2014)] and new methods [Dupuis, arXiv:2105.05342], we obtain bounds on the expected deviation from ideal decoupling either in the one-shot setting in terms of smooth min-entropies, or the finite block length setting in terms of Rényi entropies. These bounds are essentially optimal without the need to address the simultaneous smoothing conjecture, which remains unresolved. This leads to one-shot, finite block length, and asymptotic achievability results for several tasks in quantum Shannon theory, including local randomness extraction of multiple parties, multi-party assisted entanglement concentration, multi-party quantum state merging, and quantum coding for the quantum multiple access channel. Because of the one-shot nature of our protocols, we obtain achievability results without the need for time-sharing, which at the same time leads to easy proofs of the asymptotic coding theorems. We show that our one-shot decoupling bounds furthermore yield achievable rates (so far only conjectured) for multi-user randomness extraction, multipartite state merging and quantum multiple access channel communication in compound settings, that is for only partially known i.i.d. source or channel.

Quantum repeater models and protocols including or excluding quantum memories

Peter van Loock

Wednesday, June 21, 9:40, 30' + 10'

First, we give an overview of our efforts to model fiber-based, memory-based quantum repeaters for long-range quantum key distribution or more general quantum network applications. Under given experimental assumptions such as the possibility of probabilistic or deterministic entanglement swapping we calculate and optimize the final (secret key) rates for medium-size repeaters including the most important experimental parameters. In the second part, we discuss memory-free and potentially all-photon approaches based on bosonic quantum error correction codes

Maxwell's Demon, Information and Extracting Work from Heat

Raymond Ooi

Friday, June 23, 10:40, 35' + 5'

In this tutorial, I will discuss the concept of Maxwell-demon involving Szilard's engine, and the use of Stern–Gerlach apparatus in quantum heat engines. I hope to provide a convincing explanation of the quantum effects and clarify the demon conundrum, which includes some pioneering works of Bennett, Scully, and others. I will explain why the demon cannot violate the second law, which would involve a discussion on quantum information, entropy, and memory. This may also connect to the impact on the environment.

Key Assistance, Key Agreement, and Layered Secrecy for Bosonic Broadcast Channels

Roberto Ferrara

Friday, June 23, 15:20, 15' + 25'

Secret-sharing building blocks based on quantum broadcast communication are studied. The confidential capacity region of the pure-loss bosonic broadcast channel is determined, both with and without key assistance, and an achievable region is established for the lossy bosonic broadcast channel. If the main receiver has a transmissivity of $\eta < \frac{1}{2}$, then confidentiality solely relies on the key-assisted encryption of the one-time pad. We also address conference key agreement for the distillation of two keys, a public key and a secret key. A regularized formula is derived for the key-agreement capacity region in finite dimensions. In the bosonic case, the key-agreement region is included within the capacity region of the corresponding broadcast channel with confidential messages. We then consider a network with layered secrecy, where three users with different security ranks communicate over the same broadcast network. We derive an achievable layered-secrecy region for a pure-loss bosonic channel that is formed by the concatenation of two beam splitters.

Quantum enhancements for classical communications

Saikat Guha

Wednesday, June 21, 9:00, 30' + 10'

In the regime of very low received photon flux and low thermal noise, e.g., for deep-space laser communications, quantum processing within the receiver could enhance the reliable communications rate, and significantly reduce the peak transmit power requirements compared with conventional lasercom schemes for this regime, which uses a pulse position modulation format paired with a single photon detection receiver. In another regime of very low transmit photon flux and high thermal noise, e.g., for low probability of detect radio-frequency communications, pre-shared entanglement between the transmitter and the receiver would enable higher communications rate compared with what would be possible without pre-shared entanglement as an added resource. In this talk, I will give an overview of these two genres of quantum enhancements in classical communications for point-to-point communication channels, discussing information theoretic limits of such enhancements as well as hardware considerations and challenges associated with realizing such quantum benefit. I will also allude to some known results and open problems for multi-user networked communications scenarios.

Non-Linearity and its application in Quantum Communication and Computing

Shahram Dehdashti

Monday, June 19, 11:20, 15' + 25'

We investigate the impact of the Kerr effect and its influence on quantum states in various scenarios, particularly in quantum communication utilizing optical fibers. By employing a deformed bosonic dephasing channel, we effectively model the consequences of a Kerr medium on quantum systems. Surprisingly, we discover that the Kerr nonlinearity can counteract the dephasing in certain situations. Furthermore, our analysis demonstrates that, for specific nonlinearity parameters, the quantum capacity of the deformed bosonic dephasing channel surpasses that of the conventional, undeformed channel. Additionally, we introduce the concept of deformed cat qubits associated with the Kerr Hamiltonian. Our findings indicate that the deformed cat qubits exhibit increased resilience to dephasing and loss compared to normal cat qubits, during a recovery channel. Moreover, we explore the application of Kerr coherent states in the feature space for a quantum support vector machine. Remarkably, our results reveal that introducing nonlinearity in the feature space enhances the algorithm's performance

Cs-Rb mixed-atoms for femtosecond Ti:S comb laser stabilization*

Wang-Yau Cheng

Wednesday, June 21, 16:20, 15' + 25'

A 6-cm glass cell with Cs-Rb mixed-atoms was used to stabilize a femtosecond Ti:S comb laser. The systematic errors and absolute frequencies will be presented in my talk. Moreover, a fiber-laser based comb clock is now under construction, which will be significant to the field of "space-borne frequency comb metrology.

