RESEARCH CENTRE

Inria Saclay Centre at Institut Polytechnique de Paris

IN PARTNERSHIP WITH:

Institut Polytechnique de Paris

2024 ACTIVITY REPORT

Project-Team QURIOSITY

Quantum Information Processing and Communication

IN COLLABORATION WITH: Laboratoire Traitement et Communication de l'Information

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Inria

Contents

Project-Team QURIOSITY

Creation of the Project-Team: 2023 January 01

Keywords

Computer sciences and digital sciences

A3.4. – Machine learning and statistics

A4.2. – Correcting codes

A4.3. – Cryptography

A4.3.4. – Quantum Cryptography

A4.6. – Authentication

A5.9. – Signal processing

A6.1.2. – Stochastic Modeling

A6.5. – Mathematical modeling for physical sciences

A7.1. – Algorithms

A7.1.4. – Quantum algorithms

Other research topics and application domains

B5.11. – Quantum systems

B6.2. – Network technologies

B9.1. – Education

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientist

- Cambyse Rouze [INRIA, ISFP]

Faculty Members

- Romain Alléaume [Team leader, TELECOM PARIS, Professor, HDR]
- Peter Brown [TELECOM PARIS, Associate Professor]
- Augustin Vanrietvelde [TELECOM PARIS, Associate Professor]

Post-Doctoral Fellow

- Shivang Srivastava [Telecom Paris, from Nov 2024]

PhD Students

- Guilhem Doat [Telecom Paris, from Sep 2024]
- Jan Kochanowski [IP PARIS]
- Tristan Nemoz [Telecom Paris]
- Thomas Pousset [Telecom Paris]
- Guillaume Ricard [Telecom Paris]

Interns and Apprentices

- Ali Almasi [Telecom Paris, from Mar 2024 until Aug 2024]
- Błażej Kuzaka [Telecom Paris]

Administrative Assistant

- Natalia Alves [INRIA]

External Collaborators

- Mateus Araújo [Universidad de Valladolid]
- Roger Colbeck [University of York]
- Omar Fawzi [INRIA]
- Sylvain Gigan [ENS - Sorbonne University]
- Alejandro Pozas-Kerstjens [University of Geneva]
- Ernest Tan [University of Waterloo]
- Armin Tavakoli [Lund University]

2 Overall objectives

QURIOSITY's ambition is to extend the application horizon of quantum information science by addressing novel questions positioned at the intersection between theoretical research in quantum information and the engineering of quantum devices, with a focus on approaches combining digital and quantum photonics technologies.
The overarching goal of the project-team will be to push forward our ability to harness and exploit high-dimensional complex quantum systems for quantum information processing and quantum communications purposes.

Leveraging a dual approach combining fundamental research in quantum information with quantum photonics expertise, QURIOSITY will strive to take advantage of and develop strong synergies with the unique quantum ecosystem of Saclay and to pursue objectives that have the potential to bring radical advances to several application domains of quantum technologies, ranging from cryptography to computing:

- Design quantum-enhanced cryptographic hardware, leveraging concepts based on computational hardness and quantum information.
- Conceive and engineer photonic-based processors and systems capable of achieving quantum advantage in computation or communication tasks.
- Develop efficient quantum information processing schemes implementable on near-term hardware and advance the theoretical framework to understand the fundamental limits of noisy quantum information processing.

3 Research program

The research program that we aim to lead in the QURIOSITY project-team intends to embrace a relatively wide area of theoretical questions, ranging from quantum cryptography, that we ambition to combine with complexity-based schemes and establish as a framework to enhance hardware security, to the mathematical foundations of quantum information and quantum computing. Conversely, we also intend to develop research capable of leveraging photonics and digital information processing technologies to design systems capable of producing high-dimensional and controllable quantum states of light in order to push forward the frontiers of quantum information processing advantage.

3.1 Research axis 1: Quantum cryptography complexity and hardware frontiers

This axis aims to identify and solve frontier research topics in quantum cryptography, from two main perspectives. First by exploring the interplay between security models - including computational ones - and theoretical quantum cryptography, allowing to build protocols with stronger security properties and lesser resource requirements. Second by laying a special emphasis on interplay between quantum cryptography and hardware security, with the need to develop extended techniques for quantum cryptographic hardware security certification, but also the idea to strengthen hardware security and its resilience to information leakage by resorting to quantum cryptographic constructions.

3.1.1 Everlasting security from a quantum-computational hybrid model

We proposed in 2015 a security model that we later coined a *Quantum Computational Timelock* (QCT) security model. It consists in assuming that computationally secure encryption may only be broken after time much longer than the coherence time of quantum memories available at the time of protocol execution. The QCT security model opens the possibility to propose new quantum cryptographic constructions and in particular to make use of encoding and security proof

techniques that strongly depart from "traditional" quantum conjugate coding that is a central ingredient in most quantum cryptographic protocols.

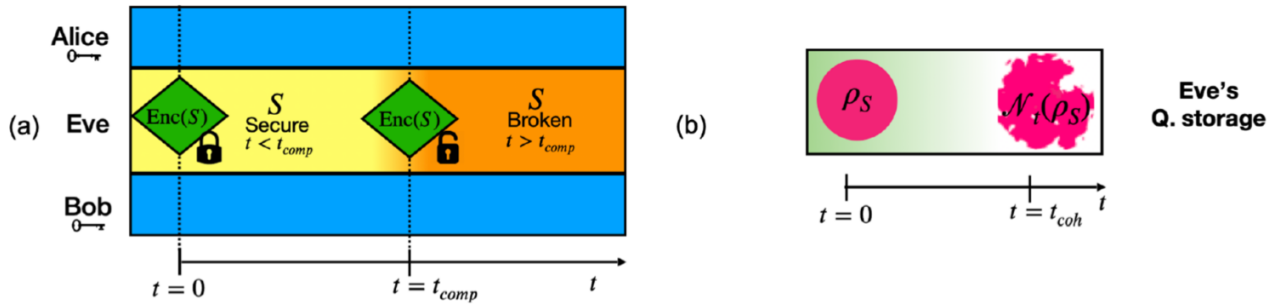

Figure 1: QCT security model: Assumption (a): Short-term secure encryption during time t_{comp}, during which Alice and Bob can exchange an ephemeral classical secret S. Assumption (b): Time-limited quantum memory, with coherence time $t_{coh} \ll t_{comp}$.

The QCT security model opens towards a rich variety of fascinating questions, that we have certainly not all identified. In the coming years we intend to push forward the theoretical analysis of several of these questions, that relate to the computational frontiers of quantum cryptography. One ongoing direction consists in studying key agreement constructions whose security can be reduced to distributed computational problems that exhibit an exponential separation in terms of quantum or classical communication complexity.

As an alternative way to build secure protocols in the QCT model, we also intend to investigate *pseudo-random quantum states*, which can be seen as a computational variant of a t-design, i.e. an ensemble of quantum states characterized by the fact that t copies of one sampled state are statistically indistinguishable from t copies of a states picked uniformly at random. Interestingly, construction of pseudo-random states can be based on quantum-secure one-way functions, and therefore from the first assumption. This line of work will also allow us to consider realistic and pratical constructions of quantum cryptographic schemes based on computational and /or quantum-hardware security assumptions. We also intend to study constructions for quantum physically uncloneable functions qPUFs and their aplication.

3.1.2 Device-independent cryptography

Device-independent cryptography allows one to perform quantum cryptography with reduced or even no trust assumptions on the quantum hardware. It remains a challenge experimentally and pushing the performance (in terms of key rate, or trust reduction) of device-independent cryptography defines an active research frontier for quatum cryptography. Recent implementations of DI-QKD[1] [50, 62, 62] have shown that whilst it is now feasible, it has a relatively low rate and can only be executed over a short distance. By improving the theoretical methods for analyzing various protocols and security proofs and by improving the protocol design we can look to boost the rates of these protocols and push them towards a more viable technology. Examples of such improvements include protocol design modifications [57, 39] and improved methods to calculate rates [27, 28], [56]. Our goals are to develop better designed protocols and security proofs (assessing their performance in experiments) and to investigate the fundamental limitations of DI protocol rates Overall pushing the practicality of DI forwards and improving our understanding of its limitations.

As a complementary line of research we will also investigate prospects of semi-device-independent protocols as a viable near-term alternative to device-independent security. Proposed protocols rely on assumptions of system energy [55], dimension bounds and bounded distrust [58] amongst

[1] DI-QKD stand for Device-Independent Quantum Key Distribution

others. We will investigate alternative assumptions and derive resulting protocols to be analyzed and subsequently implemented. We will also apply the semi-device-independent framework to the problem of hardware verification, designing tests to establish that the hardware is functioning correctly whilst placing limited trust on the components.

3.1.3 Quantum-enhanced leakage-resilience

We will also investigate some questions placed at the intersection between classical hardware security and quantum cryptography, namely how to prove the security of a cryptographic protocols when implemented using hardware, such as processors or storage, that may leak some of the security-sensitive information.

We intend to tackle leakage-resilience cryptography from a new viewpoint, that will consist in integrating quantum cryptographic constructions as a base layer within cryptographic systems, in order to obtain security guarantees even in presence of information leakage with strictly weaker assumptions than existing classical leakage-resilience protocols. We will first consider simple cryptographic protocols such as One-Time-Pad encryption or authentication protocols relying on Physically Uncloneable Functions PUFs. We intend for example to investigate how the use of hybrid classical-quantum cryptographic hardware, comprising quantum channels to interconnect processors or secure storage sites, can lead to cryptographic protocols with provable security under some realistic information leakage models.

