QCRYPT 2023

13TH ANNUAL INTERNATIONAL CONFERENCE ON QUANTUM CRYPTOGRAPHY

August 14-18, 2023
College Park, Maryland

2023.qcrypt.net

WELCOME

Dear conference attendees,

Welcome to QCrypt 2023, the 13th International Conference on Quantum Cryptography. We are glad you are here and look forward to the innovative ideas and topics we will explore as a community. And what a community it is. This year's conference has more than 220 attendees from 28 countries.

Quantum cryptography is an excellent example of the power and promise of quantum information science. From its humble beginnings, this specialized scientific field has grown to encompass a wide range of topics, including the foundations of cryptography and quantum mechanics; atomic, molecular and optical physics; the engineering of quantum memories and quantum networks; and practical schemes for secure communication in a world with quantum computers.

The QCrypt conference is designed to encourage this mixing of disciplines. We find this relevant because quantum cryptography is itself a product of theoretical insight combined with experimental implementation.

This year's conference is the result of many people's efforts. At the organizational level, QCrypt 2023 is being hosted by the Joint Center for Quantum Information and Computer Science (QuICS) at the University of Maryland, and the National Institute of Standards and Technology (NIST).

We would also like to thank the QCrypt steering committee, the QCrypt program committee, our local organizers at QuICS and NIST, staff at the University of Maryland Institute for Advanced Computer Studies (UMIACS), staff at the University of Maryland Conference & Visitor Services, the assistance and cooperation of the University of Maryland Department of Computer Science, and our many external sponsors for their assistance in supporting this conference.

These collective contributions were essential to the success of this event. We hope you enjoy the conference!

Sincerely,

Oliver Slattery
General Chair, NIST

Gorjan Alagic
General Chair, University of Maryland and NIST

A sheep is the official mascot for QCrypt conferences—a nod to Dolly (the first successfully cloned animal) and the no-cloning theorem in quantum mechanics.

QCRYPT 2023 COMMITTEES

Steering Committee

Serge Fehr, *steering committee chair*
CWI Cryptology group, Leiden University

Gorjan Alagic
University of Maryland

Rotem Arnon-Friedman
Weizmann Institute of Science

Kai-Min Chung
IIS, Academia Sinica

Qian Li
University of Toronto

Marco Lucamarini
University of York

Christoph Marquardt
Max Planck Institute for the Science of Light

Feihu Xu
University of Science and Technology of China

Program Committee Chairs

Christian Schaffner
University of Amsterdam, QuSoft
PC primary chair (theory)

Giuseppe Vallone
University of Padova
PC co-chair (experiment)

Program Committee Members

James Bartusek (UC Berkeley, US)

Mario Berta (RWTH Aachen University, DE)

Anne Broadbent (University of Ottawa, CAN)

Ivo Pietro Degiovanni
(INRIM and EURAMET EMN-Q, IT)

Eleni Diamanti (CNRS and Sorbonne Université, FR)

Frederic Dupuis (Université de Montréal, CA)

Tobias Gehring (Technical University of Denmark, DK)

Christian Kurtsiefer
(National University of Singapore, SG)

Paul Kwiat (University of Illinois Urbana-Champaign, US)

Alexander Ling (National University of Singapore, SG)

Charles Lim (JPMorgan Chase & Co., US/SG)

Yang Liu (Jinan Institute of Quantum Technology, CN)

Giulio Malavolta (Max Planck Institute for Security and Privacy, DE)

Carl Miller (NIST and University of Maryland, US)

Isaac Nape (University of the Witwatersrand, SA)

Stefano Pironio (Université libre de Bruxelles, BE)

Valerio Pruneri (ICFO and ICREA, ES)

Davide Rusca (University of Vigo, ES)

Or Sattath (Ben-Gurion University, IL)

Fang Song (Portland State University, US)

Florian Speelman (University of Amsterdam, QuSoft, NL)

Marco Tomamichel
(National University of Singapore, SG)

Dominique Unruh (University of Tartu, EE)

Vladyslav Usenko (Palacky University Olomouc, CZ)

Takashi Yamakawa
(NTT Social Informatics Laboratories, JP)

Zhiliang Yuan (Beijing Academy of Quantum Information Sciences, CN)

Zheshen Zhang (University of Michigan, US)

Advisory Committee

Charles H. Bennett (IBM Research)

Gilles Brassard (Université de Montréal)

Ivan Damgård (Aarhus University)

Artur Ekert (CQT Singapore and Oxford University)

Nicolas Gisin (Université de Genève)

Richard Hughes (Unaffiliated)

Michele Mosca (IQC, University of Waterloo)

Jian-Wei Pan (University of Science and Technology of China)

Additional Organizational Support

From NIST

Nijil Lal

Lijun Ma

From the University of Maryland

Chen Bai

Mel Coles

Danielle Degrandchamp

Kelly Hedgepeth

Maria Herd

Lisa Press

Manasi Mangesh Shingane

Andrea Svejda

Tom Ventsias

CONFERENCE OVERVIEW

To see the latest updates on all conference activities, go to the conference website at

2023.qcrypt.net

All conference talks, poster sessions and extracurricular activities are listed on the website.

Highlights during the week include:

Monday, August 14 at 6 p.m.

OPENING DAY RECEPTION

with welcome remarks by
University of Maryland President Darryll J. Pines
and NIST Associate Director for Laboratory Programs Charles H. Romine.

LOCATION: Outdoor cantilever overhang next to Antonov Auditorium
(in the event of rain this event will be held in the Iribe Center lobby)

Tuesday, August 15 at 7 p.m.

QCrypt CONFERENCE SIT-DOWN DINNER

LOCATION: Stamp Student Union

Tuesday 15 at 6 p.m.

PUBLIC DISCUSSION

"QKD and PQC: A Public Discussion"

Ray Perlner (NIST)

Scott Fluhrer (Cisco)

Ramona Wolf (ETH Zürich)

Norbert Lütkenhaus (University of Waterloo)

LOCATION: Antonov Auditorium

Thursday, August 17 at 9 a.m.

INDUSTRY PANEL

Corey McClelland, chief revenue officer at ubitekk

Jean-Sébastien Pegon, head of sales for Quantum-Safe Security, Western Europe and the Americas region at ID Quantique

Katsuyuki Hanai, senior manager at Toshiba Digital Solutions Corporation

Lily Chen, mathematician and manager of the Cryptographic Technology Group at the National Institute of Standards and Technology

LOCATION: Antonov Auditorium

QCrypt SPONSORS

QCrypt thanks all its sponsors and industry exhibitors for their support and participation.

GOLD

SILVER

COMMUNITY

Conference Venue

This year's conference is being held in the **Brendan Iribe Center for Computer Science and Engineering,** a stunning 215,000 square foot state-of-the-art facility that encourages research, collaboration and innovation.

The Iribe Center is home to the Department of Computer Science, one of the nation's largest computer science programs with more than 3,600 undergraduates currently enrolled. It also houses the University of Maryland Institute for Advanced Computer Studies, a research and innovation powerhouse that has more than 80 faculty and 200 Ph.D. students from 15 departments across the University of Maryland Campus.

"Pseudorandom Quantum States"
by Henry Yuen, Columbia University

Monday, August 14
9–10:15 a.m.

I will give a tutorial on the rapidly developing topic of quantum pseudorandomness, in particular pseudorandom quantum states. These are states that are efficiently generatable but cannot be efficiently distinguished from Haar-random states. I will discuss their motivation, constructions, and applications to cryptography and beyond.

BIO: Henry Yuen is an assistant professor of computer science at Columbia University. His research focuses on the interplay between quantum computing, complexity theory, cryptography, and information theory. Yuen received his Ph.D. in computer science at MIT in 2016. He is a recipient of an NSF CAREER award and a Sloan Fellowship.

"Recent Advancement in Measurement-Device-Independent Quantum Key Distribution"
by Xiongfeng Ma, Tsinghua University

Tuesday, August 15
9–10:15 a.m.

Quantum key distribution can establish information-theoretically secure keys based on quantum physics. There are two main issues in practice—implementation security and system performance. The proposal of the measurement-device-independent scheme primarily enhances the former. The latter is characterized by the dependence of the key rate on the channel transmittance, R(η). In this tutorial, I shall review the security proofs of various measurement-device-independent schemes. I shall emphasize the recent developments, such as twin-field and mode-pairing schemes, that achieve the quadratic key-rate improvement.

BIO: Xiongfeng Ma received his Ph.D. from the University of Toronto in 2008. In 2012, he joined Tsinghua University. Ma is currently an associate professor and holds a Changjiang Scholarship. His main research interest lies in quantum information science, particularly in quantum cryptography, quantum computing and quantum foundation. According to the Scientometric Assessment of Global Publications from 1992 to 2019, Ma was one of the most productive researchers worldwide in quantum cryptography by ResearchGate.

"Cryptography with Certified Deletion"
by James Bartusek, UC, Berkeley

Wednesday, August 16
9–10:15 a.m.

The ability to certifiably delete plaintext data is an emerging cryptographic application of quantum information. This tutorial will focus on the notion of everlasting security, which considers the following experiment. Initially, a computationally-bounded adversary receives a computationally-hiding commitment to some plaintext. Later, they issue a (classical) certificate attesting that they destroyed the underlying plaintext information via an irreversible measurement. If the certificate is found to be valid, it is guaranteed that the plaintext is now information-theoretically removed from the adversary's view. That is, they cannot recover the plaintext even if they become computationally unbounded or receive the secret key that allows them to open the original commitment.

BIO: James Bartusek is a Ph.D. candidate at UC Berkeley, where he is advised by Sanjam Garg. He is broadly interested in cryptography, with a focus on its interface with quantum information. Previously, he obtained a BSE and MSE at Princeton University, where he was advised by Mark Zhandry.

"From the Hardness of Detecting Superpositions to Cryptography: Quantum Public Key Encryption and Commitments"

by Minki Hhan, Korean Institute for Advanced Study

Monday, August 14
10:15–11 a.m.

Recently, Scott Aaronson, Yosi Atia, and Leonard Susskind (arXiv:2009.07450) showed that detecting interference between two orthogonal states is as hard as swapping these states. While their original motivation was from quantum gravity, we show its applications in quantum cryptography: the first public-key encryption scheme from cryptographic non-abelian group actions, and a simple and efficient compiler between the computational-hiding statistical-binding and the statistical-hiding computational-binding commitment.

BIO: Minki Hhan is a researcher at the Quantum Universe Center at Korean Institute for Advanced Study. He received his Ph.D. in mathematics from Seoul National University in 2022. Hhan has wide interests in quantum cryptography and its connection to computational complexity theory and classical cryptography.

"Quantum Cryptography in Algorithmica"

by William Kretschmer, UT Austin

Monday, August 14
11:30 a.m.–12:15 p.m.

In this talk, I will discuss the construction of a classical oracle relative to which P = NP yet single-copy secure pseudorandom quantum states exist. In the language of Impagliazzo's five worlds, this is a construction of pseudorandom states in "Algorithmica," and hence shows that in a black-box setting, quantum cryptography based on pseudorandom states is possible even if one-way functions do not exist. As a consequence, we demonstrate that there exists a property of a cryptographic hash function that simultaneously (1) suffices to construct pseudorandom quantum states, (2) holds for a random oracle, and thus plausibly holds for existing hash functions like SHA3, and (3) is independent of the P vs. NP question in the black box setting. This offers further evidence that one-way functions are not necessary for computationally-secure quantum cryptography. Our proof builds on recent work of Aaronson, Ingram, and Kretschmer (2022). Based on joint work with Luowen Qian, Makrand Sinha, and Avishay Tal.

BIO: William Kretschmer is a Ph.D. candidate in computer science at UT Austin, where he is advised by Scott Aaronson. He is broadly interested in quantum complexity theory, including query complexity, structural complexity, pseudorandom quantum states, learning theory, and the stabilizer formalism. In Fall 2023, Kretschmer will start a postdoc at the Simons Institute.

"Free-space Photonic Quantum Memory for Networking"

by Nathan Arnold, University of Illinois Urbana-Champaign

Tuesday, August 15
10:15–11 a.m.

Photonic quantum memories will play an essential role in many quantum information protocols, particularly for the synchronization of repeater nodes. Most photonic memories operate by storing the photon in matter-based systems, but those approaches have limitations, e.g., they are inherently narrow bandwidth and for only particular wavelengths, often require costly cryogenic overhead, and typically have low retrieval efficiency into single-mode fiber. In this work, we develop a free-space room-temperature photonic quantum memory, allowing us to avoid the aforementioned drawbacks.

