List of Poster Presentations and Panel Installation Numbering

[2] *Entropy bounds for device-independent quantum key distribution with local Bell test*

Ernest Y.-Z. Tan (Institute for Quantum Computing, University of Waterloo) and Ramona Wolf (ETH Zürich and Universität Siegen).

One of the main challenges in device-independent quantum key distribution (DIQKD) is achieving the required Bell violation over long distances, as the channel losses result in low overall detection efficiencies. Recent works have explored the concept of certifying nonlocal correlations over extended distances through the use of a local Bell test. Here, an additional quantum device is placed in close proximity to one party, using short-distance correlations to verify nonlocal behavior at long distances. However, existing works have either not resolved the question of DIQKD security against active attackers in this setup, or used methods that do not yield tight bounds on the keyrates. In this work, we introduce a general formulation of the key rate computation task in this setup that can be combined with recently developed methods for analyzing standard DIQKD. Using this method, we show that if the short-distance devices exhibit sufficiently high detection efficiencies, positive key rates can be achieved in the long-distance branch with lower detection efficiencies as compared to standard DIQKD setups. This highlights the potential for improved performance of DIQKD over extended distances in scenarios where short-distance correlations are leveraged to validate quantum correlations.

[3] *Photonic Device-Independent Quantum Key Distribution*

Corentin Lanore (IPhT - CEA), Xavier Valcarce (IPhT - CEA), Jean Etesse (Université Côté d'Azur, Institut de Physique de Nice (INPHYNI)), Anthony Martin (Université Côté d'Azur, Institut de Physique de Nice (INPHYNI)), Jean-Daniel Bancal (IPhT - CEA) and Nicolas Sangouard (IPhT - CEA).

Quantum Key Distribution (QKD) enables the expansion of cryptographic keys between two parties, allowing for proven secure communication. The main downside of QKD protocols is their vulnerability to attacks that target the physical implementation. Device Independent Quantum Key Distribution (DIQKD) is a new paradigm addressing this issue by relaxing assumptions on the physical implementation. First DIQKD experiments were reported in 2022, proving the feasibility of DIQKD. However, these experiences required highly sophisticated setups. Here, we analyse the suitability of a novel optical implementation for DIQKD. Our results show that DIQKD could be realized with a simple setup using only commercially available hardware.

[4] *Signatures From Pseudorandom States via $\perp$-PRFs*

Mohammed Barhoush (Université de Montréal (DIRO), Montréal, Canada), Amit Behera (Ben-Gurion University of the Negev, Beersheba, Israel), Lior Ozer (Ben-Gurion University of the Negev, Beersheba, Israel), Louis Salvail (Université de Montréal (DIRO), Montréal, Canada) and Or Sattath (Ben-Gurion University of the Negev, Beersheba, Israel).

Different flavors of quantum pseudorandomness have proven useful for various cryptographic applications, with the compelling feature that these primitives are potentially weaker than post-quantum one-way functions. Ananth, Lin, and Yuen (2023) have shown that logarithmic pseudorandom states can be used to construct a pseudo-deterministic PRG: informally, for a fixed seed, the output is the same with $1 - 1/\text{poly}$ probability. In this work, we introduce new definitions for $\perp$-PRG and $\perp$-PRF. The correctness guarantees are that, for a fixed seed, except with negligible probability, the output is either the same (with probability $1 - 1/\text{poly}$) or recognizable abort, denoted $\perp$. Our approach admits a natural definition of multi-time PRG security, as well as the adaptive security of a PRF. We construct a $\perp$-PRG from any pseudo-deterministic PRG and, from that, a $\perp$-PRF. Even though most mini-crypt primitives, such as symmetric key encryption, commitments, MAC, and length-restricted one-time digital signatures, have been shown based on various quantum pseudorandomness assumptions, digital signatures remained elusive. Our main application is a (quantum) digital signature scheme with classical public keys and signatures, thereby addressing a previously unresolved question posed in

Morimae and Yamakawa's work (Crypto, 2022). Additionally, we construct CPA secure public-key encryption with tamper-resilient quantum public keys.

[5] *Certification of a commercial quantum key distribution system against implementation loopholes*

Vadim Makarov (Russian quantum center; Vigo quantum communication center), Alexey Abrikosov (Russian quantum center), Poompong Chaiwongkhot (Mahidol University), Aleksey K. Fedorov (Russian quantum center), Anqi Huang (National University of Defense Technology), Evgeny Kiktenko (Russian quantum center), Mikhail Petrov (Vigo quantum communication center), Anastasiya Ponosova (Russian quantum center), Daria Ruzhitskaya (Russian quantum center), Andrey Tayduganov (National University of Science and Technology MISiS), Daniil Trefilov (Vigo quantum communication center) and Konstantin Zaitsev (Vigo quantum communication center).

We report recent advances in the development of certification for quantum key distribution (QKD) systems. We give an example of a commercial QKD system that we have analysed for possible loopholes, improved to close the vulnerabilities identified, and designed a set of tests for that can be used by a certification lab [arXiv:2310.20107]. We explain some of the testbenches in this lab, such as an ultrawide spectral characterisation testbench, automated detector testing, and laser damage testbench that verifies the quality of a power limiter. This work is in line with the requirements of the ISO standard for QKD and paves the way for the creation of certification services.

[6] *Clock offset synchronization with sublinear complexity for quantum key distribution on low-level hardware*

Jan Krause (Fraunhofer Institute for Telecommunications, Heinrich-Hertz-Institut, HHI, 10587 Berlin, Germany), Nino Walenta (Fraunhofer Institute for Telecommunications, Heinrich-Hertz-Institut, HHI, 10587 Berlin, Germany), Jonas Hilt (Fraunhofer Institute for Telecommunications, Heinrich-Hertz-Institut, HHI, 10587 Berlin, Germany) and Ronald Freund (Fraunhofer Institute for Telecommunications, Heinrich-Hertz-Institut, HHI, 10587 Berlin, Germany).

We present iQSync, a novel clock offset recovery method for quantum key distribution. Our method is specifically tailored towards low-level hardware implementations, e.g. on FPGAs or microcontrollers, and requires only very little RAM and basic CPU instructions, like additions and bit-shifts. No floating-point operations, as is the case for FFT-based approaches, are needed. Offset revovery with iQSync typically only requires a few thousand iterations over a simple loop and evaluates with sublinear average-case computational complexity, improving on previous results with super-linear complexity. We implemented our method on our real-time QKD platform and demonstrate excellent agreement with theoretically derived success probabilities for channel attenuations exceeding 70 dB.

[7] *Quantum Unpredictability*

Tomoyuki Morimae (Yukawa Institute for Theoretical Physics, Kyoto University), Shogo Yamada (Yukawa Institute for Theoritical Phisics, Kyoto University) and Takashi Yamakawa (NTT Social Informatics Laboratories).

Unpredictable functions (UPFs) play essential roles in classical cryptography, including message authentication codes (MACs) and digital signatures. In this paper, we introduce a quantum analog of UPFs, which we call unpredictable state generators (UPSGs). UPSGs are implied by pseudorandom function-like states generators (PRFSs), which are a quantum analog of pseudorandom functions (PRFs), and therefore UPSGs could exist even if one-way functions do not exist, similar to other recently introduced primitives like pseudorandom state generators (PRSGs), one-way state generators (OWSGs), and EFIs. In classical cryptography, UPFs are equivalent to PRFs, but in the quantum case, the equivalence is not clear, and UPSGs could be weaker than PRFSs. Despite this, we demonstrate that all known applications of PRFSs are also achievable with UPSGs. They include IND-CPA-secure secret-key encryption and EUF-CMA-secure MACs with unclonable tags. Our findings suggest that, for many applications, quantum unpredictability, rather than quantum pseudorandomness, is sufficient.

[8] *A Black-box Attack on Fixed-Unitary Quantum Encryption Schemes*

Cezary Pilaszewicz (Freie Universität Berlin), Lea R. Muth (Freie Universität Berlin) and Marian Margraf (Freie Universität Berlin).

We show how fixed-unitary quantum encryption schemes can be attacked in a black-box setting. We use an efficient technique to invert a unitary transformation on a quantum computer to retrieve an encrypted secret quantum state $ \ket{\psi}$. This attack has a success rate of 100\% and can be executed in constant time. We name a vulnerable scheme and suggest how to improve it to invalidate this attack. The proposed attack highlights the importance of carefully designing quantum encryption schemes to ensure their security against quantum adversaries, even in a black-box setting.

[10] *Seedless extractors for device-independent quantum cryptography*

Cameron Foreman (University College London &amp; Quantinuum) and Lluis Masanes (University College London).

Device-independent (DI) quantum cryptography aims at providing secure cryptography with minimal trust in, or characterisation of, the underlying quantum devices. An essential step in DI protocols is randomness extraction (or privacy amplification) which requires the honest parties to have a seed of additional bits with sufficient entropy and statistical independence of any bits generated during the protocol. In this work we introduce a method for extraction in DI protocols which does not require a seed and is secure against computationally unbounded quantum adversary. The key idea is to use the Bell violation of the raw data, instead of its min-entropy, as the extractor promise.

[12] *Randomness extractors for quantum cryptography and an analysis of their effect using statistical testing*

Cameron Foreman (University College London & Quantinuum), Richie Yeung (University of Oxford & Quantinuum), Alec Edgington (Cambridge Quantum Computing) and Florian Curchod (Quantinuum).

Randomness extractors are an essential component in numerous applications, for example, for privacy amplification in quantum key distribution and randomness extraction in random number generation. Despite their importance, selecting, optimising and implementing the appropriate extractor and parameters requires significant expertise and time investment. We present Cryptomite, a publicly available software library that provides a variety of two-source, seeded, and deterministic randomness extractor implementations with state-of-the-art performance. The software is efficient, numerically precise and capable of handling input sizes up to $10^{12}$, allowing for use even in resource intensive protocols, e.g. device-independent ones. Alongside the software, we provide theoretical contributions that include improvements and generalisations to existing extractors, new extractor constructions and parameter calculation in a variety of useful security models. To showcase the library, we empirically compare the properties of the output of several random number generators and the effect of different randomness extraction methods on it, using intense statistical testing.

[13] *Security of Multi-User Quantum Key Distribution with Discrete Modulation*

Florian Kanitschar (TU Wien) and Christoph Pacher (Austrian Institute of Technology & fragmentiX storage solutions).

The conventional point-to-point setting of Quantum Key Distribution (QKD) typically considers two directly connected remote parties that aim to establish secret keys. However, almost all digital communication tasks involve multiple nodes and complex network architectures. Thus, it is essential to adapt and integrate QKD protocols and their security analyses to accommodate these complex environments and ensure secure communication across interconnected systems. This work proposes a natural generalization of a well-established point-to-point discrete modulated (DM) continuous-variable (CV) QKD protocol to the multi-party setting. We explore four different trust levels among the communicating parties and provide secure key rates in lossy and noisy channels. Our study shows that discrete modulated CV-QKD is a suitable candidate to connect several dozens of users in a point-to-multipoint network, achieving high rates at low cost, using off-the-shelf components employed in modern communication infrastructure.

[15] *Noise-tolerant public-key quantum money from a classical oracle*

Peter Yuen (University of Ottawa).

Quantum money is the task of verifying the validity of banknotes while ensuring that they cannot be counterfeited. Public-key quantum money allows anyone to perform verification, while the private-key setting restricts the ability to verify to banks, as in Wiesner's original scheme. The current state of technological progress means that errors are impossible to entirely suppress, hence the requirement for noise-tolerant schemes. We show for the first time how to achieve noise-tolerance in the public-key setting. Our techniques follow Aaronson and Christiano's oracle model, where we use the ideas of quantum error correction to extend their scheme: a valid banknote is now a subspace state possibly affected by noise, and verification is performed by using classical oracles to check for membership in "larger spaces." Additionally, a banknote in our scheme is minted by preparing conjugate coding states and applying a unitary that permutes the standard basis vectors.

[16] *Continuous-variable quantum passive optical network*

Ivan Derkach (Palacky University, Olomouc), Adnan A.E. Hajomer (Technical University of Denmark), Radim Filip (Palacky University, Olomouc), Ulrik L. Andersen (Technical University of Denmark), Vladyslav C. Usenko (Palacky University, Olomouc) and Tobias Gehring (Technical University of Denmark).

We develop a novel multi-user protocol and report the first continuous-variable quantum passive optical network (CV-QPON), that supports secure key generation for eight users simultaneously. This is achieved considering practical PON topology with an 11 km span of access links. Depending on the trust assumptions about users we reach 1.5 Mbits/s and 2.1 Mbits/s of total network key generation. Novel CV-QPON protocol exploits the multi-user nature of the network allowing to extend the network size and enhance individual keys, thus offering a pathway toward establishing low-cost, high-rate, and scalable quantum access networks using standard telecom technologies that directly benefits from the existing access network infrastructure.

[17] *Quantum Control-based Key Distribution*

Nikita Kirsanov (Terra Quantum AG), Aziz Aliev (Terra Quantum AG), Vladlen Statiev (Terra Quantum AG), Ilya Zarubin (Terra Quantum AG), Daniel Strizhak (Terra Quantum AG), Alexander Bezruchenko (Terra Quantum AG), Alexandra Osicheva (Terra Quantum AG), Alexander Smirnov (Terra Quantum AG), Michael Yarovikov (Terra Quantum AG), Aleksei Kodukhov (Terra Quantum AG), Valeria Pastushenko (Terra Quantum AG), Markus Pflitsch (Terra Quantum AG) and Valerii Vinokur (Terra Quantum AG).

The primary obstacle to expanding the reach of quantum cryptography lies in the exponential losses within quantum communication channels. We address this challenge by experimentally realizing the Quantum Control-based Key Distribution (QCKD) protocol, which utilizes physical control over signal losses and ensures that leaked quantum states remain substantially non-orthogonal. The present talk will detail our experiments with QCKD over a 1,707 km fiber optic line, showcasing its effectiveness and scalability. The scaling and performance of QCKD mark a significant step toward achieving globally secure, quantum-resistant communication.

[19] *A Framework for Analyzing Practical High-Dimensional QKD Setups*

Florian Kanitschar (TU Wien & Austrian Institute of Technology) and Marcus Huber (TU Wien).

High-dimensional entanglement promises not only increased key rates but overcoming some of the obstacles faced by modern-day quantum communication. Typically, key rates are computed via convex optimization procedures, which inherently limits the dimensionality one can analyze through computational constraints. Recent progress in high-dimensional photonics far exceeds these limitations and brings forth a need for (semi-)analytic methods to compute key rates in the regime of large encoding dimensions. We present a flexible analytic framework facilitated by the dual of a semi-definite program, enabling the computation of key rates in high-dimensional systems. This method, whether purely analytical or semi-numerical, hinges on diagonalizing specific operators influenced by entanglement witnesses and efficiently solving an optimization problem. To facilitate the latter, we show how matrix completion techniques can be incorporated to yield effective and computable bounds on the key rate in paradigmatic high-dimensional systems of time- or frequency-bin entangled photons and beyond.

[22] *One-sided DI-QKD secure against coherent attacks over long distances*

Michele Masini (Université Libre de Bruxelles) and Shubhayan Sarkar (Université Libre de Bruxelles).

Quantum Key Distribution (QKD) enables provable secure communication but faces challenges in device characterization, posing potential security risks. Device-Independent (DI) QKD protocols overcome this issue by making minimal device assumptions but are limited in distance because they require high detection efficiencies, which refer to the ability of the experimental setup to detect quantum states. Our study explores an entanglement-based one-sided device-independent QKD scenario, where one party's device is semi-trusted, while the second is completely untrusted. We introduce specific assumptions about the semi-trusted device's measurements and assess the security of our protocol without post-selecting outcomes, thereby allowing one to prove security against coherent attacks. By applying the latest analytical and numerical methods, we established that our protocol can securely operate as long as the involved detection efficiencies exceed a minimal threshold of 50.1% specifically on the untrusted side. This is almost the theoretical limit achievable for protocols with two untrusted measurements and is within current experimental capabilities. Interestingly, we also show that, by placing the source of states close to the untrusted side, our protocol is secure over distances comparable to standard QKD protocols. Our findings not only reinforce the practicality of QKD systems under less stringent conditions but also serve as a feasible hybrid approach, bridging conventional QKD with DI QKD.

[25] *Pilot-reference-free continuous-variable quantum key distribution with efficient decoy-state analysis*

Xingjian Zhang (University of Science and Technology of China), Anran Jin (University of Cambridge), Pei Zeng (University of Chicago), Liang Jiang (University of Chicago) and Richard Penty (University of Cambridge).

Continuous-variable quantum key distribution (CV QKD) using optical coherent detectors is practically favorable due to its low implementation cost, flexibility of wavelength division multiplexing, and compatibility with standard coherent communication technologies. However, the security analysis and parameter estimation of CV QKD are complicated due to the infinite-dimensional latent Hilbert space. Also, the transmission of strong reference pulses undermines the security and complicates the experiments. In this work, we tackle these two problems by presenting a time-bin-encoding CV protocol with a simple phase-error-based security analysis valid under general coherent attacks. With the key encoded into the relative intensity between two optical modes, the need for global references is removed. Furthermore, phase randomization can be introduced to decouple the security analysis of different photon-number components. We can hence tag the photon number for each round, effectively estimate the associated privacy using a carefully designed coherent-detection method, and independently extract encryption keys from each component. Simulations manifest that the protocol using multi-photon components increases the key rate by two orders of magnitude compared to the one using only the single-photon component. Meanwhile, the protocol with four-intensity decoy analysis is sufficient to yield tight parameter estimation with a short-distance key-rate performance comparable to the best Bennett-Brassard-1984 (BB84) implementation.

[26] *Experimental Implementation of Continuous-Variable Quantum Key Distribution Network*

Zhenghua Li (Beijing University of Posts and Telecommunications), Xiangyu Wang (Beijing University of Posts and Telecommunications), Dengke Qi (Beijing University of Posts and Telecommunications), Ziyang Chen (Peking University) and Song Yu (Beijing University of Posts and Telecommunications).

Quantum key distribution (QKD) can provide unconditionally secure keys at the physical layer for communication system. In practical environments, communication usually occurs in multi-user and multi-scenario, and point-to-point QKD can no longer meet the modern complex network communication needs. The downstream access network downstream, as an essential component of modern networks, requires QKD technology to ensure its security. Here, we complete a four-user high-speed QKD downstream access network experiment. The repetition frequency of the system is 100 MHz, considering block size of $10^8$, four users achieved secret key rates of 430 kbps, 450 kbps, 150 kbps, and 130 kbps at channel attenuation of 4.4 dB, 4.2 dB, 5.6 dB, and 5.8 dB, respectively. Our experimental results demonstrate the feasibility of multi-user downstream CV-QKD access networks, further advancing the practical application of quantum networks in real-world environments.

[27] *Continuous-Variable QKD with key rates far above Devetak-Winter*

Arpan Akash Ray (Eindhoven University of Technology) and Boris Skoric (Eindhoven University of Technology).

Continuous-Variable Quantum Key Distribution (CVQKD) at large distances has such high noise levels that the employed error-correcting codes must have very low rate. In this regime it becomes feasible to implement random-codebook error correction, which is known to perform close to capacity.

We propose a random-codebook reverse reconciliation scheme for CVQKD that is inspired by spread-spectrum watermarking. Our scheme has a novel way of achieving statistical decoupling between the publicly sent reconciliation data and the secret key. We provide a theoretical analysis of the secret key rate and we present numerical results. The best performance is obtained when the message size exceeds the mutual information $I(X;Y)$ between Alice and Bob's measurements. This somewhat counter-intuitive result is understood from a tradeoff between code rate and frame rejection rate, combined with the fact that error correction for QKD needs to reconcile only random data. We obtain secret key lengths that lie far above the Devetak-Winter value $I(X;Y) - I(E;Y)$.

[28] *Quantum repeaters on multimode coherent states: Scalability, performance and prospects*

Roman Goncharov (ITMO University), Alexei Kiselev (ITMO University) and Vladimir Egorov (ITMO University).

We analyze the performance of a quantum repeater scheme that uses multimode Schrödinger cat states. In this scheme, the entanglement generation and swapping protocols utilize entangled cat states produced using electro-optic modulation of single-mode optical cats. In our analysis, we adapt the approach of doubling the number of links that reduces complexity of constructing the final network and simplifies analytical treatment. In order to evaluate the mean waiting time, we employ both the mean-only approximation and exact results and determine the values of the success probabilities of entanglement generation and swapping at which the approximate results are close to the exact ones. Distance dependence of the repeater rate is calculated depending on the number of elementary links. The results are used to perform a comparative analysis of quantum repeater schemes using the modulated cat states and the photon-pair states generated via spontaneous parametric down-conversion. It is shown that the use of the cat states provides several advantages over the photon pairs. Entanglement purification protocols for optical cats are discussed.

[29] *Realistic Continuous Variable Quantum Network*

Dengke Qi (Beijing University of Posts and Telecommunications), Xiangyu Wang (Beijing University of Posts and Telecommunications), Zhenghua Li (Beijing University of Posts and Telecommunications), Jiayu Ma (Beijing University of Posts and Telecommunications), Ziyang Chen (Peking University), Yueming Lu (Beijing University of Posts and Telecommunications) and Song Yu (Beijing University of Posts and Telecommunications).

Quantum networks provide opportunities and challenges across a range of intellectual and technical frontiers, including quantum computation, communication and others. Unlike traditional communication networks, quantum networks utilize quantum bits rather than classical bits to store and transmit information. As an important part of the networks, the access network can connect multiple end users to the backbone network and provide the so-called last-mile service. In our work, the first four-end-users quantum downstream access network in continuous variable quantum key distribution with a local local oscillator has been experimentally demonstrated. Our results show that each user can get a low level of excess noise and can achieve secret key rate of 546 kbps, 535 kbps, 522.5 kbps and 512.5 kbps under transmission distance of 10 km, respectively with the finite-size block of 1×10^{8}. More importantly, the successful demonstration of our quantum downstream access network also paves the way for secure broadband metropolitan and quantum networks.

[30] *The shadows of quantum gravity on Bell's inequality*

Hamid Tebyanian (University of York), Hooman Moradpour (Research Institute for Astronomy and Astrophysics of Maragha (RIAAM), Maragha 55134-441, Iran) and Shahram Jalalzadeh (Departamento de Fisica, Universidade Federal de Pernambuco, Recife, PE 50670-901, Brazil).

This study delves into the validity of quantum mechanical operators in the context of quantum gravity, recognizing the potential need for their generalization. A primary objective is to investigate the repercussions of these generalizations on the inherent non-locality within quantum mechanics, as exemplified by Bell's inequality. Additionally, the study scrutinizes the consequences of introducing a non-zero minimal length into the established framework of Bell's inequality. The findings contribute significantly to our theoretical comprehension of the intricate interplay between quantum mechanics and gravity. Moreover, this research explores the impact of quantum gravity on Bell's inequality and its practical applications within quantum technologies, notably in the realms of device-independent protocols, quantum key distribution, and quantum randomness generation.

[32] *Weak-trace-free Counterfactual Communication via Quantum Zeno effect*

Tianyi Xing (National University of Defense Technology), Anqi Huang (National University of Defense Technology), Junjie Wu (National University of Defense Technology), Ping Xu (National University of Defense Technology), Pingyu Zhu (National University of Defense Technology), Chao Wu (National University of Defense Technology), Yizhi Wang (National University of Defense Technology), Jiangfang Ding (National University of Defense Technology), Dongyang Wang (National University of Defense Technology), Yaxuan Wang (National University of Defense Technology) and Yingwen Liu (National University of Defense Technology).

The Quantum Zeno effect inhibits the evolution of quantum states through repeated yet weak measurements, thereby significantly enhancing the detection probability of interaction-free measurement (IFM). This fundamental mechanism facilitates high-efficiency counterfactual quantum communication that information delivery without particle transmission through the channel. Regrettably, the original protocol left the weak trace of particles in the channel; fortunately, an upgraded counterfactual communication protocol eliminates this issue by modifying the structure unit according to two-state vector formalism~(TSVF). However, no study has realized the application of the quantum Zeno effect in weak-trace-free counterfactual communication to achieve efficient information transmission. In this paper, we experimentally demonstrate weak-trace-free counterfactual communication via the quantum Zeno effect on a nanophotonic chip, achieving a transmission probability of 74.2 ± 1.6\% for bit 0 and 85.1 ± 1.3\% for bit 1. Furthermore, we successfully transmit our Quanta group's logo through counterfactual communication implemented on the chip.

[33] *Repeater-Like Asynchronous Measurement-Device-Independent Quantum Conference Key Agreement*

Yu-Shuo Lu (Nanjing University), Yuan-Mei Xie (Nanjing University), Zeng-Bing Chen (Nanjing University) and Hua-Lei Yin (Renmin University of China).

Quantum conference key agreement facilitates the secure communication among multiple parties through multipartite entanglement, which is anticipated as an important cryptographic primitive for future quantum networks. However, the experimental complexity and low efficiency associated with synchronous detection of multipartite entanglement state have significantly hindered the practical application. Here, we propose a measurement-device-independent conference key agreement protocol utilizing asynchronous Greenberger-Horne-Zeilinger state measurement and achieve a linear scaling of the conference key rate among multiple parties, which has the similar performance with the single-repeater scheme in quantum network. The asynchronous measurement strategy bypasses the necessity for complex global phase-locking technologies, concurrently extending the intercity transmission distance with composable security in finite key regime. Our work also showcases the advantages of the asynchronous pairing concept in multiparty quantum entanglement.

[34] *Experimental quantum e-commerce*

Xiao-Yu Cao (Nanjing University), Hua-Lei Yin (Renmin University of China) and Zeng-Bing Chen (Nanjing University).

E-commerce, a type of trading that occurs at a high frequency on the Internet, requires guaranteeing the integrity, authentication and non-repudiation of messages through long distance. As current e-commerce schemes are vulnerable to computational attacks, quantum cryptography, ensuring information-theoretic security against adversary's repudiation and forgery, provides a solution to this problem. However, quantum solutions generally have much lower performance compared to classical ones. Besides, when considering imperfect devices, the performance of quantum schemes exhibits a notable decline. Here, we demonstrate the whole e-commerce process of involving the signing of a contract and payment among three parties by proposing a quantum e-commerce scheme, which shows resistance of attacks from imperfect devices. Results show that with a maximum attenuation of 25 dB among participants, our scheme can achieve a signature rate of 0.82 times per second for an agreement size of approximately 0.428 megabit. This proposed scheme presents a promising solution for providing information-theoretic security for e-commerce.

[35] *Multi-Field Quantum Conference Key Agreement Overcoming Network Capacity Limits*

Yuan-Mei Xie (Nanjing University), Yu-Shuo Lu (Nanjing University), Zeng-Bin Chen (Nanjing University) and Hua-Lei Yin (Renmin University of China).

Quantum network allows for multi-user applications that bring advantages that are unattainable with a classical network. A crucial application of quantum networks is quantum conference key agreement (QCKA), which enables remote nodes to efficiently share information-theoretic secure group key by leveraging the laws of quantum mechanics. However, the efficacy of QCKA is hampered by inherent losses in optical fibers and the increasing number of users, impacting both bit rate and range. Here we introduce multi-field (MF) QCKA scheme, where independently sets of phase-randomized optical fields are generated at remote locations, later combining them at a central measuring station. Employing the post-measurement pairing technique, we post-select optical fields with the same random phase, establishing Greenberger-Horne-Zeilinger correlations to distill a secret conference key. This method ensures that the communication efficiency of MF-QCKA scales linearly with communication transmittance and remains independent of the number of users. Using components similar to twin-field quantum key distribution, MF-QCKA can be implemented in a practial and scalable fashion. For three-user scenario, our protocol can overcome the performance limitation of QCKA without quantum memory in the finite regime. By mitigating the impact of optical fiber losses and accommodating a larger user base, MF-QCKA protocol represents a promising step forward in the realm of quantum communication, ensuring secure and efficient parallel communication in complex quantum networks.