3.1.4 Real-world quantum cryptography

40 year of quantum cryptography (QC) have lead to major theoretical and technological advances, with fundamental impact on the field of information security. Market adoption however remains limited, with major challenges that practical QC still needs to be overcome in order to become widely used in real-world applications. We identify in particular two main challenges: 1) cryptographic advantage, namely the design of protocols for which the use of QC in combination with classical cryptography gives a competitive edge over classical cryptography only; 2) security certification of quantum cryptographic implementations. QURIOSITY intends to actively contribute to lift these barriers and to foster the development of real-world quantum cryptography and in particular to the uptake of a French and European industry. The development of a QC industry is indeed becoming an important topic, with strategic investments from leading scientific countries (China, Korea, Japan, UK, etc.) including also notably the EU27 supporthing the EuroQCI initiative. On the other hand, the adoption of quantum cryptography for real-world application remains often considered with skepticism by representatives of the cybersecurity community, stressing the dire need of cross-disciplinary vision combining best-in-class classical and quantum cryptography expertise.

Regarding cryptographic advantage, our conviction is that one should not aim at constructions where quantum cryptography would just functionally replace classical cryptography, but on the other hand to identify applications where the use of QC combined with post-quantum cryptography (PQC) can present strict security gain over PQC alone.

Regarding security certification, it has become a central challenge in particular in the context of the EuroQCI initiative aiming at developing a pan-European quantum communication infrastructure, together with an industry, in the next 10 years It constitutes a complex task, requiring the collaboration of experts from different fields. In future years, we intend to tackle this question from different angles: on the theory side, we intend to propose a shift in the security objective towards everlasting security, and demonstrate how this can make the security certification of key establishment based on QKD combined with ephemeral post-quantum cryptography primitives much more tractable. On the system engineering side and in resonance with Section 3.2, we intend to identify and close implementation security gaps in modern CV-QKD systems relying on digital signal processing, notably the complex interplay between calibration procedure and finite-size security, but also between Nyquist pulse shaping and leakage.

3.2 Research axis 2: Multimode photonic systems for quantum information processing and communications

Building a quantum processor that we could use to solve real-world problems with practical benefits might constitute one of the most burning scientific and technological challenges of the beginning of the 21st century. Very interestingly, recent results indicate that quantum optical circuits constitute a very promising approach for quantum information processing, in particularly high-dimensional linear optics systems, which can form a (weaker) non-universal quantum computing platform, and yet efficiently perform tasks intractable for a classical computer, such as Boson Sampling [16].

We will actively investigate new theoretical questions related to quantum information processing with high-dimensional photonic system, and their interplay with technology and experiments.

3.2.1 Quantum coherent communications and digital signal processing

Quantum Key Distribution (QKD) systems are among the most advanced quantum communications technologies available today. QKD therefore provides an ideal platform to test novel system designs and validate quantum communication technology over real networks Leveraging essential features of modern optical communication systems, and in particular high sampling rates and digital signal processing [43], quantum coherent communications systems constitute a recent and promising route towards high-rates, highly integrated and cost-effective quantum communication systems. They rely on two central ingredients: -Spectrally efficient modulation formats and coherent detection, exploiting phase and intensity information and able to operate a very high rates (> GHz) even with shot-noise limited receivers. - Digital signal processing that takes advantage of the high sampling rates to digitally evaluate and compensate many impairments of the communications such as optical carrier phase noise or polarization mode dispersion, using dedicated algorithms.

In collaboration with Prof. Yves Jaouen from the GTO team of Telecom Paris,and working on a state-of-the-art experimental platform, QURIOSITY has designed and demonstrated for the first time DSP-enhanced quantum communications, with noise control performances that allow to successfully run QKD over metropolitan distances while being jointly deployed over classical coherent optical link [20]. We have also filed a patent about this general concept and our inventive system design.

In the future, we then aim to leverage digital signal processing and machine learning (ML) techniques to characterize and mitigate noise in order to push further our ability to operate quantum communications over existing optical fibers, in coexistence with classical signals.

As a complementary line of research, we intend to theoretically study multimode quantum coherent communications using multimode shaping of the local oscillator, taking inspiration from [29]. We also intend to explore the possibility to rely on CV multimode encoding as a way to experimentally implement new quantum cryptographic constructions in the hybrid quantum computational security models introduced in Section 3.1.

3.2.2 Quantum information processing with a programmable frequency processor

In collaboration with the teams of Nadia Belabas and Pascale Senellart at C2N and in the context of the ParisQCI project, we study how to combine high-dimensional photonic gates in the frequency domain, to efficiently synthesize high-dimensional unitary transformations. Leveraging on the possibility to parallelize single-qubit unitaries, that we have recently analyzed [40] we intend to study how such systems could be leveraged for optical quantum information processing, and in particular for quantum metrology. In the future, we will also investigate how to scale the platform to perform information processing with high-dimensional quantum states, opening the possibility to achieve quantum computational advantage, but also implementation routes for the hybrid quantum-computational cryptographic protocols in the QCT model, studied in Section 3.1

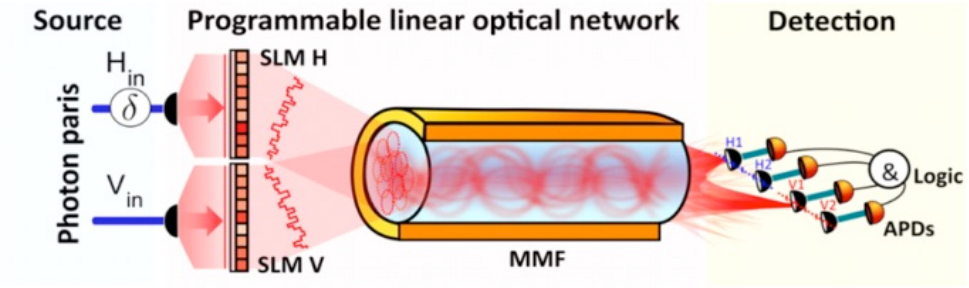

Figure 2: Multimode programmable linear optical circuit and associated experimental devices (Spatial Light Modulators: SLM, Multimode fibers: MMF, Detection of single photons multipixel APDs). This experimental platform, implemented, at the international state of the art in the team of Sylvain Gigan, at LKB, allows to create, in a programmable way, an arbitrary unitary transformation on quantum states of light, in high dimension. (Credit: Complex Quantum Optics team, LKB, ENS Paris).

3.2.3 Quantum information processing using multimode programmable linear circuits

In collaboration with the team of Sylvain Gigan at ENS Ulm, and in the context of Francesco Mazzoncini's PhD that we co-supervise, we aim to use a multimode programmable linear circuit, built around a multimode fiber (cf. Figure 2) to perform some fundamental tests and demonstrations of quantum communication advantage, related to fundamental problems such as the Vector in a Subspace [51].

The prospects of this work are very promising: first they could lead to the first experimental demonstration of a exponential communication complexity gap between one-way quantum communication and two-way classical communications and may also open towards the possibility for experimentally robust Bell inequality violations [46], with applications for quantum cryptography and also in quantum computing.

3.3 Research axis 3: Mathematical foundations of quantum information

Quantum information and computation are built upon the mathematical frameworks of functional analysis and information theory. Developing our understanding of the mathematical underpinnings of these theories can in turn lead to new insights and applications. At QURIOSITY, one of our aims is to explore quantum information theory through the lens of the underlying mathematics. In a nutshell, we will parallelly develop new analytic and numerical tools for the study of quantum entropic quantities and complex quantum systems made of spin or bosonic degrees of freedom. We will in turn consider these systems to design new, physically motivated models of noise-robust quantum computing.

3.3.1 Convex relaxations of quantum optimization problems

Convex optimization concerns the optimization of convex functions over convex sets. This family of optimization problems has several particularly nice properties, including the guarantee of global optima, which makes them particularly appealing from both the perspective of the mathematics and the applications. They are widely applicable to many domains of science but in particular they arise rather naturally in the context of quantum theory as many of the relevant objects (states, channels and measurements) form convex sets.

We will aim to develop and apply techniques in convex optimization theory to problems within quantum information and quantum computing. Recent examples of our work in this area include [27, 28] where we developed semidefinite programming relaxations for entropic optimization problems relevant to device independent cryptography. Continuing this line of research we aim to extend these techniques to other entropic quantities beyond the relative entropy, for instance to the Petz and sandwiched families of Rényi divergences. We also have the ambitious goal of understanding and characterizing what classes of functions, relevant in the context of

quantum theory, are amenable to such semidefinite programming approximations. In other words, what optimization problems in quantum information theory and quantum computing can we approximate?

A well-known example concerns strengthenings of the monotonicity of the relative entropy under the action of a quantum channel or a Markovian evolution known as strong data processing and modified logarithmic Sobolev inequalities. These fundamental inequalities are known to be hard to prove analytically, even for simple random walks on n-cycles, and convex relaxation techniques were recently successfully used to approximate them [36]. We are currently collaborating with Omar Fawzi and Daniel Stilck França from QINFO to adapt these numerical tools to the quantum realm. In the future, we will consider extending these tools to the infinite dimensional bosonic setting in order to approach long-standing conjectures such as the entropy photon number inequality [38]. This research direction will complement analytic approaches presented in Section 3.3.2.