BIO: Nathan Arnold is a physics Ph.D. student at the University of Illinois Urbana-Champaign, where he has worked under Professor Paul Kwiat on developing novel quantum memory technologies for various applications in quantum networking.

"High-speed QKD: Removing the Roadblocks for an Integration and Utilization in Real-World Networks"

by Rebecka Sax, University of Geneva

Tuesday, August 15
11:30 a.m.–12:15 p.m.

The attention towards Quantum Key Distribution (QKD) as means of secure communication is expanding more than ever. However, in order to widely deploy such systems in real-world telecommunications networks, a few more obstacles have to be surpassed. A couple of these were tackled in our group via the usage of the 3-state BB84 time-bin protocol with 1-decoy state. One challenge involves increasing the rate of secret key production. We will discuss how we managed to achieve one of the highest secret key rates by using a multipixel superconducting nanowire single-photon detector, as well as high-speed electronics and fast post-processing. Another obstacle for real-world deployment of QKD regards the merging of classical and quantum channels (CC and QC, respectively) into one single fiber-optic cable. This is highly motivated due to the high costs of fiber deployment, thus the usage of existing fibers is deeply engaging. The challenge of the implementation resides in the noise that appears due to the strong CC with respect to the single-photon-level QC. We will present a case study that was done in our group using the QC at 1310 nm and the CC at 1550 nm. Finally, we will also present the implementation of the used protocol into a more practical setup with integrated photonics. Effectively, the non-practicality of fiber-based, complex QKD setups is another issue. By integrating the QKD setup, we can simplify the implementation and allow for low-cost mass-production.

BIO: After completing her master's degree in the Department of Nuclear and Corpuscular Physics at the University of Geneva in 2019, Rebecka Sax joined Hugo Zbinden's research group at the same university in the Department of Applied Physics. Her work is mainly focused on the field of quantum key distribution (QKD), where she has collaborated on projects involving the combination of classical and quantum channels in the same fiber optic cable (through wavelength division multiplexing) and the improvement in the rate of secret key production. Sax's group now works mainly on the implementation of a QKD system using photonic integrated circuits. Recently, their employment for usage with quantum random number generations has also become a primary interest.

"Constructive Post-Quantum Reductions"

by Yael Tauman Kalai, Microsoft Research New England and MIT

Wednesday, August 16
10:15–11 a.m.

In this talk I will discuss when we can "lift" classical reductions to post-quantum ones in a constructive manner. It is customary to argue that while this is problematic in the interactive setting, non-interactive reductions immediately carry over to the post-quantum setting. In this talk I will focus on the non-interactive setting and describe technical issues that arise, related to quantum auxiliary inputs. I will show how (and when) we can overcome these issues, and successfully lift a reduction to the post-quantum setting in a constructive manner. Specifically, I will show that any non-interactive non-adaptive reduction from problems with a polynomial solution space (such as decision problems) can be made post-quantum in a constructive manner. In contrast, I will show that for problems with super-polynomial solution space (such as general search problems) this cannot be done in general.

BIO: Yael Tauman Kalai is a senior principal researcher at Microsoft Research New England and an adjunct professor at the Massachusetts Institute of Technology (MIT). She received a Ph.D. in computer science from MIT. Kalai's honors include an Outstanding Master's Thesis Prize (Weizmann Institute of Science, 2001), the George M. Sprowls Award for Best Doctoral Thesis in Computer Science (MIT, 2007). She is the recipient of the 2022 ACM Prize in Computing and is a Fellow of the International Association for Cryptologic Research (IACR). Additionally, Kalai gave an invited talk at the International Congress of Mathematics (ICM, 2018).

"Long Distance Quantum Key Distribution Gets Simpler"

by Lai Zhou, Beijing Academy of Quantum Information Sciences

Wednesday, August 16
11:30 a.m.–12:15 p.m.

Quantum cryptography promises secure communication between two distant users. However, secure key rate of point-point quantum key distribution (QKD) is bounded by the linear rate-loss limit. Twin-field (TF) QKD can break this limit, but its implementation requires global phase tracking and usually also cumbersome interferometric implementations, which are often impractical for network deployment. We remove the above shortcomings with two different solutions. In the first solution, we introduce locally generated frequency combs to stabilize an open channel and develop a simple and versatile TF-QKD setup that does not need service fibre. In the second, we implement a simple measurement device independent (MDI) QKD with post-measurement pairing technique. We demonstrate the capability of asynchronous MDI-QKD (also named mode-pairing MDI-QKD) overcoming the linear rate-loss limit without global phase tracking.

BIO: Lai Zhou is an associate research scientist at Beijing Academy of Quantum Information Sciences (BAQIS). He received his Ph.D. from Tsinghua University in 2018. Zhou was a postdoctoral research assistant in quantum communication with the University of Oxford from 2019–2020. He joined BAQIS in 2020.

Zhou's current research is focused on the long-distance quantum key distribution and the quantum networking. He developed the handheld quantum key distribution system (2019), developed a simple and versatile TF-QKD setup without the optical frequency dissemination (2023), and demonstrate the asynchronous MDI-QKD overcoming the linear rate-loss limit without global phase tracking (2023). Zhou was funded by the Youth Science Foundation Project from the National Natural Science Foundation of China in 2021.

"Satellite-Based Quantum Key Distribution Network"

by Sheng-Kai Liao, University of Science and Technology of China

Thursday, August 17
11:30 a.m.–12:15 p.m.

Quantum key distribution (QKD) can share random bits between two separated parties called Alice and Bob; Alice uses the bits to encrypt a message with a one-time-pad way and deliver it to Bob in a public channel; Bob decrypts it to get the original message; quantum mechanics and Shannon information theory guarantee the security. Since the first protocol was proposed in 1984, many experiments have been demonstrated in both fiber and free space channels with key rates and distances growing up. With long distance in a vacuum, satellite-to-ground channel has much less attenuation than fiber in the same distance of several hundred kilometers; satellite-based QKD becomes the most feasible way to construct the global QKD network. In this talk, we will present the demonstration and results of the satellite-to-ground QKD experiment and QKD network experiment with Micius satellite, Tiangong II space lab, and Jinan-1 satellite and give the outlook of the next generation of satellite-based QKD.

BIO: Sheng-Kai Liao is a professor at the University of Science and Technology of China (USTC). He received his Ph.D. in engineering for work on key technologies of the acquisition and tracking system for space-ground quantum communication from the Shanghai Institute of Technology and Physics, Chinese Academy of Science in 2010. Afterward, he joined Jianwei Pan's group at USTC, and was put in charge of the QKD payloads in the Micius satellite, Tiangong II space lab, and Jinan-1 microsatellite to demonstrate satellite-to-ground quantum key distribution and construct a quantum network globally.

Pseudorandomness With Proof of Destruction and Applications

Amit Behera (Ben-Gurion University); Zvika Brakerski (Weizmann Institute of Science); Or Sattath (Ben-Gurion University); and Omri Shmueli (Tel Aviv University)

12:15–12:35 p.m.

Two fundamental properties of quantum states that quantum information theory explores are pseudorandomness and provability of destruction. We introduce the notion of quantum pseudorandom states with proofs of destruction (PRSPD) that combines both these properties. Like standard pseudorandom states (PRS), these are efficiently generated quantum states that are indistinguishable from random, but they can also be measured to create a classical string. This string is verifiable (given the secret key) and certifies that the state has been destructed. We show that, similarly to PRS, PRSPD can be constructed from any post-quantum one-way function.

As far as the authors are aware, this is the first construction of a family of states that satisfies both pseudorandomness and provability of destruction. We show that many cryptographic applications that were shown based on PRS variants using quantum communication can be based on (variants of) PRSPD using only classical communication. This includes symmetric encryption, message authentication, one-time signatures, commitments, and classically verifiable private quantum coins.

Theory Talks, Session 1: 2–3:20 p.m.

Quantum Advantage From One-Way Functions

Tomoyuki Morimae (Kyoto University) and Takashi Yamakawa (NTT Social Informatics Laboratories)

12:15–12:35 p.m.

We demonstrate quantum advantage with several basic assumptions, specifically based on only the existence of OWFs. We introduce inefficient-verifier proofs of quantumness (IV-PoQ), and construct it from classical bit commitments. IV-PoQ is an interactive protocol between a verifier and a quantum prover consisting of two phases. In the first phase, the verifier is probabilistic polynomial-time, and it interacts with the prover. In the second phase, the verifier becomes inefficient, and makes its decision based on the transcript of the first phase. If the prover is honest, the inefficient verifier accepts with high probability, but any classical malicious prover only has a small probability of being accepted by the inefficient verifier. Our construction demonstrates the following results: (1)If one-way functions exist, then IV-PoQ exist. (2)If distributional collision-resistant hash functions exist (which exist if hard-on-average problems in SZK exist), then constant-round IV-PoQ exist.

We also demonstrate quantum advantage based on worst-case-hard assumptions. We define auxiliary-input IV-PoQ (AI-IV-PoQ) that only require that for any malicious prover, there exist infinitely many auxiliary inputs under which the prover cannot cheat. We construct AI-IV-PoQ from an auxiliary-input version of commitments in a similar way, showing that (1)If auxiliary-input one-way functions exist (which exist if CZK⊈BPP), then AI-IV-PoQ exist. (2)If auxiliary-input collision-resistant hash functions exist (which is equivalent to PWPP⊈FBPP) or SZK⊈BPP, then constant-round AI-IV-PoQ exist.

Obfuscation of Pseudo-Deterministic Quantum Circuits

James Bartusek (UC Berkeley); Fuyuki Kitagawa (NTT Social Informatics Laboratories); Ryo Nishimaki (NTT Social Informatics Laboratories); and Takashi Yamakawa (NTT Social Informatics Laboratories)

We show how to obfuscate pseudo-deterministic quantum circuits, assuming the quantum hardness of learning with errors (QLWE) and post-quantum virtual black-box (VBB) obfuscation for classical circuits. Given the classical description of a quantum circuit Q, our obfuscator outputs a quantum state $\ket{\widetilde{Q}}$ that can be used to evaluate Q repeatedly on arbitrary inputs. Instantiating the VBB obfuscator for classical circuits with any candidate post-quantum indistinguishability obfuscator gives us the first candidate construction of indistinguishability obfuscation for all polynomial-size pseudo-deterministic quantum circuits.

In particular, our scheme is the first candidate obfuscator for a class of circuits that is powerful enough to implement Shor's algorithm (SICOMP 1997). Our approach follows Bartusek and Malavolta (ITCS 2022), who obfuscate \ emph{null} quantum circuits by obfuscating the verifier of an appropriate classical verification of quantum computation (CVQC) scheme. We go beyond null circuits by constructing a publicly-verifiable CVQC scheme for quantum \emph{partitioning} circuits, which can be used to verify the evaluation procedure of Mahadev's quantum fully-homomorphic encryption scheme (FOCS 2018). We achieve this by upgrading the one-time secure scheme of Bartusek (TCC 2021) to a fully reusable scheme, via a publicly-decodable \emph{Pauli functional commitment}, which we formally define and construct in this work. This commitment scheme, which satisfies a notion of binding against committers that can access the receiver's standard and Hadamard basis decoding functionalities, is constructed by building on techniques of Amos, Georgiou, Kiayias, and Zhandry (STOC 2020) introduced in the context of equivocal but collision-resistant hash functions.

Secure Computation With Shared EPR Pair (Or: How to Teleport in Zero-Knowledge)

James Bartusek (UC Berkeley); Dakshita Khurana (University of Illinois Urbana-Champaign); and Akshayaram Srinivasan (Tata Institute of Fundamental Research)

Can a sender non-interactively transmit one of two strings to a receiver without knowing which string was received? Does there exist minimally-interactive secure multiparty computation that only makes (black-box) use of symmetric-key primitives? We provide affirmative answers to these questions in a model where parties have access to shared EPR pairs, thus demonstrating the cryptographic power of this resource.

