Introduction to post-quantum cryptography

Alice Pellet–Mary*[1]

[1]Institut de Mathématiques de Bordeaux (IMB) – Université de Bordeaux, Centre National de la Recherche Scientifique – France

Abstract

This tutorial will be an introduction to post-quantum cryptography. We will see what threat poses quantum computers on the security of the currently used cryptographic schemes, and how to circumvent this threat using different mathematical assumptions.

*Speaker

Implementation security in experimental QKD

Davide Rusca*[1]

[1]University of Vigo [Pontevedra] – Spain

Abstract

Quantum Key Distribution has advanced over the past decade from being a purely academic effort to a commercialized technology. However, research in this field is far from complete. While it is relatively easy to prove its security within the realm of abstract theory, things change when it is implemented experimentally. This talk will explore the latest efforts to bridge the gap between theory and experiment, aiming to achieve stronger and more practical implementation security. In particular, the main vulnerabilities of the most widely used protocols, such as decoy-state BB84, will be explored, along with the key solutions that have been implemented in recent years.

*Speaker

Quantum cryptography beyond key distribution and its practical challenges

Mathieu Bozzio*[1]

[1]University of Vienna (UNIVIE) – Austria

Abstract

Owing to its fundamental principles, quantum theory holds the promise to enhance the security of modern cryptography, from message encryption to anonymous communication, digital signatures, online banking, leader election, one-time passwords, and delegated computation. While quantum key distribution (QKD) has already enabled secure key exchange over hundreds of kilometers, a myriad of other quantum-cryptographic primitives are being developed to secure future applications against quantum adversaries. This tutorial will provide an intuitive introduction to the main quantum primitives and their security levels, summarize their possibilities and limits, and discuss practical challenges related to their photonic implementation and practical security.

*Speaker

Computational quantum information theory

Rotem Arnon*[1]

[1]School of Computer and Communication Sciences - EPFL – Switzerland

Abstract

Quantum information theory, particularly its entropic formulations, has made remarkable strides in characterizing quantum systems and tasks. However, a critical dimension remains underexplored: computational efficiency. While classical computational entropies integrate complexity and feasibility into information measures, analogous concepts have yet to be rigorously developed in the quantum setting. In this talk, I will present new results that lay the foundation for computational information theory and its applications to quantum cryptography and entanglement theory.
The talk will be based on the recent results https://arxiv.org/abs/2505.13710 and https://arxiv.org/abs/2506.14068

[*] Speaker

Quantum Lifting Theorems in QROM and QRPM

Alexandru Cojocaru*[1]

[1]University of Edinburgh – United Kingdom

Abstract

We give novel and tighter lifting theorems for security games in the quantum random oracle model (QROM), as well as in Noisy Intermediate-Scale Quantum (NISQ) settings such as the hybrid query model, the noisy oracle and the bounded-depth models. At the core of our main results lies a novel measure-and-reprogram framework that we call coherent reprogramming. This framework gives a tighter lifting theorem for query complexity problems. Secondly, we provide a hybrid lifting theorem for hybrid algorithms that can perform both quantum and classical queries, as well as a lifting theorem for quantum algorithms with access to noisy oracles or bounded quantum depth. Thirdly, we derive lifting theorems for establishing security in the quantum random permutation and ideal cipher models. These theorems relate the success probability of an arbitrary quantum adversary to that of a classical algorithm making only a small number of classical queries.

*Speaker

Uncloneable Encryption from Decoupling

Archishna Bhattacharyya*[1] and Eric Culf[2]

[1]University of Ottawa [Ottawa] – Canada
[2]University of Waterloo – Canada

Abstract

An uncloneable encryption scheme encodes a classical message as a quantum ciphertext in order to guarantee that two non-interacting adversaries cannot both learn the message, even when given the encryption key. This defines a stronger classically-impossible notion of security, as any classical ciphertext can be copied. So far, a security proof for uncloneable encryption has been elusive.