3.3.2 Fundamental properties of entropies

Entropies are fundamental quantities in quantum information theory, obtaining operational meanings in terms of rates of various tasks [35]. By improving our understanding of these quantities, we can in turn gain new insights into the various applications in which they appear.

For example, new chain rules for Rényi entropies [34] led to a versatile framework for cryptographic security proofs [19]. The result, known as the entropy accumulation theorem, effectively gives sufficient conditions under which the entropy of a large system can be accurately described by the entropy of its individual systems. At QURIOSITY we aim to understand under which conditions does entropy accumulate in this manner? By understanding the minimal requirements for entropy to accumulate we can understand the minimal requirements under which a randomness based cryptographic protocol functions securely. Moreover, we aim to investigate the connection between the entropy accumulation theorem and the related works of the quantum probability estimation framework [63]. This is an alternative method to break large entropies down into smaller quantities and reports several advantages over the entropy accumulation theorem. Understanding how advantages from one technique can be transferred to the other will lead to much stronger theoretical results and would have immediate applications to improve security proofs and rates of cryptographic protocols, leading to more practical technologies.

Other types of decompositions of entropic quantities of interacting complex systems into smaller components involving marginals over subsystems include generalizations of the famous strong subadditivity of the relative entropy known as approximate tensor-stability of the relative entropy. These are at the core of most successful methods for finding the speed of convergence of Gibbs sampling algorithms based on the modified logarithmic Sobolev inequality. In previous work, we successfully extended these notions to the quantum realm [37] and applied them to problems in network quantum information theory [24, 32] and open complex quantum systems [30, 21]. Extensions and refinements of these concepts will lead to new breakthroughs in both fields (see Sections 3.3.3 and 3.3.4).

3.3.3 Complexity and entanglement properties of quantum Gibbs states

A complexity theoretical definition of the quantum phase of a state ψ consists in taking the vicinity of states which are reachable from ψ after applying a local evolution during a short period of time. A topologically ordered phase has the property that the time required to reach it starting from a trivial (i.e. product) state scales extensively with the system size. In other words, topological order can be described in terms of circuit depth lower bounds. The classification of quantum phases of matter is by now a very well-established field with far-reaching applications e.g. to the construction of good quantum error-correcting codes exploiting the properties of topologically ordered phases. However, a more realistic description of a quantum mechanical system is in terms of a finite temperature Gibbs state describing its thermal equilibrium with a large environment. Despite their practical relevance, until recently Gibbs states were primarily studied by mathematical physicists, and many fundamental questions regarding their use in quantum information processing remain

open. We propose to investigate the complexity of quantum Gibbs states through the scope of their finite temperature phase transitions. Additionally to its fundamental value, this research direction will undoubtedly lead to several important practical applications, as described in section 3.3.4.

In the setting of classical Gibbs measures, analogous questions have been intensively studied from the perspective of Markov chain Monte Carlo algorithms (MCMC). On regular lattices, the analysis of the speed of convergence of MCMC for lattice spin systems is by now well-understood through the study of correlations at equilibrium. The generalization to general interaction graphs is still a very active field of research in theoretical computer science, probability theory and mathematical physics [31]. The problem becomes even harder in the quantum regime, where purely quantum mechanical effects, e.g. long-range entanglement, may cause the quantum Markov chain to slow down in an unpredicted manner. For the important case of commuting interactions, which include most hitherto studied Hamiltonians for the purpose of quantum error-correction, and for physical dynamics generated by the weak coupling of the system with a large environment (Davies dynamics), general results were obtained through spectral methods. However the latter are not powerful enough to distinguish evolutions generating topologically ordered states from rapidly mixing ones. Instead, more involved techniques, e.g. entropic inequalities, are needed. In [23, 30, 22, 21], we were able to prove rapid mixing by extending one of the most successful classical approaches to prove rapid mixing based on the modified logarithmic Sobolev inequality and the approximate tensor-stability of the relative entropy (cf Section 3.3.2). Extending this novel powerful approach, we plan to conduct a systematic joint study of mixing times and thermal stability of topological quantum order in low lattice dimensions. We will conduct this research in collaboration with Daniel Stilck França from QINFO with whom we co-authored [30]. We also see a clear connection with the research focus of Daniel Malz who was recently recruited as a junior professor at Inria Saclay, the mathematical and theoretical condensed matter physicists at CPhT, as well as the team PEIPS at CMAP (X).

3.3.4 Mathematical analysis of quantum memories

In parallel to the previous research plan, we will conduct a mathematical analysis on the storage of quantum information and the concept of self-correction in complex quantum systems. Early work on the storage time of candidates of self-correcting quantum memories relied on the connection to the energy barrier of the system, that is the energy the system must reach for a logical error to occur, via an empirical principle called the Arrhenius law. More recently, the energy barrier was rigorously related to spectral properties of the evolution, whereas some no-go theorems showed the impossibility of an exact mathematical formulation of the Arrhenius law. Here instead, we plan to relate the memory lifetime of a device directly to properties of its thermal equilibrium state. We currently work on this research direction in the setting of lattice spin systems with Anthony Leverrier and Ivan Bardet from the team COSMIQ through the development of spectral methods, and plan to extend our framework to lattices with bosonic degrees of freedom in the near future. We also plan to initiate a dialogue with Jean-René Chazottes from CPhT (X) on refinements of our techniques using concentration and entropic inequalities which already proved their usefulness in the study of hitting times of classical Markov chains and their metastability. One of our long–term goals is to find systems with thermally stable entanglement, both stable against thermal fluctuations and robust against local perturbations. Such a theoretical result would be of very high practical interest since experimental implementations are inevitably subject to noise and errors.

3.3.5 Tomography of complex quantum systems

As the size of quantum devices continues to increase beyond what can be easily simulated classically, new challenges have appeared concerning the robust and efficient characterization of their states. This often necessitates the preparation and destructive measurement of exponentially many copies of the quantum system, as well as the storage of measurement outcomes in a classical memory. Recently, new methods of tomography have been proposed which precisely leverage this important simplification to develop efficient state learning algorithms. One highly relevant development in this direction is that of classical shadows [41, 42]. In we propose a better

solution by combining classical shadows with new insights from the emerging field of quantum optimal transport. Our current first step only applies to topologically trivial quantum states such as high-temperature Gibbs states or outputs of shallow quantum circuits, and more effort is needed to adapt and generalize our algorithm to non-trivial phases. We envision three new major contributions: First, we will develop constrained versions of concentration inequalities in order to develop efficient tomography algorithms of complex quantum states, assuming the prior knowledge of their phase. This line of research is original even in the classical setting where works on constrained entropic inequalities only very recently appeared in the literature. The expertise of Jean-René Chazottes from CPhT (X) will prove crucial to the success of this project. Second, we will extend the framework of shadow tomography to CV quantum systems. The main difficulties here are two-fold: first, CV systems are infinite-dimensional in nature, and hence some physical constraints need to be imposed on the states that one can hope to learn, such as their energy. Moreover, the set of measurements (homodyne/heterodyne) available in photonic experiments further limits the type of observables that one can hope to predict. In order to ensure the wide applicability of the method and test the resulting algorithm, we will rely on the already established interactions of IQA with the groups of experimentalists at IP Paris and Saclay, and initiate a fruitful dialogue with start-up like Quandela and Pasqal. In the future, we will use these methods to devise hardware-oriented noise-learning algorithms for many-body systems. For this, we plan to get in touch with the experts on statistical learning among IP Paris, and in particular at LIX.

3.3.6 Formal tools for higher-order quantum computation

The theoretical study of quantum computation and its advantages has, in the past decade, opened to a new perspective: *higher-order* quantum computation, i.e. the way in which one can transform black-box quantum gates by inserting them into computation architectures. This is useful to study the ways in which one can query subroutines in quantum computation, a pratice that is bound to become ubiquitous, for example in delegated quantum computing. The study of higher-order quantum computation has already led to promising as well as disconcerting results, such as about the difficulty of formally defining a quantum version of the computational 'if' clause [18], or the fact that one might be able to query two unknown gates in a 'superposed order of application', using a computation architecture called the quantum switch [33]. Using the latter leads to computational advantages for certain tasks [17]. However, the mathematical study of higher-order quantum processes quickly encounters thorny formal issues related to their non-trivial compositional structure.

Overcoming these issues would require the development of a specific and robust type system, stipulating which inputs a given higher-order quantum process admits and which output it produces. Despite recent advances [44], currently available type systems are not detailed enough to provide a fully compositional view of higher-order quantum computation. Our work thus focuses on refining them, through the encoding of sectorial structure, i.e. information about how quantum channels behave with respect to certain direct-sum decompositions of their input and output spaces, using the recently developed framework of routed quantum circuits [59, 60]. Progress in this direction will pave the way to computer manipulation of complex higher-order processes, for instance to numerically optimise the advantage they yield.