[36] *Improved finite-size key rates for discrete-modulated continuous variable quantum key distribution in the presence of coherent attacks*

Carlos Pascual-Garcia (ICFO - Institute of Photonic Sciences), Stefan Baeuml (ICFO - Institute of Photonic Sciences), Mateus Araujo (Universidad de Valladolid), Rotem Liss (ICFO - Institute of Photonic Sciences) and Antonio Acin (ICFO - Institute of Photonic Sciences).

Continuous variable quantum key distribution (CVQKD) with discrete modulation combines advantages of CVQKD, such as the implementability using readily available technologies, with advantages of discrete variable quantum key distribution, such as easier error correction procedures. In this work we consider a phase-shift keying protocol using four coherent states (4-PSK protocol) and coarse-grained heterodyne measurements. We provide a security proof against coherent attacks and compute the achievable key rate in a finite size setting, i.e. with a finite number of rounds. To this end, we employ the generalized entropy accumulation theorem, as well conic optimisation, providing us with improved key rates compared to previous works. At metropolitan distances our method can provide positive key rates for the order of $10^9$ rounds. We also provide a theoretical method to overcome the assumption of a finite photon number cutoff made in previous works.

[39] *The Round Complexity of Proofs in the Bounded Quantum Storage Model*

Alex B. Grilo (CNRS) and Philippe Lamontagne (National Research Council Canada and University of Montreal).

The round complexity of interactive proof systems is a key question of practical and theoretical relevance in complexity theory and cryptography. Moreover, results such as QIP = QIP(3) (STOC'00) show that quantum resources significantly help in such a task. In this work, we initiate the study of round compression of protocols in the bounded quantum storage model (BQSM). In this model, the malicious parties have a bounded quantum memory and they cannot store the all the qubits that are transmitted in the protocol Our main results in this setting are the following: 1. There is a non-interactive (statistical) witness indistinguishable proof for any language in NP (and even QMA) in BQSM in the plain model. We notice that in this protocol, only the memory of the verifier is bounded. 2. Any classical proof system can be compressed in a two-message quan- tum proof system in BQSM. Moreover, if the original proof system is zero-knowledge, the quantum protocol is zero-knowledge too. In this result, we assume that the prover has bounded memory. Finally, we give evidence towards the "tightness" of our results. First, we show that NIZK in the plain model against BQS adversaries is unlikely with standard techniques. Second, we prove that without the BQS model there is no 2–message zero-knowledge quantum interactive proof, even under computational assumptions.

[40] *Boosting existing device-dependent QKD protocols via the Loss Control of the quantum channel*

Aleksei Kodukhov (Terra Quantum AG), Valeria Pastushenko (Terra Quantum AG), Nikita Kirsanov (Terra Quantum AG), Markus Pflitsch (Terra Quantum AG) and Valerii Vinokur (Terra Quantum AG).

The conventional approach to QKD implies that a potential eavesdropper can conduct any manipulations with a quantum channel. In the context of optical fiber implementations of QKD, we demonstrate how most of the manipulations can be detected by conducting a line tomography procedure. It allows legitimate users to accurately estimate the fraction of the signal available to the eavesdropper and, thus, adaptively modify the setup and post-processing parameters. Our approach significantly increases the secret key generation rate for existing device-dependent QKD protocols and potentially enables surpassing the fundamental PLOB bound.

[41] *Finite-size analysis of prepare-and-measure and decoy-state QKD via entropy accumulation*

Lars Kamin (Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo), Amir Arqand (Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo), Ian George (Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign), Norbert Lütkenhaus (Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo) and Ernest Y.-Z. Tan (Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo).

An important goal in quantum key distribution (QKD) is the task of providing a finite-size security proof without the assumption of collective attacks. For prepare-and-measure QKD, one approach for obtaining such proofs is the generalized entropy accumulation theorem (GEAT), but thus far it has only been applied to study a small selection of protocols. In this work, we present techniques for applying the GEAT in finite-size analysis of generic prepare-and-measure protocols, with a focus on decoy-state protocols. In particular, we present an improved approach for computing entropy bounds for decoy-state protocols, which has the dual benefits of providing tighter bounds than previous approaches (even asymptotically) and being compatible with methods for computing min-tradeoff functions in the GEAT. Furthermore, we develop methods to incorporate some improvements to the finite-size terms in the GEAT, and implement techniques to automatically optimize the min-tradeoff function. Our approach also addresses some numerical stability challenges specific to prepare-and-measure protocols, which were not addressed in previous works.

[44] *Client Authentication and Key Generation Enabled by Pseudorandom Basis Selection*

Wen Yu Kon (JPMorgan Chase), Jefferson Chu (JPMorgan Chase), Kevin Han Yong Loh (JPMorgan Chase), Obada Alia (JPMorgan Chase), Omar Amer (JPMorgan Chase), Marco Pistoia (JPMorgan Chase), Kaushik Chakraborty (JPMorgan Chase) and Charles Lim (JPMorgan Chase).

Client authentication (CA) is a cryptographic protocol where a server tries to validate the identity of a client. Fehr et. al. proposed a CA protocol with pre-shared basis information between the client and server which has a nice key recycling property, where secrets including the pre-shared basis can be securely reused after each successful round. We extend the protocol to a practical setting by including decoy state and error correction, but the leakage of pre-shared basis information via multi-photon events limits the performance of such a protocol. As such, we propose the use of a pseudorandom number generator (PRNG), assumed to be secure only during each run of the protocol, to perform basis selection to reduce information leakage. A formal proof of the protocol security is provided by modifying the entropic uncertainty relation to account for basis generated by a PRNG, which could be of independent interest as it may be applicable to other protocols such as quantum key distribution. An experimental implementation of the protocol, with appropriate post-selection, was performed to demonstrate its feasibility. We also designed a CA protocol secure in the practical setting with only two rounds of communication: a challenge by the server and a response by the client.

[45] *Networking quantum networks with minimum cost aggregation*

Koji Azuma (NTT Basic Research Laboratories).

A quantum internet holds promise for achieving distributed quantum sensing and large-scale quantum computer networks, as well as quantum communication among arbitrary clients all over the globe. The main building block is efficient distribution of entanglement,entangled bits (ebits), between arbitrary clients in a quantum network with fixed error, irrespective of their distance. In practice, this should be accomplished across multiple quantum networks, analogously to what the current Internet does in conventional communication. Here we present a practical recipe on how to give arbitrary clients ebits with fixed error efficiently, regardless of their distance, across multiple quantum networks. This recipe is composed of two new concepts, minimum cost aggregation and network concatenation. Our recipe forms the basis of designing a quantum internet protocol for networking self-organizing quantum networks to make a global-scale quantum internet.

[46] *Device independent security for quantum key distribution from monogamy-of-entanglement games*

Enrique Cervero (Centre for Quantum Technologies, Singapore) and Marco Tomamichel (National University of Singapore).

We analyse two party non-local games whose predicate requires Alice and Bob to generate matching bits, and their three party extensions where a third player receives all inputs and is required to output a bit that matches that of the original players. We propose a general device independent quantum key distribution protocol for the subset of such non-local games that satisfy a monogamy-of-entanglement property characterised by a gap in the maximum winning probability between the bipartite and tripartite versions of the game. This gap is due to the optimal strategy for two players requiring entanglement, which due to its monogamy property cannot be shared with any additional players. Based solely on the monogamy-of-entanglement property, we provide a simple proof of information theoretic security of our protocol. Lastly, we numerically optimize the finite and asymptotic secret key rates of our protocol using the magic square game as an example, for which we provide a numerical bound on the maximal tripartite quantum winning probability which closely matches the bipartite classical winning probability. Further, we show that our protocol is robust for depolarizing noise up to about $2.2\%$, providing the first such bound for general attacks for magic square based quantum key distribution.

[49] *Hybrid Cryptography from Communication Complexity*

Francesco Mazzoncini (Telecom Paris), Balthazar Bauer (CNRS), Peter Brown (Telecom Paris) and Romain Alléaume (Telecom Paris).

We introduce an explicit construction for a key distribution protocol in the Quantum Computational Timelock (QCT) security model, where one assumes that computationally secure encryption may only be broken after a time much longer than the coherence time of available quantum memories. Taking advantage of the QCT assumptions, we build a key distribution protocol called HM-QCT from the Hidden Matching problem for which there exists an exponential gap in one-way communication complexity between classical and quantum strategies.

We establish that the security of HM-QCT against arbitrary i.i.d. attacks can be reduced to the difficulty of solving the underlying Hidden Matching problem with classical information. Legitimate users, on the other hand, can use quantum communication, which gives them the possibility of sending multiple copies of the same quantum state while retaining an information advantage. This leads to an everlasting secure key distribution scheme over $n$ bosonic modes. Such a level of security is unattainable with purely classical techniques. Remarkably, the scheme remains secure with up to O(sqrt{n} \log(n)) input photons for each channel use, extending the functionalities and potentially outperforming QKD rates by several orders of magnitudes.

[51] *Polarization Drift Impact on the Performance of CV-QKD*

Margarida Almeida (Instituto de Telecomunicações), Armando N. Pinto (Instituto de Telecomunicações) and Nuno A. Silva (Instituto de Telecomunicações).

In prepare & measure continuous-variable quantum key distribution (CV-QKD) systems the quantum states generated by Alice and sent to Bob is typically performed using an optical fiber that connects both entities. However, the state of polarization (SOP) of the quantum signal transmitted in the optical fiber is inevitably disturbed due to random birefringence, impacting the overall secret key rate of the CV-QKD system. We study the secret key rate of a CV-QKD system considering the polarization drift occurring in the quantum channel. Channels with low polarization drift lightly impact the secret key rate of the system. This accounting for the SOP fluctuations. Moreover, we analyze the effect of the SOP fluctuations on the estimation of the channel transmission and of the excess noise when the polarization drift in the channel is disregarded. Such assumption results in a sub-estimation of the secret key rate, decreasing the performance of the system, when comparing with the theoretical value considering the polarization drift in the channel.

[52] ***Pilot Tone-Assisted Frequency Locking in Low-Complexity Continuous Variable Quantum Key Distribution Systems***

Andres Ruiz-Chamorro (Spanish National Research Council (CSIC)), Aida García-Callejo (Spanish National Research Council (CSIC)) and Verónica Fernández (Spanish National Research Council (CSIC)).

The present work addresses the challenge of frequency synchronization in Continuous Variable Quantum Key Distribution (CV-QKD) by implementing a novel signal processing pilot tone-assisted frequency locking algorithm. The technique here introduced thus leverages a software-based approach to maintain synchronization between the quantum signal and the true local oscillator, eliminating the need for complex electronic stabilization. Our experimental results demonstrate the feasibility of achieving a QKD transmission over 50 km, underscoring the potential for practical and low-complexity systems.

[54] ***Performance design of phase-encoding QKD system with PLC Mach-Zehnder interferometer under channel polarization disturbance***

Shinya Hirashita (NEC Corporation Advanced Network Research Laboratories), Hiroki Kawahara (NEC Corporation Advanced Network Research Laboratories) and Wakako Maeda (NEC Corporation Advanced Network Research Laboratories).

We propose statistical design method for phase-encoding BB84 quantum key distribution system performance focusing on polarization fluctuation of transmitted photons, by charactering the impact on secure key rate of polarization dependent frequency shift induced by planar lightwave circuit Mach-Zehnder interferometer.

[57] ***Multi-encoding Quantum Key Distribution transmitter for aircraft and satellite applications***

Innocenzo De Marco (DLR Institute of Communications and Navigation), Eltimir Peev (DLR Institute of Communications and Navigation), Till Dolejsky (DLR Institute of Communications and Navigation), Davide Orsucci (DLR Institute of Communications and Navigation), Javier Garcia Olmedo (DLR Institute of Communications and Navigation), Carlo Riester (DLR Institute of Communications and Navigation) and Florian Moll (DLR Institute of Communications and Navigation).

We propose a QKD transmitter that is able to encode qubits in two different degrees of freedom, namely polarisation and time-bin/phase, and according to different protocols, including but not limited to BB84, DPS and COW.

Thanks to its design, the transmitter can be embedded on an aircraft or satellite and it is able to communicate with ground stations which can potentially have different receiving apparati, improving on the issue of interoperability that is currently a topic of discussion in the field.

[58] ***Quantum key distribution with unbounded pulse correlations***

Margarida Pereira (Vigo Quantum Communication Center), Guillermo Currás-Lorenzo (Vigo Quantum Communication Center), Akihiro Mizutani (University of Toyama), Davide Rusca (Vigo Quantum Communication Center), Marcos Curty (Vigo Quantum Communication Center) and Kiyoshi Tamaki (University of Toyama).

Typical security proofs of quantum key distribution (QKD) require that the emitted signals are independent and identically distributed. In practice, however, this assumption is not met because intrinsic device flaws inevitably introduce correlations between the emitted signals. Although analyses addressing this issue have been recently proposed, they only consider a restrictive scenario in which the correlations have a finite and known maximum length that is much smaller than the total number of emitted signals. While it is expected that the magnitude of the correlations decreases as the pulse separation increases, the assumption that this magnitude is exactly zero after a certain point does not seem to have any physical justification. Concerningly, this means that existing analyses cannot guarantee the security of current QKD implementations. Here, we solve this pressing problem by developing a general framework that can handle pulse correlations of unbounded length. Our framework allows us to directly use existing proofs addressing this imperfection without the need to construct them from scratch, thus reestablishing the security of QKD in a simple and versatile manner.

[59] *Verification of Quantum Computations without Trusted Preparations or Measurements*

Elham Kashefi (School of Informatics, University of Edinburgh / LIP6, CNRS, Sorbonne Université), Dominik Leichtle (School of Informatics, University of Edinburgh), Luka Music (Quandela) and Harold Ollivier (DI-ENS, Ecole Normale Supérieure, PSL Research University, CNRS, INRIA).

With the advent of delegated quantum computing as a service, verifying quantum computations is becoming a question of great importance. Existing information theoretically Secure Delegated Quantum Computing (SDQC) protocols require the client to possess the ability to perform either trusted state preparations or measurements. Whether it is possible to verify universal quantum computations with information-theoretic security without trusted preparations or measurements was an open question so far. In this paper, we settle this question in the affirmative by presenting a modular, composable, and efficient way to turn known verification schemes into protocols that rely only on trusted gates.

Our first contribution is an extremely lightweight reduction of the problem of quantum verification for BQP to the trusted application of single-qubit rotations around the Z axis and bit flips. The second construction presented in this work shows that it is generally possible to information-theoretically verify arbitrary quantum computations with quantum output without trusted preparations or measurements. However, this second protocol requires the verifier to perform multi-qubit gates on a register whose size is independent of the size of the delegated computation.

[60] *Urban passive state QKD experiment*

Yury Kurochkin (Quantum Research Centre, Technology Innovation Institute, Abu Dhabi, UAE), Marios Papadovasilakis (Quantum Research Centre, Technology Innovation Institute, Abu Dhabi, UAE), Anton Trushechkin (Heinrich Heine University Düsseldorf, Institute for Theoretical Physics III, Düsseldorf, Germany), Rodrigo Piera (Quantum Research Centre, Technology Innovation Institute, Abu Dhabi, UAE) and James Grieve (Quantum Research Centre, Technology Innovation Institute, Abu Dhabi, UAE).

One of the most important requirements for the correct operation of the BB84 protocol is the preparation of the true random state. Most realizations follow this logic: Alice prepares random quantum states, measures them to extract random numbers, and then uses them to modulate the state of the transmitted light. The alternative approach is passive state preparation. It was proposed in 2010 [1] and recently studied for security aspects [2]. The idea is to use the natural phase randomness of the laser pulses to prepare random states. This approach can help to solve the security problem of correlating the state modulation voltage. Originally, the focus was on preparing the polarization state. This required two lasers or an additional intensity modulator. In this work, we use a laser that generates random phase pairs of subsequent pulses as a ready-to-use qubit. This allows us to simplify the Alice device. To perform a full phase characterization, we split a portion of the signal, convert it to polarization, and perform polarization tomography where we postselect four BB84 states. Without a decoy state, this QKD system is well suited for the last mile of a star quantum network with a loss budget of up to 10 dB. We have experimentally demonstrated passive state QKD over 10km deployed and spool fiber obtaining 10-100 bps of secret key correspondingly.

[1] M Curty, et al. “Passive sources for the Bennett-Brassard 1984 quantum-key-distribution protocol with practical signals.” Physical Review A 82.5 (2010): 052325 [2] W Wang, et al. “Fully-Passive Quantum Key Distribution.” arxiv.org/abs/2207.05916

[61] *A security framework for quantum key distribution implementations*

Guillermo Currás-Lorenzo (University of Vigo), Margarida Pereira (University of Vigo), Go Kato (NICT), Marcos Curty (University of Vigo) and Kiyoshi Tamaki (University of Toyama).

Quantum key distribution (QKD) promises theoretically unbreakable encryption by exploiting the principles of quantum mechanics. However, the security of real-world implementations is compromised by inevitable device imperfections, unless these are accounted for in the security proof. In this work, we introduce an innovative and powerful security proof framework that guarantees robustness against all practical source imperfections while maintaining high performances, thereby significantly bridging the gap between the theoretical promise and practical realization of QKD. In combination with measurement-device-independent QKD, which closes all security loopholes related to the measurement units, our framework can guarantee an unprecedented level of implementation security.

[62] *Threshold Symmetric Primitives in the Post-quantum Setting*

Ehsan Ebrahimi (University of Luxembourg).

In this paper, we study the post-quantum security of various threshold symmetric schemes. In a threshold scheme, the secret-key is split among multiple parties in order to protect the key. Our first observation is a security analysis in the superposition-access model might be needed for a multi-party threshold scheme in the post-quantum setting since a corrupt party may deliver its secret key to a quantum adversary. Consequently, the adversary can implement a partial evaluation of the multi-party threshold scheme on his quantum device and this can enforce a superposition access to the underlying primitive. In other words, if the underlying primitive is vulnerable to a superposition attack, then the security of the multi-party threshold scheme might break. For instance, under a reasonable assumption we show that the NPR's threshold pseudorandom function (Naor et al. Eurocrypt 99) is not post-quantum secure if the underlying pseudorandom function family is not secure in the superposition-access model.

Furthermore, we analysis the threshold message authentication codes and threshold symmetric encryption schemes constructed from the NPR's threshold pseudorandom function. In each case, we strengthen the existing security definitions and we present a scheme that satisfies our stronger notion of security. In particular, we propose indifferentiability definition and IND-CCA2 definition for a threshold pseudorandom function and a threshold symmetric encryption scheme, respectively.

[64] *Finite key performance of satellite quantum key distribution under practical constraints*

Jasminder Sidhu (University of Strathclyde), Thomas Brougham (University of Strathclyde), Duncan McArthur (University of Strathclyde), Roberto Pousa (University of Strathclyde) and Daniel Oi (University of Strathclyde).

Global-scale quantum communication networks will require efficient long-distance distribution of quantum signals. While optical fibre communications are range-limited due to exponential losses in the absence of quantum memories and repeaters, satellites enable intercontinental quantum communications. However, the design of satellite quantum key distribution (SatQKD) systems has unique challenges over terrestrial networks. The typical approach to modelling SatQKD has been to estimate performances with a fully optimised protocol parameter space and with few payload and platform resource limitations. Here, we analyse how practical constraints affect the performance of SatQKD for the Bennett-Brassard 1984 (BB84) weak coherent pulse decoy state protocol with finite key size effects. We consider engineering limitations and trade-offs in mission design including limited in-orbit tunability, quantum random number generation rates and storage, and source intensity uncertainty. We quantify practical SatQKD performance limits to determine the long-term key generation capacity and provide performance benchmarks to support the design of upcoming missions

[65] *Clock Synchronization using Thermal Correlations without External Frequency Standards*

Justin Yu Xiang Peh (Center for Quantum Technologies), Darren Koh (Center for Quantum Technologies), Zifang Xu (Department of Physics, National University of Singapore), Xi Jie Yeo (Centre for Quantum Technologies), Peng Kian Tan (Centre for Quantum Technologies) and Christian Kurtsiefer (National University of Singapore).

Clock synchronization is necessary for communication and distributed computing tasks. In quantum communication systems, photo-detection events need to be discriminated with sub-nanosecond accuracy in order to distill information from correlations at a sufficiently high rate. This typically entails significant resource overheads, such as the use of ultra-stable frequency references, that will also scale with the number of communicating endpoints.

Here, we demonstrate an alternative clock synchronization scheme using weak thermal correlations without the need for external frequency standards. The scheme relies on tracking timing correlations in the photon bunching behaviour of thermal light generated using a sub-threshold laser. The 10 MHz quartz oscillators onboard the time taggers have a typical frequency accuracy of 10^−4; by performing cross-correlation measurements to identify the position and drift rate of the bunching peak, we can continuously correct for the frequency difference to within 10^−9 of each other, comparable to that of a Rubidium frequency standard. We also identify lower bounds for peak identification using the cross-correlation method.

A similar line of work relies on strong timing correlations in photon pairs from spontaneous parametric down-conversion sources for synchronization. We believe our scheme using thermal light sources significantly improves clock synchronization over longer distances due to its intrinsically higher brightness and low attenuation within the C-band optical window of G.652D standard-compliant telecommunication fiber, whilst requiring only an easily-acquirable laser diode and simple temperature control for operation.

[67] *Vulnerabilities of fiber-based quantum key distribution systems outside operating spectral range*

Boris Nasedkin (ITMO University), Azat Ismagilov (ITMO University), Vladimir Chistiakov (ITMO University), Ilya Filipov (Laboratory for Quantum Communications, ITMO University), Fedor Kiselev (ITMO University), Andrei Gaidash (ITMO University; Steklov Mathematical Institute of Russian Academy of Sciences), Alexei Kiselev (ITMO University), Anton Tcypkin (ITMO University), Vladimir Egorov (ITMO University) and Anton Kozubov (ITMO University; Steklov Mathematical Institute of Russian Academy of Sciences).

The security of quantum key distribution (QKD) systems is constantly being tested, and attacks that utilize probing pulses are have been widely developed recently. One of the most challenging methods is the Trojan-horse attack, which has been successfully demonstrated at 1924 nm. Moreover, the induced-photorefraction attack (IPA) represent attacks that will do better in the visible spectral range. We experimentally investigate the spectral properties of several conventional QKD components. We show that transmission of various fiber optical elements beyond telecommunication range should be taken into account during QKD system design and development due to the possibility for attacks realization.

[68] *Post-Quantum Cryptographically-Secured Trusted Node for Quantum Key Distribution in a Deployed Network*

Yoann Piétri (Sorbonne Université, CNRS, LIP6), Pierre-Enguerrand Verdier (Orange Innovation), Baptiste Lacour (Orange Innovation), Maxime Gautier (Orange Innovation), Heming Huang (Telecom Paris, Institut Polytechnique de Paris), Thomas Camus (ID Quantique SA), Jean-Sébastien Pegon (ID Quantique SA), Martin Zuber (CryptoNext Security), Jean-Charles Faugère (CryptoNext Security), Matteo Schiavon (Sorbonne Université, CNRS, LIP6), Amine Rhouni (Sorbonne Université, CNRS, LIP6), Yves Jaouën (Telecom Paris, Institut Polytechnique de Paris), Nicolas Fabre (Telecom Paris, Institut Polytechnique de Paris), Romain Alléaume (Telecom Paris, Institut Polytechnique de Paris), Thomas Rivera (Orange Innovation) and Eleni Diamanti (Sorbonne Université, CNRS, LIP6).

Quantum Key Distribution (QKD) is arguably the most mature application of principles of quantum mechanics to cryptography, and several lab and field demonstrations have been realized. However the realization of QKD in deployed networks, with high distances and/or complex network architecture is still a challenge. Trusted nodes is a known solution to these issues, but requires the delegation of trust to third parties. Here, we propose a trusted node protocol where the requirements of trust delegation are lowered, with no overhead in the consumption of the key exchanged with QKD, allowing to keep the same secret key rate. This protocol is then applied to 2 links in the Parisian Quantum Network, composed of dark dedicated fibers between 8 nodes in the Parisian region, for a total fiber distance of 57 km. Our results show the overall key exchange with no degradation of the key rate.

[70] *Continuous-variable Quantum Position Verification secure against entangled attackers*

Rene Allerstorfer (CWI), Llorenç Escolà-Farràs (University of Amsterdam/QuSoft), Arpan Akash Ray (TU Eindhoven), Boris Skoric (TU Eindhoven) and Florian Speelman (QuSoft/University of Amsterdam).

Motivated by the fact that coherent states may offer practical advantages it was recently shown that a continuous-variable (CV) quantum position verification (QPV) protocol using coherent states could be securely implemented if and only if attackers do not pre-share any entanglement. In the discrete-variable (DV) analogue of that protocol it was shown that modifying how the classical input information is sent from the verifiers to the prover leads to a favourable scaling in the resource requirements for a quantum attack. In this work, we show that similar conclusions can be drawn for CV-QPV. By adding extra classical information of size $n$ to a CV-QPV protocol, we show that the protocol, which uses a coherent state and classical information, remains secure, even if the quantum information travels arbitrarily slow, against attackers who pre-share CV (entangled) states with a linear (in $n$) cutoff at the photon number. We show that the protocol remains secure for certain attenuation and excess noise.

[71] *Lossy-and-Constrained Extended Non-Local Games with Applications to Cryptography: BC, QKD and QPV*

Llorenç Escolà-Farràs (University of Amsterdam) and Florian Speelman (University of Amsterdam/QuSoft).

Extended non-local games are a generalization of monogamy-of-entanglement games, played by two quantum parties and a quantum referee that performs a measurement on their local quantum system. Along the lines of the NPA hierarchy, the optimal winning probability of those games can be upper bounded by a hierarchy of semidefinite programs (SDPs) converging to the optimal value. Here, we show that if one extends such games by considering constraints and loss, motivated by experimental errors and loss through quantum communication, the convergence of the SDPs to the optimal value still holds. We give applications of this result, and we compute SDPs that show tighter security for certain protocols in quantum cryptography such as relativistic bit commitment, quantum key distribution and quantum position verification.

[72] *Enhancing key rates of QKD protocol by Coincidence Detection*

Tanya Sharma (Physical Research Laboratory), Rutvij Bhavsar (Korea Advanced Institute of Science and Technology), Jayanth R (Physical Research Laboratory), Pooja Chandravanshi (Physical Research Laboratory), Shashi Prabhakar (Physical Research Laboratory), Ayan Biswas (York Centre for Quantum Technologies, University of York, York, United Kingdom) and Ravindra Pratap Singh (Physical Research Laboratory).

This study focuses on improving practical QKD implementations using weak coherent pulses. We enhance the conventional decoy pulse method by integrating it with the coincidence detection (CD) protocol. Additionally, we introduce an easy-to-implement algorithm for computing asymptotic key rates. Through experimental implementation, we demonstrate that our approach significantly enhances key rates under realistic conditions by monitoring coincidences in the decoy state protocol.

[73] *Secure and robust randomness with sequential quantum measurements*

Matteo Padovan (University of Padova), Giulio Foletto (University of Padova), Lorenzo Coccia (University of Padova), Giuseppe Vallone (University of Padova), Paolo Villoresi (University of Padova) and Marco Avesani (University of Padova).