First, we construct a one-shot (i.e., single message) string oblivious transfer (OT) protocol with random receiver bit in the shared EPR pairs model, assuming the (sub-exponential) hardness of LWE. Building on this, we show that {\em secure teleportation through quantum channels} is possible. Specifically, given the description of any quantum operation Q, a sender with (quantum) input ρ can send a single classical message that securely transmits $Q(\rho)$ to a receiver. That is, we realize an ideal quantum channel that takes input ρ from the sender and provably delivers $Q(\rho)$ to the receiver without revealing any other information. This immediately gives a number of applications in the shared EPR pairs model: (1) non-interactive secure computation of unidirectional \emph{classical} randomized functionalities, (2) NIZK for QMA from standard (sub-exponential) hardness assumptions, and (3) a non-interactive \ emph{zero-knowledge} state synthesis protocol.

Next, we construct a two-round (round-optimal) secure multiparty computation protocol for classical functionalities in the shared EPR pairs model that is \ emph{unconditionally-secure} in the (quantum-accessible) random oracle model. Classically, both of these results cannot be obtained without some form of correlated randomness shared between the parties, and the only known approach is to have a trusted dealer set up random (string) OT correlations. In the quantum world, we show that shared EPR pairs (which are simple and can be deterministically generated) are sufficient. At the heart of our work are novel techniques for making use of entangling operations to generate string OT correlations, and for instantiating the Fiat-Shamir transform using correlation-intractability in the quantum setting.

Cloning Games: A General Framework for Unclonable Primitives

Prabhanjan Ananth (UC Santa Barbara); Fatih Kaleoglu (UC Santa Barbara); and Qipeng Liu (Simons Institute)

The powerful no-cloning principle of quantum mechanics can be leveraged to achieve interesting primitives, referred to as unclonable primitives, that are impossible to achieve classically. In the past few years, we have witnessed a surge of new unclonable primitives. While prior works have mainly focused on establishing feasibility results, another equally important direction, that of understanding the relationship between different unclonable primitives is still in its nascent stages. Moving forward, we need a more systematic study of unclonable primitives.

To this end, we introduce a new framework called cloning games. This framework captures many fundamental unclonable primitives such as quantum money, copy-protection, unclonable encryption, single-decryptor encryption, and many more. By reasoning about different types of cloning games, we obtain many interesting implications to unclonable cryptography, including the following: (1) We obtain the first construction of information-theoretically secure single-decryptor encryption in the one-time setting. (2) We construct unclonable encryption in the quantum random oracle model based on BB84 states, improving upon the previous work, which used coset states. Our work also provides a simpler security proof for the previous work. (3) We construct copy-protection for single-bit point functions in the quantum random oracle model based on BB84 states, improving upon the previous work, which used coset states, and additionally, providing a simpler proof. 4) We establish a relationship between different challenge distributions of copy-protection schemes and single-decryptor encryption schemes. (5) Finally, we present a new construction of one-time encryption with certified deletion.

Theory Talks, Session 2: 3:50–4:30 p.m.

Publicly-Verifiable Deletion via Target-Collapsing Functions

James Bartusek (UC Berkeley); Dakshita Khurana (University of Illinois Urbana-Champaign); and Alexander Poremba (Caltech)

We build quantum cryptosystems that support publicly-verifiable deletion from standard cryptographic assumptions. We introduce target-collapsing as a weakening of collapsing for hash functions, analogous to how second preimage resistance weakens collision resistance; that is, target-collapsing requires indistinguishability between superpositions and mixtures of preimages of an honestly sampled image. We show that target-collapsing hashes enable publicly-verifiable deletion ($\PVD$), proving conjectures from [Poremba, ITCS'23] and demonstrating that the Dual-Regev encryption (and corresponding fully homomorphic encryption) schemes support $\PVD$ under the LWE assumption.

We further build on this framework to obtain a variety of primitives supporting publicly-verifiable deletion from weak cryptographic assumptions, including: Commitments with $\PVD$ assuming the existence of injective one-way functions, or more generally, {\em almost-regular} one-way functions. Along the way, we demonstrate that (variants of) target-collapsing hashes can be built from almost-regular one-way functions. Public-key encryption with $\PVD$ assuming trap doored variants of injective (or almost-regular) one-way functions.

We also demonstrate that the encryption scheme of [Hhan, Morimae, and Yamakawa, Eurocrypt '23] based on pseudorandom group actions has $\PVD$. - X with $\PVD$ for $X \in \{$attribute-based encryption, quantum fully-homomorphic encryption, witness encryption, time-revocable encryption$\}$, assuming X and trap doored variants of injective (or almost-regular) one-way functions.

Simple Tests of Quantumness Also Certify Qubits

Zvika Brakerski (Weizmann Institute of Science); Alexandru Gheorghiu (Chalmers University of Technology); Gregory D. Kahanamoku-Meyer (Lawrence Berkeley National Laboratory & UC Berkeley); Eitan Porat (Weizmann Institute of Science); and Thomas Vidick (Weizmann Institute of Science)

A test of quantumness is a protocol that allows a classical verifier to certify (only) that a prover is not classical. We show that tests of quantumness that follow a certain template, which captures recent proposals such as (Kalai et al., 2022), can in fact do much more. Namely, the same protocols can be used for certifying a qubit, a building-block that stands at the heart of applications such as certifiable randomness and classical delegation of quantum computation. Certifying qubits was previously only known to be possible based on the hardness of the Learning with Errors problem and the use of adaptive hardcore (Brakerski et al., 2018).

Our framework allows certification of qubits based only on the existence of post-quantum trapdoor claw-free functions, or on quantum fully homomorphic encryption. These can be instantiated, for example, from Ring Learning with Errors. On the technical side, we show that the quantum soundness of any such protocol can be reduced to

proving a bound on a simple algorithmic task: informally, answering "two challenges simultaneously" in the protocol. Our reduction formalizes the intuition that these protocols demonstrate quantumness by leveraging the impossibility of rewinding a general quantum prover.

This allows us to prove tight bounds on the quantum soundness of (Kahanamoku-Meyer et al., 2021) and (Kalai et al., 2022), showing that no quantum polynomial-time prover can succeed with probability larger than $\cos^2(\pi/8) \approx 0.853$. Previously, only an upper bound on the success probability of classical provers, and a lower bound on the success probability of quantum provers, were known. We then extend this proof of quantum soundness to show that provers that approach the quantum soundness bound must perform almost anti-commuting measurements. This certifies that the prover holds a qubit.

Experimental Talks, Session 1: 12:15–12:35 p.m.

The Application of Hybrid Photonic Integration to Quantum Key Distribution

Joseph Dolphin (University of Cambridge); Taofiq K. araiso (Toshiba Europe Ltd.); Han Du (Toshiba Europe Ltd.); and Andrew J. Shields (Toshiba Europe Ltd.)

Hybrid integration has the potential to overcome various limitations of integrated photonic material platforms. Here, we present the results of applying edge-couple hybrid integration to produce high performance quantum key distribution chips. We show low quantum bit error rate operation (< 1%) and positive secure key rates over 250 km of fiber spool.

Experimental Talks, Session 1: 2–3:20 p.m.

High-Rate Quantum Key Distribution Exceeding 110Mb/s

Wei Li (University of Science and Technology of China); Likang Zhang (University of Science and Technology of China); Hao Tan (University of Science and Technology of China); Yichen Lu (University of Science and Technology of China); Sheng-Kai Liao (University of Science and Technology of China); Jia Huang (Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences); Hao Li (Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences); Zhen Wang (Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences); Hao-Kun Mao (Harbin Institute of Technology); Bingze Yan (Harbin Institute of Technology); Qiong Li (Harbin Institute of Technology); Yang Liu (Jinan Institute of Quantum Technology); Qiang Zhang (University of Science and Technology of China); Cheng-Zhi Peng (University of Science and Technology of China); Lixing You (Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences); Feihu Xu (University of Science and Technology of China); and Jianwei Pan (University of Science and Technology of China)

We report a quantum key distribution system that is able to generate key at a record high key rate of 115.8 Mb/s over 10-km standard fiber. This attributes to a high-efficiency multi-pixel superconducting nanowire detector, a low-error integrated transmitter, and a fast post-processing algorithm.

10 GBaud Continuous-Variable Quantum Key Distribution Enabled by Integrated Photonic-Electronic Receivers

Adnan A.E. Hajomer (Technical University of Denmark); C´edric Bruynsteen (Ghent University-imec); Ivan Derkach (Technical University of Denmark); Nitin Jain (Technical University of Denmark); Ulrik L. Andersen (Technical University of Denmark); Xin Yin (Ghent University-imec); and Tobias Gehring (Technical University of Denmark)

Quantum key distribution (QKD) is a well-known application of quantum information theory that guarantees information-theoretically secure key exchange. While QKD systems are becoming commercially available, large-scale deployment of next-generation QKD systems requires photonic and electronic devices that are low-cost, small, and easily integrated with existing network infrastructure. Continuous variable (CV) QKD is a promising option for large-scale deployment due to its compatibility with standard telecom technology. Despite this, the secret key rates of CV-QKD systems have been limited to a few megabits per second due to the bandwidth bottleneck of the receiver and the limited symbol rate of the transmitter.

Here, we present the first discrete-modulated coherent state CV-QKD system operating at a classical telecom symbol rate of 10 GBaud. This system generates keys at rates exceeding 0.7 Gb/s over a distance of 5 km and 0.3 Gb/s over a distance of 10 km while being secure against collective attacks in both the asymptotic and finite-size regimes. This is made possible by using a high-speed, co-integrated phase-diverse receiver consisting of a silicon photonics optical front-end and a custom-designed integrated transimpedance amplifier.

Additionally, well-engineered digital signal processing is used for quantum state preparation and measurement. Our experiment sets a new record for secure quantum communication and paves the way for the next generation of CV-QKD systems.

High-Rate Point-to-Multipoint QKD Network

Yiming Bian (State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China); Yan Pan (Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China); Yichen Zhang (State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China); Heng Wang (Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China); Jie Yang (Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China); Jiayi Dou (State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China); Yang Li (Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China); Wei Huang (Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China); Song Yu (State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China); Bingjie Xu (Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China); and Hong Guo (State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China)

A coherent-state point-to-multipoint protocol is proposed to simultaneously support multiple independent quantum key distribution links between a single transmitter and massive receivers. Every prepared coherent state is measured by all receivers to generate raw keys, then processed with a secure and high-efficient key distillation method to remove the correlations between different links. The simulation results show that it can achieve remarkably high key rates even with a hundred of access points. Further, a proof-of-principle experiment with one network node and four end users has been demonstrated, where the average secret key rate of 4.1 Mbps between the transmitter and each one receiver is achieved, resulting in two orders-of-magnitude higher than previous networks. This scheme is a promising step towards a high-rate multi-user solution in a scalable quantum secure network.

Passive Continuous Variable Quantum Key Distribution

Chenyang Li (University of Toronto); Chengqiu Hu (University of Hong Kong); Wenyuan Wang (University of Hong Kong); Rong Wang (University of Hong Kong); and Hoi-Kwong Lo (University of Toronto)

Passive quantum key distribution (QKD) has been proposed for discrete variable (DV) protocols to eliminate side channels in the source. Unfortunately, the key rate of passive DV-QKD protocols suffers from sifting loss and additional quantum errors.

In this work, we propose the general framework of passive continuous variable quantum key distribution. Rather surprisingly, we find that the passive source is a perfect candidate for the discrete-modulated continuous variable quantum key distribution (DMCV QKD) protocol. With the phase space remapping scheme, we show that passive DMCV QKD offers the same key rate as its active counterpart. Considering the important advantage of removing side channels that have plagued the active ones, passive DMCV QKD is a promising alternative. In addition, our protocol makes the system much simpler by allowing modulator-free quantum key distribution. Finally, we experimentally characterize the passive DMCV QKD source, thus showing its practicality.

Merged with

Fully-Passive Twin-Field Quantum Key Distribution

Wenyuan Wang (University of Hong Kong); Rong Wang (University of Hong Kong); and Hoi-Kwong Lo (University of Hong Kong, University of Toronto, Quantum Bridge Technologies)

We propose a fully-passive twin-field quantum key distribution (QKD) setup where basis choice, decoy-state preparation and encoding are all implemented entirely by post-processing without any active modulation. Our protocol can remove the potential side-channels from both source modulators and detectors, and additionally retain the high key rate advantage offered by twin-field QKD, thus offering great implementation security and good performance. Importantly, we also propose a post-processing strategy that uses mismatched phase slices and minimizes the effect of sifting. We show with numerical simulation that the new protocol can still beat the repeaterless bound and provide satisfactory key rate.

QKD Implementation: 3:50–4:30 p.m.