3.3.7 Causal structure in quantum theory

Many of the peculiarities of quantum theory can be tracked down to it not matching our classical notion of causal structure [61]; this leads to the question of how one could develop a quantum notion of causal structure, on which some progress has been achieved recently [25]. Exploring quantum theory from a causal perspective yields potential progress in understanding its structure and potential applications, in particular for the aforementioned higher-order quantum processes, whose performances are directly connected to their causal structure. In that regard, a particularly important conjecture to prove is that of *causal decompositions* [47], which puts forward a tentative equivalence between a unitary channel's causal structure (operational data about which of its inputs can affect which of its outputs) and its compositional structure (mathematical data about

how it can be written as the composition of sub-channels). If such a conjecture (which has not been proven yet in the general case) were to be true, it would yield a remarkable mathematical lever on the relationship between the operational and formal sides of quantum theory. We investigate this conjecture mathematically with the aim to prove it in more and more general cases; this involves abstract mathematical methods employing C* algebras. More generally, we explore how the latter might provide a useful formal basis for considerations of causality in a quantum context.

4 Application domains

QURIOSITY positions its activity at the - fruitful - frontier between theoretical research in quantum computer science and mathematics, and quantum technology engineering and applications.

We in particular believe that useful quantum inventions and technologies are going to emerge from the current investments in quantum information sciences and technologies, much before large scale (and error corrected) quantum computers can be built.

Our research programs opens in particular towards such perspective, on different aspects:

- The development of more efficient and higher security quantum cryptographic protocols.
- The ability to leverage quantum cryptography principles and tecnnologies to strengthen hardware security.
- The design of cost-effective quantum communications systems that can tightly integrated into modern communication infrastructures, making them widely deployable.
- The design of better quantum memories and therefore larger quantum computer as well as quantum networks.

5 Social and environmental responsibility

5.1 Footprint of research activities

QURIOSITY members are individually, and collectively making efforts to reduce their carbon footprint, in particular by taking the plane much less than before the Covid period. Augustin Vanrietvelde and Peter Brown will moreover act as carbon footprint delegates for QURIOSITY, and report to a working group at LTCI level, whose objective will be to increase the global awareness on carbon footprint, and steer the discussions to help decide on collective regulatory measures.

5.2 Impact of research results

Scientific publication QURIOSITY aims at publishing high-impact papers in high profile journals such as Nature, Science, Physical Review, Quantum, IEEE Transactions on Information Theory, as well as top conferences in our field such as QIP, QCrypt, TQC as well as Crypto, EuroCrypt, CHES.

Innovation Telecom Paris currently holds 5 granted patents: 3 on hybrid quantum computational cryptography (axis 3.1) and 2 on quantum coherent communications (axis 3.2). We plan to patent technological innovations, including foundamental proposals for which we see a clear implementation route and possible exploitation paths.

Teaching QURIOSITY intends to play a vigorous role in the training of the future generation of quantum engineers and researchers. IQA and Romain Alléaume have been at the forefront of such development by opening the Quantum Engineering M2 Program in 2017. At Saclay level, and in collaboration notably with the QuACs Inria team but also with active Saclay quantum industry, we have the mid-term ambition to launch a master program on quantum computer science and engineering.

6 Highlights of the year

- The team had 5 papers accepted as contributed talks at QIP 2024.
  - Thomas van Himbeeck and Peter Brown. A tight and general finite-size security proof for quantum key distribution
  - Emilio Onorati, Cambyse Rouzé, Daniel Stilck Franca and James Watson. Efficient learning of ground and thermal states within phases of matter
  - Emilio Onorati, Cambyse Rouzé, Daniel Stilck França and James Watson. Provably Efficient Learning of Phases of Matter
  - Jan Kochanowski, Alvaro Alhambra, Ángela Capel and Cambyse Rouzé. Spectral gap implies rapid mixing for commuting Hamiltonians
  - Robert König and Cambyse Rouzé. Limitations of local update recovery in stabilizer-GKP codes: a quantum optimal transport approach
- Peter Brown presented an invited tutorial, entitled "Computing Key Rates" at QCrypt 2024, in Vigo.
- Review entitled "Semidefinite programming relaxations for quantum correlations" published in Review of Modern Physics [8]
- New M2 program QMI, Quantique, Mathématique, Informatique, co-operated between Telecom Paris, Ecole Polytechnique, Centrale Supélec and Université PAris-Saclay officially accepted as new element of the Mention Informatique of IP Paris.

7 New software, platforms, open data

7.1 New software

7.1.1 Ket.jl

Name: Ket.jl: Toolbox for quantum information, nonlocality and entanglement

Keywords: Julia programming language, Quantum Information

Functional Description: Ket.jl is a toolbox for quantum information, nonlocality and entanglement written in the Julia programming language.

URL: https://dev-ket.github.io/Ket.jl/dev/

Contact: Peter Johnson Brown

Partners: Universidad de Valladolid, University of Siegen, Zuse Institute Berlin

8 New results

8.1 Research axis 1: Quantum cryptography complexity and hardware frontiers

8.1.1 Computational models in quantum cryptography

Participants: Romain Alléaume, Peter Brown, Francesco Mazzoncini, Tristan Nemoz, Błażej Kuzaka.

We investigate how computational assumptions can be leveraged quantum cryptographic protocols that keep a strict security advantage, with respect to classical (computational) cryptography, while also allowing to obtain performances and properties that go beyond quantum cryptography in the plain model. To this end we have proposed a key distribution protocol in the so-called Quantum Computational Timelock model, whose security can be based on communication complexity gap between classical and quantum communication [49]. In collaboration with LKB (team of Sylvain Gigan) we also proposed a first experimental demonstration of quantum versus classical communicaton two-way complexity advantage. Francesco Mazzoncini defended his PhD in June 2024 [48], notably on these results.

In the context of the PhD of Tristan Nemoz, we have focused on the mathematical structure and applications of quantum pseudorandom states (PRS), and established a lower bound on the distinguishing probabability between any real-valued PRS and a family of Haar-random states. In parallel, we investigate how PRS security definition could be translated to the practically motivated context of bosonic coherent states (and hence implementable using existing quantum communication systems), and study how to design and prove the security of a key exchange protocol based on PRS, in the QCT model.

8.1.2 New results for device-independent cryptography

Participants: Lewis Wooltorton, Peter Brown, Roger Colbeck, Thomas Hahn, Ernest Tan.

In [9] we explore the relationship between nonlocality and secret-key, showing that perfect secret key-rates can be achieved in device-independent quantum key distribution protocols with correlations that are arbitrarily close to classical. Furthering this, we have continued to develop new results on self-testing systems and in upcoming work we show that all pure states can be self-tested with a single Bell inequality and that conference key agreement does not require genuine multipartite entanglement to operate, answering an open question recently posed.

In another direction, we have developed new numerical methods to compute device independent optimizations of Rényi entropies [12]. This includes the derivation of new variational forms for Rényi entropies. Our work opens the possibility to use new security proof techniques that allow for tighter finite size. Building on this work, we are currently developing analytical methods that solve the optimization problems exactly in symmetric settings.

8.1.3 Security proofs, finite size effects and entropies

Participants: Thomas Van Himbeeck, Peter Brown, Kriss Gutierrez Anco, Tristan Nemoz.

We have developed a new security proof framework for standard quantum key-distribution (QKD) protocols. The framework is: (i) generic, applying to all possible round based QKD protocols; (ii) tight, providing key-rates that are optimal for any given finite number of rounds up to leading order correction and (iii) computable, we develop convex optimization methods to compute the key-rates. This is achieved in part through the development of new entropic quantities that enable tight accounting of finite-size corrections. We expect the work to have significant impact on the future development of QKD protocols and security proofs.

We have also developed new understandings of the fundamental rates of randomness generation from a quantum state. We in particular give a simple formula for achievable rates of secure randomness generation from a quantum state in terms of Rényi entropies [11]. Our results can be seen as a benchmarking tool for quantum random number generators.

8.2 Research axis 2: Multimode photonic systems for quantum information processing and communications

8.2.1 Quantum Coherent Communication and Digital Signal Processing

Participants: Romain Alléaume, Gjuillaume Ricard, Nicolas Fabre, Thomas Pousset, Yves Jaouën.

Building up on [20], we are performing a systematic analysis and model of excess noise in a quantum coherent communication channel, jointly operated with a classical coherent channel, taking into account the effect of digital signal processing, and a refined analysis of time-dependent noise calibration.

We have also developped a quantized theory of Kramers-Krönig coherent detection and illustrated how it can be used in quantum communications but also applied to single-photon tomography [13].

8.2.2 Quantum Networking

Participants: Romain Alléaume, Gjuillaume Ricard, Nicolas Fabre, Yves Jaouën, Heming Huang, Thomas Rivera, Pierre-Enguerrand Verdier.

In the context of the ParisRegionQCI and FranceQCI projects, we contributed to the deployment of a dedicated fiber network driven and coordinated by Orange Innnovation in Chatillon, and have investigated time-multiplexed system design to deploy QKD and classical communication on the same fiber nework infrastructure. Moreover, we have experimentally demonstrated, over the ParisRegionQCI network, how post-quantum crypography could be used to reduce the risk associated with trusted node in a QKD nework [15]

8.2.3 Limitations of GKP-LDPC concatenated codes

Participants: Robert König, Cambyse Rouze.

In [45], we established an analytic upper bound on the fault-tolerance threshold for concatenated GKP-stabilizer codes with local update recovery. Our bound applies to noise channels that are tensor products of one-mode beamsplitters with arbitrary environment states, capturing, in particular, photon loss occurring independently in each mode. It shows that for loss rates above a threshold given explicitly as a function of the locality of the recovery maps, encoded information is lost at an exponential rate.