Quantum correlations between measurements of two or more separated observers play a fundamental role in many applications, such as randomness generation or key distribution. Although security can be certified from correlations with minimal assumptions in the device-independent scenario, the performance of such protocols is currently limited. This limitation motivates the exploration of sequential measurements, that is, defined with precise temporal ordering, as a means of improving performance through the reuse of the quantum states. To date, the study of sequential quantum protocols has been modest, lacking a comprehensive mathematical framework to explore the properties of the obtainable correlations. In this study, we adopt a geometric perspective to investigate sequential quantum correlations, providing a general mathematical framework. Here, we analytically prove a Tsirelson-like boundary for sequential quantum correlations, expressed as a trade-off between the amount of nonlocality shared by each sequential user. This boundary is particularly beneficial for the generation of secure quantum randomness. Indeed, observing a correlation on it can certify the maximum attainable bits per state in the case of one remote party and two sequential parties. In contrast to all previous schemes, this can happen even if one of the sequential users does not share any nonlocality. We demonstrate that this quantum boundary can be reached with a simple qubit protocol and investigate numerically the robustness of randomness generation under realistic noise conditions, finding that it greatly improved compared to previous proposals. Our proof-of-concept photonic implementation of the protocol confirms experimentally that our approach certifies more bits per state compared to the standard Clauser-Horne-Shimony-Holt scenario for the same noise, affirming both feasibility and robustness. This study marks a significant advance in understanding sequential quantum correlations, offering valuable insights and new mathematical tools for further fundamental studies and practical applications of efficient device-independent protocols.

[75] *Increasing Secret Key Rate in Twin Field Quantum Key Distribution using 4×4 Port Detection Network*

Ishan Pandey (Indian Institute of Science / Indian Space Research Organisation) and Varun Raghunathan (Indian Institute of Science).

Twin Field Quantum key Distribution (TF-QKD) is an promising quantum cryptography technique as it provides better secret key capacity than the fundamental limit of repeater-less transmission (i.e. PLOB bound) and extends the achievable communication distance. The key generation in TF QKD is based on selection of aligned phase slices, thereby taking a hit in the secret key rate as the inverse of the number of phase slices. Here we describe a technique for enhancing the probability of choosing phase slice by using a 4x4 port detection network with four detectors, which increases the key rate and also provides a way of detecting photon number splitting (PNS) attack.

[77] *Low-error encoder for time-bin and decoy states for quantum key distribution*

Davide Scalcon (Univeristy of Padova), Elisa Bazzani (Univeristy of Padova), Giuseppe Vallone (Univeristy of Padova), Paolo Villoresi (Univeristy of Padova) and Marco Avesani (Univeristy of Padova).

We propose the MacZac, a time-bin encoder with ultra-low intrinsic QBER (<2e-5) and high stability. The device is based on nested Sagnac and Mach–Zehnder interferometers and uses a single phase modulator for both decoy and state preparation, greatly simplifying the optical setup. The encoder does not require any active compensation or feedback system and it can be scaled for the generation of states with arbitrary dimension. We realized and tested the device performances as a stand alone component and in a complete QKD experiment.

[78] *A simple, self-testing quantum random number generator*

Ana Blázquez Coído (Vigo Quantum Communication Center), Fadri Grünenfelder (Vigo Quantum Communication Center), Anthony Martin (Université Côte d'Azur), Hugo Zbinden (University of Geneva) and Davide Rusca (Vigo Quantum Communication Center).

Quantum random number generators (QRNGs) have obtained notable attention and undergone substantial development, driven by their utility across diverse fields including simulations, gambling, and cryptography. This surge in interest stems from their unique capacity to deliver inherent randomness, which can only be derived from the probabilistic nature of quantum mechanics. The key challenge lies in validating the quantum origin of the randomness produced, which usually requires either a thorough characterization of the elements in the setup or very experimentally challenging loophole-free bell tests. In this work, we present a simple, self-testing and cost-effective quantum random number generator (QRNG) designed to operate with an untrusted measurement device and a partially characterized source, yielding a high rate of random bits. We consider a prepare-and-measure scenario where the preparation device takes a binary input x and a binary output b is received from the measurement device. Depending on the input, the preparation device sends either a weak coherent state (x=1) or a vacuum state (x=0). The measurement device employs homodyne detection to distinguish between these states, and the output value is chosen when the detector current is below (b=0) or above (b=1) a certain threshold. In order to certify the quantum origin of the randomness generated by output b, we need to track the correlations between input and output and the average energy per pulse must respect an upper bound. By using a continuous wave laser to seed the pulsed laser that generates the states, we avoid the need for expensive electro-optical modulators as used in https://arxiv.org/abs/2004.08307. With this scheme we achieve an extraction rate of certified quantum randomness of around 625kHz.

[80] *Advantage of multi-partite entanglement for quantum cryptography over long and short ranged networks*

Janka Memmen (Technische Universität Berlin), Jens Eisert (Freie Universität Berlin) and Nathan Walk (Freie Universität Berlin).

Whilst the use of multi-partite entanglement is known to offer an advantage over bi-partite protocols in certain contexts, the quest to find practical advantage scenarios is ongoing and substantial difficulties in generalising some bi-partite security proofs remain. We present rigorous results that address both these challenges. First, we prove the security of a variant of the GHZ state based secret sharing protocol against general attacks, including participant attacks which break the security of the original GHZ state scheme. We then identify parameters for a performance advantage over realistic bottleneck networks in terms of extractable secret bits per network use. We show that whilst channel losses limit the advantage region to short distances over direct transmission networks, the addition of quantum repeaters unlocks the performance advantage of multi-partite entanglement over point-to-point approaches for long distance quantum cryptography.

[82] *CVQKD payload and receiver for SPOQC mission*

Rupesh Kumar (Univeristy of York).

In this talk, I will present the research and development of a quantum payload constructed for the Satellite Platform for Optical Quantum Communications (SPOQC) - a CubeSat mission by the Quantum Communication Hub, UK, scheduled for launch in 2025. The payload generates amplitude and phase-modulated coherent states for performing Continuous Variable Quantum Key Distribution (CVQKD) with Gaussian modulated coherent state protocol with a transmitter local oscillator based design. The payload is also equipped with a shot noise-limited homodyne detector, which will act as a Quantum Random Number Generator (QRNG), as well as a shot noise-limited optical receiver unit for ground-to-space uplink communication. We have also constructed an optical receiver unit for the ground station, based on single quadrature homodyne detection with shot noise sensitivity. The talk will disclose many interesting features of the payload and receiver, such as amplitude modulation without bias control, tolerance to polarization rotation, and a large-area detector unit that avoids the use of adaptive optics, among others.

[85] *Quantum Technologies in Quantum-Safe Public Key Infrastructure Networks*

Paula Alonso Blanco (ICFO - The Institute of Photonic Sciences), Luis Trigo Vidarte (ICFO - The Institute of Photonic Sciences), Marc Romeu Casas (Quside Technologies SL), Fernando de la Iglesia (Quside Technologies SL), Jordi Mur-Petit (Nestlé Global IT Innovation Hub) and Valerio Pruneri (ICFO - The Institute of Photonic Sciences).

We feature the interplay of classical cryptography and quantum technologies, highlighting the importance of the coexistence of both paradigms in practical quantum-safe networks. We motivate the use of QRNGs in PQC protocols, showing that they can potentially increase the security of the system without affecting the performance. We continue proposing some guidelines on the alternatives for QKD authentication methods depending on the use case, the available resources, and the security needs, to improve the practicality of QKD deployment in PKI networks. Moreover, we present a novel authentication scheme for QKD, designed to reduce the key drain from the authentication, showing the results of its implementation in an experimental QKD prepare-measurement BB84 protocol with polarization encoding and decoy states.

[86] *A Practical Protocol for Quantum Oblivious Transfer from One-Way Functions*

Eleni Diamanti (Sorbonne Université, CNRS, LIP6), Alex Bredariol Grilo (Sorbonne Université, CNRS, LIP6), Adriano Innocenzi (Sorbonne Université, CNRS, LIP6), Pascal Lefebvre (Sorbonne Université, CNRS, LIP6), Verena Yacoub (Sorbonne Université, CNRS, LIP6) and Alvaro Yángüez (Sorbonne Université, CNRS, LIP6).

We present a new simulation-secure quantum oblivious transfer (QOT) protocol based on one-way functions in the plain model. With a focus on practical implementation, our protocol surpasses prior works in efficiency, promising feasible experimental realization. We address potential experimental errors and their correction, offering analytical expressions to facilitate the analysis of the required quantum resources. Technically, we achieve our results by achieving simulation security for QOT through an equivocal and relaxed-extractable quantum bit commitment.

[87] *Quantum key distribution rates from non-symmetric conic optimization*

Andrés González Lorente (University of Valladolid), Pablo V. Parellada (University of Valladolid), Miguel Castillo-Celeita (University of Valladolid) and Mateus Araújo (University of Valladolid).

Computing key rates in QKD numerically is essential to unlock more powerful protocols, that uses more sophisticated measurement bases or quantum systems of higher dimension. It is a difficult optimization problem, that depends on minimizing a convex non-linear function, the relative entropy. The gold standard for solving such problems is a primal-dual interior-point algorithm, that is highly efficient and inherently gives upper and lower bounds. Recently one such algorithm was discovered for non-symmetric cones, a category that includes the relative entropy, and was previously out of reach.

Here we adapt this algorithm to the problem of computation of key rates, obtaining a very efficient technique for lower bounding them. In comparison to previous techniques it has the advantages of flexibility, ease of use, and above all performance.

[88] *Cost of quantum secret key*

Karol Horodecki (Institute of Informatics, Faculty of Mathematics, Physics and Informatics, University of Gdańsk), Leonard Sikorski (Institute of Informatics, Faculty of Mathematics, Physics and Informatics, University of Gdańsk), Siddhartha Das (Center for Security, Theory and Algorithmic Research, International Institute of Information Technology Hyderabad India) and Mark M. Wilde (School of Electrical and Computer Engineering, Cornell University, Ithaca, New York 14850, USA).

In this paper, we develop the resource theory of quantum secret key. Operating under the assumption that entangled states with zero distillable key do not exist, we define the key cost of a quantum state, and device. We study its properties through the lens of a quantity that we call the key of formation. The main result of our paper is that the regularized key of formation is an upper bound on the key cost of a quantum state. The core protocol underlying this result is privacy dilution, which converts states containing ideal privacy into ones with diluted privacy. Next, we show that the key cost is bounded from below by the regularized relative entropy of entanglement, which implies the irreversibility of the privacy creation-distillation process for a specific class of states. We further focus on mixed-state analogues of pure quantum states in the domain of privacy, and we prove that a number of entanglement measures are equal to each other for these states, similar to the case of pure entangled states. The privacy cost and distillable key in the single-shot regime exhibit a yield-cost relation, and basic consequences for quantum devices are also provided.

[93] *Routed Bell tests and their application to device-independent quantum key distribution*

Tristan Le Roy-Deloison (Univ Lyon, Inria, ENS Lyon, UCBL, LIP and Télécom Paris-LTCI, Institut Polytechnique de Paris), Edwin Peter Lobo (Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB)), Jef Pauwels (Department of Applied Physics, University of Geneva and Constructor University) and Stefano Pironio (Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB)).

Losses in the transmission channel, which increase with distance, pose a major obstacle to photonics demonstrations of quantum nonlocality and its applications to device-independent protocols such as device-independent quantum key distribution. Recently, Chaturvedi, Viola, and Pawlowski (CVP) [arXiv:2211.14231] introduced a variation of standard Bell experiments, which we call routed Bell experiments, with the goal of extending the range over which quantum nonlocality can be demonstrated. In these experiments, in some of the rounds, photons from the source are routed by an actively controlled switch to a nearby test device instead of the distant one. CVP showed that there are quantum correlations in routed Bell experiments such that the outcomes of the remote device cannot be classically predetermined, even when its detection efficiency is arbitrarily low. In our work, we show that the correlations considered by CVP, though they cannot be classically predetermined, do not require the transmission of quantum systems to the remote device. This leads us to properly define the concept of 'short-range' and 'long-range' quantum correlations in routed Bell experiments. We then explore the conditions under which short-range quantum correlations can be ruled out. We find that routed Bell experiments do allow for reducing the detection efficiency threshold but the improvements are smaller than those suggested by CVP's analysis. We then investigate DIQKD protocols based on the routed setup. We show how to analyze the security of these protocols and compute lower bounds on the key rates using non-commutative polynomial optimization and the Brown-Fawzi-Fawzi method. We determine lower bounds on the asymptotic key rates of several simple two-qubit routed DIQKD protocols based on CHSH or BB84 correlations and compare their performance to standard protocols. We find that in an ideal case routed DIQKD protocols can significantly improve detection efficiency requirements, by up to 30%, compared to their non-routed counterparts. Notably, the routed BB84 protocol achieves a positive key rate with a detection efficiency as low as 50% for the distant device, the minimal threshold for any DIQKD protocol featuring two untrusted measurements. However, the advantages we find are highly sensitive to noise and losses affecting the short-range correlations involving the additional test device.

[94] *Optical-pumping attack on a laser source in quantum key distribution*

Maksim Fadeev (Russian Quantum Center), Anastasia Ponosova (Russian Quantum Center), Roman Shakovoi (QRate), Vadim Makarov (University of Vigo), Irina Zhluktova (Prokhorov General Physics Institute of Russian Academy of Sciences) and Vladimir Tsvetkov (Prokhorov General Physics Institute of Russian Academy of Sciences).

Quantum key distribution (QKD) technology allows sharing secret keys between two parties over an insecure channel. But there are vulnerabilities in the technical implementation of systems. Laser seeding attack is one of the examples of imperfections in QKD systems. Recent works have demonstrated that Eve can manipulate output power of Alice's laser. This leads to an increase of the average photon number, emitted by Alice. But this attack can be prevented by using passive fiber-optic elements such as isolators or DWDM-filters. In this work, we demonstrate a new kind of attack namely, the optical pumping attack. This attack utilises imperfections in passive optic elements that are used in QKD systems to prevent other types of attack. Eve can use source at different wavelength to seed Alice laser, 1064 nm for example. This radiation would be absorbed by crystal within laser and create additional population inversion to inversion created by bias current, that drives Alice laser. This pumping would change average photon number at the output of Alice, leading to wrong estimation of lower bound on the secret key rate. This creates a side-channel for Eve for obtaining key information. In this work we performed this kind of attack for several wavelengths: 1064 nm, 1310 nm, 1480 nm and 2000 nm, measured changing of pulse energy, average output power and pulse shape under attacks at different wavelengths. Finally, we provide theoretical estimation of required isolation at the tested wavelengths to protect the source against the optical-pumping attack.

[95] *On Classical Data Encryption in QKD*

Valeria Pastushenko (Terra Quantum AG).

Classical communication between legitimate users in conventional QKD protocols is assumed to be open and fully known by a potential eavesdropper. In this work, we study the potential benefits of classical data encryption under highly feasible assumptions concerning the eavesdropper's quantum memory. We contextualise the proposed method by comparing it with existing quantum data locking protocols and analyse its advantages as well as associated risks.

[97] *Impossibility of Cheat-sensitive Quantum Private Queries*

Severin Winkler (Ergon Informatik AG, Zurich, Switzerland) and Esther Hänggi (Lucerne School of Computer Science and Information Technology, Rotkreuz, Switzerland).

Symmetric private information retrieval is a cryptographic task that allows to query a database and obtain exactly one entry without revealing to the owner of the database which element was accessed. The tasks is a variant of the general two-party protocols called “secure function evaluation” and is closely related to oblivious transfer. Under the name “quantum private queries”, quantum protocols have been proposed to solve this problem in a cheat-sensitive way, where it is not impossible for dishonest participants to cheat, but they risk detection. We give an explicit attack against any such protocol, showing that quantum protocols do not allow to implement cheat-sensitive symmetric private information retrieval. Our result extends to any form of oblivious transfer and many variants of secure function evaluation.

[98] *randextract: A Library to Test and Validate Privacy Amplification Implementations*

Iyan Mendez Veiga (ETHZ) and Esther Hänggi (Lucerne University of Applied Sciences and Arts).

We provide a reference implementation for the privacy amplification functions used in quantum key distribution and quantum random number generators. Our application allows to detect security-relevant deviations from the expected functions and bugs. We show this at the example of issues in real applications.

[99] *High-dimensional quantum key distribution with resource-efficient detection*

Adam Widomski (University of Warsaw), Maciej Ogrodnik (University of Warsaw) and Michał Karpiński (University of Warsaw).

Quantum key distribution (QKD) has emerged as a leading solution to meet the increasing need for secure communication systems in the light of potential threads posed by advancements in quantum computing. Recent developments include multiple works on high-dimensional QKD systems, which outperform qubit-based solutions in terms of ro- bustness and theoretically-achievable key rates. However, such systems are more compli- cated and expensive. In this work we overcome those issues by using only one single photon detector per measurement basis. We show that high-dimensional QKD symbols can be de- tected using a single time-resolved photon detector with the Talbot effect. We report on the theoretical limitations of our method and present experimentally-obtained key rates for the two-dimensional and four-dimensional case.

[100] *Bounds on Petz-Rényi Divergences and their Applications for Device-Independent Cryptography*

Thomas A. Hahn (Weizmann Institute of Science), Ernest Y.-Z. Tan (Institute for Quantum Computing, University of Waterloo) and Peter Brown (Télécom Paris-LTCI, Institut Polytechnique de Paris).

Variational techniques have been recently developed to find incredibly tight bounds on the von Neumann entropy in a completely device-independent (DI) setting. This, in turn, has led to significantly improved key rates of DI protocols, in both the asymptotic limit as well as in the finite-size regime. In this paper, we discuss two approaches towards applying these variational methods for Petz-Rényi divergences instead. We then show how this can be used to further improve the finite-size key rate of DI protocols, utilizing a fully-Rényi entropy accumulation theorem developed in a partner work. Petz-Rényi divergences can also be applied to study DI advantage distillation, in which two-way communication is used to improve the noise tolerance of quantum key distribution (QKD) protocols. We implement these techniques to derive increased noise tolerances for DIQKD protocols, which surpass all previous known bounds.

[103] *Faithfully Simulating Near-Term Quantum Repeaters*

Julius Wallnöfer (Dahlem Center for Complex Quantum Systems, Freie Universität Berlin), Frederik Hahn (Technische Universität Berlin), Fabian Wiesner (Technische Universität Berlin), Nathan Walk (Freie Universität Berlin) and Jens Eisert (Freie Universität Berlin).

Quantum repeaters have long been established to be essential for distributing entanglement over longdistances. Consequently, their experimental realization constitutes a core challenge of quantum communi-cation. However, there are numerous open questions about implementation details for realistic near-termexperimental setups. In order to assess the performance of realistic repeater protocols, here we presentReQuSim, a comprehensive Monte Carlo–based simulation platform for quantum repeaters that faithfullyincludes loss and models a wide range of imperfections such as memories with time-dependent noise. Ourplatform allows us to perform an analysis for quantum repeater setups and strategies that go far beyondknown analytical results: This refers to being able to both capture more realistic noise models and analyzemore complex repeater strategies. We present a number of findings centered around the combination ofstrategies for improving performance, such as entanglement purification and the use of multiple repeaterstations, and demonstrate that there exist complex relationships between them. We stress that numericaltools such as ours are essential to model complex quantum communication protocols aimed at contributingto the quantum Internet.

[104] *A Passive and Self-Characterizing Receiver for Cross-Encoded Reference-Frame-Independent Quantum Key Distribution*

Massimo Giacomin (Università degli Studi di Padova), Costantino Agnesi (Università degli Studi di Padova), Francesco Bruno Leonardo Santagiustina (Università degli Studi di Padova), Giuseppe Vallone (Università degli Studi di Padova) and Paolo Villoresi (Università degli Studi di Padova).

The successful application of Quantum Key Distribution is dependent on the accurate generation and detection of quantum states, and a communication mechanism that can withstand disturbances caused in the channel. The selection of the optimal encoding strategy is complex and is influenced by external elements such as the characteristics of the quantum channel. Polarization encoding is acknowledged for its dependability and low error rate, rendering it ideal for free-space links, whereas time-bin encoding is robust to birefringence, thereby making it suitable for optical fiber networks. The strength of polarization-based protocols is based on the full characterization of the receiver, to reconstruct the information encoded in the shared qubits. This is typically achieved through tomographic analysis, which adds to the complexity of the final protocol. In this research, we introduce a unique cross-encoded method, where high precision quantum states are produced using a self-regulating, calibration-free polarization modulator and then conveyed through a polarization-to-time-bin converter. A hybrid receiver is used to carry out both time-of-arrival and polarization measurements for decoding the quantum states. Moreover, the suggested receiver is optimized to perform a self-characterization process, utilizing the same photons in which the information is encoded. The adaptability of our approach can lead to a significant advancement in the creation of hybrid networks that incorporate both optical fiber and free-space networks.

[105] *Quantum-secure multi-party deep learning*

Kfir Sulimany Solan (MIT), Sri Krishna Vadlamani (MIT), Prahlad Iyengar (MIT), Cole Brabec (MIT), Leshem Choshen (MIT-IBM Watson AI Lab) and Dirk Englund (MIT).

The necessity of multi-party computing has become increasingly evident due to the exploding demand for distributed machine learning. Offloading computationally intensive DNN inference to cloud servers introduces vulnerabilities that compromise user data security. To address this challenge, we introduce a coherent linear algebra engine for private multi-party computation of distributed machine learning tasks, leveraging conventional telecom components. We evaluate the fidelity of inner product computations, MNIST classification accuracy, and potential information leakage. Our analyses reveal a trade-off between classification accuracy and data privacy. This trade-off diminishes in significance for large-scale tasks, indicating the potential to achieve both classification accuracy and privacy simultaneously.

[106] *Finite resource performance of small satellite-based quantum key distribution missions*

Tanvirul Islam (Centre for Quantum Technologies, National University of Singapore), Jasminder Sidhu (University of Strathclyde), Brendon Higgins (Institute for Quantum Computing, University of Waterloo), Thomas Brougham (University of Strathclyde), Tom Vergoossen (SpeQtral Pte. Ltd.), Daniel Oi (University of Strathclyde), Thomas Jennewein (Institute for Quantum Computing, University of Waterloo) and Alexander Ling (Centre for Quantum Technologies, National University of Singapore).

In satellite-based quantum key distribution (QKD), the number of secret bits that can be generated in a single satellite pass over the ground station is severely restricted by the pass duration and the free-space optical channel loss. High channel loss may decrease the signal-to-noise ratio due to background noise, reduce the number of generated raw key bits, and increase the quantum bit error rate (QBER), all of which have detrimental effects on the output secret key length. Under finite-size security analysis, higher QBER increases the minimum raw key length necessary for non-zero secret key length extraction due to less efficient reconciliation and post-processing overheads. We show that recent developments in finite key analysis allow three different small-satellite-based QKD projects CQT-Sat, UK-QUARC-ROKS, and QEYSSat to produce secret keys even under very high loss conditions, improving on estimates based on previous finite key bounds. This suggests that satellites in low Earth orbit can satisfy finite-size security requirements, but remains challenging for satellites further from Earth. We analyse the performance of each mission to provide an informed route toward improving the performance of small-satellite QKD missions. We highlight the short and long-term perspectives on the challenges and potential future developments in small-satellite-based QKD and quantum networks. In particular, we discuss some of the experimental and theoretical bottlenecks, and improvements necessary to achieve QKD and wider quantum networking capabilities in daylight and at different altitudes.

[108] *Quantum Key Distribution Between Low-SWaP Mobile Platforms*

Samantha Isaac (University of Illinois), Lars Kamin (University of Waterloo), Andrew Conrad (University of Illinois at Urbana-Champaign), Roderick Cochran (The Ohio State University), Daniel Sanchez-Rosales (The Ohio State University), Timur Javid (University of Illinois), A.J. Schroeder (University of Illinois), Grzegorz Golba (University of Illinois), Norbert Lutkenhaus (University of Waterloo), Daniel Gauthier (The Ohio State University) and Paul Kwiat (University of Illinois).

While most current quantum network nodes are connected via fiber-based or free-space fixed point-to-point links, there have been many advancements in the last decade that expand these nodes to include mobile, re-configurable, and wireless platforms such as uncrewed aerial vehicles (UAVs) and satellites. The size, weight, and power (SWaP) restrictions of these platforms pose constraints that potentially impact the system performance of mobile nodes. Here, we will discuss our progress towards developing a low-SWaP mobile quantum key distribution (QKD) platform that can exchange quantum-secured random keys between both drones and cars. We implement a finite-key security proof that incorporates system imperfections in state preparation and analysis, including channel losses. These imperfections, present in any system, require consideration during key consolidation to minimize information leakage. We demonstrate average finite secure key rates between mobile platforms up to 19.6 kbit/s.

[114] *General QKD security framework and the Open QKD Security Software Suite Version 2*

John Burniston (Institute for Quantum Computing, University of Waterloo), Lars Kamin (Institute for Quantum Computing, University of Waterloo) and Norbert Lutkenhaus (Institute for Quantum Computing, University of Waterloo).

The security analysis of many protocols relies on closed form bounds on entropic quantities that model devices. These closed form expressions can typically only be found by exploiting some sort of symmetry not present in many realistic unstructured QKD protocols. Our software provides a framework for efficiently evaluating secret key rates of generic unstructured QKD protocols with tighter lower bounds while providing more flexible and realistic modelling capabilities. Through its modular structure, our software package breaks down the task of constructing a (numerical) security proof into well defined domains including protocol design, modelling implementations, security frameworks, and numerical optimization, each of which has its own community of experts. By utilizing modules built by these communities, we aim to facilitate wide spread collaboration throughout the QKD community. The newly expanded and redesigned software is expected to be released early May 2024.

[116] *Unclonable Secret Sharing*

Prabhanjan Ananth (University of California, Santa Barbara), Vipul Goyal (NTT Research, Carnegie Mellon University), Jiahui Liu (MIT) and Qipeng Liu (University of California, San Diego).

Unclonable cryptography utilizes the principles of quantum mechanics to addresses cryptographic tasks that are impossible classically. We introduce a novel unclonable primitive in the context of secret sharing, called unclonable secret sharing (USS). In a USS scheme, there are n shareholders, each holding a share of a classical secret represented as a quantum state. They can recover the secret once all parties (or at least t parties) come together with their shares. Importantly, it should be infeasible to copy their own shares and send the copies to two non-communicating parties, enabling both of them to recover the secret.

Our work initiates a formal investigation into the realm of unclonable secret sharing, shedding light on its implications, constructions, and inherent limitations.

Connections: We explore the connections between USS and other quantum cryptographic primitives such as unclonable encryption and position verification, showing the difficulties to achieve USS in different scenarios.

Limited Entanglement: In the case where the adversarial shareholders do not share any entanglement or limited entanglement, we demonstrate information-theoretic constructions for USS.

Large Entanglement: If we allow the adversarial shareholders to have unbounded entanglement resources (and unbounded computation), we prove that unclonable secret sharing is impossible. On the other hand, in the quantum random oracle model where the adversary can only make a bounded polynomial number of queries, we show a construction secure even with unbounded entanglement.

Furthermore, even when these adversaries possess only a polynomial amount of entanglement resources, we establish that any unclonable secret sharing scheme with a reconstruction function implementable using Clifford and logarithmically many T-gates is also unattainable.

[118] *Verification of Spatially Distributed Entanglement*

Yusuf Alnawakhtha (University of Maryland--College Park), Manasi Shingane (University of Maryland--College Park), Andrew Childs (University of Maryland--College Park) and Carl Miller (University of Maryland--College Park, National Institute of Standards and Technology).

Certifying the existence of entanglement between two parties is a fundamental problem in quantum information science. In this work, we develop a protocol for verifying that two parties located at specified positions share an entangled quantum state. We accomplish this by embedding the CHSH game in a quantum position verification protocol. This provides a form of entanglement testing that not only ensures that provers passing the protocol share entanglement, but that they are also located where they claim to be. This prevents parties from passing the verification test by simply forwarding the input of the verification protocol to other parties that share entanglement. The protocol has low requirements on the quantum computational abilities of honest provers---namely, it only requires the honest provers to manipulate two qubits each. It achieves security against adversaries located at incorrect positions that share at most a logarithmic amount of quantum memory with respect to the size of the classical input.

[119] *On black-box separations of quantum digital signatures from pseudorandom states*

Andrea Coladangelo (University of Washington) and Saachi Mutreja (Columbia University).