Security of Differential Phase Shift Quantum Key Distribution From Relativistic Principles

Martin Sandfuchs (ETH Zürich); Marcus Haberland (Max Planck Institute for Gravitational Physics, ETH Zürich); V. Vilasini (ETH Zürich); and Ramona Wolf (ETH Zürich)

The design of quantum protocols for secure key generation poses many challenges: On the one hand, they need to be practical concerning experimental realizations. On the other hand, their theoretical description must be simple enough to allow for a security proof against all possible attacks. Often, these two requirements are in conflict with each other, and the differential phase shift (DPS) QKD protocol exemplifies these difficulties: It is designed to be implementable with current optical telecommunication technology, which, for this protocol, comes at the cost that many standard security proof techniques do not apply to it. After about 20 years since its invention, this work presents the first full security proof of DPS QKD against general attacks, including finite-size effects. The proof combines techniques from quantum information theory, quantum optics, and relativity.

We first give a security proof of a QKD protocol whose security stems from relativistic constraints. We then show that security of DPS QKD can be reduced to security of the relativistic protocol. In addition, we show that coherent attacks on the DPS protocol are, in fact, stronger than collective attacks.

Security of Quantum Key Distribution With Imperfect Phase Randomization

Guillermo Currás-Lorenzo (University of Vigo); Kiyoshi Tamaki (University of Toyama); and Marcos Curty (University of Vigo)

The performance of quantum key distribution (QKD) is severely limited by multiphoton emissions, due to the photon-number-splitting attack. The most efficient solution, the decoy-state method, requires that the phases of all transmitted pulses are independent and uniformly random. In practice, however, these phases are often correlated, especially in high-speed systems, which opens a security loophole.

Here, we address this pressing problem by providing a security proof for decoy-state QKD with correlated phases that offers key rates close to the ideal scenario. Our work paves the way towards high-performance secure QKD with practical laser sources, and may have applications beyond QKD.

Merged with

Security Bounds for Quantum Key Distribution With Arbitrary Phase Randomization

Xoel Sixto (Universidade de Vigo); Guillermo Currás-Lorenzo (University of Toyama); Kiyoshi Tamaki (University of Toyama); and Marcos Curty (Universidade de Vigo)

Decoy-state quantum key distribution (QKD) is undoubtedly the most efficient solution to handle multi-photon signals emitted by laser sources, and provides the same secret key rate scaling as ideal single-photon sources. It requires, however, that the phase of each emitted pulse is uniformly random. This might be difficult to guarantee in practice, due to inevitable device imperfections and/or the use of an external phase modulator for phase randomization, which limits the possible selected phases to a finite set.

Here, we investigate the security of decoy-state QKD with arbitrary, continuous or discrete, non-uniform phase randomization, and show that this technique is quite robust to deviations from the ideal uniformly random scenario. For this, we combine a novel parameter estimation technique based on semi-definite programming, with the use of basis mismatched events, to tightly estimate the parameters that determine the achievable secret key rate. In doing so, we demonstrate that our analysis can significantly outperform previous results that address more restricted scenarios.

12:15-12:35 p.m.

Experimental Twin-Field Quantum Key Distribution Over 1000 km Fiber Distance

Yang Liu (Jinan Institute of Quantum Technology)

Quantum key distribution (QKD) aims to generate secure private keys shared by two remote parties. With its security being protected by principles of quantum mechanics, some technology challenges remain towards the practical application of QKD.

The major one is the distance limit, which is caused by the fact that a quantum signal cannot be amplified while the channel loss is exponential with the distance for photon transmission in optical fiber. Here using the 3-intensity sending-or-not-sending protocol with the actively-odd-parity-pairing method, we demonstrate a fiber-based twin-field QKD over 1002 km.

In our experiment, we developed a dual-band phase estimation and ultra-low noise superconducting nanowire single-photon detectors to suppress the system noise to around 0.02 Hz. The secure key rate is 9.53×10^{-12} per pulse through 1002 km fiber in the asymptotic regime, and 8.75×10^{-12} per pulse at 952 km considering the finite size effect. Our work constitutes a critical step toward the future large-scale quantum network.

10:40–11 a.m.

Quantum Key Distribution Links Between Mobile Platforms

Andrew Conrad (University of Illinois Urbana-Champaign); Samantha Isaac (University of Illinois Urbana-Champaign); Roderick Cochran (Ohio State University); Daniel Sanchez-Rosales (Ohio State University); Timur Javid (University of Illinois Urbana-Champaign); Shuen Wu (University of Illinois Urbana-Champaign); Dan Gauthier (Ohio State University); and Paul Kwiat (University of Illinois Urbana-Champaign)

As the proliferation of automation in smart transportation continues, there is a need to secure communication links of "on-the-go" future mobile platforms. In this effort, we implement decoy-state quantum key distribution (QKD), which provides provably secure communication, to mobile platforms such as drones and vehicles. Unlike demonstrations in fiber of fixed point-to-point, QKD between mobile platforms provides unique challenges such as designing systems with reduced size, weight, and power, establishing a stable line-of-sight as the platforms are in motion, and maintaining performance over a wide operating temperature range, etc.

We design our QKD transmitter and receiver using a modular design that is platform-agnostic. This allows us to deploy the same QKD system on an octocopter drone and a car without any hardware or software modifications. We describe critical subsystems including our resonant-cavity QKD source, custom prepare and measure optics, pointing, acquisition, and tracking system, single-photon detector, field-programmable gate array-based time-tagger, and qubit-based time-synchronization algorithm. Our achievements include drone-to-drone QKD, drone-to-car quantum transmission, and high-speed (70 mph) vehicle-to-vehicle quantum transmission on a U.S. interstate highway.

12:15–12:35 p.m.

Satellite-Based Quantum Key Distribution in the Presence of Bypass Channels

Masoud Ghalaii (University of Leeds); Sima Bahrani (University of Bristol); Carlo Liorni (University of Dusseldorf); Federico Grasselli (University of Dusseldorf); Hermann Kampermann (University of Dusseldorf); Lewis Wooltorton (University of Bristol); Rupesh Kumar (University of York); Stefano Pirandola (University of York); Timothy Spiller (University of York); Alexander Ling (National University of Singapore); and Bruno Huttner (ID Quantique); Mohsen Razavi (University of Leeds)

The security of prepare-and-measure satellite-based quantum key distribution (QKD), under restricted eavesdropping scenarios, is addressed. We particularly consider cases where the eavesdropper, Eve, has limited access to the transmitted signal by Alice, and/or Bob's receiver station. For instance, Eve can only receive an attenuated version of the transmitted signals. This results in settings where an uncharacterized bypass channel, inaccessible to Eve, can also carry signals to Bob.

We obtain generic bounds on the key rate in the presence of bypass channels and apply them to continuous-variable QKD protocols with Gaussian encoding as well as to the family of BB84 protocols. We find regimes of operation in which the above restrictions on Eve can considerably improve system performance. Our work opens up new security frameworks for spaceborne quantum communications systems.

Beyond QKD: 2–3:20 p.m.

On Concurrent Multi-Party Quantum Computation

Vipul Goyal (NTT Research & Carnegie Mellon University); Xiao Liang (NTT Research); and Giulio Malavolta (Max Planck Institute for Security and Privacy)

Recently, significant progress has been made toward quantumly secure multi-party computation (MPC) in the stand-alone setting. In sharp contrast, the picture of concurrently secure MPC (or even 2PC), for both classical and quantum functionalities, still remains unclear. Quantum information behaves in a fundamentally different way, making the job of adversary harder and easier at the same time. Thus, it is unclear if the positive or negative results from the classical setting still apply.

This work initiates a systematic study of concurrent secure computation in the quantum setting. We obtain a mix of positive and negative results. We first show that assuming the existence of post-quantum one-way functions (PQ-OWFs), concurrently secure 2PC (and thus MPC) for quantum functionalities is impossible. Next, we focus on the bounded-concurrent setting, where we obtain simulation-sound zero-knowledge arguments for both NP and QMA, assuming PQ-OWFs. This is obtained by a new design of simulation-sound gadget which is compatible with the quantum rewinding strategy recently developed by Ananth, Chung, and La Placa [CRYPTO '21] for bounded-concurrent post-quantum ZK.

Moreover, we show that our technique is general enough—it also leads to quantum-secure bounded-concurrent coin-flipping protocols, and eventually general-purpose 2PC and MPC, for both classical and quantum functionalities. All these constructions can be based on the quantum hardness of Learning with Errors.

Fiat-Shamir for Proofs Lacks a Proof Even in the Presence of Shared Entanglement

Frédéric Dupuis (Université de Montréal); Philippe Lamontagne (National Research Council Canada); and Louis Salvail (Université de Montréal)

We explore the cryptographic power of arbitrary shared physical resources. The most general such resource is access to a fresh entangled quantum state at the outset of each protocol execution. We call this the Common Reference Quantum State (CRQS) model, in analogy to the well-known Common Reference String (CRS). The CRQS model is a natural generalization of the CRS model but appears to be more powerful: in the two-party setting, a CRQS can sometimes exhibit properties associated with a Random Oracle queried once by measuring a maximally entangled state in one of many mutually unbiased bases. We formalize this notion as a Weak One-Time Random Oracle (WOTRO), where we only ask of the m–bit output to have some randomness when conditioned on the n–bit input. We show that when $n - m \in \omega(\lg n)$, any protocol for WOTRO in the CRQS model can be attacked by an (inefficient) adversary.

Moreover, our adversary is efficiently simulatable, which rules out the possibility of proving the computational security of a scheme by a fully black-box reduction to a cryptographic game assumption. On the other hand, we introduce a non-game quantum assumption for hash functions that implies WOTRO in the CRQ$ model (where the CRQS consists only of EPR pairs). We first build a statistically secure WOTRO protocol where $m = n$, then hash the output. The impossibility of WOTRO has the following consequences. First, we show the fully-black-box impossibility of a quantum Fiat-Shamir transform, extending the impossibility result of Bitansky et al. (TCC '13) to the CRQS model. Second, we show a fully-black-box impossibility result for a strengthened version of quantum lightning (Zhandry, Eurocrypt '19) where quantum bolts have an additional parameter that cannot be changed without generating new bolts. Our results also apply to 2–message protocols in the plain model.

Oblivious Transfer from Zero-Knowledge Proofs, Or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States

Léo Colisson (Centrum Wiskunde & Informatica, QuSoft, Netherlands); Garazi Muguruza (University of Amsterdam, QuSoft, Netherlands); and Florian Speelman (University of Amsterdam, QuSoft, Netherlands)

We provide a generic construction to turn any classical zero-knowledge (ZK) protocol into a composable (quantum) oblivious transfer (OT) protocol, mostly lifting the round-complexity properties and security guarantees (plain-model/statistical security/unstructured functions) of the ZK protocol to the resulting OT protocol. Such a construction is unlikely to exist classically as Cryptomania is believed to be different from Minicrypt. In particular, by instantiating our construction using Non-Interactive ZK (NIZK), we provide the first round-optimal (2-message) quantum OT protocol secure in the random oracle model, and round-optimal extensions to string and k-out-of-n OT.

At the heart of our construction lies a new method that allows us to prove properties on a received quantum state without revealing additional information on it, even in a non-interactive way and/or with statistical guarantees when using an appropriate classical ZK protocol. We can notably prove that a state has been partially measured (with arbitrary constraints on the set of measured qubits), without revealing any additional information on this set.

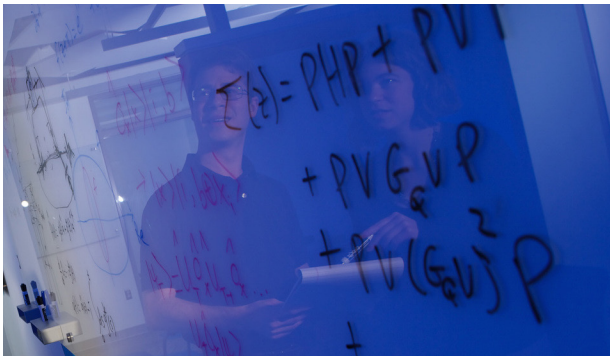
This notion can be seen as an analog of ZK to quantum states, and we expect it to be of independent interest as it extends complexity theory to quantum languages, as illustrated by the two new complexity classes we introduce, ZKstatesQIP and ZKstatesQMA.