8.3 Research axis 3: Mathematical foundations of quantum information

8.3.1 Causal models in quantum theory

Participants: Augustin Vanrietvelde, Pablo Arrighi, Octave Mestoudjian.

We are investigating the relationship (and in particular the potential equivalence) between the causal structure of quantum dynamics and their compositional structure. We are finishing a proof that there is an equivalence between the two in the case of local dynamics over a 1D array of quantum systems, at any range. This will lead to the publication of two papers.

8.3.2 Quantum reference frames and compositionality

Participants: Augustin Vanrietvelde, Guilhem Doat.

We are investigating quantum reference frames, in which a system's physical quantities are described with respect to those of a reference, potentially superposed, other system. In particular, we are trying to solve a well-known conundrum, called the paradox of the third particle, arising when one adds new systems from a quantum reference frames perspective.

8.3.3 Learning complex quantum states

Participants: Marco Fanizza, Niklas Galke, Josep Lumbreras, Cambyse Rouzé, Andreas Winter, Emilio Onorati, Daniel Stilck França, James D Watson, Tim Möbus, Andreas Bluhm, Matthia C Caro, Abert H Werner, Cambyse Rouzé.

In [54, 52, 26], we have developed robust, sample and computationally efficient quantum algorithms for tomography and learning of states and noise on many-body discrete and continuous variables quantum systems, including thermal and ground states of spin and Bosonic Hamiltonians, finitely correlated states, and Pauli noise channels with unknown underlying local structure. Next, we will investigate the problem of testing physical implementations of Gibbs sampling algorithms.

8.3.4 Complexity of quantum Gibbs states

Participants: Ivan Bardet, Ángela Capel, Li Gao, Angelo Lucia, David Perez-García, Cambyse Rouzé, Jan Kochanowski, Alvaro Alhambra, Paul Gondolf, Sebastian Stengele.

We have kept on working on the complexity of Gibbs sampling algorithms and its applications to the stability of quantum simulation and the characterization of self-correcting quantum memories [21], [22]. In particular, we have extended our previous result on the rapid mixing of Gibbs samplers of commuting Hamiltonians from 2-local to k-local interacting systems [1]. As regards to applications to quantum memories, our results imply that an entire class of quantum double models (including the 2D Toric code) reaches thermal equilibrium in logarithmic time, while the previous best thermalization time scaled linearly with the system size. The write-up of the latter is in preparation. Finally, we considered the general setting of (quasi)-local, non-commuting Hamiltonians for which efficient and exact quantum Gibbs samplers were recently introduced. In [54], [53], we proved the first general polynomial runtime bounds for such Gibbs samplers at high enough temperature. Our methods were recently extended to Fermionic Hamiltonians at any temperature, including temperatures at which the Gibbs states are entangled and where no concurrent classical method is currently known for the task of approximating physical properties. In addition, we proved rapid convergence of these algorithms for parameter regions at which classically sampling from the distribution arising form the measurement of the state in the computational basis fails under standard complexity theoretic assumptions. Finally in [54] we prove that Gibbs sampling at inverse polynomially low temperatures provides a new model of universal quantum computation equivalent to the standard cicuit model. Next, we will further investigate the connections between sampling and computing physical properties of quantum many-body systems at thermal equilibrium. More precisely, we will focus on proving lower bounds on known classical algorithms for the latter in parameter ranges for which our samplers converge in polynomial time. We will also study encodings of specific quantum algorithms into Gibbs samplers with the goal of finding better robustness of the latter against standard noise models. Extensions to infinite dimensional systems such as quantum continuous variables will also be considered.

9 Bilateral contracts and grants with industry

Participants: Romain Alléaume, Yves Jaouën, Guillaume Ricard, Pierre-Enguerrand Verdier.

9.1 Bilateral contracts with industry

Orange Innvovation

- CIFRE with Orange Innovation (Chatillon) on Discrete Variable Quantum Key Distribution and Time Multiplexing, PhD Student: Pierre-Enguerrand Verdier.
- CIFRE with Orange Innovation (Lannion) on Continous Variable Quantum Key Distribution and Wavelenght Division Multiplexing, PhD student: Marco Andersohn.

9.2 Grants with industry

Paris Region PhD Grant, collaboration with Quandela Doctoral project of Guillaume Ricard, on Quatum Coherent Communications and Digital Signal Processing, Funded by Paris funded by Paris Region (region Ile-de France) in the context of the Paris Region PhD call, with a planned collaboration with Quandela on noise mitigation in optical coherent quantum communications.

10 Partnerships and cooperations

10.1 European initiatives

10.1.1 Horizon Europe

Quantum Secure Network Partnership

Participants: Romain Alléaume, Peter Brown, Tristan Nemoz, Francesco Mazzoncini, Guillaume Ricard, Thomas Van Himbeeck, Thomas Pousset, Nicolas Fabre, Yves Jaouën.

Partner Institutions: The Quantum Secure Networks Partnership (QSNP) aims at creating a sustainable European ecosystem in quantum cryptography and communication. Its 42 partners are world-leading academic groups, research and technology organizations (RTOs), quantum component and system spin-offs, cybersecurity providers, integrators, and telecommunication operators. The Partnership thus has the expertise in all technology development phases, from new designs to field deployment, making it ideal to carry out the future Specific Grant Agreement (SGA) projects.

1. ICFO-The Institute of Photonic Sciences, Spain, (Coordinator)
2. Centre National de la Recherche Scientifique, France
3. Institut Polytechnique de Paris, France
4. Technical University of Denmark, Denmark
5. Universidad Politécnica de Madrid, Spain
6. Friedrich-Alexander University Erlangen-Nuremberg, Germany
7. QuTech, at the Technical University Delft, Netherlands
8. Università di Padova, Italy

9. AIT Austrian Institute of Technology, Austria
10. Palacky University Olomouc, Czech Rep.
11. Instituto Superior Técnico, Portugal
12. Universidade de Vigo, Spain
13. Katholieke Universiteit Leuven, Belgium
14. Universität Wien, Austria
15. Université libre de Bruxelles, Belgium
16. University of Warsaw, Poland
17. University of Malta, Malta
18. Institute of Communications and Computer Systems, Greece
19. Universität Paderborn, Germany
20. Inria Cosmiq team, France
21. National and Kapodistrian University of Athens (NKUA),Greece
22. Instituto De Telecomunicacoes, Portugal
23. Politecnico di Bari, Italy,
24. Fraunhofer Heinrich-Hertz-Institut, Germany
25. Commissariat à l'Energie Atomique et aux Energies Alternatives, France
26. Technische Universiteit Eindhoven, Netherland
27. Interuniversity Microelectronics Centre, Belgium
28. University College Cork, Ireland
29. QuSide, Spain
30. LuxQuanta, Spain
31. Micro Photon Devices, Italy
32. ThinkQuantum, Italy
33. VPIphotonics GmbH, Germany
34. Alea Quantum Technologies ApS, Denmark
35. Q*Bird, Nertherlands
36. Cryptonext Security, France
37. Nokia Bell Labs, France
38. Nextworks, Italy
39. Deutsche Telekom, Germany
40. Telefónica, Spain
41. TIM S.p.A, Italy
42. Orange SA,France

Contract ID: HORIZON-CL4-2022-QUANTUM-04-SGA

Information on the Contract: Special Grant Agreement in the context of a Federated Grant Agreement related to the Quantum Communications Pillar of the European Quantum Technology Flagship.

Duration: March 2023 – August 2026

Description: The Quantum Secure Networks Partnership (QSNP) is structured around three main Science and Technology (ST) pillars. The first two pillars, "Next Generation Protocols" and "Integration", focus on frontier research and innovation led mostly by academic partners and RTOs. The third ST pillar "Use cases and Applications" aims at expanding the industrial and economic impact of QSN technologies and is mostly driven by companies. In order to achieve the specific objectives within each pillar and ensure that know-how transfer and synergy between them are coherent and effective, QSNP has established ST activities corresponding to the three main layers of the technology value chain, "Components and Systems", "Networks" and "Cryptography and Security". Future SGA projects will be able to efficiently rely on this framework, in such a way that the ultimate objective of developing quantum communication technology for critical European infrastructures, such as EuroQCI, and private information and communication market sectors, will be achieved. QSNP will contribute to achieving European sovereignty in quantum technology for cybersecurity. At the same time, it will generate significant economic benefits to the whole society, including training a new generation of scientists and engineers, and the creation of high-tech jobs in the rapidly growing quantum industry.

Role of QURIOSITY: QURIOSITY has important participations on Quantum Coherent Communications System Design (WP2), Theory of Quantum Cryptography and in particular on Device-Independent Quantum Crypography (WP3), Hybrid Quantum-Computational Cryptography (WP4 and WP6).

- Romain Alléaume leads one of the 3 pillars of the project, devoted to Integration (at hardware, middleware and cryptographic applications levels) and is member of the Executive Board of QSNP
- Romain Alléaume leads WP6 on Quantum and Classical Cryptography Integration.
- Romain Alléaume leads IP Paris contribution to WP4 on Quantum Cryptographic Protocols beyond QKD.
- Peter Brown leads IP Paris contribution to WP3 on Device-Independent QKD and QRNG.
- Several teams from IP Paris participates to the project: QURIOSITY, GTO, C2 at Telecom Paris and GRACE at LIX/Ecole Polytechnique.