We show that uncloneable encryption exists with no computational assumptions, with security inverse-polynomial in the security parameter. We use properties of a monogamy-of-entanglement game associated with the Haar-measure encryption to guarantee that any state that succeeds with high probability cannot be close to maximally-entangled between the referee and either of the players, whence we can apply a decoupling theorem to show that either player becomes completely uncorrelated, and therefore cannot win significantly better than random guessing.

Based on arXiv 2503.19125, this is joint work with Eric Culf.

*Speaker

Narrowing security gaps and boosting qubit rates in quantum communication

Boris Korzh*[1], Shashank Kumar[1], Alessandro Marcomini[2], Towsif Taher[1], and Loïc Millet[1]

[1]Group of Applied Physics, Université de Genève (GAP) – Switzerland
[2]University of Vigo [Pontevedra] – Spain

Abstract

Ongoing research directions in secure quantum communication include addressing gaps between theoretical and implementation security, component and system certification, improving the compactness and deployability of systems, as well as boosting the throughput in terms of secret-bits/s and ebit/s, all to achieve broad utility, maturity and traceability. In this talk, we will discuss progress towards closing one of the implementation security gaps in quantum key distribution, namely phase correlations of qubits at high frequencies. We will then review progress towards next-generation superconducting nanowire detectors (SNSPDs) which combine many state-of-the-art metrics into a single system, to achieve boosted clock-rates in quantum communication. We will also discuss on-going efforts to improve the deployability of SNSPDs through the development of large-scale arrays, which promise to drastically lower the cost-per-channel in next generation quantum networks.

*Speaker

Slovak deployment of BBM92 across a 248km fully-meshed 4-nodes inter-city quantum network

Djeylan Aktas*[1]

[1]Institute of Physics SAS – Slovakia

Abstract

Quantum Key Distribution promises an unconditional security based on the laws of quantum physics referred as Information Theoretically Secure. Ideally implemented that means an eavesdroppers cannot retrieve key information without introducing detectable errors. This allows for two remote parties to share sequences of private random bits which can be primitives to implement secure communication protocols that do not necessarily rely on the assumption of a bounded computing power for the attacker. As of late, recent work has shown that entanglement-based QKD could be one of the most suitable candidates for fully-meshed topologies, which greatly reduces the overhead cost of adding a new user without the need for trusted-nodes. In this talk, I will present the Slovak strategy for the deployment of a backbone infrastructure for the national quantum test-bed. I will discuss how the design of a broadband entangled photon pairs generator can leverage spontaneous parametric down conversion of periodically poled lithium niobate crystal within a Sagnac interferometer together with a specific demultiplexing strategy to create what we call a Quantum Network Provider. We optimized our network by introducing the condition of uniquely connected. We adopted a wavelength-assignment strategy that avoids allowing a pair of users to share more than one entangled channel. Simply put, a given pair of signal and idler which are symmetrically distributed around the degeneracy should uniquely link two distinct users in the network defined by the QNP table. I will present our latest deployment of this scheme across four Slovak cities.

*Speaker

Quantum Networks for Research and Education

Garazi Muguruza Lasa*[1]

[1]SURF – Netherlands

Abstract

For whom are we building quantum networks and for what? While immersing ourselves in niche research problems often brings its own joy and rewards, taking a moment to zoom out allows us to understand the broader implications of our work. In this talk, I would like to share SURF's vision for a quantum internet as an infrastructure that supports both research and education, and discuss which technical, theoretical and social challenges we face along the way. I hope to create a space for all of us to reflect on the impact of our work on areas beyond academia.

*Speaker

Anonymous communication in quantum networks

Gláucia Murta*[1]

[1]TU Wien – Austria

Abstract

A fundamental cryptographic task is secure communication, in which two or more parties exchange confidential messages in the presence of an eavesdropper. In some scenarios, however, the identity of the communicating parties may also be sensitive information. In these situations, it is essential to ensure that the identities remain concealed throughout the protocol. In this talk, I will explore how quantum systems bring advantages to anonymous communication. I will then focus on the task of anonymously establishing a secret key among several users in a quantum network, introducing a security framework that encompasses both secrecy of the key and user anonymity. I will present efficient and noise-tolerant protocols that exploit the correlations of multipartite Greenberger–Horne–Zeilinger (GHZ) states, demonstrating clear advantages over approaches based on bipartite entanglement, and discuss a recent experiment showing that these multipartite advantages can already be observed with current technology. Finally, I will outline future directions and open challenges for quantum communication network protocols.