Single-qubit Loss-Tolerant Quantum Position Verification Protocol Secure Against Entangled Attackers

Llorenc Escola Farras (QuSoft) and Florian Speelman (University of Amsterdam, QuSoft)

We give a tight characterization of the relation between loss-tolerance and error rate of the most popular protocol for quantum position verification (QPV), which is based on BB84 states, and generalizations of this protocol. Combining it with classical information, we show for the first time a fault-tolerant protocol that is secure against attackers who pre-share a linear amount of entanglement (in the classical information), arbitrarily slow quantum information, and that tolerates a certain amount of photon loss.

We also extend this analysis to the case of more than two bases, showing even stronger loss-tolerance for that case. Finally, we show that our techniques can be applied to improve the analysis of one-sided device-independent QKD protocols.



Theory Talks: 3:50–4:30 p.m.

On the Finite Size Security of Quantum Key Distribution

Peter Brown and Thomas an Himbeeck (Telecom Paris)

We consider the security of quantum key distribution (QKD) protocols consisting of a finite number of rounds. We provide a security proof that is both and provides tight finite-size correction terms. In particular, when expanded in the block length n, the rate of randomness generation has the optimal asymptotic rate and optimal leading-order finite-size correction term. The proof is also general, applying to generic randomness generation and QKD protocols that have fully characterized devices and consist of a finite number of rounds.

Quantum Secure Non-malleable Randomness Encoder and its Applications

Rishabh Batra (CQT, NUS); Naresh Goud Boddu (NTT Research); and Rahul Jain (CQT, NUS)

"Non-Malleable Randomness Encoder" (NMRE) was introduced by Kanukurthi, Obbattu and Sekar [KOS18] as a useful cryptographic primitive helpful in the construction of non- malleable codes. To the best of our knowledge, their construction is not known to be quantum secure.

We provide a construction of a first rate-$1/2$, 2-split, quantum secure NMRE and use this in a black-box manner, to construct for the first time the following: 1. rate $1/11$, 3-split, quantum non-malleable code, 2. rate $1/3$, 3-split, quantum secure non-malleable code, 3. rate $1/5$, 2-split, quantum secure non-malleable code.

Merged with

Split-State Non-Malleable Codes for Quantum Messages

Naresh Goud Boddu (NTT Research); Vipul Goyal (Carnegie Mellon University and NTT Research); Rahul Jain (National University of Singapore); and Joao Ribeiro (NOVA LINCS and NOVA School of Science and Technology)

Non-malleable codes are fundamental objects at the intersection of cryptography and coding theory. These codes provide security guarantees even in settings where error correction and detection are impossible, and have found applications to several other cryptographic tasks. Roughly speaking, a non-malleable code for a family of tampering functions guarantees that no adversary can tamper (using functions from this family) the encoding of a given message into the encoding of a related distinct message.

We focus on the split-state tampering model, one of the strongest and most well-studied adversarial tampering models. In this model, a codeword is split into two parts which are stored in physically distant servers, and the adversary can then independently tamper with each part using arbitrary functions. Previous works on non-malleable codes in the split-state tampering model only considered the encoding of classical messages. Furthermore, until the recent work by Aggarwal, Boddu, and Jain (arXiv 2022), adversaries with quantum capabilities and shared entanglement had not been considered, and it is a priori not clear whether previous coding schemes remain secure in this model.

In this work, we introduce the notion of split-state non-malleable codes for quantum messages secure against quantum adversaries with shared entanglement. We construct explicit codes in this model by relying on a recent quantum-secure two-source non-malleable randomness encoder by Batra, Boddu, and Jain [BBJ23], arguments from Aggarwal, Boddu and Jain [ABJ22] and with use of unitary two-designs. (1) More precisely, we construct the first efficiently encodable and decodable split-state non-malleable code for quantum messages (while preserving entanglement with external systems) achieving security against quantum adversaries having shared entanglement with codeword length n, any message length at most $n^\Omega(1)$, and error $2^{-n^{\Omega(1)}}$. (2) For the case of uniform quantum message, we provide the first constant rate (rate 1/11) non-malleable code (while preserving entanglement with external systems) achieving code- word length n and error $2^{-n^{\Omega(1)}}$.

Photonic Integration: 9–11 a.m.

100 Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations

Cedric Bruynsteen (imec-Ghent University); Tobias Gehring (Technical University of Denmark); Cosmo Lupo (Politechnico Di Bari); and Johan Bauwelinck (imec-Ghent University); Xin Yin (imec-Ghent University)

Emerging communication and cryptography applications call for reliable, fast, unpredictable random number generators. Quantum random number generation allows for the creation of truly unpredictable numbers thanks to the inherent randomness available in quantum mechanics. A popular approach is using the quantum vacuum state to generate random numbers. While convenient, this approach was generally limited in speed compared to other schemes.

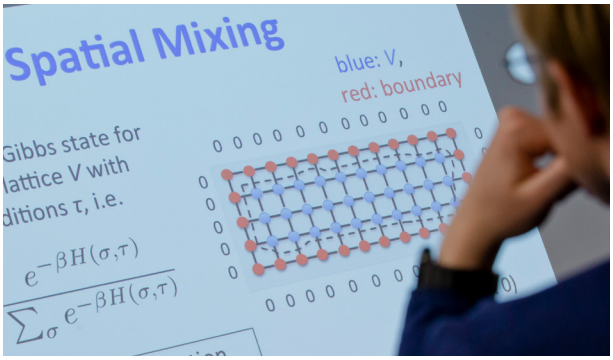
Here, through custom co-design of opto-electronic integrated circuits and side-information reduction by digital filtering, we experimentally demonstrated an ultrafast generation rate of 100 Gbit/s, setting a new record for vacuum-based quantum random number generation by one order of magnitude. Furthermore, our experimental demonstrations are well supported by an upgraded device-dependent framework that is secure against both classical and quantum side-information and that also properly considers the non-linearity in the digitization process. This ultrafast secure random number generator in the chip-scale platform holds promise for next generation communication and cryptography applications.

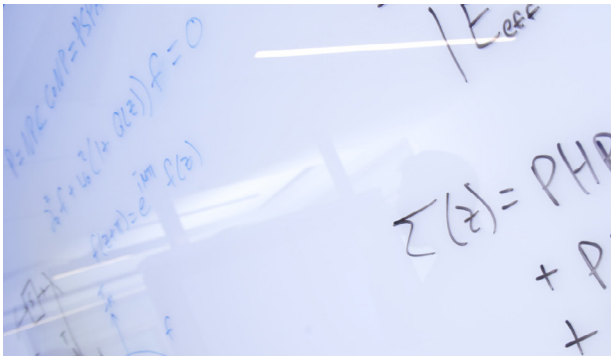
Ultra-fast Multipixel SNSPD Arrays With Photon-Number Capabilities for Quantum Applications

Giovanni V. Resta (ID Quantique SA); Lorenzo Stasi (ID Quantique SA); Matthieu Perrenoud (University of Geneva); Rob Thew (niversity of Geneva); Hugo Zbinden (University of Geneva); and Félix Bussières (ID Quantique SA)

Superconducting-nanowire single-photon detectors (SNSPDs) have enabled the realization of several quantum optics technologies thanks to their high detection efficiency, low dark-counts, and fast recovery time. Here, we will present a 14-pixel SNSPD array with a maximum system detection efficiency (SDE) of 90% that remains above 80% up to 400 Mcps, and we demonstrate the ability to reach detection rates of 1.5 Gcps with an absolute SDE of 45%. Furthermore, we will explain how such device has been integrated in a QKD set-up and enabled high-speed QKD, with secret-key rates exceeding 60 Mbps over a distance of 10 km.

Moreover when used in a QKD setup, the array can improve resilience against blinding attacks by monitoring the coincidence clicks between the pixels. Finally we will show that the detector is able to distinguish few-photon number states in an optical pulse with high fidelity, without posing strict limitations on the shape of the incoming light. We achieve a 2-photon fidelity of 74% and 57% for a 3-photon state, which represent state-of-the-art results for fiber-coupled SNSPDs. Such detectors could find immediate application in LOQC protocols where the capability to distinguish few photon-number states is sufficient—that is, either '1' vs 'more than 1 photons.'





Resource-Efficient Quantum Key Distribution With Using Integrated Silicon Photonics

Kejin Wei (School of Physical Science and Technology, Guangxi University, Nanning 530004, China); Xiao Hu (National Information Optoelectronics Innovation Center (NOEIC), Wuhan 430074, China); Yongqiang Du (School of Physical Science and Technology, Guangxi University, Nanning 530004, China); Xin Hua (National Information Optoelectronics Innovation Center (NOEIC), Wuhan 430074, China); Zhengeng Zhao (School of Physical Science and Technology, Guangxi University, Nanning 530004, China); Ye Chen (School of Physical Science and Technology, Guangxi University, Nanning 530004, China); Chunfeng Huang (School of Physical Science and Technology, Guangxi University, Nanning 530004, China); Xi Xiao (National Information Optoelectronics Innovation Center (NOEIC), Wuhan 430074, China)

Integrated photonics provides a promising platform for quantum key distribution (QKD) system in terms of miniaturization, robustness and scalability. Tremendous QKD works based on integrated photonics have been reported. Nonetheless, most current chip-based QKD implementations require additional off-chip hardware to demodulate quantum states or perform auxiliary tasks such as time synchronization and polarization basis tracking.

Here, we report a demonstration of resource-efficient chip-based BB84 QKD with a silicon-based encoder and decoder. In our scheme, the time synchronization and polarization compensation are implemented relying on the preparation and measurement of the quantum states generated by on-chip devices, thus no need additional hardware. The experimental tests show that our scheme is highly stable with a low intrinsic QBER of 0.50 ± 0.02% in a 6-h continuous run. Furthermore, over a commercial fiber channel up to 150 km, the system enables realizing secure key distribution at a rate of 866 bps. Our demonstration paves the way for low-cost, wafer-scale manufactured QKD system.

Merged with

Fully Chip-Based Decoder for Polarization-Encoding Quantum Key Distribution

Yongqiang Du (School of Physical Science and Technology, Guangxi University, Nanning 530004, China); Xun Zhu (National Information Optoelectronics Innovation Center (NOEIC), Wuhan 430074, China); Xin Hua (National Information Optoelectronics Innovation Center (NOEIC), Wuhan 430074, China); Zhengeng Zhao (School of Physical Science and Technology, Guangxi University, Nanning 530004, China); Xiao Hu (National Information Optoelectronics Innovation Center, Wuhan 430074, China); Yi Qian (National Information Optoelectronics Innovation Center, Wuhan 430074, China); Xi Xiao (National Information Optoelectronics Innovation Center (NOEIC), Wuhan 430074, China); and Kejin Wei (School of Physical Science and Technology, Guangxi University, Nanning 530004, China)

Silicon-based polarization-encoding quantum key distribution (QKD) has been extensively studied due to its advantageous characteristics of its low cost and robustness. However, given the difficulty of fabricating polarized independent components on the chip, previous studies have only adopted off-chip devices to demodulate the quantum states or perform polarization compensation. In the current work, a fully chip-based decoder for polarization-encoding QKD was proposed. The chip realized a polarization state analyzer and compensated for the BB84 protocol without the requirement of additional hardware, which was based on a polarization-to-path conversion method utilizing a polarization splitter-rotator. The chip was fabricated adopting a standard silicon photonics foundry, which was of a compact design and suitable for mass production. In the experimental stability test, an average quantum bit error rate of 0.59% was achieved through continuous operation for 10 h without any polarization feedback. Furthermore, the chip enabled the automatic compensation of the fiber polarization drift when utilizing the developed feedback algorithm, which was emulated by a random fiber polarization scrambler. Moreover, a finite-key secret rate of 240 bps over a fiber spool of 100 km was achieved in the case of the QKD demonstration. This study marks an important step toward the integrated, practical, and large-scale deployment of QKD systems.

Experimental Certification of Quantum Transmission via Bell's Theorem

Simon Neves (University of Geneva, Sorbonne Université); Laura Dos Santos Martins (Sorbonne Université, CNRS, LIP6); Verena Yacoub (Sorbonne Université, CNRS, LIP6); Pascal Lefebvre (Sorbonne Université, CNRS, LIP6); Ivan Supic (Sorbonne Université, CNRS, LIP6); Damian Markham (Sorbonne Université, CNRS, LIP6); and Eleni Diamanti (Sorbonne Université, CNRS, LIP6)

Quantum transmission links are central elements in essentially all implementations of quantum information protocols. Emerging progress in quantum technologies involving such links needs to be accompanied by appropriate certification tools. In adversarial scenarios, a certification method can be vulnerable to attacks if too much trust is placed on the underlying system.