10.1.2 Digital Europe

FranceQCI

Participants: Romain Alléaume, Peter Brown, Tristan Nemoz, Francesco Mazzoncini, Guillaume Ricard, Thomas Van Himbeeck.

Partner Institutions:

1. Orange SA,France (Coordinator)
2. Institut-Mines-Telecom (IMT), France
3. Airbus Defense and Space, France
4. Thales SIX, France
5. CryptoNext Security, France
6. CNRS, France
7. Thales Alenia Space, France
8. CNRS Université Cote d'Azur, France
9. Sorbonne Université, France
10. WeLinQ SAS, France

11. VeriQloud, France
12. Direction des Services de la Navigation Aérienne, DSNA, France

Contract ID: Project: 101091675 — FranceQCI — DIGITAL-2021-QCI-01

Information on the Contract: Call DIGITAL-2021-QCI-01-DEPLOY-NATIONAL, Topic 1 from the Digital Europe Call on Quantum Communication Infrastructures.

Duration: January 2023 – June 2025

Description: The objective of the project is to test use cases of quantum communication technologies and to deploy advanced national quantum systems with existing communication networks in support of national QCI initiatives.

Role of QURIOSITY: Quriosity, represented as IMT, contributes to network design and deployment (WP2), to security studies (WP3), and leads the activity on training (WP7) by coordinating the first executive education training offfer (in France) on quantum communication and cryptography, in collaboration with Sorbonne University and Orange Innovation.

10.1.3 Other european programs/initiatives

PETRUS

Participants: Romain Alléaume.

Partner Institutions:
1. Deutsche Telekom
2. Airbus Defense and Space, France
3. Thales SIX, France
4. Austrian Institute of Technology, AIT, Austria

Contract ID: DIGITAL-2021-QCI-01 Digital European Program under grant agreement no. PETRUS 101091719.

Information on the Contract: PETRUS is the Coordination and Support Action for the national Quantum Communication Infrastructures.

Duration: July 2023 – December 2025

Description: The European Quantum Communication Infrastructure (EuroQCI)is to be rolled out in the EU Member States over the coming years. PETRUS supports the Digital Europe Program projects that aim to form the basis for a European industrial ecosystem for secure quantum technologies. PETRUS brings together former consortium leaders of the most relevant studies and projects on EuroQCI, bundles their experience and expertise and includes top experts from industry and the academic quantum community.

Role of QURIOSITY: Romain Alléaume acts as Scientific Expert for the project.

10.2 National initiatives

PEPR QCommTestbed

Participants: Romain Alléaume, Peter Brown, Nicolas Fabre, Yves Jaouën, Tristan Nemoz, Thomas Pousset, Thomas Van Himbeeck.

Partner Institutions:
1. Institut-Mines-Telecom (IMT), France

2. CNRS Université Cote d'Azur, France
3. Sorbonne Université, France
4. CEA Leti, France
5. C2N, France
6. Université Paris-Cité, France

Contract ID: PC 4.3 « QCommTestbed » (Quantum communication testbeds)

Duration: 01/07/2022 – 30/06/2027

Description: The objective of the QcommTestbed project is to lay the foundations for fiber optic and free-space quantum networks on a regional and longer-term national scale, making it possible to connect systems including quantum elements (transmitters and receivers, processors, sensors) via repeater nodes. The project also aims to make decisive advances in the TRL of quantum communication systems, and also in their security evaluation and testing, to pave the way for their wider adoption and ubiquituous deployment.

Role of QURIOSITY**:**
- Demonstration of ITS secure communication over a single fiber, based on joint CV-QKD and classical communication integration.
- Performance and Cost of Long-Term Secure Storage based on CV-QKD
- Vulnerability analysis of a QKD (VAN) system. Definition of an evaluation methodology (based on the Common Criteria.
- Experimental Demonstration of Mulimode Frequency-encoded Key Distribution in the QCT model

11 Dissemination

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

General chair, scientific chair

- Romain Alléaume: Quantum meets Classical Cryptography, conference organization and co-chair, Paris January 2024.

11.1.2 Scientific events: selection

Chair of conference program committees

- Augustin Vanrietvelde: Causalworlds 2024 Conference (PC co-chair)

Member of the conference program committees

- Augustin Vanrietvelde: QPL 2024 Conference
- Peter Brown: QCrypt 2024 Conference
- Romain Alléaume: QCNC 2024

11.1.3 Journal

Reviewer - reviewing activities

- Augustin Vanrietvelde: Quantum, PRL, Communications Physics
- Peter Brown: Nature, Quantum, PRL
- Romain Alléaume: PRX, Quantum, PRL
- Cambyse Rouzé Quantum, IEEE, Communications in mathematical physics

11.1.4 Invited talks

- Peter Brown : Invited tutorial lecture at QCrypt 2024. Title: Computing key-rates

11.1.5 Leadership within the scientific community

- Romain Alléaume is one of the 3 Pillar Leaders, WP6 Leader and a member of the Executive Board of the Quantum Secure Network Partnership Flagship Project.

11.1.6 Scientific expertise

- Augustin Vanrietvelde: Application review for the QuanG/Quantedu doctoral funding
- Romain Alléaume: Member of the Alliance Quantum Evaluation Committee, at NSERC, in charge of scientific evaluation of Canada Quantum Grants Applications.
- Romain Alléaume: Member of the Evaluation Committee for the admission of Polytecniciens, at Telecom Paris (double degree)
- Romain Alléaume: Chair of the recruitement committee for the Junior Professor position in Quantum Networks Procesing at Telecom Paris, November, 2024.

11.1.7 Research administration

- Romain Alléaume: REP of Quriosity team.
- Romain Alléaume: member of ÌNFRES department direction (in charge of research) until June 2024.
- Romain Alléaume: member of the Comex of Quantum-Saclay.
- Romain Alléaume: member of LTCI Conseil de laboratoire.
- Romain Alléaume: member of IP Paris IDIA bureau.

11.2 Teaching - Supervision - Juries

11.2.1 Teaching

L3 courses, at Telecom Paris

- Romain Alléaume is teaching in PHY101: Introduction to Quantum Technologies. Courses: 9 hetd ∼110 students, TD: 27 hetd ∼25 students.
- Peter Brown, Augustin Vanrietvelde, Jan Kochanowski, Tristan Nemoz A quantum hackathon, 4.5+4.5+4+3 hetd, 30 students.

M1 courses at Telecom Paris

- Peter Brown, Continuous Optimization and Numerical Analysis, ∼30 students, 31.5 hetd.
- Peter Brown, Augustin Vanrietvelde and Romain Alléaume, Introduction to quantum information and quantum computing, ∼25 students, 18 + 9 + 4.5 hetd.

M2 courses in the Quantum Engineering Program at Telecom Paris, (in collaboration with ARTeQ, ENS Paris-Saclay)

- Romain Alléaume coordinates (2017-) the Quantum Engineering Program, a Access PhD Program (M2 level) on Quantum Maths and TCS, and Quantum Technologies, that is currently held in collaboration with ARTeQ (ENS Paris-Saclay) and M2 QDCS (Université Paris-Saclay). The program will next year be transformed into the M2 QMI, a joint program between IP Paris and UPS, coordinated by Augustin Vanrietvelde.
- Augustin Vanrietvelde, Peter Brown, Romain Alléaume Quantum information crash courses, ∼10 students, M2 QEng+ARTeQ, 9+9+9 hetd.
- Peter Brown Quantum Shannon Theory, ∼10 students, 36 hetd.
- Romain Alléaume Quantum Cryptography, ∼5 students, 24 hetd.
- Augustin Vanrietvelde, Guilhem Doat and Romain Alléaume, Quantum programming and QKD, M2 SR2I, ∼30 students, 15 hetd.
- Augustin Vanrietvelde has started a new Quantum Computing course for the students of QEng and ARTeQ, dedicated to advanced quantum algorithms (the Quantum Singular Value Transform and the Hidden Subgroup Problem).Taught 30 hetd, for ∼30 students.
- Cambyse Rouzé has continued and further developped an advanced Quantum Computing course for the students of QEng.
  - This course on the exploration of near-term quantum advantage delves into contemporary advancements in the theory of quantum computing and quantum information processing. It covers a spectrum of topics, ranging from demonstrating quantum advantage in sampling tasks with a specific focus on BosonSampling experiments, to exploring variational quantum algorithms tailored for solving constrained satisfaction problems and their interplay with adiabatic quantum algorithms. Additionally, participants were introduced to quantum state tomography, with the study of cutting-edge shadow tomography algorithms.
  - Taught 18 hetd, for ∼5 students

Teaching in other contexts and programs

- Peter Brown gave an Invited lecture at Asiago QSI school (Jan 2024) on Semidefinite Programming for Quantum Cryptography.

11.2.2 Supervision

- Augustin Vanrietvelde: co-supervision (50%) of Octave Mestoudjian (PhD student at Université Paris Saclay).
- Romain Alléaume and Augustin Vanrietvelde: PhD supervision of Guilhem Doat within Quriosity.
- Romain Alléaume and Nicolas Fabre: PhD supervision of Thomas Pousset.
- Romain Alléaume and Guillaume Ricard: PhD supervision of Guillaume Ricard.