Ultra Low-loss Silicon Nitride Photonic Integrated Circuits: Fabrication and Application

Xinchen Ji

Monday, June 19, 12:00, 15' + 25'

As an emerging material, silicon nitride has attracted extensive interest due to its ability to achieve ultra-low loss while maintaining small footprints. It has been widely used in fields such as biophotonics, telecommunications, sensing, quantum optics, and nonlinear optics. Here, we will discuss the fabrication method and the application of ultra-low loss silicon nitride photonic integrated circuits.

Integrated Lithium Niobate Photonic Quantum Sources

Yen-Hung Chen

Monday, June 19, 17:00, 15' + 25'

The generation, manipulation, and encoding of the information carriers such as entangled photon pairs or single photons lies at the heart of the technology for implementing practical photonic quantum sources. In this talk, I will present our recent studies on the development of quantum light sources using the integrated lithium niobate (LN) photonic circuit technology, including a novel four-stage integrated optical circuit based on a periodically poled LN (PPLN) waveguide. Besides, we also demonstrate a time-frequency entanglement distribution over a 2.64-km fiber network deployed in NCU campus based on a PPLN SPDC source. Demonstrated results show the sources are of great potential for applications in quantum information processing and communications.

High-performance quantum memory based on electromagnetically induced transparency

Ying-Cheng Chen

Wednesday, June 21, 14:40, 30' +10'

We report our advancement on the development of high-performance quantum memory (QM) based on electromagnetically induced transparency (EIT) during the past few years. Using optically dense cold atomic media, we have achieved EIT optical memory with a record-high efficiency of 92 % [1]. By increasing the intensity of the control field, we also extend the bandwidth of EIT memory to 31 MHz with an efficiency of larger than 50 %, limited by the available control power [2]. We also report the application of EIT memory to photonic polarization (or frequency) converter [3]. To realize the quantum storage, we developed a bright heralded single-photon source based on cavity-enhanced spontaneous parametric downconversion that can be locked to atomic transition [4]. We interface this solid-state photon source with the atomic memories by demonstrating the quantum storage and manipulation of heralded single photons [5]. In addition, we encode the polarization qubits into the single photons and realize the EIT-based quantum memory of polarization qubits with an efficiency of larger than 70% and a fidelity of larger than 96% [6].

- [1] Y-F Hsiao, P-J Tsai, H-S Chen, S-X Lin, C-C Hung, C-H Lee, Y-H Chen, Y-F Chen, I. A. Yu*, and Y-C Chen*, “Highly efficient coherent optical memory based on electromagnetically induced transparency”, *Phys. Rev. Lett.* 120, 183602 (2018).
- [2] Y-C Wei, Y.-F. Hsiao, B.-H. Wu, P.-J. Tsai, and Y.-C. Chen*, “Broadband coherent optical memory based on electromagnetically induced transparency”, *Phys. Rev. A* 102, 063720 (2020).
- [3] Y.-C. Wei, S.-X. Lin, P.-J. Tsai, and Y.-C. Chen*, “Memory-based optical polarization conversion in a double- Λ atomic system with degenerate Zeeman states”, *Scientific Reports*, 10:13990 (2020).
- [4] P-J Tsai, and Y-C Chen*, “Ultrabright, narrow-band photon-pair source for atomic quantum memory”, *Quant Sci. and Techno.*, 3, 034005 (2018).
- [5] P.-J. Tsai, Y.-F. Hsiao, and Y.-C. Chen*, “Quantum storage and manipulation of heralded single photons in atomic memories based on electromagnetically induced transparency”, *Phys. Rev. Research*, 2, 033155 (2020).
- [6] Y.-C. Tseng, Y.-C. Wei and Y.-C. Chen*, “Efficient quantum memory for heralded single photons generated by cavity-enhanced spontaneous parametric down-conversion”, *Opt. Express*, 30, 19944 (2022).

