11th Colloquium of the CNRS GDR № 3322 on Quantum Engineering, Foundations & Applications

Ingénierie Quantique, des aspects Fondamentaux aux Applications – IQFA

Université Grenoble Alpes (UGA) – *entirely held virtually*

December 2 - 4, 2020

IQFA'11 – Book of Abstracts

Contents

1 What is IQFA ?

1.1 A CNRS "Research Network" (Groupement de Recherche)

The **GDR IQFA**[1], **"Ingénierie Quantique, des aspects Fondamentaux aux Applications"**, GDR № 3322 of the Centre National de la Recherche Scientifique (CNRS[2]), is a Research Network supported by the CNRS Institutes of Physics (INP[3]), Systems & Engineering Sciences (INSIS[4]), and Computer Sciences & their interactions (INS2I[5]), with which the quantum information community is mostly associated. This GDR gathers ∼60 French laboratories through which more than a 100 teams are involved.

The goal of the GDR IQFA is two-fold: first, to establish a common base of knowledge, and second, to use this platform to emulate new knowledge.

IQFA's main road-map can be summarized as follows:

- a willingness to shape the discipline in order to create stronger bridges between the various thematics;
- establishment of a shared basis of knowledge through specific lecturing activities during the colloquiums;
- promotion of foundations & applications of Quantum Information in a "bound-free laboratory" to facilitate the emergence of new projects which meet the current and future challenges of the field.

IQFA is organized along the 4 newly identified thematics - ART[6] **-** that are currently highly investigated all around the world, and particularly with the next European Flaghsip project:

- Quantum Communication & Cryptography – Qcom,
- Quantum Sensing & Metrology – Qmet,
- Quantum Processing, Algorithms, & Computation – Qpac,
- Quantum Simulation – Qsim,

all surrounded by transverse Fundamental Quantum Aspects – Fqa.

For more details on those thematics, e.g. scope and perspectives, please visit IQFA webpage: http://gdriqfa.cnrs.fr/.

1.2 Scientific Committee of the GDR IQFA

Members: Alexia Auffèves (CNRS, Uni. Grenoble Alpes),
Patrice Bertet (CEA, Uni. Paris Saclay),
Antoine Browaeys (CNRS, Inst. d'Optique Graduate School, Uni. Paris Saclay),
Thierry Chanelière (CNRS, Uni. Grenoble Alpes),
Eleni Diamanti (CNRS, Sorbonne Uni., Paris),
Anaïs Dréau (CNRS, Uni. Montpellier), Vice-head,
Pascal Degiovanni (CNRS, ENS Lyon),
Iordanis Kerenidis (CNRS, Uni. de Paris),
Tristan Meunier (CNRS, Uni. Grenoble Alpes),
Alexei Ourjoumtsev (CNRS, Collège de France),
Simon Perdrix (CNRS, Uni. de Lorraine Metz-Nancy),
Sébastien Tanzilli (Head, CNRS, Uni. Côte d'Azur),
Nicolas Treps (ENS Paris, Sorbonne Uni., Paris),

Administration assistant: Nathalie Koulechoff (CNRS, Uni. Côte d'Azur).

[1] French acronym for "Ingénierie Quantique, des aspects Fondamentaux aux Applications".
[2] http://www.cnrs.fr/
[3] http://www.cnrs.fr/inp/
[4] http://www.cnrs.fr/insis/
[5] http://www.cnrs.fr/ins2i/
[6] In French: Axes de Réflexion Thématiques.

2 IQFA'11 Colloquium – Scientific Information

2.1 Welcome !

IQFA'11 is organized by IQFA Scientific Committee members and by the Institut Néel[7]. Due to the Covid-19 sanitary situation, the entire colloquium is held virtually.

From the scientific side, the main goal of this colloquium is to gather all the various communities working in Quantum Information, and to permit, along 3 days, to exchange on the recent advances in the field. The colloquium will be outlined along 3 communication modes:

- 5 tutorial talks, having a clear pedagogical purpose, on the very foundations and most advanced applications of the field, as well as 3 invited talks;
- 11 contributed talks on the current hot topics within the strategic thematics (ARTs) identified by the GDR IQFA (see online the ARTs[8] for more details);
- and 2 poster sessions gathering ∼32 posters, again within IQFA's strategic thematics (ARTs).

In total this year, **IQFA's Scientific Committee (see Sec. 1.2) has received 43 scientific contributions**.

Moreover, **the third day of IQFA'11 is dedicated to Quantum Computing realizations and advances**, encompassing all of its aspects.

You will find in this book of abstracts an overview of all the contributions, *i.e.* including the tutorial lectures, invited and contributed talks, as well as poster contributions.

We wish all the participants a fruitful colloquium.