It is well-known that digital signatures can be constructed from one-way functions in a black-box way. While one-way functions are essentially the minimal assumption in classical cryptography, this is not the case in the quantum setting. A variety of qualitatively weaker and inherently quantum assumptions (e.g. EFI pairs, one-way state generators, and pseudorandom states) are known to be sufficient for non-trivial quantum cryptography. While it is known that commitments, zero-knowledge proofs, and even multiparty computation can be constructed from these assumptions, it has remained an open question whether the same is true for quantum digital signatures schemes (QDS). In this work, we show that there does not exist a black-box construction of a QDS scheme with classical signatures from pseudorandom states with linear, or greater, output length. Our result complements that of Morimae and Yamakawa (2022), who described a one-time secure QDS scheme with classical signatures, but left open the question of constructing a standard multi-time secure one.

[120] *A reconfigurable multi-user quantum network with ground to space link*

Stephane Vinet (Institute for Quantum Computing, University of Waterloo), Ramy Tannous (Institute for Quantum Computing, University of Waterloo) and Thomas Jennewein (Institute for Quantum Computing, University of Waterloo).

We present a reconfigurable quantum network architecture which enables the interconnectivity between a satellite node and a multitude of users on the ground. The network has dual-functionality : during the satellite-pass the network adopts a point-to-multipoint topology where all the users communicate with the satellite in an uplink configuration. Outside of a satellite pass, the signal is rerouted through telecom fibre to form a fully-connected network on the ground. To minimize the hardware requirements, we consider a multiplexed pulsed entangled photon source combined with a frequency-to-time mapping. We evaluate the potential of the proposed network configuration by simulating its performance for different quantum key distribution scenarios. Our results show that high key rates can be achieved in spite of limited resources on the satellite. An experimental verification of the protocol is under way, and we will present the latest findings. The promising scalability and easy integration make this network architecture a good candidate for future quantum communication networks.

[128] *Modular Approach to Unclonable Cryptography*

Prabhanjan Ananth (UCSB) and Amit Behera (Ben-Gurion University).

We explore a new pathway to designing unclonable cryptographic primitives. We propose a new notion called unclonable puncturable obfuscation (UPO) and study its implications for unclonable cryptography. Using UPO, we present modular (and in some cases, arguably, simple) constructions of many primitives in unclonable cryptography, including, public-key quantum money, quantum copy-protection for many classes of functionalities, unclonable encryption, and single-decryption encryption.

Notably, we obtain the following new results assuming the existence of UPO:

- We show that any cryptographic functionality can be copy-protected as long as this functionality satisfies a notion of security, which we term puncturable security. Prior feasibility results focused on copy-protecting specific cryptographic functionalities.

- We show that copy-protection exists for any class of evasive functions as long as the associated distribution satisfies a preimage-sampleability condition. Prior works demonstrated copy-protection for point functions, which follows as a special case of our result.

We put forward a candidate construction of UPO and prove two notions of security, each based on the existence of (post-quantum) sub-exponentially secure indistinguishability obfuscation and one-way functions, the quantum hardness of learning with errors, and a new conjecture called simultaneous inner product conjecture.

[131] *Experimental demonstration of Einstein--Podolsky--Rosen steering in high-speed telecommunication system with detection loophole closed*

Qiang Zeng (Beijing Academy of Quantum Information Sciences), Huihong Yuan (Beijing Academy of Quantum Information Sciences), Haoyang Wang (Beijing University of Posts and Telecommunications), Lai Zhou (Beijing Academy of Quantum Information Sciences) and Zhiliang Yuan (Beijing Academy of Quantum Information Sciences).

Nonlocal correlation represents the key feature of quantum mechanics, which is exploited as a resource in quantum information processing. However, the loophole issues hamper the practical applications. We report the first demonstration of steering nonlocality with detection loophole closed at telecommunication wavelengths. In this endeavour, we design and fabricate a low-loss silicon chip for efficient entanglement generation, and further apply direct modulation technique to its optical pump to eliminate phase-encoding loss at the steering side. The newly proposed phase-encoding measurement setting adapts to an ultra fast modulation rate (GHz). Consequently, we build a fiber-optic setup that can overcome the detection efficiency that is required by quantum steering with multiple measurement settings. Our setup provides an immediate platform for exploring applications based on steering nonlocality, especially for quantum communication.

[132] *Squeezed state continuous-variable quantum key distribution over 40 km fibre with local local oscillator*

Huy Nguyen (Technical University of Denmark), Ivan Derkach (Technical University of Denmark), Hou-Man Chin (Technical University of Denmark), Adnan Hajomer (Technical University of Denmark), Nitin Jain (Technical University of Denmark), Ulrik Andersen (Technical University of Denmark), Vladyslav Usenko (Palacky University) and Tobias Gehring (Technical University of Denmark).

Squeezed states of light promise significant advantages for enhancing the performance of continuous-variable quantum key distribution (CV-QKD) systems. These advantages include the ability to reach longer distances, tolerate higher levels of excess noise, and operate at lower information reconciliation efficiency. So far those advantages were only predicted in theory. In this work, we experimentally demonstrate a CV-QKD system over 40 km fibre using squeezed light achieving a secret key rate of 0.0318 bits per channel use, surpassing the equivalent coherent state system. Similar to state-of-the-art coherent state QKD systems our system employs digital signal processing for impairment compensation eliminating the need for complex locking mechanisms and enhancing its suitability for practical implementations.

[137] *Bridging the Gap: EAGLE-1 long distance space based QKD; from research laboratory to an industry driven space mission*

T. Hiemstra (Tesat-Spacecom GmbH & Co. KG).

The EAGLE-1 mission is an important step towards a pan-European ultra-secure quantum key distribution network. The mission is planned, developed and built in a consortium of Universities, research institutes, and space companies partially funded by ESA, the European Commission, and supported by national delegations. The EAGLE-1 satellite will be launched into space at the end of next year or early 2026 and represents the first European space-based quantum key distribution (QKD) system. Within the EAGLE-1 consortium, Tesat-Spacecom GmbH & Co. KG is responsible for developing and integrating the payload assembly of the EAGLE-1 satellite. Quantum technologies are an emerging technology, which are starting to reach the maturity for industrialisation. Companies are identifying business cases that support the development of quantum technologies for commercial applications. The knowledge transfer between researchers and industry poses an important bottleneck for a fast implementation of new products. In addition, the harsh and "unusual" environment of space missions poses a unique set of requirements on the development and qualification of devices. In this contribution, we report on the implementation of the EAGLE-1 mission as well as the challenges in transferring a technology from academia to an industrial product for space.

[138] *Quantum Pseudorandomness Cannot Be Shrunk In a Black-Box Way*

Garazi Muguruza (QuSoft, University of Amsterdam) and Samuel Bouaziz-Ermann (Sorbonne Université, CNRS, LIP6).

Pseudorandom Quantum States (PRS) were introduced by Ji, Liu and Song as quantum analogous to Pseudorandom Generators. They are an ensemble of states efficiently computable but computationally indistinguishable from Haar random states. Subsequent works have shown that some cryptographic primitives can be constructed from PRSs. Moreover, recent classical and quantum oracle separations of PRS from One-Way Functions strengthen the interest in a purely quantum alternative building block for quantum cryptography, potentially weaker than OWFs.

However, our lack of knowledge of extending or shrinking the number of qubits of the PRS output still makes it difficult to reproduce some of the classical proof techniques and results. Short-PRSs, that is PRSs with logarithmic size output, have been introduced in the literature along with cryptographic applications, but we still do not know how they relate to PRSs. Here we answer half of the question, by showing that it is not possible to shrink the output of a PRS from polynomial to logarithmic qubit length while still preserving the pseudorandomness property, in a relativized way. More precisely, we show that relative to Kretschmer's quantum oracle (TQC 2021) short-PRSs cannot exist (while PRSs exist, as shown by Kretschmer's work).

[139] *Classical-Quantum Dual Encoding for Laser Communications in Space: Enhancing Security and Efficiency*

Matthew Winnel (The ARC Centre of Excellence for Quantum Computation and Communication Technology), Ziqing Wang (School of Electrical Engineering and Telecommunications), Robert Malaney (School of Electrical Engineering and Telecommunications), Ryan Aguinaldo (Northrop Grumman Mission Systems), Jonathan Green (Northrop Grumman Mission Systems) and Timothy Ralph (The ARC Centre of Excellence for Quantum Computation and Communication Technology).

In conventional laser communications, classical information is transmitted by modulating the laser beam's amplitude and is measured via direct detection. Our research introduces a layer of quantum security to this standard process, specifically designed for free-space channels. We explore a hybrid communication method that simultaneously handles classical information in the traditional manner and quantum information through fluctuations in a sub-Poissonian noise-floor. Our approach utilizes a continuous-variable quantum key distribution (CV QKD) protocol, employing a Gaussian ensemble of squeezed states combined with direct detection. This allows for the generation of secure keys while maintaining classical communication, under passive attacks. This quantum-enhanced method offers simplicity, robustness, and efficiency without compromising classical data transfer rates. We have conducted detailed simulations to evaluate the protocol's performance in a free-space atmospheric channel and assessed the security of the CV QKD protocol in the composable finite-size scenario. This added quantum layer provides a practical, secure enhancement to standard laser communication systems.

[140] *Experimental implementation of quantum oblivious transfer from one-way functions*

Adriano Innocenzi (Sorbonne Université, CNRS, LIP6), Verena Yacoub (Sorbonne Université, CNRS, LIP6), Alvaro Yanguez (Sorbonne Université, CNRS, LIP6), Pascal Lefebvre (Sorbonne Université, CNRS, LIP6), Alex Bredariol Grilo (Sorbonne Université, CNRS, LIP6) and Eleni Diamanti (Sorbonne Université, CNRS, LIP6).

We present the implementation of a new simulation-secure quantum oblivious transfer protocol based on one-way functions. The protocol allows an efficient and noise-tolerant experimental realization, surpassing prior works' performances in terms of required quantum and classical resources. We provide the complete integration of a software and an experimental source, achieving a black-box implementation of the quantum oblivious transfer primitive, to be leveraged in the future for secure multiparty computation.

[142] *Maximal Intrinsic Renyi Randomness*

Kriss Gutierrez Anco (Telecom Paris), Tristan Nemoz (Telecom Paris) and Peter Brown (Telecom Paris).

The amount of cryptographically secure randomness one can extract from a source can be linked to an optimization over conditional sandwiched Rényi entropies. Though these can be difficult to compute in general, we consider a simplified setting in which closed-form expressions can be obtained. More precisely, we consider a quantity we call the maximal intrinsic Rényi randomness and combine it with recent results on privacy amplification to derive simple expressions for the maximal quantity of $\epsilon$-secure randomness that can be extracted from finite uses of some memoryless source (which may be entangled with some eavesdropper). Overall this gives a simple method to compute this operationally relevant quantity and provides a benchmarking tool for the rates of finite size security proofs for randomness generation and quantum key distribution protocols. Along the way, we also prove closed-form expressions for the intrinsic randomness measured with respect to other Rényi entropy families.

[143] *A Simple and Effective Countermeasure against Time-Shift to Quantum Key Distribution Systems*

Toshitsugu Kato (Hokkaido University) and Akihisa Tomita (Hokkaido University).

Since the first QKD protocol was proposed by Bennett and Brassard in 1984, practical QKD systems have been successfully demonstrated. Despite these developments, QKD systems have not been widely deployed due to imperfections in real-world devices. Many eavesdropping methods have been proposed to exploit the imperfections. One of those is the time-shift attack that exploits mismatches in temporal responses of avalanche photodiodes (APDs) to control the receiver's detection. Zhao's group demonstrated the time-shift attack successfully in 2008. The time-shift attack can be realized with current technology, and it will threaten the secure key distribution. We propose a simple and effective countermeasure to the time-shift attack by connecting additional APDs to detection ports through beamsplitters to average temporal responses of APDs. This method can reduce the photon detection mismatches between port 0 and port 1. Our simulation shows that averaging the temporal responses of APDs efficiently neutralizes the attack.

[144] *String commitment from unstructured noisy channels*

Jiawei Wu (National University of Singapore), Masahito Hayashi (The Chinese University of Hong Kong, Shenzhen) and Marco Tomamichel (National University of Singapore).

Noisy channel is a valuable resource for cryptography. It can be used to build cryptographic primitives like bit commitment and oblivious transfer that are information-theoretically secure between two untrusting parties. Existing studies on this topic focus on the channel that does not change over successive uses. In this work, we study non-independent and identically distributed (non-i.i.d.) channels with constraint on min-entropy. The dishonest player is able to configure the channel at his will under the constraint. We devise a protocol that is complete, hiding, and binding, and give its commitment rate.

[145] *Frequency multiplexed entanglement at telecom wavelengths: toward multipartite quantum communications*

David Fainsin (Laboratoire Kastler Brossel), Victor R. Rodriguez (ICFO), Olena Kovalenko (Palacky University), Guilherme L. Zanin (Federal University of Goiás), Nicolas Treps (Laboratoire Kastler Brossel), Vladyslav Usenko (Palacky University), Eleni Diamanti (LIP6) and Valentina Parigi (Laboratoire Kastler Brossel).

Continuous variable encoding of quantum information requires the deterministic generation of highly correlated quantum states of light in the form of quantum networks, which, in turn, necessitates the controlled generation of a large number of squeezed modes. In this work, we present an experimental source of multimode squeezed states of light at telecommunication wavelengths. Generation at such wavelengths is especially important as it can enable quantum information processing, communication, and sensing beyond the laboratory scale. We use a single-pass spontaneous parametric down-conversion process in a non-linear waveguide pumped with the second harmonic of a femtosecond laser. We demonstrate multiparty entanglement by measuring the state's covariance matrix. Our measurements reveal significant squeezing in more than 21 frequency modes, with a maximum squeezing value exceeding 2.5 dB. We finally present a frequency-multiplexed quantum key distribution protocol and the expected key rates in bipartite and in multipartite scenarii.

[146] *Robust and composable device-independent quantum protocols for oblivious transfer and bit commitment*

Rishabh Batra (CQT, NUS), Sayantan Chakraborty (NUS), Rahul Jain (National University of Singapore) and Upendra Kapshikar (Center for Quantum Technologies, National university of Singapore).

We present robust and composable device-independent quantum protocols for oblivious transfer (OT) and bit commitment (BC) using Magic Square devices. We assume there is no long-term quantum memory, that is, after a finite time interval, referred to as \textbf{DELAY}, the states stored in the devices decohere. By robustness, which is a highlight of our protocols, we mean that the protocols are correct and secure even when devices are slightly off from their ideal specifications (the \emph{faulty but non-malicious} regime). This is an important property, since in the real world, devices would certainly have small manufacturing errors and cannot be expected to be ideal. To the best of our understanding and knowledge, none of the known DI protocols for OT and BC in the literature are robust; they can not guarantee correctness in the faulty but non-malicious regime. Our protocols are sequentially composable and hence, can be used as building blocks to construct larger protocols, while still preserving security guarantees.

[147] *Ground-to-ground tests for the QKD pathfinder satellite mission QUBE*

Moritz Birkhold (LMU Munich), Adomas Baliuka (LMU Munich), Michael Auer (LMU Munich), Michael Steinberger (LMU Munich), Harald Weinfurter (LMU Munich), Paul Wagner (DLR IKN), Benjamin Rödiger (DLR IKN), Florian Moll (DLR IKN), Jonas Pudelko (FAU Nuernberg), Joost Vermeer (FAU Nuernberg), Christoph Marquardt (FAU Nuernberg) and Lukas Knips (LMU Munich).

To establish a reliable Quantum Key Distribution (QKD) link from a satellite in low-earth orbit (LEO) to a ground station, a series of ground-to-ground tests are essential. These tests, varying in distance and objectives, are for fine-tuning both the sender and receiver systems to address the unique challenges of satellite communications. We detail the methods and outcomes of progressively complex QKD tests, for the different components of the satellite and ground station. The experiments clearly show the performance of the quantum optics payload as well as the capability of the QKD receiver and the optical ground station (OGS).

[150] *Second-generation quantum repeaters enabled by high-dimensional entanglement*

Tomohiro Yamazaki (NTT Basic Research Laboratories, NTT Corporation) and Koji Azuma (NTT Basic Research Laboratories, NTT Corporation).

Linear-optical entanglement swapping works only probabilistically. Quantum repeater protocols based on it, classified in the first generation, inevitably need classical communication between non-adjacent nodes, which makes the protocols very slow and requires quantum memories with long coherence time. One way to realize faster quantum repeater protocols, classified in the second generation, is to use matter qubits, which enables deterministic entanglement swapping. However, such matter qubits are still experimentally challenging. Here we propose a linear-optical circuit that projects two input qudits of dimension d onto a Bell state defined in a two-qubit subspace with the probability of 1 − d−1, which can be used to realize almost deterministic entanglement swapping for large d. Based on it, we propose a quantum repeater protocol consisting of linear optical elements, photon detectors, high-dimensional quantum memories, and photonic three-qudit GHZ states. In the protocol, the classical communication between non-adjacent nodes becomes unnecessary thanks to the high success probability of the entanglement swapping, making the protocol be categorized into the second generation.

[151] *Quantum Machine Learning Assisted Improvement in Disturbance Threshold and Information Gain*

Chitra Shukla (SnT, University of Luxembourg, 1855 Luxembourg, Luxembourg), Abhishek Shukla (Institute for Materials Research (IMO), Hasselt University, Wetenschapspark 1, B-3590 Diepenbeek, Belgium) and Oscar Dahlsten (SIQSE, Southern University of Science and Technology, Shenzhen 518055, China).

In a quantum key distribution protocol, an eavesdropper Eve extracts information by performing the measurement on flying qubits. If the measurement basis does not match with the basis in which the qubit is prepared, it leads to a disturbance in the qubit state with 1/2 probability. There is an optimal condition between Information Gain and tolerable disturbance. Leveraging machine learning techniques, several advances have been made in the rapid development of quantum applications. In order to achieve the (upper) bound for Information Gain vs. disturbance trade-off, we investigate this optimal condition for the BB84 protocol using the gradient descent algorithm. By employing such a numerical method, we report an improvisation in the upper bound of the disturbance compare to the existing best threshold reported in Phys. Rev. A, 56 1163 (1997). Interestingly, the Information Gain by Eve at this bound is relatively less than reported in the above paper. It means with our strategy Alice-Bob are in advantageous position in both ways as they do not have to abort the protocol as early as required in Phys. Rev. A, 56 1163 (1997) at d=0.146447, as well as now the information leaked to Eve is also lowered.

[152] *Continuous-variable quantum key distribution with noisy squeezed states*

Akash Nag Oruganti (Palacky University), Ivan Derkach (Palacky University) and Vladyslav Usenko (Palacky University).

We address and theoretically analyze continuous-variable quantum key distribution (CV QKD) with noisy squeezed states. The noise in such states unavoidably emerges due to optical losses in the state preparation and has to be taken into account in any practical scenario, with the outcomes depending on the trust assumption on such noise. We show that the untrusted noise should pessimistically be allocated to the anti-squeezed (AS) quadrature and can break the security of the protocols already in the asymptotic regime. In the finite-size regime we analyze the impact of the AS noise on the parameter estimation, showing that it limits the performance of the protocols even if assumed trusted and requires the protocol modifications in terms of modulation and detection schemes. We also consider the noisy squeezed-state CV QKD in the channels with transmittance fluctuations (typical for the atmospheric channels) and show that even trusted AS noise can break the security of the protocols in this regime due to fluctuations-related channel excess noise, which has to be assumed untrusted. Our results demonstrate the importance of the squeezing purity in practical realizations of squeezed-state CV QKD.

[153] *Efficient entanglement swapping via lossy channels*

Wan Zo (Korea Institute of Science and Technology), Bohdan Bilash (Korea Institute of Science and Technology), Donghwa Lee (Korea Institute of Science and Technology), Yosep Kim (Korea University), Hyang-Tag Lim (Korea Institute of Science and Technology), Kyunghwan Oh (Yonsei University), Syed Assad (Australian National University) and Yong-Su Kim (Korea Institute of Science and Technology).

We investigate an entanglement swapping protocol using photon-number-encoded states to alleviate quantum channel losses without requiring quantum memories. The protocol achieves entanglement distribution probability scaling linearly with channel transmission. Unbalanced channel losses can degrade the entanglement, but this is compensated by optimally adjusting the initial states.

[154] *Overcoming Noise Limitations in QKD with Quantum Privacy Amplification*

Philipp Sohr (Vienna University of Technology / Quantum Technology Laboratories GmbH), Sebastian Ecker (Quantum Technology Laboratories GmbH), Lukas Bulla (Quantum Technology Laboratories GmbH), Martin Bohmann (Quantum Technology Laboratories GmbH) and Rupert Ursin (Quantum Technology Laboratories GmbH).

High-quality, distributed quantum entanglement is the distinctive resource for quantum communication and forms the foundation for the unequalled level of security that can be assured in quantum key distribution. While the entanglement provider does not need to be trusted, the secure key rate drops to zero if the entanglement used is too noisy. In this work, we show experimentally that QPA is able to increase the secure key rate achievable with QKD by improving the quality of distributed entanglement, thus increasing the quantum advantage in QKD. Beyond that, we show that QPA enables key generation at noise levels that previously prevented key generation. We provide a detailed characterisation of the gain in secure key rate achieved in our proof-of-principle experiment at different noise levels. The use of hyperentanglement in the field-tested polarisation and energy-time degrees of freedom enhances the efficiency of our scheme, making it an attractive option for deployment in high-loss regimes.

[155] *Analyzing protocol efficiency and Bell inequality tests in quantum networks with NetSquid*

David Perez Castro (Universidade de Vigo).

Quantum technologies have evolved in the last few years to the point where experiments that were once thought theoretical have become experimentally feasible. In this context, we have developed a quantum network simulator based on NetSquid, in which we have incorporated different network protocols and applications. This simulator supports arbitrary topologies and entanglement based QKD protocols. Additionally, traffic models and routing are implemented, through an abstract Network Manager. These experiments aim to recognize the experimental limitations that could emerge in a functional quantum network, emphasising in the use of state of the art quantum technology models, which will be parametrized by any of the properties that define the components of a quantum network: quantum channel distances, damping and dephasing proper times in memories, fidelity of quantum sources, photon fiber coupling, etc. We propose a thorough study to find, of all the aforementioned properties, which of them are the limiting factor in network applications. To characterize these boundaries, two types of applications have been considered of interest:

1. Quantum correlation tests, to see if a Bell Inequality violation is possible when current depolarization and decoherence rates are considered. In particular, the simulation of a CHSH (Clauser-Horne-Shimony-Holt) game is carried out in different setups and with different strategies, to verify the achievability of Tsirelson's bound. This will be used to quantify the loss of quantum correlation in the network.   2. Capacity tests, to see how do quantum switches behave in an entanglement based network and which bitrates are obtainable through state of the art technologies. Of our knowledge, special attention has been dedicated to the case of one single switch, and we contribute to the state of the art by supporting arbitrary network topologies with multiple switches. We will test different network protocols based on entanglement to achieve end to end communication. This will be used to characterize the capacity of the network.

In summary, our research aims to provide better understanding of the achievable fidelity and capacity of general quantum networks, and to recognize the weakest points in current technology that undermine the overall performance of these networks, contributing to the goal of realizing robust and efficient quantum communications.

[156] *Security of decoy-state quantum key distribution with information leakage*

Xoel Sixto (Vigo Quantum Communication Center, Universidade de Vigo), Álvaro Navarrete (Vigo Quantum Communication Center, Universidade de Vigo), Margarida Pereira (Vigo Quantum Communication Center, Universidade de Vigo), Guillermo Currás-Lorenzo (Vigo Quantum Communication Center, Universidade de Vigo), Kiyoshi Tamaki (University of Toyama) and Marcos Curty (Vigo Quantum Communication Center, Universidade de Vigo).

A crucial assumption in most quantum key distribution (QKD) security proofs, is that no information about the selected settings is leaked to the channel. A secure space around the users' devices is usually required to ensure both parties can generate and handle classical data securely. However, this condition is not feasible in practice, since the devices usually leak some information passively, and an eavesdropper could even run a Trojan horse attack (THA) by injecting bright light into the QKD apparatuses, causing an active leak of information. In this paper, we present the first security proof for a decoy state protocol that considers an arbitrary leakage from every setting selected in the source due to passive or active information leakage. Furthermore, we apply our security proof to various cases of practical interest and we analyze the effectiveness of placing an extra phase modulator in the source to improve the secret key rate. Our analysis is also experimentally friendly, as it only requires one parameter to encapsulates all side-channel imperfections. We believe that our results constitute a vital step in closing the existing gap between theory and implementation in QKD.

[157] *Entanglement protocol in a generalized quantum network with $\ket{W}$ states*

Mateo Blanco (Universidade de Vigo).

The field of quantum communications has developed significantly in recent years, both theoretically and experimentally. Several protocols have emerged, allowing secure communications between $n$-parties, and devices capable of implementing them are becoming increasingly common. Foundational protocols, such as BB84 and COW4, have been achieved and are commercially available, but the ultimate goal remains the creation of a global quantum network.

We propose a layered architecture for a quantum network \cite{HierarchicalArch}, where a Central Controller manages all network resources and allocations. This controller connects to several clusters with quantum switches deployed in arbitrary topologies to meet the network's needs. The quantum switches are arranged in a star formation, each connecting to several individual nodes. This setup is simulated in NetSquid \cite{Coopmans2021}.

Our proposed entanglement distribution scheme is based on $ \ket{W} $ states in atom-photon-photon systems. Each switch can create several such trios and manage communications. Each node is equipped with an atom capable of absorbing one of the photons. The process, assuming node $A$, $n_A$, in switch $A$, $Sw_A$, and node $B$, $n_B$, in switch $B$, $Sw_B$, wish to communicate, is as follows: a $ \ket{W} $ state is generated in each switch, with one photon sent to each respective node, and entanglement measurements performed, resulting in two Bell pairs on each side. The other photon is sent through the network, acting as a virtual switch, and the Bell measurement on photon $A$ and $B$ results in shared entanglement between $Sw_A$ and $Sw_B$. Finally, the remaining photons in the nodes swap entanglement with the switches, achieving end-to-end entanglement between $n_A$ and $n_B$.

Although this method involves more steps than the regular entanglement swapping proposed for general network architectures, it allows for longer decoherence times \cite{Abobeih2018}. This enables more rounds of purification, achieving more stable communications and better ensuring successful pairing between users. It can trivially extend to $n$-parties with generalized entanglement measurements for the flying photons.

[158] *Certifying High-Dimensional Quantum Entanglement using Matrix Completion Methods*

Roman Solař (qtlabs, TU Wien) and Matej Pivoluska (qtlabs).

This work introduces a novel approach to certifying high-dimensional quantum entanglement using matrix completion methods. Instead of relying on complete state tomography, our method measures select elements of the density matrix and completes the remaining elements through convex optimization to minimize the entanglement measure. This allows us to compute a lower bound for the Schmidt number and the entanglement of formation, providing a practical alternative to traditional techniques. Our approach is flexible and does not require measurements in specific bases, making it particularly advantageous for time-bin entanglement scenarios.

Our results indicate that measuring just a few specific diagonals of the density matrix can yield nearly optimal entanglement certification. We identify the best-performing combinations of diagonals and provide guidelines for selecting these based on the quantum system's dimensionality. Furthermore, we are extending this research to quantum key distribution (QKD) to determine if the optimal diagonals for entanglement measures also enhance QKD key rates. This work builds on existing research and offers significant improvements in the practical certification of high-dimensional quantum entanglement.

[159] *SiC micro-cavity enhanced quantum memory for fiber-based quantum communication and networks*

Lijun Ma (National Institute of Standards and Technology), Tian Zhong (University of Chicago), Qing Li (Carnegie Mellon University) and Oliver Slattery (National Institute of Standards and Technology).

Quantum memory is an essential device for quantum communication and network. We are working to realize a SiC-based micro-cavity source with integrated quantum memory at the telecom band. A low loss SiC photonic devices are fabricated using high-quality-factor micro-ring resonators for the efficient generation of entangled photon pairs, and atomic frequency comb quantum memories based on spin-initialized 167Er:YSO crystals realize the storage of photons. Such memories are expected to generate remote entanglement between nodes in quantum networks.