*Speaker

Computational Bell Inequalities

Ilya Merkulov*[1]

[1]Weizmann Institute of Science [Rehovot, Israël] – Israel

Abstract

We introduce a systematic approach for analyzing device-independent single-prover interactive protocols under computational assumptions. This is done by establishing an explicit correspondence with Bell inequalities and nonlocal games and constructing a computational space of correlations. We show how computational assumptions are converted to computational Bell inequalities, in their rigorous mathematical sense, a hyperplane that separates the sets of classical and quantum verifier-prover interactions. We reveal precisely how the nonsignaling assumption in standard device-independent setups interchanges with the computational challenge of learning a hidden input (that we define). We further utilize our fundamental results to study explicit protocols using the new perspective. We take advantage of modular tools for studying nonlocality, deriving tighter Tsirelson bounds for single-prover protocols and bounding the entropy generated in the interaction, improving on previous results. Our work thus establishes a modular approach to analyzing single-prover quantum certification protocols based on computational assumptions through the fundamental lens of Bell inequalities, removing many layers of technical overhead. The link that we draw between single-prover protocols and Bell inequalities goes far beyond the spread intuitive understanding or known results about ”compiled nonlocal games”; Notably, it captures the exact way in which the correspondence between computational assumptions and locality should be understood also in protocols based on, e.g., trapdoor claw-free functions (in which there is no clear underlying nonlocal game).

*Speaker

Measurement-Device-Independent Quantum Bit Commitment with Realistic Photon Sources

Juliette Van Mil*[1], Timothé Bramas , Kaushik Senthoor , and Stephanie Wehner[2]

[1]QuTech, Delft University of Technology (TU Delft) – Netherlands
[2]Delft University of Technology (TU Delft) – Netherlands

Abstract

Bit commitment is a fundamental primitive of secure two-party computation. While unconditional quantum security remains impossible without additional assumptions, the bounded-storage model offers a path forward by assuming limited adversarial quantum memory. Existing protocols in the bounded-storage models have addressed realistic photon sources. However, Measurement-Device-Independence (MDI), a powerful technique primarily focused on Quantum Key Distribution to eliminate vulnerabilities from untrusted devices, has never been applied to bit commitment.

In this regard, we present two distinct MDI-Randomised String Commitment (RSC) protocols designed for realistic photon sources. Our first protocol handles multiphoton emissions from weak coherent pulses using decoy-state techniques. We demonstrate that positive secure committed string rates are achievable in the bounded-storage model despite source imperfections. We then introduce a different phase-encoded MDI-RSC protocol employing coherent states, inspired by recent Twin-Field Quantum Key Distribution techniques. For this second protocol, we provide a security sketch in the bounded-storage model, opening a new direction for MDI bit commitment.

Our work takes initial steps toward experimental feasibility of quantum MDI bit commitment by addressing realistic source limitations, while highlighting open problems for future research.

*Speaker

Quantum Protocols for XOR and Rabin Oblivious Transfer

Lara Stroh*[1], Erika Andersson[1], Ittoop V. Puthoor[2], James T. Peat[1], Mats Kroneberg[1], Nikola Horová[3], Robert Stárek[3], Michal Mičuda[3], and Miloslav Dušek[3]

[1]Heriot-Watt University – United Kingdom
[2]Newcastle University – United Kingdom
[3]Palacky University – Czech Republic

Abstract

Oblivious transfer (OT) is a fundamental cryptographic primitive with applications in secure multiparty computation. We explore quantum implementations of two variants: XOR oblivious transfer (XOT) and Rabin oblivious transfer.
For 1-out-of-n XOT, we present a quantum protocol, analysing the cheating probabilities, and introduce a "reversed" protocol for 1-out-of-2 XOT where the receiver sends a quantum state to the sender while still implementing OT from sender to receiver. This is beneficial in scenarios where the parties have limited preparation/measurement capabilities and can be shown to not impact security. For Rabin OT, we present protocols using both pure and mixed quantum states, demonstrating that mixed states outperform pure states when analysing cheating probabilities.