Beam shaping and steering with integrated photonics

You-Chia Chang

Monday, June 19, 15:20, 15' + 25'

Integrated photonics has recently expanded its applications to delivering free-space emissions for detecting or manipulating external objects. Light needs to emit from an integrated photonic chip to the free space with specific spatial modes and different directions. In this talk, I will present two integrated photonic platforms to manipulate free-space beams. In the first platform, we integrate metasurfaces monolithically on silicon photonic integrated circuits. We demonstrate experimentally diffraction-limited beam focusing with a Strehl ratio of 0.82 and holographic projection of an image above the silicon photonic chip. In the second platform, we report an optical phased array for active beam steering and focusing. We demonstrate a 10 Gbit/s free-space optical communication system in which the beam is actively steered by the optical phased array.

PARTICIPANTS

Adrià Sansa Perna	<i>Quantum Optics Jena GmbH</i>
Akshay Walkoli	<i>Institute of Photonics Technologies (NTHU)</i>
Alonso Eduardo Viladomat Jasso	<i>Technical University of Munich (TUM)</i>
Anandu Kalleri Madhu	<i>National Tsing Hua University</i>
Anirban Pathak	<i>JiIT</i>
Anshul Singhal	<i>TUM</i>
Ashutosh Rai	<i>KAIST</i>
Boulat Bash	<i>University of Arizona</i>
Bulzan George Andrei	<i>University of Bucharest</i>
Carlo Daniel	
Chien-Ming Wu	<i>National Tsing Hua University</i>
Chung-Yu Hsu	
Christian Hirche	<i>TUM and NUS</i>
Christian Deppe	<i>TUM</i>
Davide Li Calsi	<i>TUM</i>
Dorina Ismaili	<i>TUM</i>
Elyakim Zlotnick	<i>Technion</i>
Filip Rozpedek	<i>University of Massachusetts Amherst</i>
Friedrich Sbresny	<i>Technical University of Munich</i>
Georg Maringer	<i>Technical University of Munich</i>
Gelo Noel Tabia	<i>National Center for Theoretical Sciences</i>
Gregor Pieplow	<i>Humboldt Universität zu Berlin</i>
Huali Chen	<i>National Tsing Hua University</i>
Hsien Yi Hsieh	<i>National Taiwan Tsing Hua University</i>
Ian George	<i>University of Illinois at Urbana-Champaign</i>
Janis Nötzel	<i>TUM</i>
Jiyoung Yun	<i>KAIST</i>
JinHyeock Choi	<i>Technische Universität München</i>
Johannes Rosenberger	<i>Technical University of Munich</i>
Joonwoo Bae	<i>KAIST</i>
Julia Alina Kunzelmann	<i>HHU Düsseldorf</i>
Kai Müller	<i>Technical University of Munich</i>
Kai-Yu Lin	
Kambiz Jamshidi	<i>TU Dresden</i>
Kareem El-Safty	<i>TUM</i>
Kiran Adhikari	<i>Technical University of Munich</i>
Lars Zimmermann	<i>TU Berlin / IHP</i>
Marc Geitz	<i>Deutsche Telekom / T-Labs</i>
Marco Tomamichel	<i>National University of Singapore</i>
Maryam Naeem	<i>TUM employer</i>
Matheus Ribeiro Sena	<i>Deutsche Telekom AG</i>
Matteo Rosati	<i>Università Roma Tre</i>
Neel Kanth Kundu	<i>University of Melbourne</i>
Nithin Raveendran	<i>The University of Arizona</i>
Norbert Hanik	<i>TU München</i>
Pau Colomer	<i>TUM</i>
Paul Kohl	<i>Technische Universität München</i>
Ping-Yen Hsieh	<i>National Yang Ming Chiao Tung University</i>
Pin Ju Tsai	<i>National Central University</i>

Riccardo Bassoli	<i>TU Dresden</i>
Roberto Ferrara	<i>TUM LNT</i>
Rohit P Thampy	<i>Defence Institute Of Advaced Technology</i>
Saikat Guha	<i>University of Arizona</i>
Seif Mostafa	<i>Alexandria University</i>
Shabnam Sodagari	<i>CSU</i>
Shahram Dehdashti	<i>TUM</i>
Sheng-Hung Wang	<i>National Central University</i>
Simon Sekavčnik	<i>Technical University Munich</i>
Stefano Rini	<i>NYCU</i>
Stephen DiAdamo	<i>Cisco</i>
Sumit Chaudhary	<i>Indian Institute of Technology Delhi</i>
Tien-Dat Pham	<i>National Central University</i>
Tzuchin Yang	<i>National Tsing Hua University</i>
Uzi Pereg	<i>Technion</i>
Yan-Cheng Shih	<i>National Central University</i>
Yingjian Wang	<i>TU Dresden</i>
Yi-Ru Chen	
You-Chia Chang	<i>National Yang Ming Chiao Tung University</i>
Zi-Hao Shi	
Zuhra Amiri	<i>TUM</i>