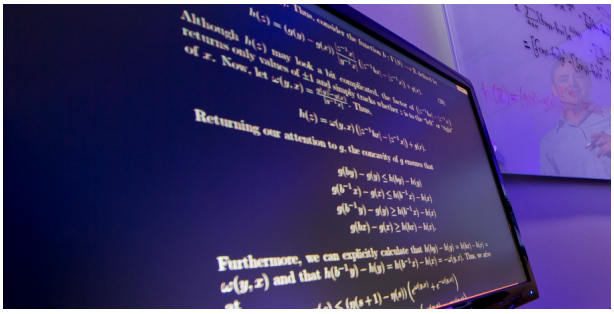
Here, we propose a protocol in a device independent framework, which allows for the certification of practical quantum transmission links in scenarios where minimal assumptions are made about the functioning of the certification setup. We take in particular unavoidable transmission losses into account by modeling the link as a completely-positive trace-decreasing map. We also crucially remove the assumption of independent and identically distributed samples, which is known to be incompatible with adversarial settings.

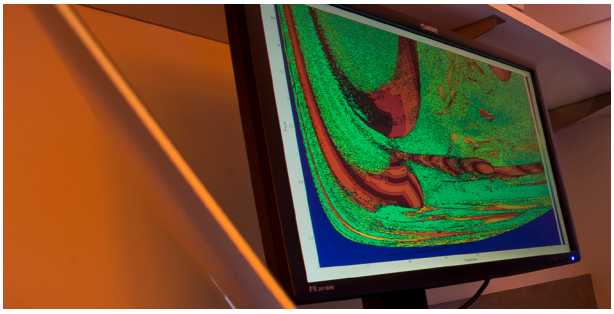
Finally, in view of the use of the certified transmitted states for follow-up applications, our protocol allows to estimate the quality of the state and does not certify the channel only. To illustrate the practical relevance and the feasibility of our protocol with currently available technology we provide an experimental implementation based on a state-of-the-art polarization entangled photon pair source in a Sagnac configuration and analyze its robustness for realistic losses and errors.

Experimental Cheat-Sensitive Quantum Weak Coin Flipping

Simon Neves (University of Geneva, Sorbonne Université); Verena Yacoub (Sorbonne Université, CNRS, LIP6); Ulysse Chabaud (CNRS, INRIA, ENS); Mathieu Bozzio (University of Vienna); Iordanis Kerenidis (Université de Paris, CNRS, IRIF); and Eleni Diamanti (Sorbonne Université, CNRS, LIP6)

As in modern communication networks, the security of quantum networks will rely on complex cryptographic tasks that are based on a handful of fundamental primitives. Weak coin flipping (WCF) is a significant such primitive which allows two mistrustful parties to agree on a random bit while they favor opposite outcomes. Remarkably, perfect information-theoretic security can be achieved in principle for quantum WCF, which is impossible for a classical coin flip without computational assumptions or trusting a third party. In this work, we overcome conceptual and practical issues that have prevented the experimental demonstration of this primitive to date, and demonstrate how quantum resources can provide cheat sensitivity, whereby each party can detect a cheating opponent, and an honest party is never sanctioned. Such a property is not known to be classically achievable with information-theoretic security. Our experiment implements a refined, loss-tolerant version of a recently proposed theoretical protocol and exploits heralded single photons generated by spontaneous parametric down-conversion, a carefully optimized linear optical interferometer including beam splitters with variable reflectivities and a fast optical switch for the verification step. High values of our protocol benchmarks are maintained for attenuation corresponding to several kilometers of telecom optical fiber.





Device Independence: 11:30 a.m.–12:30 p.m.

Group Coset Monogamy Games and an Application to Device-Independent Continuous-Variable QKD

Eric Culf (University of Waterloo); Thomas Vidick (Caltech and Weizmann Institute of Science); and Victor V. Albert (National Institute of Standards and Technology and University of Maryland)

We develop an extension of a recently introduced subspace coset state monogamy-of-entanglement game [Coladangelo, Liu, Liu and Zhandry; Crypto '21] to general group coset states, which are uniform superpositions over elements of a subgroup to which has been applied a group-theoretic generalization of the quantum one-time pad. We give a general bound on the winning probability of a monogamy game constructed from subgroup coset states that applies to a wide range of finite and infinite groups.

To study the infinite-group case, we use and further develop a measure-theoretic formalism that allows us to express continuous-variable measurements as operator-valued generalizations of probability measures. We apply the monogamy game bound to various physically relevant groups, yielding realizations of the game in continuous-variable modes as well as in rotational states of a polyatomic molecule. We obtain explicit strong bounds in the case of specific group-space and subgroup combinations.

As an application, we provide the first proof of one sided-device independent security of a squeezed-state continuous-variable quantum key distribution protocol against general coherent attacks.

Entropy Accumulation Under Post-Quantum Cryptographic Assumptions

Ilya Merkulov and Rotem Arnon-Friedman (Weizmann Institute of Science)

In device-independent (DI) quantum protocols, the security statements are oblivious to the characterization of the quantum apparatus—they are based solely on the classical interaction with the devices as well as some well-defined assumptions. The most commonly known setup is the so-called non-local one, in which two devices that cannot communicate with each other present a violation of a Bell inequality.

In recent years, a new variant of DI protocols, requiring only a single device, arose. In this novel research avenue, the no-communication assumption is replaced with a computational assumption which states that the device cannot solve certain post-quantum cryptographic tasks. The protocols in literature that have been analyzed in this setting, e.g., randomness certification, used ad hoc proof techniques. In addition, the strength of the achieved results is hard to judge due to their complexity.

Here, we build on ideas coming from the study of non-local DI protocols and develop a new modular proof technique for the single-device computational setting. We present a flexible framework for proving the security of such protocols by utilizing a combination of tools from quantum information theory, such as the entropic uncertainty relation and the entropy accumulation theorem. This leads to an insightful and simple proof of security as well as to explicit quantitative bounds. Our work thus acts as the basis for the analysis of future protocols for DI randomness generation, expansion, amplification, and key distribution based on post-quantum cryptographic assumptions.

Quantum Delegation With an Off-the-Shelf Device

Anne Broadbent (University of Ottawa); Arthur Mehta (University of Ottawa); and Yuming Zhao (University of Waterloo)

Given that reliable cloud quantum computers are becoming closer to reality, the concept of delegation of quantum computations and its verifiability is of central interest. Many models have been proposed, each with specific strengths and weaknesses.

Here, we put forth a new model where the client trusts only its classical processing, makes no computational assumptions, and interacts with a quantum server in a \ emph{single} round. In addition, during a set-up phase, the client specifies the size n of the computation and receives an untrusted, \emph{off-the-shelf (OTS)} quantum device that is used to report the outcome of a single constant-sized measurement from a predetermined logarithmic-sized input. In the OTS model, we thus picture that a single quantum server does the bulk of the computations, while the OTS device is used as an untrusted and generic verification device, all in a single round. We show how to delegate polynomial-time quantum computations in the OTS model. Scaling up the technique also yields an interactive proof system for all of QMA, which, furthermore, we show can be accomplished in statistical zero-knowledge. This yields the first relativistic (one-round), two-prover zero-knowledge proof system for QMA. A

As a proof approach, we provide a new self-test for n-EPR pairs using only constant-sized Pauli measurements, and show how it provides a new avenue for the use of simulatable codes for local Hamiltonian verification. Along the way, we also provide an enhanced version of a well-known stability result due to Gowers and Hatami and show how it completes a common argument used in self-testing.

Poster Session 1: 4:30–6 p.m.

A Practical Transmitter Device for Passive State BB84

Yury Kurochkin, Marios Papadovasilakis and James Grieve (Technology Innovation Institute)

Reference-Frame-Independent Quantum Communication Among Multiple Parties

Donghwa Lee, Kyujin Shin, Hyang-Tag Lim, Yosep Kim and Yong-Su Kim (Korea Institute of Science and Technology)

Powerful Primitives in the Bounded Quantum Storage Model

Mohammed Barhoush and Louis Salvail (University of Montreal)

On the Two-Sided Permutation Inversion Problem

Gorjan Alagic (University of Maryland and the National Institute of Standards and Technology); Chen Bai (University of Maryland); Alexander Poremba (Caltech); and Kaiyan Shi (University of Maryland)

Uncloneable Cryptographic Primitives with Interaction

Anne Broadbent (University of Ottawa) and Eric Culf (University of Waterloo)

Eavesdropper Localization in Quantum Channels Using Stimulated Brillouin Scattering

Alexandra Popp (Max Planck Institute for the Science of Light); Florian Sedlmeir (University of Otago); Birgit Stiller (Max Planck Institute for the Science of Light); and Christoph Marquardt (Friedrich-Alexander-Universität Erlangen-Nürnberg)

Access-Controlled Entanglement Source Against Memory Attack in Quantum Cryptography

Haoyang Wang (Beijing University of Posts and Telecommunications); Qiang Zeng (Beijing Academy of Quantum Information Sciences); Huihong Yuan (Beijing Academy of Quantum Information Sciences); Yuanbin Fan (Beijing Academy of Quantum Information Sciences); Lai Zhou (Beijing Academy of Quantum Information Sciences); Yuanfei Gao (Beijing Academy of Quantum Information Sciences); Haiqiang Ma (Beijing University of Posts and Telecommunications); and Zhiliang Yuan (Beijing Academy of Quantum Information Sciences)

Fundamental Limits on Quantum Cloning From the No-Signalling Principle

Yanglin Hu (National University of Singapore, Centre for Quantum Technologies) and Marco Tomamichel (National University of Singapore)

Finite Key Performance of Satellite Quantum Key Distribution Under Practical Constraints

Jasminder S. Sidhu, Thomas rougham, Duncan McArthur, Roberto G. Pousa and Daniel K. L. Oi (University of Strathclyde)

Real-world Data Encryption With Continuous-Variable Measurement Device-Independent Quantum Key Distribution

Adnan A.E. Hajomer, Ulrik L. Andersen and Tobias Gehring (Technical University of Denmark)

Interactive Oracle Arguments in the QROM and Applications to Succinct Verification of Quantum Computation

Islam Faisal (Boston University)

Unifying Quantum Verification and Error-Detection: Theory and Tools for Optimisations

Theodo os Kapourniotis (University of Warwick); Elham Kashefi (LIP6, Sorbonne niversity; University of Edinburgh); Dominik Leichtle (LIP6, Sorbonne University); Luka Music (Quandela); and Harold Ollivier (INRIA Paris)

Comparative Analysis of Hybrid Quantum Error Correction (QEC)-Quantum Key Distribution (QKD) Protocols: Technical Considerations, Efficiency and Feasibility.