*Speaker

Computational Monogamy of Entanglement and Quantum Key Distribution

Giulio Malavolta*[1]

[1]Giulio Malavolta – Italy

Abstract

The monogamy of entanglment is a fundamental principle in quantum mechanics. In this talk, we discuss generalizations of this notion through the lens of computational complexity and applications to round-optimal quantum key distribution.

*Speaker

Pioneering platform for integrated quantum memories with rare earth doped crystals

Margherita Mazzera*[1,2]

[1]Heriot-Watt University [Edinburgh] (HWU) – United Kingdom
[2]Scottish Universities Physics Alliance (SUPA) – United Kingdom

Abstract

The coherent interaction between photons and atoms underpins quantum information science and is essential for quantum networks. Solid-state systems, in particular rare-earth-doped crystals, are promising platforms for such interfaces. Additionally, waveguide-based quantum memories offer a path toward scalable, on-chip quantum photonic circuits. Our work uses type I femtosecond-laser-written waveguides in Pr:YSO, where we have demonstrated quantum-state storage, highly multimode operation, and entanglement storage in a fibre-integrated device. This platform offers guiding modes with diameter compatible with the core of telecom fibres, low insertion and bending losses, versatility of fabrication and unique 3D capability. However, achieving on-demand storage remains challenging, as the waveguide confinement increases vulnerability to photonic noise from the strong control pulses required for on-demand readout. We propose two routes to enable on-demand storage in waveguides. The first is implementing a gradient echo memory, exploiting electric-field control of the absorption profile; the compact geometry allows electrodes close to the waveguide for efficient, low-voltage tuning with minimal cross-talk. The second combines the atomic frequency comb protocol with off-resonant cascaded absorption, originally developed for ladder-type vapour memories. This hybrid approach could store broadband telecom photons while suppressing noise thanks to the large frequency separation between single-photon inputs and strong control pulses.

*Speaker

The space-time hardness of lattice problems

Martin Albrecht*[1]

[1]King's College London – United Kingdom

Abstract

To assume the non-existence of probabilistic polynomial time algorithms for certain hard problems, such as hard lattice problems, is the bread and butter of cryptography. For some applications, some authors also assume the non-existence of algorithms solving these problems in subexponential rather than polynomial time. In this talk, I want to talk about the class of algorithms that runs in single-exponential time but polynomial memory. The non-existence of such algorithms has been conjectured by Lombardi and Vaikuntanathan (CRYPTO'20) and is backed by extensive effort by cryptanalysts. In this talk I will then also show a perhaps surprising connection of this conjecture to the hardness of hinted lattice problems. Roughly, this hinted lattice problem states that the Inhomogeneous Short Integer Solutions (ISIS) problem is still hard given a short trapdoor for the same matrix, as long as the norm bound required of the ISIS solution is only marginally longer than the norm of the trapdoor. This suggests that the space-time hardness of lattice problems is a promising foundation for some advanced cryptographic primitives that have recently been proposed but, so far, are based on ad-hoc lattice assumptions with hints.

Based on joint work with Russell W. F. Lai and Eamonn Postlethwaite.

*Speaker

Experimental Progress Towards Scalable Quantum Network

Qiang Zhang*[1]

[1]University of Science and Technology of China – China

Abstract

Quantum communication can provide secure and efficient information transmission guaranteed by the basic principle of quantum physics. Here, I shall focus on recent experimental progress in quantum key distribution and quantum repeater, including twin-field quantum key distribution over 1000 km fiber network, memory-memory entanglement establishment and device independent quantum key distribution over 100 km fiber.