- Romain Alléaume (50%) and Peter Brown (50%): PhD supervision of Tristan Nemoz.
- Roger Colbeck (50%) and Peter Brown (50%): PhD supervision of Lewis Wooltorton.
- Omar Fawzi (50%) and Cambyse Rouzé (50%): PhD supervision of Jan Kochanowski.
- Simone Warzel (50%) and Cambyse Rouzé (50%): PhD supervision of Sebastian Stengele.
- Angela Capel (50%) and Cambyse Rouzé (50%): PhD supervision of Paul Gondolf.
- Omar Fawzi (50%) and Cambyse Rouzé (50%): PhD supervision of Jan Kochanowski.
- Augustin Vanrietvelde: Supervision of Ilyass Mejdoub's PRIM project (M2 research project).
- Peter Brown: Tutor of IPP PhD track student Ali Almasi
- Peter Brown (50%) and Cambyse Rouze (50%) : Supervision of 6 month M1 Internship, Ali Almasi.
- Peter Brown : Supervision of 4 month PRIM M2 research project, Maissa Beji.
- Peter Brown : Supervision of 4 month PRIM M2 research project, Frédéric Nugues (Forrelation as a communication complexity problem and its implementation).

11.2.3 Juries

- Peter Brown: PhD Examiner for Matteo Padovan, Univeristy of Padua.
- Peter Brown: PhD Examiner for Carlos Pascual-García, ICFO.
- Romain Alléaume: PhD Examiner for Verena Yacoub, Dec 2024,Sorbonne University.

12 Scientific production

12.1 Major publications

[1] Á. Capel, P. Gondolf, J. Kochanowski and C. Rouzé. *Quasi-optimal sampling from Gibbs states via non-commutative optimal transport metrics*. 2024. DOI: 10.48550/arXiv.2412.01732. URL: https://hal.science/hal-04896057 (cit. on p. 15).

[2] F. Mazzoncini, B. Bauer, P. Brown and R. Alléaume. *Hybrid Quantum Cryptography from Communication Complexity*. 27th Nov. 2023. URL: https://telecom-paris.hal.science/hal-04328448.

[3] G. de Palma, M. Marvian, C. Rouzé and D. Stilck Franca. 'Limitations of variational quantum algorithms: a quantum optimal transport approach'. In: *PRX Quantum* 4 (23rd Jan. 2023), p. 010309. DOI: 10.1103/PRXQuantum.4.010309. URL: https://hal.science/hal-03675790.

[4] L. Wooltorton, P. Brown and R. Colbeck. *Device-independent quantum key distribution with arbitrarily small nonlocality*. 18th Sept. 2023. URL: https://hal.science/hal-04267174.

12.2 Publications of the year

International journals

[5] P. Brown, H. Fawzi and O. Fawzi. 'Device-independent lower bounds on the conditional von Neumann entropy'. In: *Quantum* 8 (27th Aug. 2024), p. 1445. DOI: 10.22331/q-2024-08-27-1445. URL: https://hal.science/hal-03581631.

[6] L. Gao and C. Rouzé. 'Coarse Ricci curvature of quantum channels'. In: *Journal of Functional Analysis* (Jan. 2024), p. 110336. DOI: 10.1016/j.jfa.2024.110336. URL: https://hal.science/hal-04406061.

[7] C. Rouzé and D. Stilck França. 'Learning quantum many-body systems from a few copies'. In: *Quantum* 8 (2024), p. 1319. DOI: 10.22331/q-2024-04-30-1319. URL: https://hal.science/hal-04622145.

[8] A. Tavakoli, A. Pozas-Kerstjens, P. Brown and M. Araújo. 'Semidefinite programming relaxations for quantum correlations'. In: *Reviews of Modern Physics* 96.4 (4th Dec. 2024), p. 045006. DOI: 10.1103/RevModPhys.96.045006. URL: https://hal.science/hal-04267171 (cit. on p. 12).

[9] L. Wooltorton, P. Brown and R. Colbeck. 'Device-independent quantum key distribution with arbitrarily small nonlocality'. In: *Physical Review Letters* 132.21 (22nd May 2024), p. 210802. DOI: 10.1103/PhysRevLett.132.210802. URL: https://hal.science/hal-04267174 (cit. on p. 13).

[10] Y. Yao, F. Miatto and N. Quesada. 'Riemannian optimization of photonic quantum circuits in phase and Fock space'. In: *SciPost Physics* (18th Sept. 2024). DOI: 10.21468/SciPostPhys. URL: https://telecom-paris.hal.science/hal-04701974.

Reports & preprints

[11] K. G. Anco, T. Nemoz and P. Brown. *How much secure randomness is in a quantum state?* 2024. DOI: 10.48550/arXiv.2410.16447. URL: https://telecom-paris.hal.science/hal-04892001 (cit. on p. 13).

[12] T. Hahn, E. Tan and P. Brown. *Bounds on Petz-Rényi Divergences and their Applications for Device-Independent Cryptography*. 2024. DOI: 10.48550/arXiv.2408.12313. URL: https://telecom-paris.hal.science/hal-04887338 (cit. on p. 13).

[13] T. Pousset, M. Federico, R. Alléaume and N. Fabre. *Kramers-Kronig detection in the quantum regime*. 2024. DOI: 10.48550/arXiv.2407.20827. URL: https://inria.hal.science/hal-04891719 (cit. on p. 14).

[14] T. L. Roy-Deloison, E. P. Lobo, J. Pauwels and S. Pironio. *Device-independent quantum key distribution based on routed Bell tests*. 1st Apr. 2024. URL: https://hal.science/hal-04595717.

Other scientific publications

[15] H. Huang, Y. Jaouën, N. Fabre, R. Alléaume, J.-S. Pegon, T. Camus, M. Zuber, J.-C. Faugère, P.-E. Verdier, B. Lacour, M. Gautier, T. Rivera, Y. Piétri, M. Schiavon, A. Rhouni and E. Diamanti. 'Post-Quantum Cryptographically-Secured Trusted Node for Quantum Key Distribution in a Deployed Network'. In: QCRYPT 2024 - 14th International Conference on Quantum Cryptography. Vigo, Spain, 2nd Sept. 2024. URL: https://hal.science/hal-04722437 (cit. on p. 14).

12.3 Cited publications

[16] S. Aaronson and A. Arkhipov. 'The computational complexity of linear optics'. In: *Proceedings of the forty-third annual ACM symposium on Theory of computing*. 2011, pp. 333–342 (cit. on p. 6).

[17] M. Araújo, F. Costa and Ċ. Brukner. 'Computational advantage from quantum-controlled ordering of gates'. In: *Physical review letters* 113.25 (2014), p. 250402. DOI: 10.1103/PhysRevLett.113.250402. arXiv: 1401.8127 [quant-ph] (cit. on p. 10).

[18] M. Araújo, A. Feix, F. Costa and Ċ. Brukner. 'Quantum circuits cannot control unknown operations'. In: *New Journal of Physics* 16.9 (2014), p. 093026. DOI: 10.1088/1367-2630/16/9/093026. arXiv: 1309.7976 [quant-ph] (cit. on p. 10).

[19] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner and T. Vidick. 'Practical device-independent quantum cryptography via entropy accumulation'. In: *Nature communications* 9.1 (2018), p. 459 (cit. on p. 8).

[20] R. Aymeric, Y. Jaouën, C. Ware and R. Alléaume. 'Symbiotic joint operation of quantum and classical coherent communications'. In: *arXiv preprint arXiv:2202.06942* (2022) (cit. on pp. 6, 14).

[21] I. Bardet, Á. Capel, L. Gao, A. Lucia, D. Pérez-García and C. Rouzé. 'Entropy decay for Davies semigroups of a one dimensional quantum lattice'. In: *arXiv preprint arXiv:2112.00601* (2021) (cit. on pp. 8, 9, 15).

[22] I. Bardet, Á. Capel, L. Gao, A. Lucia, D. Pérez-García and C. Rouzé. 'Rapid thermalization of spin chain commuting Hamiltonians'. In: *arXiv preprint arXiv:2112.00593* (2021) (cit. on pp. 9, 15).

[23] I. Bardet, Á. Capel and C. Rouzé. 'Approximate Tensorization of the Relative Entropy for Noncommuting Conditional Expectations'. In: *Annales Henri Poincaré* 23.1 (2021), pp. 101–140 (cit. on p. 9).

[24] I. Bardet, M. Junge, N. Laracuente, C. Rouzé and D. S. França. 'Group Transference Techniques for the Estimation of the Decoherence Times and Capacities of Quantum Markov Semigroups'. In: *IEEE Transactions on Information Theory* 67.5 (2021), pp. 2878–2909. DOI: 10.1109/TIT.2021.3065452 (cit. on p. 8).

[25] J. Barrett, R. Lorenz and O. Oreshkov. 'Quantum causal models'. In: (). DOI: 10.48550/arXiv.1906.10726. arXiv: 1906.10726 [quant-ph] (cit. on p. 10).

[26] S. Becker, N. Datta, L. Lami and C. Rouzé. 'Classical shadow tomography for continuous variables quantum systems'. In: *arXiv preprint arXiv:2211.07578* (2022) (cit. on p. 15).

[27] P. Brown, H. Fawzi and O. Fawzi. 'Computing conditional entropies for quantum correlations'. In: *Nature communications* 12.1 (2021), pp. 1–12 (cit. on pp. 4, 7).

[28] P. Brown, H. Fawzi and O. Fawzi. 'Device-independent lower bounds on the conditional von Neumann entropy'. In: *arXiv preprint arXiv:2106.13692* (2021) (cit. on pp. 4, 7).