Alexia AUFFÈVES (IQFA's CS member & President of IQFA'11),
Thierry CHANELIÈRE (IQFA's CS member),
Tristan MEUNIER (IQFA's CS member),
Maud VINET (CEA Leti),
Xavier THIBAULT (Al2GRI, Grenoble),
& **Sébastien TANZILLI** (IQFA's Director),

On behalf of IQFA*'s Scientific Committee.*

[7] https://neel.cnrs.fr/
[8] http://gdriqfa.unice.fr/spip.php?rubrique2

2.2 Program of the colloquium

IQFA'11 - Université Grenoble Alpes - Institut Néel CNRS - All by visio-conferencing

	Wednesday the 2nd of December 2020	Thursday the 3rd of December 2020	Friday the 4th of December 2020 *Quantum Computing Day*
08:30	**Welcome - A. Auffèves (CNRS) & S. Tanzilli (CNRS)**		**National Quantum Initiative - J.-P. Bourgoin (MESRI)** ***with IQFA scientific committee***
09:00	***Tutorial*** **- QSIM - F. Ferlaino (Uni. Innsbruck, IQOQI, Austrian Acad. Science, AT):** ***Supersolidity in the ultracold: when atoms behave as crystal and superfluid at the same time***	***Invited*** **- QCOM - T. Vidick (CALTECH, USA):** ***MIP* = RE and Tsirelson's problem***	***See special program sheet*** *Sessions Qubit Chips, Quantum-quantum Communication*
09:30		Contrib - QCOM - A. Durand (Univ. Montpellier, FR): *Single artificial atoms in silicon emitting at telecom wavelengths*	
10:00	***Invited*** **- QSIM - T. Lahaye (CNRS, Int. Optique GS, FR):** ***Many-body physics in arrays of single Rydberg atoms***	Contrib - QPAC - M. Fellous (CNRS, Uni. Grenoble Alpes, FR): *Limitations in quantum computing from resource constraints*	
10:30	*Coffee break*	*Coffee break*	*Coffee break*
11:00	Contrib - QSIM - B. Vermersch (Uni. Grenoble Alpes, CNRS, FR): *Probing Quantum Entanglement with Randomized Measurements*	***Invited*** **- QMET - Y. Chu (ETH Zurich, CH):** ***Quantum information processing with mechanical systems***	***See special program sheet*** *Session Quantum Computing-oriented Nanotechnology*
11:30	QSIM - M. Robert-De-Saint-Vincent (Uni. Sorbonne Paris Nord, FR): *Adiab. spin-dpndnt momentum transfer in an SU(N) degen. Fermi gas*	Contrib - QMET - A. Ranadive (CNRS, Uni. Grenoble Alpes, FR): *A SNAIL Travelling Wave Parametric Amplifier*	
12:00	QSIM - I. Frerot (ICFO, Barcelona, ES): *Scalable device-independent certification of many-body entanglement using statistical inference*	Contrib - QMET - P.-A. Bourdel (Sorbonne Uni., CNRS, ENS Paris, FR): *Cavity Protected Polaritons in a Cold Atom Ensemble*	
12:30	*Lunch*	*Lunch*	*Lunch*
14:00	***Tutorial*** **- QCOM - E. Kashefi (CNRS, Sorbonne Uni., Paris, FR):** ***Quantum Cyber Security: Challenges and Opportunities***	***Tutorial*** **- FQA - I. Dotsenko (Sorbonne Uni., CNRS, ENS Paris, Coll. France, FR):** ***Quantum thermodynamics with individual atoms and trapped photons***	***See special program sheet*** *Session Quantum Computing Systems*
14:30			
15:00	Contrib - QCOM - H. Defienne (Univ. Glasgow, UK): *Unscrambling entanglement through a complex medium*	Contrib - FQA - A. Abbott (Univ. Geneva, CH): *Computational advantage from quantum superposition of multiple temporal orders of gates*	
15:30	*Coffee break*	*Coffee break*	*Coffee break*
16:00	***Tutorial*** **- QPAC - J. Petta (Princeton Uni., USA):** ***Quantum Information Processing with Spins in Silicon***	***Tutorial*** **- QPAC - C. Gidney (Google AI Quantum, USA):** ***Spacetime tradeoffs when optimizing large quantum computations***	***See special program sheet*** *Session Quantum Chip Control*
16:30			
17:00	Contrib - QPAC - P. Besserve (ATOS/EP, Palaiseau, FR): *Tackling many-body problems with a noisy quantum computer*	Contrib - QPAC - E. Gouzien (CEA Sacaly, FR): *How to hack 2048 RSA code with 8100 qubits and a multimode memory with 2 hours storage*	
17:30	**Poster session 1** *All posters*	**Poster session 2** *All posters*	
19:00	*End of the day*	*End of the day*	*End of the Colloquium IQFA'11*

Figure 1: Detaild of the multi-thematic program, on Wednesday-Thursday the 2^{nd}-3^{rd} of December 2020.