*Speaker

Implementation Security of TF-QKD: Fast Intensity Modulation of the Reference Light Attack and Countermeasures

Alessandro Marcomini*[1,2], Sergio Juarez[3], Mikhail Petrov[2], Robert I. Woodward[3], Toby J. Dowling[3], R. Mark Stevenson[3], Marcos Curty[2], and Davide Rusca[2]

[1]Vigo Quantum Communication Center (VQCC) – Spain
[2]University of Vigo [Pontevedra] – Spain
[3]Toshiba Research Europe Ltd – United Kingdom

Abstract

Twin-field quantum key distribution (TF-QKD) promises to extend secure key exchange over lossy channels by leveraging single-photon interference, doubling point-to-point distances with respect to conventional protocols. Practical implementations most often rely on optical injection locking (OIL), where independent lasers at remote parties (Alice and Bob) are synchronized in phase and frequency via an external reference beam. While the reference injection is essential for high-visibility interference at a central node, it opens potential side channels which, if unaccounted for, threat to undermine the performance and the security of the key.

In this work we show that rapid intensity modulation of the reference beam can induce intensity oscillations in the OIL-locked laser, enhancing the amplitude of the emitted QKD pulses by more than 50% while completely evading conventional monitoring techniques. We discuss the impact of this attack on performance and provide technical requirements of novel countermeasures to completely mitigate this threat. Furthermore, we experimentally validate these countermeasures on a lab TF-QKD setup mimicking deployed networks.

Our findings highlight the need for comprehensive reference-channel surveillance in OIL-TF-QKD, providing deployable defenses for real-world quantum networks.

*Speaker

A Practical Protocol for Quantum Oblivious Transfer from One-Way Functions

Álvaro Yángüez*[1], Eleni Diamanti , Alex Grilo , Adriano Innocenzi , Verena Yacoub , and Pascal Lefebvre

[1]Information Quantique [LIP6] – Sorbonne Université, CNRS, LIP6 – France

Abstract

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 simulation security for QOT through an equivocal and relaxed-extractable quantum bit commitment.

*Speaker

Provable decryption failure security for practical lattice-based PKE

Fabrizio Sisinni*[1] and Christian Majenz[2]

[1]Technical University of Denmark (DTU) – Denmark
[2]Technical University of Denmark (DTU) – Denmark

Abstract

Recently, Hövelmanns, Hülsing, and Majenz introduced a security notion called Find Failing Plaintext – Non Generic (FFP-NG), which captures the ability of an adversary to find decryption failures by making non-trivial use of the public key. A first analysis of this property for lattice-based schemes was presented by Majenz and Sisinni, who showed that the Learning With Errors (LWE) problem reduces to breaking the FFP-NG security of the PVW scheme with discrete Gaussian noise. In this work, we generalize their result by analysing the FFP-NG security of widely used schemes based on Ring-LWE and Module-LWE. To keep our analysis as general as possible, we consider a family of subgaussian distributions that includes, among others, discrete Gaussians and centered binomials.

*Speaker

Query bounds are inherent for the security of memory-hard functions

Gina Muuss*[1,2]

[1]QuSoft – Netherlands
[2]Universiteit van Amsterdam (UvA) – Netherlands

Abstract

Memory-hard functions (MHFs) and Proofs of Space (PoS) are important cryptographic building blocks, used for example in password hashing and blockchains. In the random-oracle model, the memory complexity of MHFs can be lower-bound, however, these bounds also contain a term involving the amount of queries an attacker makes. It was previously unclear whether this term is fundamentally necessary or just an artifact of the proof technique. Recent advances in complexity theory culminated in an algorithm by Cook and Mertz which uses less space than expected for a similar problem. Concretely, by applying the Cook–Mertz algorithm to the MHF constructions, we show that the query term in earlier security proofs is unavoidable, and not just an artifact of the proof techniques.