[29] Y. Cai, J. Roslund, G. Ferrini, F. Arzani, X. Xu, C. Fabre and N. Treps. 'Multimode entanglement in reconfigurable graph states using optical frequency combs'. In: *Nature communications* 8.1 (2017), pp. 1–9 (cit. on p. 6).

[30] Á. Capel, C. Rouzé and D. S. França. 'The modified logarithmic Sobolev inequality for quantum spin systems: classical and commuting nearest neighbour interactions, (QIP talk, presented at ICMP)'. In: *arXiv:2009.11817* (2020) (cit. on pp. 8, 9).

[31] Z. Chen, K. Liu and E. Vigoda. 'Optimal Mixing of Glauber Dynamics: Entropy Factorization via High-Dimensional Expansion'. In: *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. STOC 2021. Virtual, Italy: Association for Computing Machinery, 2021, 1537?1550. DOI: 10.1145/3406325.3451035. URL: https://doi.org/10.1145/3406325.3451035 (cit. on p. 9).

[32] H.-C. Cheng, N. Datta and C. Rouzé. 'Strong Converse Bounds in Quantum Network Information Theory'. In: *IEEE Transactions on Information Theory* 67.4 (2021), pp. 2269–2292. DOI: 10.1109/TIT.2021.3058166 (cit. on p. 8).

[33] G. Chiribella, G. M. D'Ariano, P. Perinotti and B. Valiron. 'Quantum computations without definite causal structure'. In: *Physical Review A* 88.2 (2013), p. 022318. DOI: 10.1103/PhysRevA.88.022318. arXiv: 0912.0195 [quant-ph] (cit. on p. 10).

[34] F. Dupuis, O. Fawzi and R. Renner. 'Entropy accumulation'. In: *Communications in Mathematical Physics* 379 (2020), pp. 1–47 (cit. on p. 8).

[35] P. Faist. 'The Entropy Zoo'. In: *https://phfaist.com/entropyzoo* () (cit. on p. 8).

[36] O. Faust and H. Fawzi. 'Sum-of-Squares proofs of logarithmic Sobolev inequalities on finite Markov chains'. In: *arXiv preprint arXiv:2101.04988* (2021) (cit. on p. 8).

[37] L. Gao and C. Rouzé. 'Complete Entropic Inequalities for Quantum Markov Chains'. In: *Archive for Rational Mechanics and Analysis* 245.1 (May 2022), pp. 183–238. DOI: 10.1007/s00205-022-01785-1. URL: https://doi.org/10.1007/s00205-022-01785-1 (cit. on p. 8).

[38] S. Guha, B. I. Erkmen and J. H. Shapiro. 'The Entropy Photon-Number Inequality and its consequences'. In: *2008 Information Theory and Applications Workshop*. 2008, pp. 128–130. DOI: 10.1109/ITA.2008.4601037 (cit. on p. 8).

[39] T. A. Hahn and E. Y.-Z. Tan. 'Fidelity Bounds for Device-Independent Advantage Distillation'. In: *arXiv preprint arXiv:2105.03213* (2021) (cit. on p. 4).

[40] A. Henry, R. Raghunathan, G. Ricard, B. Lefaucher, F. Miatto, N. Belabas, I. Zaquine and R. Alléaume. 'Parallelizable Synthesis of Arbitrary Single-Qubit Gates with Linear Optics and Time-Frequency Encoding'. In: *Physical Review A* 107.6 (June 2023), p. 062610. DOI: 10.1103/PhysRevA.107.062610. URL: https://hal.science/hal-03876857 (cit. on p. 6).

[41] H.-Y. Huang, R. Kueng and J. Preskill. 'Predicting many properties of a quantum system from very few measurements'. In: *Nature Physics* 16.10 (June 2020), pp. 1050–1057. DOI: 10.1038/s41567-020-0932-7. URL: https://doi.org/10.1038/s41567-020-0932-7 (cit. on p. 9).

[42] H.-Y. Huang, R. Kueng, G. Torlai, V. V. Albert and J. Preskill. 'Provably efficient machine learning for quantum many-body problems'. In: *arXiv preprint arXiv:2106.12627* (2021) (cit. on p. 9).

[43] K. Kazuro. 'Fundamentals of Coherent Optical Fiber Communications'. In: *in Journal of Lightwave Technology vol. 34, N¬∞1* (2016) (cit. on p. 6).

[44] A. Kissinger and S. Uijlen. 'A categorical semantics for causal structure'. In: *Logical Methods in Computer Science* Volume 15, Issue 3 (2019). DOI: 10.23638/LMCS-15(3:15)2019. arXiv: 1701.04732 [quant-ph] (cit. on p. 10).

[45] R. König and C. Rouzé. 'Limitations of local update recovery in stabilizer-GKP codes: a quantum optimal transport approach'. In: *arXiv preprint arXiv:2309.16241* (2023) (cit. on p. 14).

[46] S. Laplante, M. Laurière, A. Nolin, J. Roland and G. Senno. 'Robust Bell inequalities from communication complexity'. In: *Quantum* 2 (2018), p. 72 (cit. on p. 7).

[47] R. Lorenz and J. Barrett. 'Causal and compositional structure of unitary transformations'. In: *Quantum* 5 (2021), p. 511. DOI: 10.22331/q-2021-07-28-511. arXiv: 2001.07774 [quant-ph] (cit. on p. 10).

[48] F. Mazzoncini. 'Multimode Quantum Communications and Hybrid Cryptography'. Theses. Institut Polytechnique de Paris, June 2024. URL: https://theses.hal.science/tel-04656723 (cit. on p. 13).

[49] F. Mazzoncini, B. Bauer, P. Brown and R. Alléaume. 'Hybrid Quantum Cryptography from Communication Complexity'. working paper or preprint. Dec. 2023. URL: https://telecom-paris.hal.science/hal-04328448 (cit. on p. 13).

[50] D. Nadlinger, P. Drmota, B. Nichol, G. Araneda, D. Main, R. Srinivas, D. Lucas, C. Ballance, K. Ivanov, E. Tan et al. 'Device-independent quantum key distribution'. In: *arXiv preprint arXiv:2109.14600* (2021) (cit. on p. 4).

[51] O. Regev and B. Klartag. 'Quantum one-way communication can be exponentially stronger than classical communication'. In: *Proceedings of the forty-third annual ACM symposium on Theory of computing*. 2011, pp. 31–40 (cit. on p. 7).

[52] C. Rouzé and D. S. Franca. 'Efficient learning of the structure and parameters of local Pauli noise channels'. In: *arXiv preprint arXiv:2307.02959* (2023) (cit. on p. 15).

[53] C. Rouzé, D. S. França and Á. M. Alhambra. 'Optimal quantum algorithm for Gibbs state preparation'. In: *arXiv preprint arXiv:2411.04885* (2024) (cit. on p. 15).

[54] C. Rouzé, D. Stilck França, E. Onorati and J. D. Watson. 'Efficient learning of ground and thermal states within phases of matter'. In: *Nature Communications* 15.1 (2024), p. 7755 (cit. on p. 15).

[55] D. Rusca, T. Van Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner and H. Zbinden. 'Self-testing quantum random-number generator based on an energy bound'. In: *Physical Review A* 100.6 (2019), p. 062338 (cit. on p. 4).

[56] E. Y.-Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja and C. C.-W. Lim. 'Computing secure key rates for quantum cryptography with untrusted devices'. In: *npj Quantum Information* 7.1 (2021), pp. 1–6 (cit. on p. 4).

[57] E. Y.-Z. Tan, P. Sekatski, J.-D. Bancal, R. Schwonnek, R. Renner, N. Sangouard and C. C.-W. Lim. 'Improved DIQKD protocols with finite-size analysis'. In: *arXiv preprint arXiv:2012.08714* (2020) (cit. on p. 4).

[58] A. Tavakoli. 'Semi-device-independent framework based on restricted distrust in prepare-and-measure experiments'. In: *Physical Review Letters* 126.21 (2021), p. 210503 (cit. on p. 4).

[59] A. Vanrietvelde, H. Kristjánsson and J. Barrett. 'Routed quantum circuits'. In: *Quantum* 5 (July 2021), p. 503. DOI: 10.22331/q-2021-07-13-503. arXiv: 2011.08120 [quant-ph] (cit. on p. 10).

[60] A. Vanrietvelde, N. Ormrod, H. Kristjánsson and J. Barrett. 'Consistent circuits for indefinite causal order'. In: (June 2022). arXiv: 2206.10042 [quant-ph] (cit. on p. 10).

[61] C. J. Wood and R. W. Spekkens. 'The lesson of causal discovery algorithms for quantum correlations: causal explanations of Bell-inequality violations require fine-tuning'. In: *New Journal of Physics* 17.3 (Mar. 2015), p. 033002. DOI: 10.1088/1367-2630/17/3/033002. URL: http://dx.doi.org/10.1088/1367-2630/17/3/033002 (cit. on p. 10).

[62] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, V. Scarani, C. C.-W. Lim and H. Weinfurter. 'Experimental device-independent quantum key distribution between distant users'. In: *arXiv preprint arXiv:2110.00575* (2021) (cit. on p. 4).

[63] Y. Zhang, H. Fu and E. Knill. 'Efficient randomness certification by quantum probability estimation'. In: *Physical review research* 2.1 (2020), p. 013016 (cit. on p. 8).