Aida García-Callejo, Andrés Ruiz-Chamorro, Pablo Arteaga, Daniel Cano and Verónica Fernández (Spanish National Research Council)

Sample-Size-Reduction of Quantum States for the Noisy Linear Problem and Approximate QRAM

Kabgyun Jeong (Seoul National University)

Multi-User Continuous-Variable Quantum Key Distribution with Discrete Modulation

Florian Kanitschar (Technische Universität Wien & AIT Austrian Institute of Technology) and Christoph Pacher (AIT Austrian Institute of Technology & FragmentiX Storage Solution GmbH)

Advantage of the Key Relay Protocol Over Secure Network Coding

Go Kato (National Institute of Information and Communications Technology); Mikio Fujiwara (National Institute of Information and Communications Technology); and Toyohiro Tsurumaru (Mitsubishi Electric Corporation)

Experimental Demonstration of a QKD Platform Over Long-distance-, Metro-, and Last-mile Links

Jan Krause, Nino Walenta, Benedikt Lezius, Richard Schilling and Ronald Freund (Fraunhofer Institute for Telecommunications, Heinrich Hertz Institute)

Twin-Field Quantum Key Distribution in Network Configurations

Carlo Liorni (Leonardo Labs Quantum Technologies); Gianluca Bertaina (INRIM); Cecilia Clivati (INRIM); Simone Donadello (INRIM); Alice Meda (INRIM); Salvatore Virzi' (INRIM); Marco Gramegna (INRIM); Ulpiani Pierfrancesco (Leonardo Labs Quantum Technologies); Ivo Pietro Degiovanni (INRIM); and Massimiliano Dispenza (Leonardo Labs Quantum Technologies)

Twin-Field Quantum Key Distribution with Three Mutually Unbiased Bases

Yao Zhou (CAS Key Laboratory of Quantum Information, USTC); Zhen-Qiang Yin (CAS Key Laboratory of Quantum Information, USTC)

Impossibility of Probabilistic Quantum Private Queries

Silvia Onofri and Vittorio Giovannetti (Scuola Normale Superiore)

Interoperable Key Relay Between Heterogeneous QKDNs

Mayuko Koezuka (Toshiba Corporation); Ririka Takahashi (Toshiba Corporation); Yoshimichi Tanizawa (Toshiba Corporation); Yasuhiro Fujiyoshi (Toshiba Corporation); Yasuhiro Katsube (Toshiba Corporation); Hideaki Sato (Toshiba Corporation); Masanori Suzuki (NEC Corporation); Kazushi Sugyo (NEC Corporation); Takao Ochi (NEC Corporation); Kaoru Kenyoshi (National Institute of Information and Communications Technology); Mikio Fujiwara (National Institute of Information and Communications Technology); and Masahide Sasaki (National Institute of Information and Communications Technology)

Effect of Kalman Filter on Coarse Tracking System for Quantum Key Distribution System Moving at Constant Velocity

Minchul Kim, Kyongchun Lim, Byung-seok Choi, Joong-Seon Choe, Kap-Joong Kim, Ju Hee Baek, Young-Ho Ko and Chun Ju Youn (Electronics and Telecommunications Research Institute)

Pre-Privacy Amplification: A Method to Boost Key Rate in Resource Constrained Environments

John Burniston and Norbert Lütkenhaus (University of Waterloo)

Authentication in Secure Delegated Quantum Computation Based on Quantum Trusted Execution Environment

M. Prem Laxman Das and Natarajan Venkatachalam (Society For Electronic Transactions and Security, Chennai)

Feasibility of Distributing Composable Keys With Discrete-modulated Continuous Variable Quantum Cryptography

Nitin Jain (Technical University of Denmark); Florian Kanitschar (Vienna Center for Quantum Science and Technology); Adnan A.E. Hajomer (Technical University of Denmark); Ulrik L. Andersen (Technical University of Denmark); Christoph Pacher (AIT Austrian Institute of Technology); and Tobias Gehring (Technical University of Denmark)

Semi-Quantum Copy-Protection and More

Céline Chevalier (CRED, DIENS); Paul Hermouet (CRED, DIENS, LIP6); and Quoc Huy Vu (LIP6)

Finite-Size Effects of Decoy State Methods

Lars Kamin, Scott Johnstun and Norbert Lütkenhaus (University of Waterloo)

Experimental Anonymous Quantum Conference Key Agreement

Jonathan Webb (Heriot-Watt University); Joseph Ho (Heriot-Watt University); Federico Grasselli (Heinrich-Heine-Universitat Dusseldorf); Glaucia Murta (Heinrich-Heine-Universitat Dusseldorf); Alexander Pickston (Heriot-Watt University); and Andres Ulibarrena (Heriot-Watt University); Alessandro Fedrizzi (Heriot-Watt University)

Time-Resolved Quantum Key Distribution Using Semiconductor Quantum Dots With Oscillating Photonic States

Matteo Pennacchietti (Institute for Quantum Computing, University of Waterloo); Brady Cunard (Institute for Quantum Computing, University of Waterloo); Mohd Zeeshan (National Research Council of Canada); Shlok Nahar (Institute for Quantum Computing, University of Waterloo); Sayan Gangopadhyay (University of Waterloo, IQC); Philip J. Poole (National Research Council of Canada); Dan Dalacu (National Research Council of Canada); Andreas Fognini (Single Quantum B.V.); Klaus Jöns (Institute for Photonic Quantum Systems, Center for Optoelectronics and Photonics Paderborn and Department of Physics, Paderborn University); Val Zwiller (Department of Applied Physics, Royal Institute of Technology); Thomas ennewein (Institute for Quantum Computing, University of Waterloo); Norbert Lütkenhaus (Institute for Quantum Computing, University of Waterloo); and Michael E. Reimer (Institute for Quantum Computing, University of Waterloo)

Using Cascade in Quantum Key Distribution

Devashish Tupkary and Norbert Lutkenhaus (Institute for Quantum Computing, University of Waterloo)

Simple Active Polarization Stabilizer for Practical Fiber-Based Quantum Key Distribution

Kyongchun Lim, Byung-Seok Choi, Ju Hee Baek, Minchul Kim, Joong-Seon Choe, Kap-Joong Kim, Dong Churl Kim and Chun Ju Youn (Electronics and Telecommunications Research Institute)

Continuous Fiber Polarization Stabilization With Single-Photon-Level Light

Yicheng Shi (National Institute of Standards and Technology)

Demonstration of Free-Space Discrete-Modulated Continuous-Variable QKD Using Real Error Correction Codes and Finite-Size Effects

Kevin Jaksch (Max Planck Institute for the Science of Light, Erlangen and Friedrich-Alexander-Universität Erlangen-Nürnberg); Thomas Di meier (Max Planck Institute for the Science of Light, Erlangen and Friedrich-Alexander-Universität Erlangen-Nürnberg); Yannick Weiser (Max Planck Institute for the Science of Light, Erlangen and Friedrich-Alexander-Universität Erlangen-Nürnberg); Stefan Richter (Max Planck Institute for the Science of Light, Erlangen and Friedrich-Alexander-Universität Erlangen-Nürnberg); Ömer Bayraktar (Max Planck Institute for the Science of Light, Erlangen and Friedrich-Alexander-Universität Erlangen-Nürnberg); Bastian Hacker (Max Planck Institute for the Science of Light, Erlangen and Friedrich-Alexander-Universität Erlangen-Nürnberg); Conrad Rößler (Max Planck Institute for the Science of Light, Erlangen, Germany + Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany); Imran Khan (Max Planck Institute for the Science of Light, Erlangen and Friedrich-Alexander-Universität Erlangen-Nürnberg); Stefan Petscharning (Austrian Institute of Technology, Center for Digital Safety & Security); Thomas rafenauer (Austrian Institute of Technology, Center for Digital Safety & Security); Bernhard Ömer (Austrian Institute of Technology, Center for Digital Safety & Security); Christoph Pacher (Austrian Institute of Technology, Center for Digital Safety & Security); Florian Kanitschar (Austrian Institute of Technology, Center for Digital Safety & Security and Vienna Center for Quantum Science and Technology; Technische Universität Wien; and Institute for Quantum Computing, University of Waterloo); Twesh Upadhyaya (Institute for Quantum Computing, University of Waterloo); Jie Lin (Institute for Quantum Computing, University of Waterloo); Norbert Lütkenhaus (Institute for Quantum Computing, University of Waterloo); Gerd Leuchs (Max Planck Institute for the Science of Light, Erlangen and Friedrich-Alexander-Universität Erlangen-Nürnberg); and Christoph Marquardt (Max Planck Institute for the Science of Light, Erlangen and Friedrich-Alexander-Universität Erlangen-Nürnberg)

Characterising Higher-Order Phase Correlations in Gain-Switched Laser Sources With Application to Decoy-State QKD

Alessandro Marcomini, Guillermo Currás-Lorenzo, Davide Rusca and Marcos Curty (Vigo Quantum Communication Center)

CHSH Inequality Violation in Experimental Entanglement Based QRNG Validation

Witold Jacak (Wroclaw University of Science and Technology); Piotr Jóźwiak (Wroclaw University of Science and Technology); Janusz Jacak (Wroclaw University of Science and Technology, Poland); Wojciech Donderowicz (CompSecur and SeQre)

Robust Global Quantum Networks

Jan-Michael Mol, Kaisa Laiho, Davide Orsucci, Philipp Kleinpass, Florian Moll, Jaspar Meister, Waldemar Herr, Christian Schubert, Jens Kruse and Carsten Klempt and Lisa Wörner (German Aerospace Center)

Unprovable Security of Statistical NIZK in the Quantum Setting

Chuhan Lu and Nikhil Pappu (Portland State University)

Poster Session 2: 4:30–6 p.m.

Effect of Light Injection on the Security of Practical Quantum Key Distribution

Liying Han, Yang Li, Hao Tan, Weiyang Zhang, Wenqi Cai, Juan Yin, Jigang Ren, Feihu Xu, Shengkai Liao and Chengzhi Peng (University of Science and Technology of China)

Implementation of a Privacy Preserving Publicly Verifiable Quantum Random Number Generator

Tanvirul Islam (CQT, National University of Singapore); Anindya Banerji (CQT, National University of Singapore); Chin Jia Boon (CQT, National University of Singapore); Wang Rui (CQT, National University of Singapore); Ayesha Reezwana (CQT, National University of Singapore); James A. Grieve (Quantum Research Centre, Technology Innovation Institute, Abu Dhabi); Rodrigo Piera (Quantum Research Centre, Technology Innovation Institute, Abu Dhabi); and Alexander Ling (Department of Physics and CQT, National University of Singapore)

General Treatment of Trusted Gaussian Noise in Continuous Variable Quantum Key Distribution

Shinichiro Yamano (University of Tokyo); Takaya Matsuura (RMIT University); Yui Kuramochi (Kyushu University); Toshihiko Sasaki (University of Tokyo); and Masato Koashi (University of Tokyo)

Lattice-Based Quantum Advantage From Rotated Measurements

Yusuf Alnawakhtha (University of Maryland); Atul Mantri (University of Maryland); Carl Miller (University of Maryland and National Institute of Standards and Technology); and Daochen Wang (University of Maryland)
Robustness of Implemented Device-Independent Protocols and Device-Dependent QKD Against Constrained Leakage
Ernest Y.-Z. Tan (University of Waterloo)

Robustness of Implemented Device-Independent Protocols and Device-Dependent QKD Against Constrained Leakage

Ernest Y.-Z. Tan (University of Waterloo)

Device-Independent Uncloneable Encryption

Srijita Kundu and Ernest Y.-Z. Tan (University of Waterloo)

Efficient Polar Encoding for Information Reconciliation in QKD

Snehasis Addy, Somnath Panja, Sabyasachi Dutta, Daniel Oblak and Reihaneh Safavi-Naini (University of Calgary)

Sampled Sub-Block Hashing for Large Input Randomness Extraction

Hong Jie Ng, Wen Yu Kon, Ignatius William Primaatmaja, Chao Wang and Charles Lim (National University of Singapore)

Parameter Optimisation for CV-QKD with Arbitrary Modulation

João dos Reis Frazão, Aaron Albores-Mejia, Boris Škorić, and Chigo Okonkwo (Eindhoven University of Technology)

Simulation of Device-Independent Quantum Key Distribution Protocols

Ottó Hanyecz (Eötvös Loránd University and Wigner Research Centre for Physics) and Mátyás Koniorczyk (Wigner Research Centre for Physics)

Establishing Shared Secret Keys on Quantum Line Networks: Protocol and Security

Mina Doosti (University of Edinburgh); Lucas Hanouz (VeriQloud); Anne Marin (VeriQloud); Elham Kashefi (University of Edinburgh); and Marc Kaplan (VeriQloud)

Implementation of a Multiplexed Quantum Key Distribution System Simulator With a Detailed Secure Key Generation Model

Masashi Ito (Corporate Research and Development Center, Toshiba Corporation); Yutaro Ishigaki (Corporate Research and Development Center, Toshiba Corporation); Keisuke Mera (Corporate Research and Development Center, Toshiba Corporation); Yoshimichi Tanizawa (Corporate Research and Development Center, Toshiba Corporation); Taofiq K. Paraiso (Cambridge Research Laboratory, Toshiba Euro Limited); Katsuyuki Kimura (Corporate Research and Development Center, Toshiba Corporation); Koji Kanazawa (Corporate Research and Development Center, Toshiba Corporation); Andrew J. Shields (Cambridge Research Laboratory, Toshiba Euro Limited)

Practical High-Dimensional Quantum Key Distribution Protocol Over Deployed Multicore Fiber

Mujtaba Zahidy (Technical University of Denmark); Domenico Ribezzo (University of Naples Federico II); Claudia De Lazzari (QTI S.r.l.); Ilaria Vagniluca (QTI S.r.l.); Nicola Biagi (QTI S.r.l.); Tommaso Occhipinti (QTI S.r.l.); Leif K. Oxenlowe (Technical University of Denmark); Michael Galili (Technical University of Denmark); Tetsuya Hayashi (Optical Communications Laboratory, Sumitomo Electric Industries, Ltd.); Dajana Cassioli (University of L'Aquila); Antonio Mecozzi (University of L'Aquila); Cristian Antonelli (University of L'Aquila); Alessandro Zavatta (Istituto Nazionale di Ottica, Consiglio Nazionale delle Ricerche); and Davide Bacco (University of Florence)

Long-Distance Continuous-Variable Quantum Key Distribution Over 100 km Fiber With Local Local Oscillator

Adnan Hajomer, Ivan Derkach, Nitin Jain, Hou-Man Chin, Ulrik L. Andersen and Tobias Gehring (Technical University of Denmark)

Asymmetric Quantum Secure Multi-Party Computation With Weak Clients Against Dishonest Majority

Theodo os Kapourniotis (University of Warwick); Elham Kashefi (niversity of Edinburgh; LIP6, Sorbonne Université); Dominik Leichtle (LIP6, Sorbonne Université); Luka Music (Quandela); Harold Ollivier (DIENS, Ecole Normale Supérieure, INRIA)

Quantum Cryptanalysis of Affine Cipher

Mahima Mary Mathews and Panchami V (Indian Institute of Information Technology, Kottayam)

High-Dimensional Quantum Key Distribution Using Time-Bin Entanglement

Florian Kanitschar, Alexandra Bergmayr, Matej Pivoluska and Marcus Huber (Technische Universität Wien)

On Zero-Knowledge Proofs Over the Quantum Internet

Mark Carney (Quantum Village Inc.)