*Speaker

Rethinking Quantum Repeaters: Balancing Scalability, Feasibility, and Interoperability

Javier Rey Domínguez*[1] and Mohsen Razavi[1]

[1]University of Leeds – United Kingdom

Abstract

In the past few years, many quantum repeater protocols have been proposed to enable quantum communications at long distances. However, most proposals focus only on specific aspects of the protocol's practicality. In this presentation, we present our recently proposed strategy for entanglement distribution, which aims to be a scalable and feasible solution that remains easy to integrate with current infrastructure. The strategy relies on the sequential distribution of entanglement with error detection at each repeater node. We analyse the performance of a QKD system using our solution in a two-user, repeater chain setup. We show that our strategy enables distribution of secret key within Europe ($>$ 1000km) when considering a realistic topology of the underlying network and soon-to-be-available hardware. What is more, we approximate the effective cost of the repeater chain when using our solution versus parallel distribution strategies, and find that the sequential approach could lead to more effective resource utilization in many-user quantum networks.

*Speaker

A simple clock synchronization algorithm for time-bin quantum key distribution

Loïc Millet*[1,2], Rob Thew[2], Boris Korzh[2], and Gianluca Boso[1]

[1]ID Quantique, CH-1227 Genève, Switzerland – Switzerland

[2]Department of Applied Physics, University of Geneva, CH-1211 Genève, Switzerland – Switzerland

Abstract

We present a simple clock synchronization algorithm for time-bin BB84 QKD that compensates frequency mismatches and time-offset fluctuations directly from detection timestamps. It requires no dedicated channel or auxiliary qubits and works in low-photon-count regimes with standard hardware. We validate it with successful key exchange in a deployed QKD network using commercial systems.

*Speaker

Algorithms for the Underdetermined MQ problem

Massimo Ostuzzi*[1]

[1]Ruhr University Bochum = Ruhr-Universität Bochum [Bochum] (RUB) – Germany

Abstract

In this talk, I will present Just Guess, an algorithm that takes full advantage of quantum computations to solve the underdetermined MQ problem. Research on such algorithms is motivated by the signature schemes MAYO and QR-UOV, which in fact base their security on the computational hardness of this variant of the MQ problem.

*Speaker

GHz-rate polarization-based QKD system for fiber and satellite applications

Matias Bolaños*[1], Edoardo Rossi[1], Federico Berra[1], Alberto De Toni[1], Ilektra Karakosta-Amarantidou[1], Daniel Lawo[1], Costantino Agnesi[2], Marco Avesani[3], Francesco Vedovato[2], Andrea Stanco[3], Paolo Villoresi[4], and Giuseppe Vallone[4]

[1]University of Padova, Department of Information Engineering (DEI) – Italy
[2]University of Padova, Department of Information Engineering (DEI) – Italy
[3]University of Padova, Department of Information Engineering (DEI) – Italy
[4]University of Padova, Department of Information Engineering (DEI) – Italy

Abstract

Quantum key distribution (QKD) leverages the principles of quantum mechanics to exchange a secret key between two parties.
Despite its promising features, QKD also faces several practical challenges such as transmission loss, noise in quantum channels and finite key size effects. Addressing these issues is crucial for the large-scale deployment of QKD in fiber and satellite networks. We present a 1550 nm QKD system realizing the efficient-BB84 protocol and based on the iPOGNAC scheme. The system achieved repetition rates up to 1.5 GHz and showed an intrinsic QBER of _˜0.4%. The system was first tested on a laboratory fiber link and then on an intermodal link in the field, consisting of both deployed fiber and a 620 m free-space channel. The experiment was performed in daylight conditions, exploiting the Qubit4Sync synchronization protocol. With this trial, we achieved a new benchmark for free-space BB84 QKD systems by generating a sustained secret key rate above 1 Mb/s for 1 hour. Finally, exploiting a recently discovered finite-size bound, we achieved a secure key rate of about 10 Mb/s at low losses (5 dB), and around 6.5 kb/s in the high-loss (38.5 dB), low block length (N=10ˆ4) regime. The latter results demonstrate the system's suitability for highly lossy and time-constrained scenarios such as QKD from low Earth orbit satellites.