[160] *Mixing Classical and Quantum Oblivious Transfer Protocols*

James Peat (Heriot-Watt University), Lara Stroh (Heriot-Watt University) and Erika Andersson (Heriot-Watt University).

Oblivious transfer is a two-party cryptographic primitive which has been the interest of study as it can be used as a building block for multiparty computation, such as building a voting system between distrusting parties. It has been shown, however, that perfectly secure oblivious transfer is impossible in both the classical and quantum setting. This has pushed the study of oblivious transfer in two directions. The first is applying assumptions about the abilities of a cheating party such as in the bounded storage model. The second is looking for the absolute bounds on a cheating party with no restrictions. We study the latter area, using one version of oblivious transfer known as Rabin oblivious transfer. This is a two-party protocol where the sender holds one bit, and the receiver obtains this bit with a set probability.

We first explore bounds on cheating in classical protocols by constructing a general probabilistic strategy for Rabin oblivious transfer, and obtain a trade-off relation between the cheating probabilities for sender and receiver. We then build and investigate two quantum protocols which use pure quantum states, and compare these to the classical strategy, mapping out in what parameter regions the classical or quantum protocols result in lower cheating probabilities. By probabilistically mixing the two quantum protocols individually with the classical strategy, a quantum advantage can be obtained across the whole parameter space. This shows the benefits of mixed quantum states over pure quantum states in quantum oblivious transfer.

[161] *Characterization of Intensity Correlation via Single-photon Detection in Quantum Key Distribution*

Tianyi Xing (National University of Defense Technology), Junxuan Liu (National University of Defense Technology), Likang Zhang (University of Science and Technology of China), Min-Yan Wang (University of Science and Technology of China), Yu-Huai Li (University of Science and Technology of China), Ruiyin Liu (National University of Defense Technology), Qingquan Peng (National University of Defense Technology), Dongyang Wang (National University of Defense Technology), Yaxuan Wang (National University of Defense Technology), Haifang Zhou (National University of Defense Technology), Hongwei Liu (China Information Technology Security Evaluation Center, Beijing, 100085, China), Wei Li (University of Science and Technology of China), Yuan Cao (University of Science and Technology of China) and Anqi Huang (National University of Defense Technology).

One of the most significant vulnerabilities in the source unit of quantum key distribution~(QKD) is the correlation between quantum states after modulation, which shall be characterized and evaluated for its practical security performance. In this work, we propose a methodology to characterize the intensity correlation according to the single-photon detection results in the measurement unit without modifying the configuration of the QKD system. In contrast to the previous research that employs extra classical optical detector to measure the correlation, our method can directly analyse the detection data generated during the raw key exchange, enabling to characterize the feature of correlation in real-time system operation. The basic method is applied to a BB84 QKD system and the characterized correlation significantly decreases the secure key rate shown by the security proof. Furthermore, the method is extended and applied to characterize the correlation from the result of Bell-state measurement, which demonstrates its applicability to a running full-scheme MDI QKD system. This study provides an approach for standard certification of a QKD system.

[162] *Quantum Cryptanalysis: Leveraging Shor's and Grover's Algorithms to Decrypt FIPS 140-3 Compliant Encryption Standards such as AES, Triple DES, RSA and ECC*

Yash Deore (MSBTE) and Dinesh Deore (Mumbai University).

The advancement of quantum computing presents both unprecedented opportunities and significant threats to contemporary cryptographic systems. This research explores the potential of quantum algorithms, specifically Shor's algorithm and Grover's algorithm, in decrypting widely used cryptographic standards, including AES, Triple DES, RSA, and ECC, which are integral to the Federal Information Processing Standards (FIPS) 140-3. Shor's algorithm, known for its polynomial-time factorization capabilities, poses a direct threat to RSA and ECC by efficiently solving the underlying mathematical problems that ensure their security. Meanwhile, Grover's algorithm, which offers quadratic speedup for unstructured search problems, can effectively reduce the security margins of symmetric key algorithms such as AES and Triple DES. This paper provides a comprehensive analysis of the vulnerabilities exposed by these quantum algorithms, evaluates the current cryptographic landscape, and discusses the implications for information security. Additionally, we explore potential quantum-resistant cryptographic approaches to mitigate these threats, ensuring robust security in the advent of practical quantum computing.

[163] *Differentiated Service Entanglement Routing for Quantum Networks*

Hui Han (National University of Defense Technology), Bo Liu (National University of Defense Technology), Bangying Tang (Academy of Military Sciences), Siyu Xiong (Sichuan Normal University), Jinquan Huang (Shenzhen Campus of Sun Yat-sen University), Fangzhao Li (National University of Defense Technology), Wei Zhong (National University of Defense Technology), Wanrong Yu (National University of Defense Technology) and Shuhui Chen (National University of Defense Technology).

The entanglement distribution networks with various topologies are mainly implemented by active wavelength multiplexing routing strategies. However, designing an entanglement routing scheme, which achieves the maximized network connections and the optimal overall network efficiency simultaneously, remains a huge challenge for quantum networks. In this article, we propose a differentiated service entanglement routing (DSER) scheme, which firstly finds out the lowest loss paths and supported wavelength channels with the tensor-based path searching algorithm, and then allocates the paired channels with the differentiated routing strategies. The evaluation results show that the proposed DSER scheme can be performed for constructing various large scale quantum networks.

[164] *Practical Approach to External Assessment of QRNG-Generated Sequences*

Rodrigo Piera (Technology Innovation Institute), Jaideep Singh (Technology Innovation Institute), Yury Kurochkin (Technology Innovation Institute) and James Grieve (Technology Innovation Institute).

Randomness is a critical resource of modern cryptosystems. Quantum mechanics offers the best properties of an entropy source for unpredictability. However, these sources are often fragile and can fail silently. Therefore, statistical tests on their outputs should be performed continuously. Testing a sequence for randomness can be very resource-intensive, especially for longer sequences, and transferring this to other systems can put the secrecy at risk. In this paper, we present a method that allows a third party to publicly perform statistical testing without compromising the confidentiality of the random bits by connecting the quality of a public sequence to the private sequence generated using a quantum process. We implemented our protocol over two different optical systems and compared them.

[165] *Efficient Arbitrated Quantum Digital Signature with Multi-Receiver Verification*

Siyu Xiong (School of Mathematical Sciences, Sichuan Normal University, Chengdu 610068, China), Bangying Tang (Strategic Assessments and Consultation Institute, Academy of Military Science, Beijing 100091, China), Hui Han (College of Computer, National University of Defense Technology, Changsha 410073, China), Jinquan Huang (School of Electronics and Communication Engineering, Sun Yat-sen University, Shenzhen 518107, China), Mingqiang Bai (School of Mathematical Sciences, Sichuan Normal University, Chengdu 610068, China), Fangzhao Li (College of Advanced Interdisciplinary Studies, National University of Defense Technology, Changsha 410073, China), Wanrong Yu (College of Computer, National University of Defense Technology, Changsha 410073, China), Zhiwen Mo (School of Mathematical Sciences, Sichuan Normal University, Chengdu 610068, China) and Bo Liu (College of Advanced Interdisciplinary Studies, National University of Defense Technology, Changsha 410073, China).

Quantum digital signature is used to authenticate the identity of the signer with information theoretical security, while providing non-forgery and non-repudiation services. In traditional multireceiver quantum digital signature schemes without an arbitrater, the transferability of one-to-one signature is always required to achieve unforgeability, with complicated implementation and heavy key consumption. In this article, we propose an arbitrated quantum digital signature scheme, in which the signature can be verified by multiple receivers simultaneously, and meanwhile, the transferability of the signature is still kept. Our scheme can be simplified performed to various quantum secure networks, due to the proposed efficient signature calculation procedure with low secure key consumption and low computation complexity, by employing one-time universal hashing algorithm and one-time pad encryption scheme. The evaluation results show that our scheme uses at least two orders of magnitude less key than existing signature schemes with transferability when signing files of the same length with the same number of receivers and security parameter settings.

[166] *A compact quantum random number generator using commercial off the shelf components*

Jaideep Singh (Technology Innovation Institute), Rodrigo Piera (Technology Innovation Institute), Yury Kurochkin (Technology Innovation Institute) and James A Grieve (Technology Innovation Institute).

Random number generators are critical components for modern cryptosystems. Deterministic methods of producing random numbers cannot guarantee true randomness due to their susceptibility to external perturbations and deterministic origins. Quantum mechanics due to its probabilistic nature can be used to generate random numbers that cannot be predicted. Here we describe the design of a compact, inexpensive, and manufacturable QRNG based on balanced detection of shot noise from an LED in a commercially available off-the-shelf package which can be integrated into existing devices.

[167] *Long-Distance Fiber Quantum Key Distribution using Wavelength-Multiplexed Entanglement*

Shichang Zhuang (University of Science and Technology of China), Bo Li (University of Science and Technology of China), Yixi Zeng (University of Science and Technology of China), Yuhuai Li (University of Science and Technology of China) and Yuan Cao (University of Science and Technology of China).

Fiber-based quantum key distribution (QKD) is a cornerstone technology for ensuring secure communication. Leveraging the spontaneous parametric down-conversion (SPDC) of periodically poled lithium niobate waveguide, we have generated a high-brightness and broad-band polarization-entangled photon source. By integrating this source with wavelength division multiplexing technology, we demonstrated an entanglement-based QKD experiment spanning over 400 km of optical fiber, marking a substantial advancement in extending distribution distances. This experiment represents a significant stride towards realizing future entanglement-based quantum networks.

[168] *Security of time-bin encoding BB84 protocol with passive interferometer*

Shun Kawakami (NTT Network Innovation Laboratories, NTT Corporation), Koji Azuma (NTT Basic Research Laboratories & NTT Research Center for Theoretical Quantum Information, NTT Corporation), Atsushi Taniguchi (NTT Network Innovation Laboratories, NTT Corporation), Hirokazu Takahashi (NTT Network Innovation Laboratories, NTT Corporation) and Koichi Takasugi (NTT Network Innovation Laboratories, NTT Corporation).

Time-bin encoding is more favorable in fiber-based implementation of quantum key distribution (QKD) than polarization encoding as it avoids issues inherent for polarization encoding, such as birefringence, caused by optical fibers. QKD only with passive devices is desirable to prevent side-channel attacks possible in the case of use of active devices such as modulators. The Bennett-Brassard 1984 (BB84) protocol is a strong candidate for an implementation with satisfying these; it can be implemented using time bins with a passive delayed interferometer that inevitably generates "satellite time bins", two pulses outside the phase-interference timing. Although time-bin encoding BB84 has been frequently demonstrated, there is no consensus whether satellite time bins can be used to extract a key. Besides, there is no security proof for either case. Here, we prove the security of time-bin encoding BB84 protocol with a passive delayed interferometer and threshold detectors. If satellite time bins are used for key generation, we show that an additional operation is necessary for security. The result is not limited only to BB84 but can be applied to Bennett-Brassard-Mermin 1992 and quantum conference key agreement based on time bins.

[169] ***Long-distance device-independent conference key agreement***

Makoto Ishihara (Keio University), Anders J. E. Bjerrum (Technical University of Denmark), Wojciech Roga (Keio University), Jonatan B. Brask (Technical University of Denmark), Ulrik L. Andersen (Technical University of Denmark) and Masahiro Takeoka (Keio University).

We propose a long-distance device-independent conference key agreement (DI-CKA) protocol. We use an efficient GHZ state distribution protocol based on entanglement swapping. We calculate a key rate of our protocol from violation of a multipartite Bell inequality and show that our protocol can distribute a secret key over longer distance than a direct transmission DI-CKA protocol. We also consider practical displacement-based measurement and show experimental feasibility of our protocol.

[170] ***Study of High-intensity entangled photon-pair source towards high-loss regime***

Jinwoo Kim (KAIST), Suseong Lim (KAIST), Heonoh Kim (KAIST) and June-Koo Rhee (KAIST).

In 1995, a research team including P. G. Kwiat developed high-intensity entangled photon pair sources[1]. In 2000, C. Simon and D. Bouwmeester theoretically studied the multi-photon effects of entangled photon pairs[2]. Such research provides valuable tools for designing and analyzing longdistance entanglement distribution experiments in high-loss regime or satellite-to-ground QKD systems, which require high-intensity entangled photon pair sources. In this study, unlike previous papers that analyzed only specific scenarios[3,4], we numerically presented measurement results achievable through analysis in general scenarios. Based on these measured probability values, we confirmed that the results of state tomography. To prepare entangled photon pair sources, the spontaneous parametric down-conversion (SPDC) phenomenon is commonly utilized. A notable characteristic of this SPDC phenomenon is that as the intensity of the incident pump beam increases, the quantum state tends to take the form of a two-mode squeezed vacuum (TMSV) state. In this scenario, where photons corresponding to each arm of the quantum state, namely the idler and signal photons, are distributed to Alice and Bob, respectively, the quantum state undergoing loss channels can be analyzed in the beam splitter scheme. Leveraging this fact, we analytically calculated the probability values of measurement outcomes in a general scenario where Alice and Bob each have different loss channels and measurement bases are determined by their choices. Here, we assumed that both of Alice and Bob employ systems utilizing two threshold detectors for photon measurements. Analyzing the computed measurement outcomes reveals that the resulting state always takes the form of the Werner state, regardless of factors such as the intensity of the entangled photon pair source, channel losses, and the relative measurement basis angles of Alice and Bob. This suggests that even in long-distance entanglement distribution experiments in high-loss regime, the optimization and preservation of measurement bases using twirling techniques can be applied effectively, even when using high-intensity entangled photon pair sources[5].

[171] ***High-count-rate single photon detection system using multi-pixel SSPD with SFQ circuit and FPGA TDC***

Toshimori Honjo (NTT Basic Research Laboratories, NTT Corporation), Shigeyuki Miyajima (Advanced ICT Research Institute, National Institute of Information and Communications Technology), Shigehito Miki (Advanced ICT Research Institute, National Institute of Information and Communications Technology), Hirotaka Terai (Advanced ICT Research Institute, National Institute of Information and Communications Technology), Hsin-Pin Lo (NTT Basic Research Laboratories, NTT Corporation), Takuya Ikuta (NTT Basic Research Laboratories, NTT Corporation), Yuya Yonezu (NTT Basic Research Laboratories, NTT Corporation) and Hiroki Takesue (NTT Basic Research Laboratories, NTT Corporation).

We report a high-count-rate single photon detection system using a 16-pixel superconducting single photon detector (SSPD) with a single-flux-quantum (SFQ) multiplex circuit and custom FPGA-based time-to-digital converter (TDC). The system demonstrates continuous single photon counting at the rate of 300 M cps.

[173] *MULTIPROTOCOL QKD NODES IMPLEMENTED WITH INTEGRATED ELECTRONIC AND PHOTONIC DEVICES*

Daniel Balado (ITEFI-CSIC), Adrián Llanos (ITEFI-CSIC) and Verónica Fernández (ITEFI-CSIC).

The implementation of quantum networks (QN) is becoming a strategic field globally as it addresses security and defense concerns. In defense scenarios such as military networks, the use of small QKD nodes that can be incorporated into ground mobile units and airborne platforms such as drones, working with different QKD protocols, is required [1]. To achieve this, it is necessary to use miniaturized technology such as integrated photonics combined with integrated electronics. Moreover, for implementing QKD between nodes in a free space network, a Pointing, Acquisition, and Tracking (PAT) system is required.

Quantum integrated photonics has emerged as a very promising technology to implement QKD in real quantum network scenarios due to its numerous advantages. These integrated technologies enable miniaturization, cost-effectiveness, and mass production. Photonic integrated circuits (PICs) can serve as QKD transmitters and receivers, replacing traditional optical modules, and offering greater versatility, higher stability against fluctuations, and more practicality [2]. A single PIC can function as a transceiver, being simultaneously a transmitter and receiver, facilitating the implementation of multi-protocol and even high-dimensional QKD in a single device, thus ensuring higher security levels and versatility of use in different conditions [3]. A PIC transceiver has certain digital signal processing requirements, such as modulation signal generation (transmitter) and signal capture (receiver), synchronization using time-tagging techniques and key distillation using post-processing techniques. Additionally, a PAT control system is necessary to align a Free Space optical link. Therefore, integrated electronics are essential as an enabling technology for QKD, providing the necessary processing power and memory capacity to handle these complex tasks [4].

In this work, we aim to design mobile quantum nodes for a defense communication network. Specifically, we simulate multi-protocol and high-dimensional QKD implemented on PICs and study the integrated electronics required to support them.

[174] *An optical ground station for quantum communication in Singapore*

Ayesha Reezwana (Centre for Quantum Technologies, National University of Singapore), Xi Wang (Centre for Quantum Technologies, National University of Singapore), Shaik Muhammad Abdillah Bin Hanifah Marican (Centre for Quantum Technologies, National University of Singapore), Moritz Mihm (Centre for Quantum Technologies, National University of Singapore) and Alexander Ling (Centre for Quantum Technologies, National University of Singapore).

Satellite-based quantum communication has emerged as a promising solution to overcome the range limitations of ground-based systems. In this implementation, network nodes in space can connect different global ground points coherently. Building an optical ground station (OGS) is a precursor towards satellite-to-ground quantum communication that can operate in an uplink or downlink configuration.

In this work, we discuss the design and construction of an OGS that we have established on the National University of Singapore campus. We give an outline of all the different subsystems, namely pointing, acquisition and tracking, polarization correction system, and the quantum receiver. To commission the OGS, we have performed an array of tests that include tracking satellites at different altitudes in orbit. In these tests, we have performed the acquisition of several satellites using their telemetry data and captured long exposure images. These images are post-processed to evaluate the stability and accuracy of the tracking by the OGS telescope mount.

In our analysis, we have found that satellites can be confined within a 0.002-0.035 degrees angular Field of view (FOV) during tracking. This meets the requirement for the initial open loop coarse tracking for a satellite quantum key distribution experiment that we set during the design of the satellite-to-ground quantum communication system. This is the first step towards maintaining a high-precision alignment of the satellite-to-ground optical link that would eventually be achieved with a closed loop fine tracking.

Lastly, we will discuss our efforts and progress on the cross-compatibility of OGS(s) that are required for a demonstration of a multi-node quantum network. In recent times, several global efforts have been initiated around the world to build optical ground stations for quantum communication. Ensuring cross compatibility among all these ground stations will help accelerate the development of a global scale quantum network.

[175] *Polarization-based QKD transmitter tested over a 50 km metropolitan fiber-link*

Ignacio Hernán López Grande (ICFO - Institut de Ciencies Fotoniques,), Nicolás Linale (ICFO - Institut de Ciencies Fotoniques), Lorenzo Castelvero (ICFO - Institut de Ciencies Fotoniques) and Valerio Pruneri (ICFO - Institut de Ciencies Fotoniques,   ICREA-Institucio Catalana de Recerca i Estudis Avançats).

We present a simple polarization transmitter designed to implement protocols from the BB84 + decoy-state family. Operating at a repetition rate of 615 MHz, the transmitter demonstrates low intrinsic quantum bit error rates over several hours of measurements. It is based on self-stable structures for both polarization and intensity modulation, ensuring robust and easy operation. Here, we provide a characterization of the transmitter and some preliminary results obtained from transmitting quantum states over a 50 km deployed fiber link.

[176] *Optical fuse for protection of QKD transmitters against light-injection attacks*

Ekaterina Borisova (Russian Quantum Center), Anastasiya Ponosova (Russian Quantum Center; NTI Center for Quantum Communications, National University of Science and Technology MISiS), Boris Galagan (Prokhorov General Physics Institute of the Russian Academy of Sciences), Vasiliy Koltashev (Dianov Fiber Optics Research Center, Prokhorov General Physics Institute of the Russian Academy of Sciences), Natalia Arutyunyan (Prokhorov General Physics Institute of the Russian Academy of Sciences), Elena Obraztsova (Prokhorov General Physics Institute of the Russian Academy of Sciences; Moscow Institute of Physics and Technology), Alexey Shilko (Russian Quantum Center; NTI Center for Quantum Communications, National University of Science and Technology MISiS) and Vadim Makarov (Russian Quantum Center; Vigo Quantum Communication Center, University of Vigo).

We propose an original device that can protect quantum key distribution (QKD) systems from the effects of intense laser radiation. Carbon nanomaterials dispersed in a polymer can be used as a fuse that interrupts key distribution when Eve tries to hack the system by high-power laser emission. Moreover, it saves system components from laser damage.

[177] *Generalized Rényi entropy accumulation theorem and generalized quantum probability estimation*

Amir Arqand (University of Waterloo), Thomas Hahn (Weizmann Institute of Science) and Ernest Y.-Z. Tan (Institute for Quantum Computing, University of Waterloo).

The entropy accumulation theorem, and its subsequent generalized version, is a powerful tool in the security analysis of many device-dependent and device-independent cryptography protocols. However, it has the drawback that the finite-size bounds it yields are not necessarily optimal, and furthermore, it relies on the construction of an affine min-tradeoff function, which in practice can often be challenging to construct optimally. In this work, we address both of these challenges simultaneously by deriving a new entropy-accumulation bound. Our bound yields significantly better finite-size performance, and can be computed as a convex optimization without any specification of affine min-tradeoff functions. Furthermore, it can be applied directly at the level of Rényi entropies if desired, yielding fully-Rényi security proofs. Our proof techniques are based on elaborating on a connection between entropy accumulation and the framework of quantum probability estimation, and in the process we obtain some new results with respect to the latter framework as well.

[178] *Towards the certification of quantum key distribution systems*

Jerome Wiesemann (Fraunhofer HHI), Jan Krause (Fraunhofer HHI), Davide Rusca (Vigo Quantum Communication Center) and Nino Walenta (Fraunhofer HHI).

Quantum key distribution (QKD) is at the verge of becoming a commercially viable security solution, backed by mathematically formulated security proofs. In the last two decades, much effort has been devoted to closing the gap between the models and practical implementations in order to account for device imperfections and counter the resulting side-channel attacks. As a result, the topic of evaluating and certifying QKD systems against these attacks is increasingly coming to the forefront. This last step however presents its own challenges, currently hindering the widespread adoption of QKD. In this work, we lay at the intersection between theory and practice, focusing on the process of preparing an in-house QKD system for evaluation. We first present a consolidated and accessible security proof for the one-decoy and two-decoy state BB84 protocols, which serves as a baseline for our QKD system. Building on this security proof, we identify the critical side-channels by evaluating the risk of most of today's known attacks. We then tackle the most critical attacks by discussing existing countermeasures that can be implemented both in the QKD system and within the security proof, where applicable. In this process, we develop new methods to characterize and evaluate QKD systems, which can later be used in evaluation laboratories. Evaluating the security of QKD systems additionally involves performing attacks to potentially identify new loopholes. Thus, we also aim to perform the first real-time Trojan horse attack on a decoy state BB84 system, further highlighting the need for robust countermeasures. By providing a critical evaluation of our QKD system and incorporating robust countermeasures against side-channel attacks, our research contributes to advancing the practical implementation and evaluation of QKD as a trusted security solution.

[179] *In-orbit dark count rate performance and radiation damage high-temperature annealing of silicon avalanche photodiode single-photon detectors of Micius satellite*

Meng Yang (Hefei National Laboratory), Sheng-Kai Liao (Unversity of Science and Technology of China) and Wen-Shuai Tang (Hefei National Laboratory).

Silicon avalanche photodiode (APD) single-photon detectors in space are continuously affected by radiation, which gradually degrades their dark count performance. From August 2016 to June 2023, we conducted approximately seven years (2507 days) of in-orbit monitoring of the dark count performance of APD single-photon detectors on the Micius Quantum Science Experimental Satellite. The results showed that due to radiation effects, the dark count growth rate was approximately 6.79 cps/day @ -24 °C and 0.37 cps/day @ -55 °C, with a significant suppression effect on radiation-induced dark counts at lower operating temperature. Based on the proposed radiation damage induced dark count annealing model, simulations were conducted for the in-orbit dark counts of the detector, the simulation results are consistent with in-orbit test data. In May 2022, four of these detectors underwent a cumulative 5.7 hours high-temperature annealing test at 76 °C, dark count rate shows no measurable changes, consistent with annealing model. As of now, these ten APD single-photon detectors on the Micius Quantum Science Experimental Satellite have been in operation for approximately 2507 days and are still functioning properly, providing valuable experience for the future long-term space applications of silicon APD single-photon detectors.

[180] *An Implementation of a Proactive and Dynamic Key Routing Method for Large-scale QKD Networks*

Ririka Takahashi (Toshiba Corporation), Yu Yu (TOSHIBA), Mayuko Koezuka (Toshiba Corporation) and Yoshimichi Tanizawa (Toshiba Corporation).

In this paper, we describe a key routing method for large-scale quantum key distribution (QKD) networks. The proactive and dynamic key routing method decides the amount of key for distribution which is based on the key usage history of each application and stored key status of each link. Furthermore, we also propose a key routing method which applies multiple routing protocols according to the network domain of destination. The method provides key usage efficiently and promotes scalability for large-scale QKD networks.

[181] *Enhanced Performance through Extinction Ratio Optimization in Asymmetric Delay Interferometers for Chip-based QKD*

Junsang Oh (Electronics and Telecommunications Research Institute), Kyongchun Lim (Electronics and Telecommunications Research Institute), Joong-Seon Choe (Electronics and Telecommunications Research Institute), Byung-seok Choi (Electronics and Telecommunications Research Institute), Kap-Joong Kim (Electronics and Telecommunications Research Institute), Dong Churl Kim (Electronics and Telecommunications Research Institute), Minchul Kim (Electronics and Telecommunications Research Institute) and Chun Ju Youn (Electronics and Telecommunications Research Institute).

Research on quantum key distribution (QKD) using discrete variables is intensively progressing towards commercialization. The development of Photonic Integrated Chips is essential for this success. Specifically, in fiber-based QKD systems utilizing time-bin and phase-encoding, the characteristics of the asymmetric delay line interferometer play a critical role in the system's performance. This paper investigates the variations in the extinction ratio of interferometer based on the power loss ratio between optical signals traversing the short and long paths and the time delay error in the interferometer. Additionally, we analyze how the characteristics of the input optical waveform affect the extinction ratio of the interferometer.

[182] *Application of quantum cryptography in financial field*

Wei Qi (8618721842708), Minghan Li (8618721842708) and Yuzhou Wang (8615821335756).

The improvement of quantum computing capability will bring a fatal threat to the traditional encryption and decryption system, and directly threaten the security of business data such as transaction data encryption, digital signatures, electronic contracts, and cross-domain transmission.This report introduces the research progress and successful cases of the application of quantum encryption in the financial field in China, and introduces the progress and research direction of the integration of QKD and PQC.

[183] *How temporal jitter affects the performance of high-speed QKD systems*

Pablo Arteaga-Díaz (Spanish National Research Council) and Veronica Fernandez (Spanish national Research Council).

Quantum Key Distribution (QKD) systems' performance is highly affected by losses and background noise, decreasing the secure bit rate in long-distance and/or high noise links. This is one of the limitations of this technology, implying long times for sharing cryptographic keys. One of the solutions for this problem consists in simply sending more pulses in less time, that is to say, increasing the bit rate. However, this solution has a problem when it comes to discrete variable QKD systems using single photon detectors, especially with semiconductor Single Photon Avalanche Diodes (SPADs). Commercially available SPADs introduce high temporal jitter to the measurements, increasing the probability of inter-symbol interference. Temporal jitter can produce measurements of a bit in the temporal window of previous or next bits, which may generate measurement errors increasing the Quantum Bit Error Rate (QBER). This means that we achieve higher bit rates but we may also increase QBER, decreasing secure bit rate, imposing a limit in the bit rate. In this work, we model the effect of temporal jitter on the QBER, validate the model with actual measurements, and use the model to study the effect of temporal jitter on high-speed QKD systems. In the case of commercial SPADs, with standard deviation values for the temporal jitter near 150 ps, the optimum bit rate is about few GHz. In order to operate at higher speeds we need single photon detectors with less jitter, what we can achieve with superconducting nanowire single-photon detector (SNSPD).