IQFA'11 – Friday the 4th of December 2020 – Special Day on Quantum Computing

- 9h00 Introduction of the Q computing day, Tristan Meunier, (CNRS Institut Néel)

Session Qubit chips

- 9h10 Superconducting cat qubits: a shortcut to universal fault tolerance, Théau Peronnin (Alice et Bob)
- 9h30 CMOS Superconducting Qubits, François Lefloch (CEA IRIG)
- 9H50 Spin Qubits in Si semiconductor, Benoit Bertrand (CEA-CNRS Grenoble)
- 10h10 Development of an integrated photonic platform on silicon for photonic qubits, Ségolène Olivier (CEA LETI)
- 10h30 Carbon Qubits, Pierre Desjardins (C12 Quantum Electronics)
- 10h50 Atomic Qubits, Georges Olivier Reymond (Institut d'Optique, Pasqal)
- 11H10 Pause 10 minutes

Session Quantum-quantum Communication

- 11h20 Spin photon coupling, Loïc Lanco (CNRS C2N)
- 11h40 Electro-opto-mechanics for microwave-to-optical photon conversion, Sébastien Hentz (CEA LETI, MPQ, CNRS Institut Néel)

Session Quantum Computing-oriented Nanotechnology

- 12H00 3D Integration & Packaging for Si quantum circuits, Jean Charbonnier (CEA LETI)
- 12h20 NanoFabrication for Superconducting quantum circuits, Denis Vion (CEA Saclay)

Session Quantum Computing Systems

- 14h00 How to integrate a quantum computer in a computing centre? Jacques-Charles Lafoucrière (CEA DAM)
- 14h20 System architecture for quantum computing, Eric Guthmuller (CEA LIST)
- 14h40 Hybrid programming in the NISQ era, Thomas Ayral (ATOS)
- 15h00 Quantum bit computer aided design (QCAD), Yann Michel Niquet (CEA IRIG)
- 15h20 Quantum Computing for Programmers: Compilation Challenges, Henri Pierre Charles (CEA LIST)
- 15h40 Pause 20 minutes
- 16h00 Quantum engineering at INRIA, Anthony Leverrier (INRIA)
- 16H20 Quantum Architecture with photons, Shane Mansfield (Quandela)

Session Quantum Chip Control

- 16h40 Cryo-CMOS control circuits for quantum circuits, Gérard Billiot (CEA LETI)
- 17h00 Superconducting amplifiers, Luca Planat (CNRS Institut Néel)
- 17h20 Cryogeny for quantum computing, Philippe Camus (CNRS Institut Néel)

Figure 2: Detailed program of the Quantum Computing Day, on Friday the 4^{th} of December 2020.

3 Université Grenoble Alpes & the Institut Néel

3.1 Université Grenoble Alpes

Anchored on its territory, multidisciplinary and open to the international, Université Grenoble Alpes (UGA[9]) brings together the main public higher education institutions of Grenoble and Valence. In association with the national research organisations and the international research facilities present on its territory, it builds its research and innovation policy on a global scale. As a driving force for progress and a laboratory for initiatives, it acts with its many partners to accompany the evolution of society.

UGA, a university geared towards innovation in higher education, research, and technology
UGA is a major player in higher education and research in France. It is firmly rooted in its region, while prioritizing its international engagements in the search to expand scientific knowledge and cultural understanding. From the research side, UGA has world-class research programs that boost hundreds of selected projects for more than a billion Euros in direct funding. Research teams enjoy a wide network of international partners over all the continents. Moreover, Grenoble consistently ranks among the world?s top most innovative cities. With a very high ratio of patents per inhabitants, the city relies on a unique and efficient system of innovation and knowledge transfer.

3.2 The Institut Néel

The Institut Néel[10] is a research laboratory in condensed matter physics located on the Polygone Scientifique in Grenoble, France. It is named after scientist Louis Néel, who was awarded the Physics Nobel Prize in 1970 for his pioneering studies of the magnetic properties of solids.

The institute is a CNRS research unit (UPR2940) created in 2007 as a reorganization of four research laboratories: the center for research in very low temperatures (Centre de Recherches sur les très basses températures (CRTBT)), the laboratory for the study of electronic properties of solids (Laboratoire d'étude des propriétés électroniques des solides (LEPES)), the Louis **Néel** laboratory (Laboratoire Louis **Néel** (LLN)), and the Laboratory of crystallography (Laboratoire de cristallographie (LdC)).