*Speaker

Implementation Security of TF-QKD: Trojan-Wavelength In the Reference Light Attacks and Countermeasures

Sergio Juarez*[1], Alessandro Marcomini[2], Mikhail Petrov[2], Robert I. Woodward[1], Toby J. Dowling[1], R. Mark Stevenson[1], Marcos Curty[2], and Davide Rusca[2]

[1]Toshiba Research Europe Ltd – United Kingdom
[2]University of Vigo [Pontevedra] – Spain

Abstract

Twin-Field Quantum Key Distribution (TF-QKD) has emerged as a leading candidate for long-distance quantum communications, overcoming the repeaterless rate-distance limit. Practical implementations commonly rely on Optical Injection Locking (OIL) to establish frequency and phase coherence between distant transmitters via an untrusted reference beam distributed through a service channel. However, this architecture introduces a potential pathway to attacks that cannot be fully closed without defeating its purpose, creating potential vulnerabilities that must be carefully addressed.

We present the Trojan-Wavelength In the Reference Light (TWIRL) attack, which exploits the wavelength-dependent response of monitoring devices and encoder components. By injecting high-power optical signals at wavelengths beyond the detection range of standard InGaAs photodetectors an eavesdropper could potentially extract complete information about encoding settings. Our experimental characterization of DFB laser cavities reveals substantial reflectivity in the 1600-1700 nm range, precisely where conventional watchdogs become ineffective.

We demonstrate that this vulnerability can be effectively neutralized through straightforward spectral filtering using commercially available narrowband filters. Cascading multiple units provides the required out-of-band suppression with minimal impact on system efficiency.

*Speaker

GHz-Rate Phase-Randomized Time-Bin QKD Source Based on a SLED Platform

Shashank Kumar*[1], Alessandro Marcomini[2], Loïc Millet[1,3], Towsif Taher[1], Raphael Houlmann[1], David Cabrerizo[1], Gianluca Boso[3], Robert Thew[1], and Boris Korzh[1]

[1]Department of Applied Physics, University of Geneva – Switzerland

[2]University of Vigo – Spain

[3]ID Quantique, CH-1227 Genève, Switzerland – Switzerland

Abstract

Phase randomization is essential for the security of practical quantum key distribution (QKD) systems and is commonly achieved using gain-switched semiconductor lasers. We present a 1.25 GHz phase-randomized QKD source based on a super luminescent diode (SLED) operating in the C-band as a compact and cost-effective alternative. The source generates ˜100 ps optical pulses with 400 ps time-bin separation, compatible with high-speed time-bin encoding. Interferometric measurements demonstrate > 99% visibility between adjacent time bins, confirming strong first-order coherence within a qubit, while the spontaneous-emission-driven nature of the SLED ensures intrinsic qubit-to-qubit phase randomization. The broadband architecture further enables operation across multiple ITU channels, supporting wavelength-multiplexed QKD from a single emitter. This work establishes a scalable SLED-based platform for high-speed time-bin QKD systems.

*Speaker

Quantum-Secure Classical Protocols: Reprogramming Permutations for Tight(er) Proofs

Silvia Ritsch*[1], Yu-Hsuan Huang , Andreas Huelsing , Varun Maram , and Abishanka Saha

[1]Eindhoven University of Technology – Netherlands

Abstract

Classical cryptographic protocols such as those for key exchange and messaging traditionally rely on idealized models of random permutations and functions to establish security. With the advent of quantum adversaries, there is a pressing need to extend these proofs to the quantum setting. While the Quantum Random Oracle Model (QROM) offers robust tools for analyzing functions, Programmable Quantum Random Permutations (QRPMs) present unique challenges and opportunities.

In this talk, we demonstrate how the Feistel construction and measure-reprogramming enable us to simulate and reprogram permutations in response to adversarial queries. This reprogrammable approach facilitates (tighter) security proofs for classical protocols facing quantum adversaries. We explain the mechanics of reprogramming and its critical role in advancing the analysis of quantum-secure classical cryptography.

*Speaker

Concentration bounds and satellite QKD

Vaisakh Mannalath*[1]

[1]Vigo Quantum Communciation Centre (VQCC) – Spain

Abstract

Talk on the recent developments in sharp finite statistics in QKD and its application to satellite communication.

*Speaker