[184] *Quantum Data Centres in the Presence of Noise*

Kenny Campbell (School of Electrical and Electronic Engineering, University of Leeds), Ahmed Lawey (School of Electrical and Electronic Engineering, University of Leeds) and Mohsen Razavi (School of Electrical and Electronic Engineering, University of Leeds).

Quantum data centres (QDCs) are a promising way of scaling up quantum computers. In a single-processor quantum computer, the number of high-quality computational qubits is limited by cross talk and difficulties in addressing individual qubits when many qubits share the same housing. QDCs circumvent these challenges by linking together multiple small quantum processing units (QPUs) over short distances. With this architecture, the intra-QPU noise is kept small, but additional noise is introduced due to the latency of and imperfections in the inter-QPU links. Understanding the trade-offs between these different types of noise is essential for guiding future efforts in QDC manufacture and compilation. We develop and use a classical simulator to emulate the execution of different quantum circuits on an imperfect QDC. An individual inter-QPU CNOT gate is first-considered and then a selection of larger circuits are investigated. In both cases, we implement inter-QPU gates using cat-comm and three variants of TP-comm, which we call 1TP-comm, 2TP-comm and TP-safe, respectively. We find that 1TP-comm and cat-comm yield different output fidelities despite both schemes having the same number of gates, measurements and inter-QPU entanglements. We also determine the relative impacts of entanglement error, intra-QPU gate error and memory depolarisation.

[185] *10 Gbps Photonic Integrated Circuit-Based Quantum Random Number Generator Utilizing Vacuum Fluctuations*

Sooyoung Park (SK Telecom), Jeongwoon Choi (SK Telecom), Chulwoo Park (SK Telecom), Jaeyoung Kwak (SK Telecom), Sanghyuk Kim (SK Telecom), Seunghun Lee (Femtory), Sung-il Chu (Femtory), Hang Nga Nguyen (Femtory), Jung-Hyun Kim (IDQ) and Giwon Eom (IDQ).

In this research, we present the development of a quantum random number generator (QRNG) based on photonic integrated circuit (PIC) technology for use in secure communication networks. Using PIC technology, we have currently been developing a compact (10 mm by 10 mm) entropy source chip. The raw entropy data, generated at a rate of 20 Gbps from this chip, is conditioned to produce 10 Gbps of full entropy data as specified in NIST SP 800-90B. This full entropy data is then used to implement a NIST SP 800-90C compliant non-deterministic random bit generator (NRBG). The final 10 Gbps QRNG is expected to generate secure random numbers required for cryptographic applications, including key generation, in secure communications.

ACKNOWLEDGMENTS This work is supported by the Challengeable Future Defense Technology Research and Development Program through the Agency for Defense Development (ADD), funded by the Defense Acquisition Program Administration (DAPA) in 2024 [No. 915068201]

[186] *Maximizing extractable randomness from optical device-independent randomness expansion experiments using robust self-testing families of Bell inequalities*

Shashank Kumar Ranu (Department of Mathematics, University of York) and Roger Colbeck (Department of Mathematics, University of York).

Recent advancements in device-independent randomness expansion (DIRE) protocols have shown significant improvements in random bit generation rates yet remain slower than other methods. Optical systems, ideal for long-distance quantum information transmission, face challenges due to noisy photon sources and inefficient detectors, resulting in lower randomness rates of photonics-based DIRE implementations. In this work, we demonstrate how to tune DIRE protocols and the underlying Bell tests to specific noise levels, thereby enhancing the extractable randomness in photonics-based DIRE implementations.

[187] *State estimation of multi-partite single photon path entanglement*

Hikaru Shimizu (Keio University), Joe Yoshimoto (Keio University), Junko Hayase (Keio University), Tomoyuki Horikiri (Yokohama National University), Rikizo Ikuta (Osaka University) and Masahiro Takeoka (Keio University).

We propose a new method for the measurement of multi-mode single photon path entanglement which can be distributed with the same rate of bi-partite entanglement. We also demonstrate the method with two different states and succeeded to reconstruct the density matrix for each of them with high accuracy.

[188] *Post-processing scheme for free-space continuous-variable quantum key distribution*

Yujie Wang (Northwest University), Xinlei Chen (Northwest University), Lei Wang (Northwest University), Yujie Zhang (Northwest University), Zhengwen Cao (Northwest University) and Geng Chai (Northwest University).

The post-processing process is an indispensable part of the continuous variable quantum key distribution (CVQKD), which converts partially relevant and partially secure measurement data to a completely consistent and information-theoretic secure key. Among them, parameter estimation is an important means of evaluating system parameters, and provides parameter basis for subsequent key extraction processes. However, the existed methods usually divide the free space into several relatively stable subchannels and use sampling estimation to achieve parameter estimation, which are limited by the quality and quantity of statistical samples. Here, we firstly propose a free-space parameter estimation scheme based on Bayesian estimation. Experiment has been proven that Bayesian schemes has advantages in estimation accuracy and stability compared to sampling statistical schemes, and has good performance in both free space and fiber channels, with high robustness and accuracy. Moreover, key reconciliation is also a highly anticipated aspect of CVQKD post-processing. But when the signal-to-noise ratio of the quantum channel changes, constant-bit-rate correction codes lead to a decrease in reconciliation efficiency, further deteriorating the system performance. We further propose a rate-adaptive Polar code reconciliation scheme and a scheme based on intermediate channel low-density parity check code cascaded polar code (IC-LDPC Polar code) to improve reconciliation efficiency and cope with practical long-distance CVQKD systems.

[189] *Advantages and limitations of channel multiplexing for discrete-variable quantum key distribution*

Mikolaj Lasota (Nicolaus Copernicus University) and Indranil Maiti (Nicolaus Copernicus University).

Numerous imperfections of realistic setup elements required for the implementation of quantum key distribution (QKD) protocols impose strong limitation on their performance, particularly in terms of the obtainable key generation rate. A possible way to increase this quantity in the case of utilizing spontaneous parametric down-conversion (SPDC) source, producing strongly correlated pairs of photons, is to use wavelength-division-multiplexing (WDM) modules in order to direct photons of different wavelengths into separate detection systems utilized by the trusted parties. In this way it can be possible to generate multiple cryptographic keys in paralell, significantly increasing the overall key rate. In this work we theoretically investigate the potential improvement offered by such possibility in the case of entanglement-based version of the BB84 protocol realized with pulsed-pump SPDC source. We optimize the properties of the produced photon pairs and the intensity of the utilized pumping laser in order to maximize the potential improvement over the traditional, non-WDM, setup configuration. We consider both noiseless case, with ideal single-photon detectors utilized by the trusted parties and more practical situation with imperfect binary detectors, in which case we develop formulas for optimizing the detection window when the temporal filtering method is used to reduce the quantum bit error rate.

[190] *Intermode-interaction-induced dynamics of continuous variable quantum key distribution observables*

Andrei Gaidash (ITMO University), Alexei Kiselev (St. Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University)), George Miroshnichenko (ITMO University) and Anton Kozubov (ITMO University).

We theoretically study dynamical regimes of the observables that govern the operating conditions of continuous variable (CV) quantum key distribution (QKD) systems, depending on quantum-channel-induced intermode interactions. In contrast to the widely used approach, where losses and thermal broadening are introduced through a beamsplitter transformation, our analysis uses the exactly solvable quantum channel model describing the Lindblad dynamics of multimode bosonic systems interacting with a heat bath and additionally takes into account imperfections of the homodyne detection scheme. The analytical results for the photon count difference and the quadrature probability distributions are used to derive the expression for the mutual information between legitimate parties, which explicitly links the information properties of CV QKD and the parameters of the channel. For the important special case of a two-mode photonic system propagating in a fiber channel, the latter can be conveniently parameterized using the frequency and the relaxation rate vectors that characterize the coherent (dynamical) intermode couplings and the incoherent (environment mediated) interaction between the bosonic modes, respectively. It turned out that these vectors determine four qualitatively different dynamical regimes of the mutual information and the phase difference between the signal and the local oscillator that may significantly affect the operation of CV QKD.

[191] *Randomness extraction analysis simplified by Pearson's criterion*

Andrei Gaidash (ITMO University), Anton Kozubov (ITMO University) and George Miroshnichenko (ITMO University).

We investigate multi-pixel quantum random number generators as a Gaussian entropy source. The procedure of randomness extraction implies maximization of the conditional probability as a step of conditional min-entropy estimation, implying an eavesdropper may influence the signal. Usually, it requires to artificially limit the dynamic range of the variable that an eavesdropper may control. We propose the approach that may expel a necessity of this assumption by utilizing Pearson's goodness-of-fit criterion, such that the histogram of measured outcomes fits well into the dynamical range and well approximated by a Gaussian. The latter greatly simplifies the min-entropy estimations and may be incorporated in security criterion estimation.

[192] *An Open-Source Library for Information Reconciliation in Continuous-Variable QKD*

Erdem Eray Cil (Karlsruhe Institute of Technology / Communications Engineering Lab) and Laurent Schmalen (Karlsruhe Institute of Technology / Communications Engineering Lab).

This paper presents an easy-to-use open-source software library for continuous-variable quantum key distribution (CV-QKD) systems. The library, written in C++, simplifies the crucial task of information reconciliation, ensuring that both communicating parties share the same secret key despite the noise. It offers a comprehensive set of tools, including modules for multidimensional reconciliation, error correction, and data integrity checks. Designed with user-friendliness in mind, the library hides the complexity of error correction, making it accessible even to users without knowledge of error-correcting codes.

[193] *Composable CVQKD over 20 km with a 10 kHz local local oscillator laser*

Hou Man Chin (Technical University of Denmark), Ulrik Andersen (Technical University of Denmark) and Tobias Gehring (Technical University of Denmark).

We present the results of our experimental polarisation diverse continuous variable quantum key distribution system operating over 20km SMF at 100 Mbaud, implemented using a 10 kHz laser as a free running local oscillator. A composable finite size key is achieved with 200 million states.

[194] *Distribution of genuine time-bin entanglement at telecom wavelength*

Kannan Vijayadharan (Università degli Studi di Padova), Francesco B. L Santagiustina (Università degli Studi di Padova, ThinkQuantum S.R.L.), Costantino Agnesi (Università degli Studi di Padova), Paolo Villoresi (Università degli Studi di Padova) and Giuseppe Vallone (Università degli Studi di Padova).

Entanglement is a unique and invaluable resource for quantum information processing because it highlights the non-locality property, which allows for device-independent (DI) quantum communication protocols, such as Quantum Key Distribution and Quantum Random Number Generation. However, the distribution of entanglement over long distances is challenging due to propagation losses and instability. Time-bin entanglement is a promising solution since it is robust in long-distance distribution over fiber optics and immune to the polarization distortion such a channel can introduce. Time-bin has also been demonstrated to be compatible with NV center-based quantum technologies, representing a crucial interface between the different devices in quantum networks. Nevertheless, its most common implementation suffers from a post-selection loophole (PSL), which invalidates Bell non-locality tests and renders it vulnerable to quantum hacking attacks, thus preventing its use for device-independent protocols. We present a scheme using optical switches to obtain only detection events displaying non-local interference, thereby closing the PSL. Our scheme works with 1550nm biphotons for entanglement distribution over existing fiber-based telecom networks. The switches show a high extinction ratio of up to 30dB and stability over extended periods. We also measure interferometric visibilities of over 94%, which corresponds to a CHSH S parameter of 2.65

[195] *EXPERIMENTAL OBSERVATION AND IN-DEPTH STUDY OF THE HONG-OU-MANDEL EFFECT*

Inés Meili Díaz García (Spanish National Research Council (CSIC)), Daniel Cano Reol (Spanish National Research Council (CSIC)) and Verónica Fernández Mármol (Spanish National Research Council (CSIC)).

Inés Díaz, Spanish National Research Council (CSIC) C. de Serrano, 144, Madrid, Spain T: +34 636514928, ines.diaz@csic.es Daniel Cano, Spanish National Research Council (CSIC) Verónica Fernández, Spanish National Research Council (CSIC)

Quantum Key Distribution (QKD) encompasses a combination of protocols that allow for the exchange of a secret key between two communicating parties (Alice and Bob) under unconditional security by exploiting quantum mechanics principles. However, not all QKD setups fulfill the ideal model requirements, since imperfections in real devices have been proved to make the secret exchange vulnerable to certain attacks. These types of vulnerabilities are overcome by new Measurement Device Independent (MDI) QKD protocols, which protect the security against detector side-channel attacks and enable secure communication over longer distances [1]. As such, the MDI-QKD protocol involves a third-party relay (Charlie) who might be under the control of an eavesdropper and to which Alice and Bob send their states for the Hong-Ou-Mandel effect to take place. The Hong-Ou-Mandel effect is a quantum interference phenomenon between two indistinguishable photons at a beam splitter that bears significant weight within the context of Bell state measurements and is crucial for the security of MDI-QKD and its realistic implementation. In this work, we put together an experimental setup to observe and monitor the Hong-Ou-Mandel interference. By synchronizing two indistinguishable weak coherent pulses (WCP) to arrive simultaneously at a 50:50 beam splitter (following [2]), it has been possible to verify that the two photons exit together through the same output only if the quantum interference takes place. Consequently, detection event occurs at just one detector. The most significant experimental evidence of such effect is the Hong-Ou-Mandel dip [3], a plot representing the number of coincidence detections against the temporal delay induced in one of the pulses. It should be noted that, since we are using WCPs instead of photon number states, the interference contrast is 50%. We successfully attested to the Hong-Ou-Mandel effect by obtaining a clear and pronounced dip. To enhance its visibility, we varied and tested several experimental components. These results thus obtained, along with the discussion of the experimental techniques relevant to test such a phenomenon, provide valuable insights for future advancements in quantum interference studies in the context of quantum communications. References 1. Lo, H. K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. Physical review letters, 108(13), 130503. 2. Chen, H., An, X. B., Wu, J., Yin, Z. Q., Wang, S., Chen, W., & Han, Z. F. (2016). Hong–Ou–Mandel interference with two independent weak coherent states. Chinese Physics B, 25(2), 020305 3. Ge, H., Tomita, A., Okamoto, A., & Ogawa, K. (2023). Analysis of the effects of the two-photon temporal distinguishability on measurement-device-independent quantum key distribution. IEEE Transactions on Quantum Engineering, 4, 1-8. Figure 1 – Experimental Hong-Ou-Mandel dip Acknowledgements This work had the support of Grant PID2020-118178RB-C22 funded by AEI/10.13039/501100011033 and QURSA project (TED2021- 130369BC33, MCIN/AEI/10.13039/501100011033).

[196] *Hierarchical Quantum Secret Sharing for Multi-Node Satellite Communication Network using the Qline Architecture*

Chitra Shukla (SnT, University of Luxembourg, 1855 Luxembourg, Luxembourg), Abhishek Shukla (Institute for Materials Research (IMO), Hasselt University, Wetenschapspark 1, B-3590 Diepenbeek, Belgium), Milos Nesladek (IMO-IMOMEC, Hasselt University, Wetenschapspark 1, B-3590 Diepenbeek, Belgium) and Symeon Chatzinotas (SnT, University of Luxembourg, 1855 Luxembourg, Luxembourg).

We propose to design a hierarchical quantum secret sharing (HQSS) for multi-node satellite communication network, leveraging the Qline architecture [1], represents unique topology that features a linear quantum network configuration, where qubit generation and measurement occur at the endpoint satellites, with intermediate satellite nodes are limited to single-qubit unitary transforms. In designing a HQSS for multi-node satellite communication network, we consider a group of at least four satellites (A, B, C, D), in linear quantum network configuration, where qubit generation and measurement occur at the endpoint Satellites A and D respectively, with two intermediate satellites B and C limited to single-qubit measurement and unitary transforms. This setting will restrict the two intermediate satellites B and C to allow using lower powers needing the cooperation from the endpoint Satellites A and D, however, endpoint Satellite D utilizes the higher powers to reconstruct the secret without the measurement outcome of one of the lower power intermediate Satellite B or C. The hierarchical structure depends on the trusted (end node Satellite D) or untrusted (intermediate Satellite B, C) locations within a satellite quantum network. Our motivation is to use this hierarchical power for long-distance QSS, allowing leading Satellite A to securely share a quantum secret to Satellite D while bypassing one of the intermediate satellites B or C. Satellite A utlizes a 4-qubit cluster quantum entangled state with Satellites B, C, and D to perform HQSS in Qline architecture. The simplicity of hardware at intermediate nodes in the Qline architecture facilitates easier implementation of proposed HQSS for multi-node satellites. Our HQSS based on Q-line configuration shows that hierarchy [2] with minimal hardware [1, 3] would be the standard requirements in future terrestrial and non-terrestrial quantum networks [2, 3]. Further, we also explore the links of our proposed HQSS protocol to semi-quantum (classical) regime [3] operated by intermediate satellite nodes. Moreover, unlike traditional QKD networks, our design based on Qline architecture doesn't require key routing through intermediate nodes, enhancing security by avoiding exposure to these nodes, without consuming established keys for routing security. Rather established keys can be efficiently consumed by a leading Satellite A to securely distributed the entanglement among intermediate Satellites B, C and endpoint Satellite D nodes. As the security of key establishment on Qline networks is composable [1], ensuring that established keys can be utilized for secure entanglement distribution executed by Satellite A among inter-satellite quantum communication network, thereby advancing larger constellations securely.

References:

1. Mina Doosti, Lucas Hanouz, Anne Marin, Elham Kashefi and Marc Kaplan, “Establishing shared secret keys on quantum line networks: protocol and security” arXiv:2304.01881v1 2023. 2. C. Shukla, P. Malpani, K. Thapliyal, “Hierarchical Quantum Network using Hybrid Entanglement. Quantum Inf. Process, Vol. 20, 121, 2021. 3. C. Shukla, K. Thapliyal, A. Pathak, “Semi-quantum communication: Protocols for key agreement, controlled secure direct communication and dialogue”, Quantum Inf. Process. 16, 295, 2017.

[197] *Orthogonal-state-based Measurement Device Independent Quantum Communication*

Chitra Shukla (SnT, University of Luxembourg, 1855 Luxembourg, Luxembourg), Abhishek Shukla (Institute for Materials Research (IMO), Hasselt University, Wetenschapspark 1, B-3590 Diepenbeek, Belgium), Milos Nesladek (IMO-IMOMEC, Hasselt University, Wetenschapspark 1, B-3590 Diepenbeek, Belgium) and Symeon Chatzinotas (University of Luxembourg).

We attempt to propose the first orthogonal-state-based (OSB) protocols of measurement-device-independent quantum secure direct communication (MDI-QSDC) using single basis, i.e., Bell basis as decoy qubits for eavesdropping checking, for which OSB protocols are known to achieve unconditional security fundamentally different than the conventional conjugate-coding based protocols. Further, we investigate our proposed OSB MDI-QSDC in the noisy environment and compare it with conjugate coding MDI-QSDC. We aim for achieving superior performance of OSB protocols than conjugate-coding based protocols under certain noisy environment, supported with the existing study of best basis choice of decoy qubits required for secure quantum communication. Furthermore, we have analyzed the security of the proposed protocols under several attacks such as intercept-and-resend attack, entangle-and-measure attack, fake entangled particles attack and flip attack. We show that with some modifications, the proposed OSB MDI-QSDC protocols can also be reduced to OSB MDI versions of QKD protocols.

[198] *Security against coherent attacks in discrete-modulated continuous-variable quantum key distribution*

Archishna Bhattacharyya (Institute for Quantum Computing, University of Waterloo), Ian George (University of Illinois at Urbana Champaign), Florian Kanitschar (TU Wien and Austrian Institute of Technology) and Norbert Lutkenhaus (Institute for Quantum Computing, University of Waterloo).

Discrete-Modulated Continuous-Variable Quantum Key Distribution (DMCVQKD) protocols are amenable for deployment in quantum communication networks due to their experimental simplicity, but pose theoretical challenges impeding their tight security analyses. Major progress has recently been made in the finite-size regime against independent and identical (iid) collective attacks [Kanitschar, F. et. al., (2023), PRX Quantum, 4(4), p.040306]. However, a complete and rigorous analysis must take into account correlated rounds of attack beyond the iid-collective assumption, and must not assume a photon-number cutoff on the signal states. The difficulty of achieving this lies in the absence of an information-theoretic framework for proving security that handles infinite dimensional multipartite quantum states that are a priori unstructured, i.e., beyond the asymptotic iid setting. We present a composable security proof against coherent attacks in the finite-size regime for a general DMCVQKD protocol. We introduce a framework to handle states that are in part iid and in part unstructured (almost iid) in infinite dimensional Hilbert spaces. We use a de Finetti reduction for infinite dimensional almost iid states [Renner, R., Cirac, J. I., Phys. Rev. Lett. 102, 110504 (2009)], and generalise the acceptance test and the energy test to almost iid states handling Eve's correlated infinite dimensional side information. As work in progress, we address the issue of a missing chain rule that formulates an explicit key rate expression. Numerical simulation of key rates [Winick, A. et. al., Quantum 2, 77 (2018)] can then be performed, demonstrating the efficacy of the security proof.

[199] *Heterogeneous Integration of High-responsivity InAs Quantum Well Phototransistors for Quantum Photonic Integrated Circuits*

Dae-Hwan Ahn (Korea Institute of Science and Technology (KIST)), Jae-Hyeon An (Korea Institute of Science and Technology (KIST)), Jae-Hoon Han (Korea Institute of Science and Technology (KIST)) and Sang-Wook Han (Korea Institute of Science and Technology (KIST)).

Quantum photonic integrated circuits (QPICs) operating at telecommunication wavelengths hold great potential for large-scale deployment of quantum key distribution (QKD) systems [1]. Low-propagation loss materials, such as LiNbO3, SiNx, Si, AlN, allow for high-efficiency waveguide-based optical circuits, including phase/intensity modulator, beam splitter, and polarization controller, on a semiconductor wafer. To realize a QPIC-based QKD chip, photodetectors should be integrated onto optical circuits fabricated with low propagation loss materials. In this study, we discuss the heterogeneous integration technology of III-V photodetectors on low propagation loss materials. Particularly, we demonstrated InGaA/InAs/InGaAs quantum well (InAs QW) phototransistors integrated onto Si substrates through wafer bonding and layer transfer techniques. Our InAs QW phototransistors can detect low-intensity light at a wavelength of 1.55 um owing to their photoconductive gain based on photovoltaic effects. The photovoltaic effects in phototransistor induce a threshold voltage shift because the holes accumulate in the transistor body under light illumination. The threshold voltage shift results in a higher photocurrent than the number of photo-generated carriers under light illumination at a 1.55 um wavelength. This implies that high transconductance is desirable to obtain a high photocurrent for the phototransistor. We achieved the high responsivity in our phototransistors by optimizing InAs channel structure featuring superior transconductance characteristics [2]. For future work, we will integrate InAs QW photodetectors with membrane and nanowire structures onto waveguide-based optical circuits fabricated with low propagation loss materials. We believe that our proposed phototransistor will help to demonstrate a high performance power monitoring system in QPIC.

[1] G. Zhang et al., "An integrated silicon photonic chip platform for continuous-variable quantum key distribution", Nature Photonics 13, 839 (2019), [2] D.-H Ahn et al., "High-responsivity InAs quantum well photo-FET integrated on Si substrates for extended-range short-wave infrared photodetector applications", Photonics Research 11, 1465 (2023)

[200] *All forms of QKD are susceptible to memory attacks*

Ernest Y.-Z. Tan (Institute for Quantum Computing, University of Waterloo).

In device-independent cryptography, it is known that reuse of devices across multiple protocol instances can introduce a vulnerability against memory attacks. We highlight in this work that device-dependent or measurement-device-independent protocols are in fact also susceptible to similar attacks. Furthermore, even if we only consider a single protocol instance, memory effects across rounds are enough to cause substantial difficulties in applying many existing non-IID proof techniques for device-dependent or measurement-device-independent protocols, such as de Finetti reductions and complementarity-based arguments (e.g. analysis of phase errors). We present a quick discussion of these issues, including some tailored scenarios where protocols admitting security proofs via those techniques become insecure when memory effects are allowed, and we highlight connections to recently discussed attacks on DIQKD protocols that have public announcements based on the measurement outcomes. This discussion indicates the challenges that would need to be addressed in order to apply those techniques in the presence of memory effects (for either the device-dependent or device-independent case), whether for devices reused across multiple protocol instances, or for a single protocol instance.

[201] *Towards genuine randomness in the presence of experimental imperfections*

Jose Manuel Aguero Trejo (The University of Auckland).

The generation of random numbers has an essential role in cryptography, with most practical applications still relying on Pseudo Random Number Generators (PRNGs). However, strings generated by PRNGs are always computable, representing a fatal flaw for their use in cryptographic protocols. For this reason, we designed a QRNG protocol that generates maximally unpredictable strings by localising value indefiniteness, therefore having a provable advantage over any PRNG. Moreover, a photonic implementation without the need for entanglement is possible for this approach, making it suitable for practical applications. However, the role of errors in an operational photonic embodiment is yet to be fully understood. Thus, this work aims to start the development of an error analysis framework to guarantee incomputability even in the presence of experimental imperfections.

[202] *Quantum strategic information transmission*

Kareem Raslan (The University of Adelaide), Azhar Iqbal (The University of Adelaide), Ayse Kizilersu (The University of Adelaide), James Quach (Commonwealth Scientific & Industrial Research Organisation (CSIRO)) and Derek Abbott (The University of Adelaide).

Game theory provides unique mathematical tools to analyse strategic interactions. A ‘game’ is a generalised term referring to a mathematical model involving players who follow a structured set of rules. Classical games can be shifted to their quantum versions via a quantisation protocol. These protocols involve the employment of entangled or complex super-positioned states. Quantum game theory offers potentially beneficial properties to games that cannot be realised in their classical counterparts. This draws interest in turning classical games into quantum games and investigating whether favourable behaviours arise. We focus on the classical game known as strategic information transmission [1]. Quantum strategic information transmission offers possible benefits that can potentially be implemented via current quantum key distribution protocols, improving the security and effectiveness of information transmission.

Strategic information transmission involves two players, a sender of information, and a receiver. The sender starts the game by observing information and upon doing so, sends a report to the receiver. The receiver then takes an action that affects both players. If players have diverging preferences, the sender may purposefully alter the transmitted report to the receiver by adding a bias in order to sway the action the receiver takes for their own self-interest. One form of game theoretic analysis, known as backward induction, highlights that there only exists one solution in which both players receive the optimal outcome in the classical version of the game, that is when there is no bias. This begs the question, is it possible for the receiver to compromise with their action and obtain an optimal outcome for both players regardless of the information transferred?

Through applying a quantisation method known as the Marinatto-Webber scheme [2], a quantum version of the game is developed. As such, players communicate via super-positioned qubit states, providing a different structure compared to the classical game. Applying the backward induction method to the quantum version of the game provides a complex solution compared to the classical version and as such may lead to improved outcomes for both players. While the classical game can only be optimised for both players when they share the same preferences (no bias), it may be possible for the quantum version to have a solution for diverging preferences. This paper will present our latest progress in formulating a quantum version and showing its consequences.

References [1] M. J. Osborne, An Introduction to Game Theory. Oxford University Press, 2009. [2] L. Marinatto and T. Weber, “A quantum approach to static games of complete information,” Physics Letters. A, vol. 272, no. 5, pp. 291–303, 2000.

[203] *The Rome Quantum Key Distribution Network and the EuroQCI program*

Carlo Liorni (Leonardo S.P.A.), Giuseppe De Falco (Leonardo S.P.A.) and Massimiliano Dispenza (Leonardo S.P.A.).