Maximal Device-Independent Randomness Certification by More Than Two Observers Through Bipartite Bell Tests

Lewis Wooltorton (University of York, UK); Peter Brown (Télécom Paris, France); and Roger Colbeck (University of York, UK)

An Optical Ground Station in Singapore for Satellite-to-ground Quantum Communication

Ayesha Reezwana, Moritz Mihm, Xi Wang, Karabee Batta and Alexander Ling (CQT, National University of Singapore)

Procrustean Entanglement Concentration for Quantum-classical Coexistence

Hsuan-Hao Lu (Oak Ridge National Laboratory); Muneer Alshowkan (Oak Ridge National Laboratory); Jude Alnas (Duke University); Joseph M. Lukens (Arizona State University); and Nicholas A. Peters (Oak Ridge National Laboratory)

Measurement Device-Independent Quantum Key Distribution With Vortex Vector Modes Under Diverse Weather Conditions

Mhlambululi Mafu (Case Western Reserve University) and Comfort Sekga (Botswana International University of Science and Technology)

A Simple and Self-Testing Quantum Random Number Generator

Fadri Grünenfelder, Ana Blázquez, Davide Rusca and Hugo Zbinden (University of Vigo)

Taking Quantum Key Distribution From Fundamental Science to Accredited Systems in Space

Philipp Sohr (Vienna University of Technology; Quantum Technology Laboratories GmbH); Matej Pivoluska (Vienna University of Technology; Quantum Technology Laboratories GmbH); Sebastian Ecker (Quantum Technology Laboratories GmbH); Manuel Erhard (Quantum Technology Laboratories GmbH)

Security of Partially Corrupted Repeater Chains
Walter Krawec (University of Connecticut); Adrian Harkness (Lehigh University); and Bing Wang (University of Connecticut)

Finite-Size Analysis of Prepare-and-Measure and Decoy-State Quantum Key Distribution via Entropy Accumulation
Lars Kamin (Institute for Quantum Computing, University of Waterloo); Amir Arqand (Institute for Quantum Computing, University of Waterloo); Ian George (University of Illinois Urbana-Champaign); Jie Lin (University of Toronto); Norbert Lutkenhaus (University of Waterloo) and Ernest Y.-Z. Tan (Institute for Quantum Computing, University of Waterloo)

Practical Implementation of a Simplified BB84 Protocol Resilient to Source Imperfections
Ana Blázquez Coído, Fadri Grünenfelder, Hugo Zbinden and Davide Rusca (Vigo Quantum Communication Center)

Quantum Secure Direct Communication With Private Dense Coding Using General Preshared Quantum State
Jiawei Wu (National University of Singapore); Gui-Lu Long (Tsinghua University); and Masahito Hayashi (the Chinese University of Hong Kong)

An Efficient Method for Certifying Quantum Properties With Non-i.i.d. Spot-checking Trials
Yanbao Zhang (Oak Ridge National Lab); Akshay Seshadri (University of Colorado Boulder); and Emanuel Knill (National Institute of Standards and Technology-Boulder)

FPGA-Based LED Source with Indistinguishable States for Decoy State QKD
Daniel Sanchez Rosales, Roderick D. Cochran and Daniel J. Gauthier (Ohio State University)

Qubit-based Clock Synchronization Using a Bayesian Approach Applied to Drone-Based QKD Systems
Roderick D. Cochran and Daniel J. Gauthier (Ohio State University)

Analysis of a High-dimensional Restricted Quantum Key Distribution Protocol
Hasan Iqbal and Walter Krawec (University of Connecticut)

Postselection Technique for Optical Prepare-and-measure QKD Protocols
Devashish Tupkary, Shlok Nahar, Yuming Zhao, Norbert Lutkenhaus and Ernest Tan (Institute for Quantum Computing, University of Waterloo)

Impact of Multiphoton States in Entangled Photon Distribution
Jin-Woo Kim, Junsang Oh, Heonoh Kim and June-Koo Kevin Rhee (KAIST, Daejeon 34141)

Reliable Lower Bounds for Practical Variants of Coherent One-Way Protocols
Shihong Pan, Shlok Ashok Nahar, John Burniston and Norbert Lütkenhaus (Institute for Quantum Computing, University of Waterloo)

Separating SNARGs From Falsifiable Assumptions in the Quantum Setting
Chuhan Lu and Nikhil Pappu (Portland State University)

Quantum Randomness From Untrusted Light Using a Single Photodiode
Runjia Zhang, Bradley Longstaff, Kie an Wilkinson, Jonatan Bohr Brask and Tobias Gehring (Center for Macroscopic Quantum States, Technical University of Denmark)

Experimental Investigation of Residual Phase Impact on CV-QKD
Hou-Man Chin, Ulrik L. Andersen and Tobias Gehring (Technical University of Denmark)

New Concepts and Construction of Quantum Random Number Generators
Witold Jacak and Piotr Jóźwiak (Wroclaw University of Science and Technology)

The Quantum Chernoff Divergence in Advantage Distillation for QKD and DIQKD
Mikka Stasiuk, Norbert Lutkenhaus and Ernest Y.-Z. Tan (Institute for Quantum Computing, University of Waterloo)

Quantum Key Distribution With Multiple Photon Number Distributions

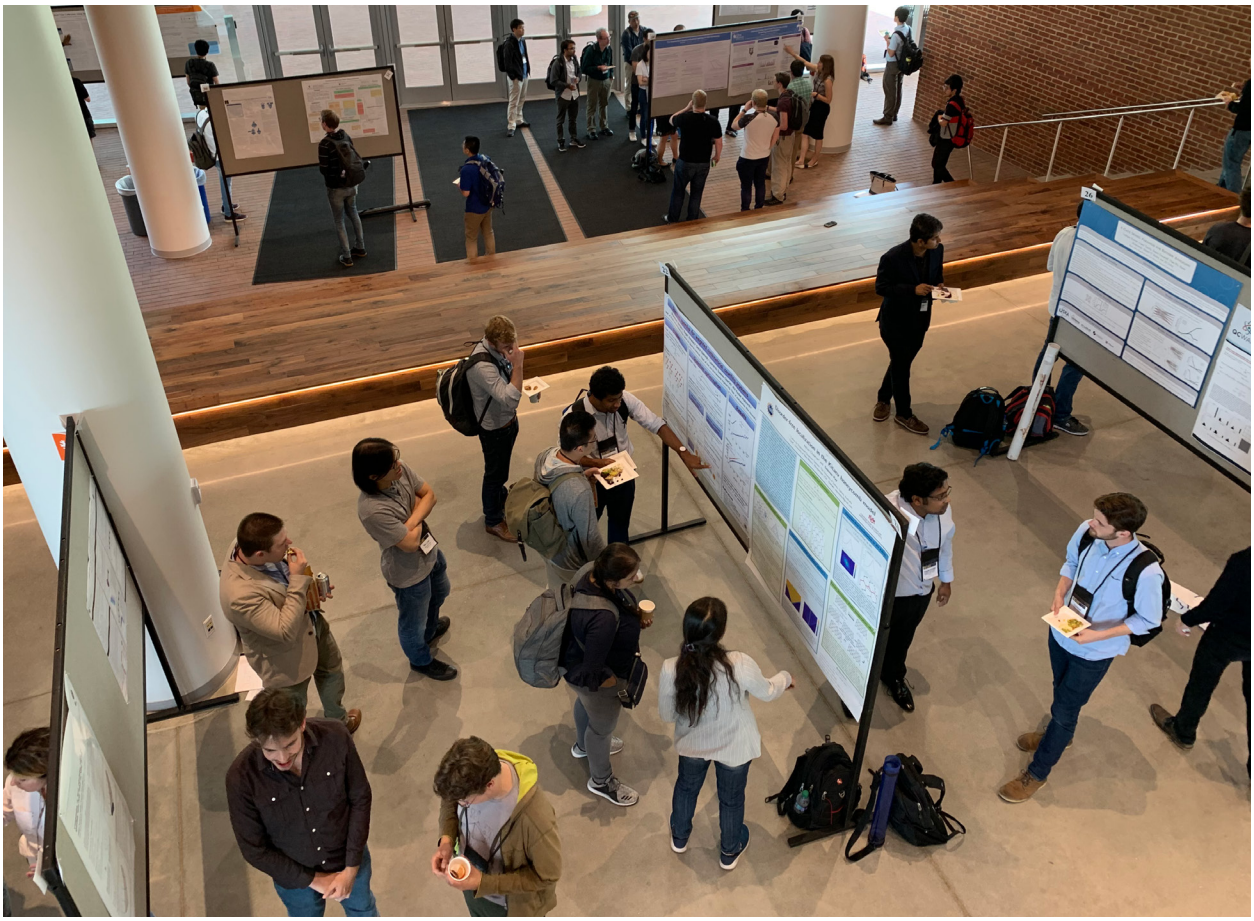
Roberto G. Pousa, Daniel Oi and John Jeffers (niversity of Strathclyde)

Time-Bin Entanglement Swapping

Samantha I. Davis (Alliance for Quantum Technologies, California Institute of Technology); Rahaf Youssef (Alliance for Quantum Technologies, California Institute of Technology); Raju Valivarthi (Alliance for Quantum Technologies, California Institute of Technology); Lautaro Narváez (Alliance for Quantum Technologies, California Institute of Technology); Neil Sinclair (Alliance for Quantum Technologies, California Institute of Technology and John A. Paulson School of Engineering and Applied Sciences, Harvard University); Cristián Peña (Alliance for Quantum Technologies, California Institute of Technology and Fermi National Accelerator Laboratory); Si Xie (Alliance for Quantum Technologies, California Institute of Technology and Fermi National Accelerator Laboratory); Boris Korzh (Jet Propulsion Laboratory); Matthew Shaw (Jet Propulsion Laboratory); Panagiotis Spentzouris (Fermi National Accelerator Laboratory); and Maria Spiropulu (Alliance for Quantum Technologies, California Institute of Technology)

Generation of Time-Bin GHZ States

Samantha I. Davis (Alliance for Quantum Technologies, California Institute of Technology); Chang Li (Alliance for Quantum Technologies, California Institute of Technology); Neil Sinclair (Alliance for Quantum Technologies, California Institute of Technology and John A. Paulson School of Engineering and Applied Sciences, Harvard University); Raju Valvarthi (Alliance for Quantum Technologies, California Institute of Technology); and Maria Spiropulu (Alliance for Quantum Technologies, California Institute of Technology)



This year's conference is proudly organized by the
Joint Center for Quantum Information and Computer Science
at the University of Maryland
and the National Institute of Standards and Technology.

QuICS JOINT CENTER FOR QUANTUM INFORMATION AND COMPUTER SCIENCE

quics.umd.edu

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

nist.gov