Quantum key distribution (QKD) is an innovative technology allowing information-theoretically-secure key sharing among distant users relying only on fundamental rules of quantum physics, without assumptions about the computational power of the attacker. This work presents the architecture of the Rome QKD Metropolitan Area Network (QMAN), the different layers required to sustain such network, including the Key Management System developed by Leonardo and the interconnection with the Italian Quantum Backbone to intregrate this network in the EuroQCI program. The Rome QMAN is a quantum-safe hybrid network, made up of several nodes that are connected with both commercial fibre and a free-space link.

[204] *Multiplexed high rate QKD system*

Akira Murakami (Toshiba Corp.), Keidai Wakamatsu (Toshiba Corp.), Mamiko Kujiraoka (Toshiba Corp.), Yoshimichi Tanizawa (Toshiba Corp.) and Yasuhiro Fujiyoshi (Toshiba Corp.).

We improved secure bit rates by multiplexing QKD systems without any additional optical dark fibers.

[205] *Quantum Backdoor - Performing Electronic Side-Channel Analysis on Quantum Key Distribution Systems*

Beatriz Lopes da Costa (Instituto Superior Técnico, Universidade de Lisboa), Matías R. Bolaños Wagner (Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova), Ricardo Chaves (Instituto Superior Técnico, Universidade de Lisboa), Claudio Narduzzi (Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova), Marco Avesani (Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova), Davide Giacomo Marangon (Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova), Andrea Stanco (Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova), Giuseppe Vallone (Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova), Paolo Villoresi (Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova) and Yasser Omar (Instituto Superior Técnico, Universidade de Lisboa).

Over the last decades, Quantum Key Distribution (QKD) has risen as a promising solution for secure communications, a pressing subject in the aftermath of the security threat posed by Quantum Computers and the Shor's Algorithm. Offering a theoretically secure way to share secret keys between parties, QKD state of the art has witnessed remarkable progress in the last years. Nonetheless, although theoretically secure, QKD is not implementation-secure and until now, the study of physical vulnerabilities in QKD setups has mainly focused on the optical channel. The concept of attacking a cryptographic system via its physical characteristics and associated leakages, known as side-channel analysis, was firstly introduced in classical cryptography, with the seminal work of Paul Kosher. Since then, power and electromagnetic side-channel analysis have become a staple in classical cryptanalysis. However, these concepts have hardly been applied to QKD. In this work, we propose and implement a new method for side-channel analysis on QKD systems, by exploiting the power consumption of the electronic driver controlling the electro-optical components of the QKD transmitter. For high-rate transmission, QKD modules typically require electronic drivers, such as Field Programmable Gate Arrays (FPGAs). Here, we will show that the FPGA's power consumption can leak information about the QKD operation, and consequently the transmitted key. The analysis was performed on the QKD transmitter at the University of Padua. Our results are consistent and show critical information leakage, having reached a maximum accuracy of 73.35% in the prediction of transmitted random keys at 100 MHz repetition frequency.

[206] *Secure Implementation and Verification of a Certifiable Source Device Independent Quantum Random Number Generator*

Kaiwei Qiu (School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore), Yu Cai (School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore), Nelly Ng (School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore) and Jing Yan Haw (Centre for Quantum Technologies, National University of Singapore).

Quantum physics provides some natural ways to generate genuine randomness, however, the generation of certifiable randomness still meets various theoretical and technical challenges. Recently, a work on a source device independent protocol was proposed, where the measurement apparatus is fully trusted and no assumption about the incoming light source is made. Here, we experimentally implement and verify a source device independent quantum random number generator (SDI-QRNG), built with off-the-shelf optical and electronic components. Furthermore, a series of quantum attacks were performed to evaluate the security and implementation vulnerability of the SDI-QRNG.

[207] *Measurement-device-independent QRNG based on mode-competition in a gain-switched VCSEL*

Blanca Mir (Quside Technologies S.L.), Tomás Fernández Martos (Quside Technologies S.L.), Miquel Rudé (Quside Technologies S.L.), Gabriel Senno (Quside Technologies S.L.) and Domenico Tulli (Quside Technologies S.L.).

In this work, we present a new measurement-device-independent QRNG developed within Quside based on operating a vertical cavity surface emitting laser (VCSEL) in a gain-switching manner. We prove security in the finite-size regime using the EAT and obtain positive rates for as low as 7x10^4 rounds.

[208] *Impact of information leakage in modulator-free quantum key distribution transmitters*

Álvaro Navarrete (Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain), Víctor Zapatero (Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain) and Marcos Curty (Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain).

Recently, different modulator-free decoy-state quantum key distribution transmitters have been proposed. Among their advantages, they are essentially immune to information leakage, including that potentially induced by an adversary via e.g. a Trojan-horse attack. However, practical implementations of these transmitters emit, in addition to the desired signals, some extra pulses that are not used as quantum carriers, but still may contain sensitive information about the intensity and bit/basis encoding of the signals. This unwanted pulses can be actively blocked with an intensity modulator (or an optical switch), but the extinction ratio of these devices is always finite, and thus it is still crucial to account for the residual amount of information leakage at the security-proof level. In this work, we analyze the security of these transmitters and evaluate their performance in the presence of this kind of inherent information leakage. We find that the secret-key rate of the protocol is severely affected when the information leakage is not sufficiently attenuated, which highlights the importance of accounting for such type of imperfections.

[209] *Performance Degradation in Polarizationn Encoded Quantum Key Distribution by Polarization Dependent Loss*

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

Since the first quantum key distribution (QKD) BB84 was proposed, various relevant QKD systems have been proposed. The systems mainly are implemented based on bulk-optics. The bulk-optics based implementation has large volume, heavy weight, high power consumption, and high cost, so that it is not easy to compatible to current communication system and is hard to be commercialized. In order to overcome the aforementioned, recently photonic integrated chip (PIC) based implementation of QKD systems have been proposed. Unfortunately, PIC based implementation has inevitable polarization depende loss (PDL), which can be induced by imperfect fabrication of waveguide, or plasma dispersion effect which can change absorption in case of a polarization modulator. Additionally, a QKD system currently cannot be implemented with only PIC so that it requires additional optical components that has PDL as well. PDL may cause the severe performance degradation of QKD, by destroying the mutually unbiasedness between the states in QKD and increasing quantum bit error rate (QBER). In this study, we analyze effect of PDL in QKD. First, we experimentally analyze state change of polarization qubit depending on PDL which can be emulated by a PDL emulator. Based on this, we theoretically calculate intrinsic quantum bit error rate (QBER) and the corresponding secure key rate of QKD.

[210] *Integrated Photonic Self-Testing QRNG*

Maria Ana Afonso Pereira (University of Geneva), Rebecka Sax (University of Geneva), Davide Rusca (Vigo Quantum Communication Center), Rob Thew (University of Geneva) and Hugo Zbinden (University of Geneva).

With the maturity of Quantum Technologies, namely Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG), there has been mounting interest in scalable and inexpensive solutions for both academia and industry. To address the practicality and security requirements for QRNGs, we are developing a self-testing QRNG system based on homodyne detection with a fully integrated optical set-up. We use an Indium Phosphide (InP) photonic integrated circuit (PIC) with a high-speed 2.5GHz phase modulation that was designed and developed in collaboration with HHI Fraunhofer. All optical components are integrated in a 12×10 mm2 chip. It is then glued to a PCB designed in-house with electrical connections to the chip for full control and read-out of the results of the homodyne measurements. Another PCB, also designed in-house, is used to interface between the PIC and a field-programmable gate array (FPGA), which determines the quantum states to be prepared and reads out the homodyne detection. A graphics processing unit (GPU) connected to the FPGA then performs the statistical analysis of the data. The system operates at 1.25GHz and extraction rates above 18% are expected.

[211] *Addressing the afterpulse QKD bottleneck - investigating quantum defects in InGaAs avalanche photodiodes*

Anthony Vaquero-Stainer (NPL), Ted Santana (NPL), Benyam Dejen (NPL), Luke Arabskyj (NPL) and Masaya Kataoka (NPL).

Single-photon avalanche photodiodes (SPADs) are ubiquitous in many photon-counting and low-light sensing applications including quantum key distribution (QKD) which is the most commercially advanced quantum technology. The performance of these systems is however limited by the detection rate of the SPAD detectors, which is in turn limited by the deadtime which is applied. This is necessary due to afterpulsing, an effect which causes spurious detections due to the thermal excitation of trapped charge carriers in defect states in the SPAD. Characterisation of these defect states is therefore essential to improving material quality and hence the performance of detectors and their associated uses such as QKD. This work will present several measurements performed on InGaAs SPADs to characterise their defect states.

[212] *Performance of a QKD System Using WDM Filter and Chip-based Component for Channel Integration*

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

In this study, we report the performance of our polarization-based BB84 protocol QKD system using a silica-based polarization encoding chip and a fiber-based WDM filter, which can easily combine the quantum channel of 785nm with the synchronization channel of 1550nm. Among the optical transmission windows in the atmosphere, 785nm was selected as the wavelength of the quantum channel due to its availability for high-performance silicon-based single-photon avalanche diodes and laser diodes. Additionally, 1550nm was selected for beam tracking and synchronization signal for its availability in commercial transceivers and optical amplifiers. The operation speed of the system was 100 MHz. The sifted key rate and quantum bit error rate (QBER) were measured in real-time by a field programmable gate array(FPGA). The system was installed in an indoor laboratory, and the QBER and sifted key rate were measured while increasing channel attenuation to test the system’s performance in lossy environments. We obtained superior QKD performance with a QBER of 0.62% and a sifted key rate of 1.61 Mbps at no attenuation, and 5.64% and 5.69 kbps at 25dB attenuation, showing potential application for outdoor operation over longer distances.

[213] *Quantifying the Impact of Systematic Deviations during Practical CV-QKD Receiver Calibration*

Jonas Berl (Adva Network Security GmbH | Communications Engineering Lab, Karlsruhe Institute of Technology), Tobias Fehenberger (Adva Network Security GmbH) and Laurent Schmalen (Communications Engineering Lab, Karlsruhe Institute of Technology).

With state-of-the-art coherent detection techniques, the two-step CV-QKD receiver calibration introduces inevitable systematic deviations. In this work, we propose an empirical pre-calibration phase that allows to quantify the impact of these deviations on security.

[214] *Intensity correlations in decoy-state BB84 QKD systems*

Daniil Trefilov (Vigo Quantum Communication Center, University of Vigo), Xoel Sixto (Vigo Quantum Communication Center, University of Vigo), Víctor Zapatero (Vigo Quantum Communication Center, University of Vigo), Anqi Huang (National University of Defense Technology), Marcos Curty (Vigo Quantum Communication Center, University of Vigo) and Vadim Makarov (Russian Quantum Center ; Vigo Quantum Communication Center).

The decoy-state method is a prominent approach to enhance the performance of quantum key distribution (QKD) systems that operate with weak coherent laser sources. Current experimental decoy-state QKD setups increase their secret key rate by raising the repetition rate of the transmitter, which can lead to correlations between subsequently emitted optical pulses. This phenomenon leaks information about the encoding settings, including the intensities of the generated signals, thus invalidating a basic premise of decoy-state QKD. Here, we experimentally characterize intensity correlations between the nearest-neigbouring optical pulses in two commercial prototypes of decoy-state BB84 QKD systems and show that they significantly reduce the asymptotic key rate. In addition, we study intensity correlations between pulses spaced further apart (higher-order correlations) and find that, in contrast to what has been conjectured, their impact on the intensity of the generated signals can be much higher than that of the nearest-neighbour (first-order) correlations.

[215] *An auto-calibrated time-to-digital converter for Quantum Communication*

Matías Rubén Bolaños Wagner (Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B - 35131 Padova, Italy), Daniele Vogrig (Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B - 35131 Padova, Italy), Paolo Villoresi (Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B - 35131 Padova, Italy), Giuseppe Vallone (Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B - 35131 Padova, Italy) and Andrea Stanco (Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B - 35131 Padova, Italy).

For quantum communication applications, time-to-digital converters (TDCs) are a crucial tool whose performance can severely affect the quality of the entire application. Nowadays, FPGA-based TDCs present a viable alternative to ASIC ones, once the nonlinear behaviour due to the intrinsic nature of the device is properly mitigated. To compensate said nonlinearities, a calibration procedure is required. Maintaining this calibration consistent during long measurements requires either interpolation methods or stopping data acquisition for a fixed time to perform the calibration process. Here we present a design and demonstration of an FPGA-based TDC showing a residual jitter of 27 ps, that is scalable for multichannel operation. We present a unique calibration method that exploits single-photon detection, which does not require stopping the data acquisition or using any interpolation methods, while keeping the device calibrated to the best of its ability. This allows Bob to receive time-tags with the best possible accuracy while also removing data-loss phases. This calibration method was tested in a relevant environment, investigating the device behaviour between 5 °C and 80 °C, where the residual jitter of the TDC was shown to be kept under control.

[216] *Practical Characterisation of channel loss for satellite-to-ground CV-QKD*

Emma Tien Hwai Medlock (University of York), Vinod Rao (University of York) and Rupesh Kumar (University of York).

Continuous variable quantum key distribution (CV-QKD) uses modulation of amplitude and phase of electromagnetic fields to encode information and shot noise limited detectors for decoding. The shot noise limited detection shows superior tolerance to noise and therefore a promising candidate for space-to-ground quantum communications, especially in daylight conditions. The parameters that affect the secure key generation rate of CV-QKD systems are the channel parameters- transmittance and uncalibrated noise (excess noise). On a typical static channel, such as an optical fibre link, the channel transmittance stays constant over a long period of signal transmission. On a dynamic channel, such as a Low Earth Orbit (LEO) based satellite to ground optical link, the transmittance of the channel varies concerning the zenith angle of the satellite.

In this poster we analyse the sources of channel loss and calculate the total loss for the full CV-QKD pass with varying channel parameters such as turbulence strengths. With percentage contributions of each of the parameters that contribute to the channel loss also shown. We demonstrate how tracking error affects and mitigates some of these losses. This was done for a CV-QKD channel as a part of the Satellite Platform for Optical Quantum communications (SPOQC) mission. In this poster we discuss the impact of the variation of channel transmittance in satellite-to-ground CV-QKD and propose a method of maximising key rate.

[217] *1002 km Twin-Field Quantum Key Distribution with Finite-Key Analysis*

Yang Liu (Jinan Institute of Quantum Technology), Wei-Jun Zhang (Shanghai Institute of Microsystem and Information Technology), Cong Jiang (Jinan Institute of Quantum Technology), Jiu-Peng Chen (Jinan Institute of Quantum Technology), Di Ma (Jinan Institute of Quantum Technology), Chi Zhang (Jinan Institute of Quantum Technology), Wen-Xin Pan (University of Science and Technology of China), Hao Dong (University of Science and Technology of China), Jia-Min Xiong (Shanghai Institute of Microsystem and Information Technology), Cheng-Jun Zhang (Photon Technology (Zhejiang) Co. Ltd), Hao Li (Shanghai Institute of Microsystem and Information Technology), Rui-Chun Wang (Yangtze Optical Fibre and Cable Joint Stock Limited Company), Chao-Yang Lu (University of Science and Technology of China), Jun Wu (Yangtze Optical Fibre and Cable Joint Stock Limited Company), Teng-Yun Chen (University of Science and Technology of China), Lixing You (Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences), Xiang-Bin Wang (Tsinghua University), Qiang Zhang (University of Science and Technology of China) and Jian-Wei Pan (University of Science and Technology of China).

Quantum key distribution (QKD) holds the potential to establish secure keys over long distances. The distance of point-to-point QKD secure key distribution is primarily impeded by the transmission loss inherent to the channel. In the quest to realize a large-scale quantum network, increasing the QKD distance under current technology is of great research interest. Here we adopt the 3-intensity sending-or-not-sending twin-field QKD (TF-QKD) protocol with the actively-odd-parity-pairing method. The experiment demonstrates the feasibility of secure QKD over a 1002 km fibre channel considering the finite size effect. The secure key rate is $3.11\times10^{-12}$ per pulse at this distance. Furthermore, by optimizing parameters for shorter fiber distances, we conducted performance tests on key distribution for fiber lengths ranging from 202 km to 505 km. Notably, the secure key rate for the 202 km, the normal distance between major cities, reached 111.74 kbps.

[218] *Modelling and characterization of pulse correlations for quantum key distribution*

Ainhoa Agulleiro (Vigo Quantum Communication Center, University of Vigo), Fadri Grünenfelder (Vigo Quantum Communication Center, University of Vigo), Margarida Pereira (Vigo Quantum Communication Center, University of Vigo), Guillermo Currás-Lorenzo (Vigo Quantum Communication Center, University of Vigo), Hugo Zbinden (Vigo Quantum Communication Center, University of Vigo), Marcos Curty (Vigo Quantum Communication Center, University of Vigo) and Davide Rusca (Vigo Quantum Communication Center, University of Vigo).

Quantum key distribution (QKD) has raised as an attractive alternative to classical cryptography due to its security being provided by quantum mechanics rather than relying on algorithms that could potentially be broken in the future, rendering current communications insecure. However, many of the security proofs rely on assumptions that may not agree with reality, for instance, device imperfections can open loopholes that could potentially be exploited by a malicious party in order to extract part, if not all, of the secret key.

In the practical implementation of QKD, a big concern is correlations arising from the limited bandwidth of real devices such as phase or intensity modulators, which causes memory effects that can leak information about previous setting choices. Some attempts have been made at introducing this type of correlations into security proofs, but most of them make the strong assumption that the maximum correlation length is finite. More recently, unbounded pulse correlations have been addressed by adding a term to the security parameter that accounts for the neglected correlations when only a finite correlation length is considered, but in turn it requires a measure of the correlations to an infinite order. Experimentally, this is very hard to achieve, which is why it is important to understand where correlations come from.

In this context, we propose a theoretical model that uses the transfer function of a linear system to explain setting-choice dependent correlations. We show that by bounding the error introduced by this transfer function in the step response of

the system, the correlation strength can be upper bounded with an exponential decay. Lastly, we show some preliminary experimental results which highlight the relative practicality of the proposed method, and we apply the results of the existing security proof to estimate a reasonable effective maximum correlation length for our setup.

[219] *Intermodal QKD with active switching between fiber and free-space channels*

Ilektra Karakosta-Amarantidou (University of Padova), Francesco Picciariello (European Space Agency), Edoardo Rossi (University of Padova), Marco Avesani (University of Padova), Luca Calderaro (ThinkQuantum s.r.l.), Giulio Foletto (KTH Royal Institute of Technology), Giuseppe Vallone (University of Padova), Paolo Villoresi (University of Padova) and Francesco Vedovato (University of Padova).

Intermodal quantum key distribution enables the integration of fiber networks and free-space channels, essential components for developing a global quantum network. We conducted a field trial of an intermodal quantum key distribution system, featuring two polarization-based transmitters and a single receiver. In this trial, the active channel was alternately switched between a 620-meter free-space link and a 17-kilometer deployed fiber in the metropolitan area of Padova. The free-space channel's performance was assessed in relation to atmospheric turbulence strength. The field trial, conducted over several hours in daylight, demonstrated the intermodal functionality between fiber and free-space channels. Our switching system offers a cost-effective solution for a trusted quantum key distribution network, minimizing the number of necessary devices across different network topologies.

[220] *Machine Learning enhanced reference frame tracking in CV-QKD*

Jennifer Bartlett (University of York), Abdulsalam Alsulami (University of York) and Rupesh Kumar (University of York).

Continuous-Variable Quantum Key Distribution (CV-QKD) uses continuous variables of the electromagnetic field, such as amplitude and phase, to transmit quantum information between two users, Alice and Bob. In this regime, there are two standard practical implementations: the transmitted local oscillator (TLO) and the local-local oscillator (LLO), where the LLO has recently reached 100km in laboratory-based fibre. Despite this success, the LLO also suffers major disadvantages like reduced quantum signal bandwidth capacity. Typically, only 50% of the transmission is for exchanging common phase references between Alice and Bob using reference signals. Subsequently, the key rate is reduced by half over all the transmission distances. In this work, we propose using a machine learning algorithm such as Long Short-Term Memory(LSTM) to predict the reference phase. The algorithm is trained with a sufficient number of phase reference data. Then, it predicts the phase drift with minimal usage of the reference signals, thereby reducing the reference signal bandwidth and increasing the key rate.

[221] *Implementations of QKD security in different use-cases*

Ilaria Vagniluca (QTI s.r.l.), Claudia De Lazzari (QTI s.r.l.), Saverio Francesconi (QTI s.r.l.), Nicola Biagi (QTI s.r.l.), Fernando Chirici (QTI s.r.l.), Tommaso Occhipinti (QTI s.r.l.), Alessandro Zavatta (QTI s.r.l., CNR-INO) and Davide Bacco (QTI s.r.l., University of Florence).

The advances in quantum key distribution (QKD) during the last 30 years have been outstanding in terms of reachable distance and key generation rate. However, the integration of quantum systems in real telecommunication networks generates multiple challenges, from technology availability to the design of inter-operable QKD systems, interconnected to key management layers and cyphers, and that can be embedded in existing telecommunication network topologies. We present several use-cases of implementation and integration of our QKD systems, in different contexts and involving Italy and neighboring countries in Europe.

[222] *Improving security and efficiency of key distribution in complex QKD networks*

Kevin Layat (ID Quantique) and Thomas Camus (ID Quantique).

Quantum Key Distribution (QKD) is a secure communication method that uses quantum mechanics principles to exchange keys between parties. The security of QKD relies on the fundamental properties of quantum physics, making it a crucial technology for achieving highly secure data transmission, in particular in the quantum computer era. Among the

impediments of the use of QKD in complex and inter-connected networks is the limited key rate provided by such system, the limited distance between two nodes that want to communicate and the need of confidentiality within the trusted relay. When QKD is implemented in large size networks, running on long distances, the usual solution is to use a lot of intermediate nodes with the consequence of reducing the performance and increasing the need of security inside these intermediate nodes. However, it is still extremely interesting for a user to implement the QKD in such types of topologies because of the high security it allows despite the limitation in bandwidth and the complexity in network topology. We propose a new approach to solve the above-mentioned problems. The core of the solution is to develop a key distribution system that can operate in a new mode; multiplying the bandwidth, in any network topology, while basing the overall security on QKD-exchanged keys.

[223] *Practical Implementation of a Quantum-augmented Communications Network*

W. Cyrus Proctor (Amazon Web Services), Lee Sattler (Verizon Communications), Matthew W. Turlington (Verizon Communications), Xinhua Ling (Amazon Web Services) and Lucian Comandar (Amazon Web Services).

This work reports on the development, deployment, and continuous field operation of a federated trusted node quantum network in service to a separate, quantum-resistant classical network. In this demonstration, we developed the infrastructure needed to connect commercial off-the-shelf quantum key distribution (QKD) systems into a four-site, multi-vendor mesh network shared by Amazon Web Services (AWS) and Verizon Communications in the Boston metropolitan area. Encrypted network links leverage QKD-enabled protocol suites, including IPsec and MACsec with data transfer rates up to 100 Gbps connecting on-premises locations to the cloud edge via the AWS Direct Connect service. Detailed health and performance monitoring data gathered over half a year allow for gap analysis with today's current commercial quantum network technologies. Coupled with symmetric encryption key demand forecasts, this sets the foundation for defining the paths forward to meet carrier-grade network redundancy and resilience requirements.

[224] *Phase and coupling efficiency stabilisation in horizontal free-space quantum key distribution*

Ry Render (University of York), Ben Amies-King (University of York), Rupesh Kumar (University of York) and Marco Lucamarini (University of York).

Development of Quantum Key Distribution (QKD) over long horizontal distances has provided both potential use cases for horizontal links within future quantum networks and testbeds to test protocols for satellite QKD. However, the majority of these implementations have used the polarisation of light as encoding scheme, with little work performed on phase-encoded schemes. Given the advantages that recent phase-based protocols such as 'twin-field' (TF) QKD have within fibre, it is possible the same distance-rate benefits can be found with free-space phase-based protocols.

To implement these protocols effectively, both the temporal phase and the spatial phase must be precisely stabilised, the former of which to our knowledge has not been tested within free-space channels. We performed a laboratory interference experiment to evaluate the feasibility of TF-QKD using both free-space and fibre channels, providing a hybrid channel configuration. Our results demonstrate a reduction in the channels' phase noise while maintaining a stable coupling efficiency. This paves the way towards future field trials of phase-encoded protocols within free-space and hybrid channel networks.

[225] *One-shot Oblivious Transfer from Noisy Quantum Storage*

Ricardo Faleiro (IT-Aveiro), Manuel Goulão (OIST) and Emmanuel Zambrini Cruzeiro (IST-Lisbon).

Few primitives are as intertwined with the foundations of cryptography as Oblivious Transfer (OT). Not surprisingly, with the advent of quantum resources in information processing, OT played a central role in establishing new possibilities (and defining impossibilities) pertaining to the use of these novel assets. A major research path is minimizing the required assumptions to achieve OT, and studying their consequences. Regarding its computation, it is impossible to construct unconditionally-secure OT without extra assumptions; and, regarding communication complexity, achieving one-shot (and even non-interactive) OT has proved to be an elusive task, widely known to be impossible classically. In this work, we devise a \textit{one-shot OT}, showig how this construction is indeed possible using quantum resources, if we assume the existence of one-way functions and sequential functions in the Noisy-Quantum-Storage Model.

[226] *Decoy state quantum key distribution with a bright telecom wavelength quantum dot single-photon source*

Frederik Brooke Barnes (Heriot-Watt University), Christopher Morrison (Heriot-Watt University), Roberto Pousa (University of Strathclyde), Francesco Graffiti (Heriot-Watt University), Zhe Koong (Heriot-Watt University), Peter Barrow (Heriot-Watt University), John Jeffers (University of Strathclyde), Daniel Oi (University of Strathclyde), Brian Geradot (Heriot-Watt University) and Alessandro Fedrizzi (Heriot-Watt University).

Quantum key distribution (QKD) with solid-state single-photon emitters is gaining traction due to their rapidly improving performance and compatibility with future quantum networks. We report a bright quantum dot based source of telecom photons by frequency converting a near- infrared InGaAs quantum dot to the telecom C-band [1]. We implement polarisation encoded BB84 quantum key distribution (QKD), achieving a positive asymptotic key rate over 175 km of optical fibre. We also present finite key analysis optimised for typically non-ideal single- photon sources, achieving 8 orders of magnitude improvement with finite key rates of 40 kbps over 50 km in practical acquisition times of one hour [2]. To extend the distances further, we take inspiration from decoy state QKD protocols – typically used to overcome photon- splitting attacks when using weak coherent states – and demonstrate a QD excitation scheme for implementing modulation of the photon number distribution. We show experimentally that the decoy state protocol enables the distribution of a secret key over more than 200 km of optical fibre.

References [1] C. L. Morrison, et al., "A bright source of telecom single photons based on quantum frequency conversion," Applied Physics Letters, 118, 174003 (2021). [2] C. L. Morrison, et al., "Single-emitter quantum key distribution over 175 km of fibre with optimised finite key rates," Nature Communications, 14, 3573 (2023).

[227] *Quantum key distribution with small data block sizes*

Vaisakh Mannalath (Vigo Quantum Communication Centre), Victor Zapatero (Vigo Quantum Communication Centre) and Marcos Curty (Vigo Quantum Communication Centre).

Quantum Key Distribution (QKD) is a crucial technology for secure communication, relying on the principles of quantum mechanics. The security of QKD protocols is often analyzed by bounding the probability of a "failure" during the parameter estimation step. This failure probability is typically addressed using tail bounds on the hypergeometric distribution. However, existing methods can sometimes be conservative, leading to inefficiencies. In this work, we present an alternative approach that provides a more refined bound by exploiting a simple yet effective link between hypergeometric and binomial random variables.

[228] *High Secret Key Rates with Hybrid Photonic Integrated Circuits*

Julius Römer (Universität Heidelberg), Erik Jung (Universität Heidelberg) and Wolfram Pernice (Universität Heidelberg).

Advancements in quantum computing pose significant threats to the security of conventional encryption standards. Although quantum key distribution systems offer inherent security, they face challenges in achieving practical secret-key rates over long transmission distances [2]. Multiplexing schemes can substantially enhance key rates, and integrated photonic chip technologies provide the necessary scalability and system efficiency for high key rates using wavelength-division time-bin protocols. We propose a hybrid sender module that employs on-chip lasers and fast modulators on the indium-phosphide platform for qubit state preparation. The multiplexer is fabricated on a low-loss silicon nitride chip, utilizing ring resonators and Bragg reflectors. We report progress in developing a sender module designed to achieve secret key rates in the gigabit per second range. Additionally, the system is compatible with a receiver that integrates waveguide-based superconducting nanowire single-photon detectors with on-chip de-multiplexing, ensuring high detection efficiency and key rates [1]. This design supports the implementation of protocols such as the one-decoy state time-bin BB84 protocol and promises further scalability.

[229] *Diversification of trust in satellite quantum key distribution*

Gianluca De Santis (Technology Innovation Institute), Konstantin Kravtsov (Technology Innovation Institute), Sana Amairi-Pyka (Technology Innovation Institute) and James A. Grieve (Technology Innovation Institute).

Quantum key distribution (QKD) via satellite links is the only currently viable solution to create quantum-backed secure communication at a global scale. To achieve intercontinental coverage with available technology one must adopt a “flying trusted node” paradigm, in which users fully trust the satellite platform. The major part of the poster will focus on our latest work where inspired by the concept of distributed secret sharing and the imminent projected launch of several QKD-equipped satellites, we proposed a parallel trusted node approach, in which key distribution is mediated by several satellites in parallel. This distributes the trust, removes single points of failure, and reduces the necessary assumptions. In addition, we discussed the versatility that an optical ground station should provide to execute such a protocol and, in general, to be fully integrated into a multi-party global quantum network. Finally, one last section of the poster will focus on how we will implement the idea of versatility and adaptability at the Abu Dhabi Quantum Optical Ground Station from a hardware perspective.

[230] *A coherence-witnessing game and applications to semi-device-independent quantum key distribution*

Mário Silva (Université de Lorraine, CNRS, Inria, Nancy, France), Ricardo Faleiro (Instituto de Telecomunicações, Av. Rovisco Pais 1, 1049-001, Lisboa, Portugal), Paulo Mateus (Departamento de Matemática, Instituto Superior Técnico, Av. Rovisco Pais 1, 1049-001, Lisboa, Portugal) and Emmanuel Zambrini Cruzeiro (Instituto de Telecomunicações, Av. Rovisco Pais 1, 1049-001, Lisboa, Portugal).

Device-independence (DI) is the golden standard for quantum key distribution (QKD) security: it allows unconditional security based on the laws of physics even for untrusted or maliciously designed devices [1]. Nevertheless, DI-QKD, for now, remains extremely challenging. The first proof-of-principle experiments having been performed only very recently [2,3], almost 40 years after the invention of BB84. It then becomes naturally interesting to study scenarios which may reach a compromise between experimental challenge and security: for example, by assuming than the users have a partial description of the devices. This intermediate scenario is called semi-device-independent (SDI) QKD and aims for a reasonable trade-off between the highest level of security, device-independence, and experimental feasibility.

Alternatively, semi-quantum key distribution [4] is an interesting approach whose purpose is to reduce the quantum technological requirements of users, whilst still guaranteeing security, in order to develop simple and hardware fault-tolerant quantum key distribution protocols. There, one is interested in limiting Alice or Bob to a single measurement basis, for instance, or force them to only perform detection or reflection of photons [5].

In this work, we take a first step towards the intersection of semi-device-independent and semi-quantum protocols. We do so by introducing a coherence-based semi-quantum, semi-device-independent, quantum key distribution protocol where users only need to implement classical operations i.e. single-basis measurements. The protocol is based on the noise-robust version of a coherence-based game introduced by del Santo and Dakić [6], that witnesses different types of coherence. The unconditional security of the protocol is proven in the bounded quantum storage model, and is obtained from the optimal quantum bounds of the users' performance in the game, constrained by a noise parameter, in order to prevent the use of resources that trivialize the game. Furthermore, the game can be interpreted as a coherence witness allowing for the certification of different type of coherence resources.

Our protocol is a proof-of-concept for the unification of both frameworks of device-independent and semi-quantum key distribution. The novelty relies in using a coherence-based game for testing randomness, rather than the usual Bell tests, as a basis for the security of the protocol. This allows for the certification on quantum correlations with fixed single-basis measurements, both for Alice and Bob. Our findings are relevant in the context of establishing fault-tolerant and robust tests of non-classicality for quantum communication.

Acknowledgments

This is joint work with Mário Silva, Ricardo Faleiro and Prof. Paulo Mateus. The published version can be found in the journal Quantum [7].

References

[1] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. 98, 230501 – Published 4 June 2007.

[2] Zhang, W., van Leent, T., Redeker, K. et al. A device-independent quantum key distribution system for distant users. Nature 607, 687–691 (2022).

[3] Nadlinger, D.P., Drmota, P., Nichol, B.C. et al. Experimental quantum key distribution certified by Bell's theorem. Nature 607, 682–686 (2022).

[4] Michel Boyer, Ran Gelles, Dan Kenigsberg, and Tal Mor, Semiquantum key distribution, Phys. Rev. A 79, 032341 – Published 30 March 2009.

[5] Francesco Massa et al, Experimental Semi-quantum Key Distribution With Classical Users, Quantum 6, 819 (2022).

[6] Flavio Del Santo and Borivoje Dakić, Coherence Equality and Communication in a Quantum Superposition, Phys. Rev. Lett. 124, 190501 – Published 14 May 2020.

[7] Silva, Mário, Ricardo Faleiro, Paulo Mateus, and Emmanuel Zambrini Cruzeiro. "A coherence-witnessing game and applications to semi-device-independent quantum key distribution." Quantum 7 (2023): 1090.

[231] *Numerical Key Rates Calculations for BB84, No Public Announcement of Basis BB84 and SARG04 with Weak Coherent Pulses*

Aodhan Corrigan (University of Waterloo), Zhiyao Wang (University of Waterloo) and Norbert Lütkenhaus (University of Waterloo).

We examine the performance of three Quantum Key Distribution (QKD) protocols with different classical announcement structures, namely BB84, SARG04 and No Public Announcement of Basis (NPAB) BB84, using numerical security proof techniques. We simulate these protocols in a Weak Coherent Pulse (WCP) implementation in order to characterize their behaviour in a realistic implementation without decoy states. We vary the quantum channel characteristics and compare key rates of the three protocols in asymptotic and finite-size regimes. The three protocols show different relative advantages depending on the channel behaviour. Canonical BB84 shows robustness against errors and depolarization, SARG04 demonstrates resilience against high loss channels and NPAB BB84 shows potential advantages when we introduce physical misalignment between QKD devices.

[232] *Optical payload design for downlink quantum key distribution and keyless communication using CubeSats*

Gonçalo Teixeira (Instituto de Telecomunicações - Lisboa).

Quantum physics provides the framework for quantum communication protocols to achieve unconditionally secure communication by utilizing the laws of physics to detect potential eavesdroppers. Quantum key distribution is the used protocol, however, is costly and, at the moment, offers low performance in space applications. Other more recent protocols could offer a potential practical solution to this problem. In this work, a preliminary optical payload design using commercial off-the-shelf elements for a quantum communication downlink in a 3U CubeSat is proposed. It is shown that this quantum state emitter allows the establishment of two types of quantum communication between the satellite and the ground station: quantum key distribution and quantum keyless private communication. Numerical simulations are provided that show the feasibility of the scheme for both protocols as well as their performance. For the simplified BB84, a maximum secret key rate of about 80 kHz and minimum QBER of slightly more than 0.07 % is found, at the zenith, while for quantum private keyless communication, a 700 MHz private rate is achieved. This design serves as a platform for the implementation of novel quantum communication protocols that can improve the performance of quantum communications in space.

[233] *Polarization-based quantum keyless private communication*

Pedro Mendes (Instituto de Telecomunicações) and Emmanuel Zambrini Cruzeiro (Instituto de Telecomunicações).

Quantum communication ensures security by using quantum mechanics, typically through Quantum Key Distribution (QKD) which is limited to a few hundred kilometers for useful secret key rates. This study examines Quantum Keyless Private Communication (QKPC), inspired by the classical wiretap model, which allows secure one-way communication without shared keys. Two implementations are explored: the original On-Off Keying (OOK) and a new polarization-based version. Both methods are implemented experimentally and the results confirm their effectiveness and potential as practical alternatives to traditional QKD for secure, long-distance communication.

[234] *National Quantum Communication Infrastructure in Sweden*

Giulio Foletto (KTH, Royal Institute of Technology), Hilma Karlsson (KTH, Royal Institute of Technology), Xiaodan Pang (KTH, Royal Institute of Technology), Vaishali Adya (KTH, Royal Institute of Technology) and Katia Gallo (KTH, Royal Institute of Technology).

The main goal of the NQCIS project is to build a quantum key distribution (QKD) network centered in Stockholm and that is adapted to the particular geographical properties of Sweden. The center of the network will be the AlbaNova hub, which will also be open to selected users to test the QKD technology. From there, fiber links will reach two nodes in the metropolitan area (<20 km in length) and two longer distance points (80-150 km-long links), which will require also a trusted node. The network will use both continuous and discrete-variable devices, the latter being augmented by superconducting nanowire detectors. Furthermore, we are refurbishing an astronomical telescope to serve as an optical ground station for QKD, giving satellite-tracking capabilities. The project has also goals that go beyond deployment. One is advancing research in quantum communication with a study of stabilization techniques for twin field QKD and of noise contribution hindering different QKD protocols, and the other is forming the Swedish quantum work force through coordinated courses, seminars, and outreach events. This poster gives an overview of the entire project.

[235] *Experimental of multi-user continuous-variable quantum key distribution*

Adnan A.E. Hajomer (Technical University of Denmark), Ivan Derkach (Palacky University), Radim Filip (Palacky University), Ulrik L. Andersen (Technical University of Denmark), Vladyslav C.Usenko (Palacky University) and Tobias Gehring (Technical University of Denmark).

We report the experimental demonstration of multi-user continuous-variable quantum key distribution based on a passive optical network (QPON) that supports se- cure key generation for 5 users simultaneously. This is achieved considering practical PON topology with an 11 km span of access links.

[236] *Quantum Communications Feasibility Tests over a UK-Ireland 224 km Undersea Link*

Karolina Schatz (School of Physics, Engineering & Technology and York Centre for Quantum Technologies, University of York), Ben Amies-King (School of Physics, Engineering & Technology and York Centre for Quantum Technologies, University of York), Haofan Duan (School of Physics, Engineering & Technology and York Centre for Quantum Technologies, University of York), Ayan Biswas (School of Physics, Engineering & Technology and York Centre for Quantum Technologies, University of York), Sophie Albosh (School of Physics, Engineering & Technology and York Centre for Quantum Technologies, University of York), Rupesh Kumar (School of Physics, Engineering & Technology and York Centre for Quantum Technologies, University of York) and Marco Lucamarini (School of Physics, Engineering & Technology and York Centre for Quantum Technologies, University of York).

The future quantum internet will leverage existing communication infrastructures, including deployed optical fibre networks, to enable novel applications that outperform current information technology. In this scenario, we perform a feasibility study of quantum communications over an industrial 224 km submarine optical fibre link deployed between Southport in the United Kingdom (UK) and Portrane in the Republic of Ireland (IE). With a characterisation of phase drift, polarisation stability and the arrival time of entangled photons, we demonstrate the suitability of the link to enable international UK–IE quantum communications for the first time.

[237] *Security evaluation of the transmitted quantum states of a commercial QKD system operated in test sequence (TS) mode*

Christian Daniel Munoz (National Physical Laboratory), Benjamin White (National Physical Laboratory), Christopher Chunnilall (National Physical Laboratory), Gianluca Boso (ID Quantique) and Benjamin Strudwick (ID Quantique).

This work reports on the implementation of a test sequence mode in a commercial QKD system, the methods and instrumentation designed to characterize the quantum states transmitted by such a system in TS mode, and the results obtained. These results are the first reported on a commercial QKD system operated in such a mode.

[238] *Grobner basis of partially commuting variables*

Abhishek Mishra (Université Libre de Brussels), Moisés Moran (Université Libre de Brussels) and Stefano Pironio (Université Libre de Brussels).

Our motivation is to exploit the partial commutation structure between the variables in non-commutative polynomial optimisation problems to boost the performance. We provide an efficient normal form for free words in partially commuting letters based on the maximal cliques of the non-commutation graph between the letters. We adapt several non-commutative computations to the partially commuting setting exploiting this additional structure. In particular, we provide an algorithm to compute Grobner bases for polynomial ideals in partially commuting variables that overcomes some difficulties appearing in the non-commutative cases: sometimes infinite Grobner basis can be avoided using the normal form based on these cliques.

[239] *Developing a flexible Quantum Key Distribution support layer based on White Rabbit time synchronisation*

Ben Amies-King (School of Physics, Engineering and Technology, University of York) and Marco Lucamarini (School of Physics, Engineering and Technology, University of York).

Quantum key distribution (QKD) enables secure communications against an adversary with unbounded classical and quantum computing capability. Since the original BB84 protocol was proposed, various other protocols have been developed with specific hardware requirements on the quantum layer. However, in general time synchronisation and a classical communications channel remain core ancillary requirements of QKD on the typically classical support layer. The White Rabbit (WR) technology, developed at CERN, provides a convenient means to achieve sub-nanosecond timing synchronisation over optical fibre. In order to enhance its suitability as an ancillary system to QKD, we demonstrate a significant extension of the range of WR over a single uninterrupted stretch of fibre to 250 km, and report on our success in transferring the timing accuracy of WR to coordinating a simultaneous 'start time' between Alice and Bob.

[240] *Decrease of certifiable randomness when entanglement is allowed in energy-constrained QRNGs*

Gabriel Ignacio Senno (Quside Technologies SL) and Antonio Acín (ICFO - Institute of Photonic Sciences, Barcelona, Spain).

In this work, we study the consequences of entanglement-assistance (EA) for randomness generation in the semi-DI framework based on energy constraints introduced in [van Himbeeck et al., Quantum 1, 33 (2017)]. We show that, given an energy bound $\omega$, the minimum min-entropy that non-EA honest devices can certify decreases when entanglement between the prepare and measurement boxes (of the devices prepared by Eve) is allowed.

[241] *CV-QRNG and Optical Receiver Module on SPOQC CV Payload*

Vinod N. Rao (University of York), Emma Medlock (University of York), Tim Spiller (University of York) and Rupesh Kumar (University of York).

This poster presentation demonstrates the quantum random number generation (QRNG) from a shotnoise-limited homodyne detector. The detector is part of the continuous variable quantum key distribution (CVQKD) payload developed for the Satellite Platform for Optical Quantum Communications (SPOQC) mission. We also show how the onboard homodyne detector works as a CVQKD receiver on the satellite.

[242] *Free-Space Twin-Field Quantum Key Distribution*

Yu-Huai Li (University of Science and Technology of China).

Twin-field quantum key distribution (TF-QKD) improves the secure key rate from the linear scale of channel loss to the square root scale while preserving the security of measurement-device-independent. This scheme is well suited to building the global-scale quantum network that suffers from extremely high channel loss. Since it was proposed, fiber-based demonstrations have been rapidly developed. However, TF-QKD over a free-space channel remains experimentally

challenging due to the effect of atmospheric turbulence. Here, we realized the first free-space TF-QKD protocol over two 7.1-km urban atmospheric channels, which exceeds the effective atmospheric thickness. A secure key rate exceeding the repeaterless secret key capacity was demonstrated. By controlling the time and phase of optical pulses through the open channel, our setup avoids the requirement of an additional channel to construct a closed interferometer. Our experiment takes a significant step toward the satellite-based global quantum network with a high level of practical security.

[243] *Improving the secure key rate of free-space twin-field quantum key distribution under turbulent atmosphere*

Min-Yan Wang (University of Science and Technology of China), Yu-Huai Li (University of Science and Technology of China) and Yuan Cao (University of Science and Technology of China).

Twin-field quantum key distribution (TF-QKD) allows a secure key rate to break the repeaterless bound, which is known as the Pirandola-Laurenza-Ottaviani-Bianchi (PLOB) bound. Together with the security of measurement device independence, it is important in the future global quantum network. TF-QKD requires single photon interference between two independent optical fields transmitted through different channels. In free-space channels, atmospheric turbulence strongly disturbs the laser beam's wavefront, leading to a significant intensity fluctuation of received photons. This random fluctuation causes intensity distinguishability between two beams, thus reducing the visibility of interference and the secure key rate. Here, we proposed a scheme to increase the secure key rate under such unstable channels. The characteristics, especially the intensity fluctuation, of free-space channels are presented. Numerical analysis is performed to demonstrate the improvement of the secure key rate with our strategy. The result shows that, under a typical atmospheric condition of 14 km distance, the secure key rate of TF-QKD can be increased to 3.75 times. Our method can be a general tool widely used in the future long-distance horizontal or satellite-based free-space quantum key distribution.

[244] *Toward Certifiable QKD: Addressing Side Channels and Implementation Attacks in a Standardized Testing Framework*

Florian Prawits (Austrian Institute of Technology), Daniel Pereira (Austrian Institute of Technology), Mariana Ferreira-Ramos (Austrian Institute of Technology), Hannes Hübel (Austrian Institute of Technology) and Martin Stierle (Austrian Institute of Technology).

Quantum Key Distribution (QKD) promises unprecedented security based on the principles of quantum mechanics. However, practical implementations of QKD systems are susceptible to various side-channel and implementation attacks that can compromise their security. We presents a comprehensive overview of the literature on side channels and implementation attacks on QKD systems, a systematic categorization of different attack vectors and proposed counter measures and analysis of their impact on security. Furthermore, we propose a structured approach for developing standardized tests to evaluate the robustness of QKD systems against these vulnerabilities. Our work aims to bridge the gap between theoretical security and practical implementation, providing a roadmap for future certification of QKD products to be deployed within the European Quantum Communication Infrastructure (EuroQCI).

[245] *Quantum key distribution over connectionless quantum repeater networks*

Javier Rey-Domínguez (University of Leeds) and Mohsen Razavi (University of Leeds).

Quantum networks use platforms like quantum repeaters to enable quantum communications at arbitrary distances. Early quantum networks are expected to be deployed on pre-existing infrastructure, sharing resources with classical networks, and thus can benefit from compatible design principles and behaviours. In particular, most of the research on quantum repeater networks based on entanglement distribution assume that some connection is established in order to reserve resources for the distribution attempt. However, the most prominent classical network, the Internet, is built upon the concept of connectionless communications, and therefore this approach might not be ideal for the early stages of deployment. In our work, we investigate the performance of connectionless protocols over quantum networks. To do so, we consider both unencoded (standard) but deterministic repeaters, and repeaters using a 3-quit repetition code. We analyse the achievable secret key rates for both of these setups in different regimes of errors. Our results suggest that

error correction techniques such as the usage of encoded quantum repeaters will be crucial to the success of early quantum networks.

[246] *Hybrid encoder for discrete and continuous variable QKD*

Mattia Sabatini (University of Padova), Tommaso Bertapelle (University of Padova), Marco Avesani (University of Padova), Giuseppe Vallone (University of Padova) and Paolo Villoresi (University of Padova).

We present a versatile hybrid encoder for quantum key distribution that supports both discrete variable (DV) and continuous variable (CV) protocols. The encoder, based on an iPOGNAC modulator, utilizes commercial off-the-shelf components and can be reconfigured for efficient polarization modulation in DV protocols or polarization-independent phase modulation in CV protocols. This innovative design enhances flexibility, enabling the selection of the most efficient protocol based on link parameters. We experimentally realized the proposed device and tested it with both DV and CV receivers to demonstrate its performance.

[247] *Experimental characterisation of second-order phase correlations in gain-switched laser sources for decoy-state QKD*

Alessandro Marcomini (University of Vigo), Fadri Grünenfelder (University of Vigo), Guillermo Currás-Lorenzo (University of Vigo), Angel Valle (Instituto de Física de Cantabria), Kiyoshi Tamaki (University of Toyama), Hugo Zbinden (University of Vigo), Marcos Curty (University of Vigo) and Davide Rusca (University of Vigo).

Quantum key distribution (QKD) protocols leverage quantum mechanics to achieve information theoretically secure communication, yet real-world implementations must address experimental limitations, particularly phase correlations in weak coherent laser pulses (WCPs). High-speed gain-switching lasers, commonly used in QKD, can exhibit residual photons causing phase correlations between consecutive pulses, challenging the perfect phase randomization assumption crucial for the decoy-state BB84 protocol. Theoretical work has proposed security proofs that require knowledge of how closely each phase's probability distribution approximates uniformity, which is complex to estimate experimentally. In this study we introduce an experimental method to characterise phase correlations of any length under realistic conditions by modelling the phase generation process within the laser cavity. Additionally, we experimentally benchmark this practical routine for measuring second-order correlations using a double Michelson interferometer with tunable amplitude attenuators, allowing comprehensive characterisation of the phase generation process and accurate measurement of the phase probability distribution, thus enhancing the security of QKD systems.

[248] *Finite size analysis of quantum key distribution with advantage distillation*

Jonas Treplin (DLR), Philipp Kleinpaß (DLR) and Davide Orsucci (DLR).

Quantum Key Distribution (QKD) can be performed securely only when the Quantum Bit Error Rate (QBER) is below a certain threshold which, due to the unavoidable presence of noise, limits the maximum transmission distance. Advantage Distillation (AD) is a classical post-processing technique that enhances QKD protocols by increasing error tolerance, thus extending the communication range. AD operates by post-selecting blocks of bits and extracting fewer correlated bits between Alice and Bob, which exhibits a reduced QBER, while Eve's mutual information does not significantly increase. This process ultimately lowers the information disclosure in the information reconciliation step, while the relative key shortening during privacy amplification remains largely unaffected. In this study, we present the first comprehensive finite key size analysis of the decoy-state version of the BB84 protocol including AD post-processing. Our results demonstrate a notable improvement in QBER tolerance through AD, with the 1-decoy version outperforming the 2-decoy version of the protocol. This analysis has significant implications for long-distance and satellite-based QKD applications, which are constrained by QBER, as it shows that substantial performance enhancements can be achieved by improved post-processing techniques.

[249] *Port-Based State Preparation and Applications*

Garazi Muguruza (QuSoft, University of Amsterdam) and Florian Speelman (QuSoft, University of Amsterdam).

We introduce Port-Based State Preparation (PBSP), a teleportation task where Alice holds a complete classical description of the target state and Bob's correction operations are restricted to only tracing out registers. We show a protocol that implements PBSP with error decreasing exponentially in the number of ports, in contrast to the polynomial trade-off for the related task of Port-Based Teleportation, and we prove that this is optimal when a maximally entangled resource state is used.

As an application, we introduce approximate Universal Programmable Hybrid Processors (UPHP). Here the goal is to encode a unitary as a quantum state, and the UPHP can apply this unitary to a quantum state when knowing its classical description. We give a construction that needs strictly less memory in terms of dimension than the optimal approximate Universal Programmable Quantum Processor achieving the same error. Additionally, we provide lower bounds for the optimal trade-off between memory and error of UPHPs.

[250] *Entangled photon pair source for Quantum Key Distribution*

Álvaro Magdalena (VQCC, university of Vigo), Hannah Thiel (VQCC, university of Vigo), Davide Rusca (VQCC, university of Vigo) and Antía Lamas-Linares (VQCC, university of Vigo; AWS).

In this work we are designing and building an entangled photon pair source based on spontaneous parametric down-conversion. The source is highly non-degenerate to accommodate transmission in both fiber and free space. This source is intended for use in QKD applications. To achieve this, we explain and characterize the dependence on the temperature, poling period, phase matching, temporal walk-off, beam waist and the expected performance of this source.

[251] *The National Quantum-Safe Network in Singapore*

Hao Qin(CQT, NUS), Jing Yan Haw(CQT, NUS), Matthew Wee (CQT, NUS), Cassey Liang (CQT, NUS), Xiao Duan(FSR@NTU), Yu Cai(SPMS, NTU), Sanat Sarda(FSR@NTU), KaiWei Qiu (NTU), Ramana Murthy (CQT, NUS), Romain Frappier (ECE, NUS), Nelly Ng (SPMS, NTU), Biplab Sikdar (ECE, NUS), Christian Kurtsiefer (CQT, Dept. of Physics, NUS), Michael Kasper (FSR@NTU), Alexander Ling (CQT, Dept. of Physics, NUS)

The National Quantum-Safe Network (NQSN) in Singapore is a nationwide collaborative platform and a field-deployed test-bed aimed at demonstrating quantum-safe cryptography solutions. NQSN links up academic, public and private members, targets trials for quantum key distribution (QKD) network with different QKD protocols, post-quantum cryptography (PQC) and classical symmetric key technologies.

[252] *Trusted noise treatment in discrete-modulation continuous-variable quantum key distribution*

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

The trusted device scenario is the assumption that an adversary cannot access imperfections in the detectors such as electronic noise, aiming at improving the key rate of quantum key distribution (QKD) protocol. In the case of trusted Gaussian noises in the detectors of continuous-variable (CV) QKD, there is a method based on rescaling that is applicable to any protocol using homodyne or heterodyne detectors. Here, we are interested in what kind of CV-QKD protocols tend to benefit more from the trusted scenario. Using prior research that extended the covariance matrix analysis from Gaussian modulation to discrete modulation, we evaluated the quantitative effect of rescaling on the key rate with arbitrary modulation. Our results revealed that the performance asymptotically improves in any discrete modulation protocol, and this improvement is more significant compared to Gaussian modulation. Additionally, we developed a method to address unbalanced heterodyne measurements, where the noise and transmittance of the two homodyne detectors differ. This allows for a more realistic measurement model to be addressed with discrete modulation.

[253] *A highly modular and configurable Python framework for QKD*

Felix Kunzmann (Fraunhofer Institute for Integrated Circuits IIS Design Automation Division EAS), Christian Skubich (Fraunhofer Institute for Integrated Circuits IIS Design Automation Division EAS), Holger Priwitzer (Fraunhofer Institute for Integrated Circuits IIS Design Automation Division EAS), Stefan Krause (Fraunhofer Institute for Integrated Circuits IIS Design Automation Division EAS) and Kay-Uwe Giering (Fraunhofer Institute for Integrated Circuits IIS Design Automation Division EAS).

See attached PDF.

[254] *Conditional disclosure of secrets with quantum resources*

Alex May (Institute for Quantum Computing and Perimeter Institute for Theoretical Physics), Vahid Reza Asadi (University of Waterloo), Kohdai Kuroiwa (Institute for Quantum Computing and Perimeter Institute for), Debbie Leung (Institute for Quantum Computing and Perimeter Institute for Theoretical Physics), Sabrina Pasterski (Perimeter Institute for Theoretical Physics) and Chris Waddell (Perimeter Institute for Theoretical Physics).

The conditional disclosure of secrets (CDS) primitive is among the simplest cryptographic settings in which to study the relationship between communication, randomness, and security. CDS involves two parties, Alice and Bob, who do not communicate but who wish to reveal a secret $z$ to a referee if and only if a Boolean function $f$ has $f(x,y)=1$. Alice knows $x,z$, Bob knows $y$, and the referee knows $x,y$. Recently, a quantum analogue of this primitive called CDQS was defined and related to $f$-routing, a task studied in the context of quantum position-verification. CDQS has the same inputs, outputs, and communication pattern as CDS but allows the use of shared entanglement and quantum messages. We initiate the systematic study of CDQS, with the aim of better understanding the relationship between privacy and quantum resources in the information theoretic setting. Following the classical literature on CDS for guidance, we establish closure under negation, an amplification property, and prove a number of lower bounds on CDQS based on communication complexity.