The Scientific activities of the Institut Néel cover a large area: supra-conductor, quantum fluids, new materials, crystallography, surface science, quantum nanoelectronics, nanomechanics, nonlinear optics, quantum optics, spintronics, magnetism, etc. To reach a critical size in order to ensure competitiveness, the 450 laboratory members are gathered in research teams and technology support groups according to their shared common goals, concerns, and expertise.

Here are some **key figures** of the Institut Néel:

- **Staff members**: ∼450 people, including 125 scientists and 50 professors / associate professors, 130 engineers, technicians and administratives, as well as 145 non-permanent staff;
- **Organization**: 3 departments, 16 research teams, 18 services and technological support groups;
- **Building area**: 21,500 m^2;
- **Publications**: 400/year in peer-reviewed journals;
- **PhD applicants**: at least 30 PhD thesis defenses per year;
- **Master students**: ∼80 internships per year;
- **Industrial partnership**: links with 30 partners through research contracts, 38 active patents, 24 licensing.

Within the context of supporting scientific research & colloquiums, the institut Néel highly supports and welcomes* IQFA *'11 colloquium.

[9] https://www.univ-grenoble-alpes.fr/english/
[10] https://neel.cnrs.fr/

4 IQFA'11 Colloquium – Practical Information

4.1 Venue

Due to the Covid-19 sanitary situation, all sessions are held virtually, including poster sessions. All registered participants are provided with visio-conferencing links.

4.2 Organization & financial supports

This colloquium is organized by: the GDR IQFA,
& members of the Institute Néel, the CEA Leti, and the LANEF Grenoble,

with the financial supports of: the CNRS, through its INSTITUTES INP, INSIS, and INS2I[11],
the Institut Néel[12], CNRS in Grenoble,
the CEA LETI[13] in Grenoble,
the Maison MINATEC[14] in Grenoble
the Foundation NANOSCIENCES[15], Université Grenoble Alpes UGA[16],
the Région AUVERGNE RHÔNE ALPES[17],
the Laboratoire d'Alliances Nanosciences-Énergie du Futur LANEF[18],
the GRENOBLE ALPES MÉTROPOLE[19],
and ID QUANTIQUE[20].
that are warmly acknowledged.

4.3 Local organization committee for IQFA'11 @ UGA

President: Alexia Auffèves, CNRS, Uni. Grenoble Alpes;

IQFA CS Members: Thierry Chanelière (CNRS, Institut Néel), Tristan Meunier (CNRS, Institut Néel);

CEA Member: Maud Vinet (Leti);

LANEF Member: Xavier Thibault (Laboratory of nanoscience alliances);

Institut Néel Members: Aurélie Laurent, Admin, CNRS, Uni. Grenoble Alpes,
Caroline Bartoli, Admin, CNRS, Uni. Grenoble Alpes.

With the remote help of: Anaïs Dréau, CNRS, Uni. Montpellier, vice-head,
Sébastien Tanzilli, CNRS, Uni. Côte d'Azur, head,
Nathalie Koulechoff, CNRS, Uni. Côte d'Azur,
& Bernard Gay-Para, CNRS, Uni. Côte d'Azur.

[11] http://www.cnrs.fr/la-recherche
[12] https://neel.cnrs.fr/
[13] https://www.leti-cea.com/cea-tech/leti/english/
[14] https://www.minatec.org/en/congress-center/congress-center/
[15] hhttps://fondation.univ-grenoble-alpes.fr/fr/
[16] https://www.univ-grenoble-alpes.fr/english/
[17] https://www.auvergnerhonealpes.fr
[18] https://www.grenoble-lanef.fr
[19] https://www.grenoblealpesmetropole.fr
[20] https://www.idquantique.com

5 Abstracts of the contributions

In the following, you can find, after the tutorial lectures, invited talks, and contributed talks, all the poster contributions sorted per ART.
The contributed talks correspond to poster contributions that have been selected by our Scientific Committee for oral presentations, as can be seen in the Program in Sec. 2.2.

Table of contents

Tutorial Talks

Quantum thermodynamics with individual atoms and trapped photons

Igor Dotsenko[1]*
[1] *Laboratoire Kastler Brossel, Collège de France, CNRS, ENS-Université PSL, Sorbonne Université, Paris, France*

We report on the experimental realization of an autonomous Maxwell's demon in a cavity QED system. The modelled system is a qubit exchanging heat with a cavity (high-quality microwave resonator) under the control of a demon. Both qubit and demon are coded with a single three-level atom (circular Rydberg atom). The developed experimental tools provide us with the access to the system's evolution at quantum trajectory level. This allows us to demonstrate the entropy production measurements based on several different expressions for this quantity which is responsible for the irreversibility of thermodynamic processes both at classical and quantum scale. We present and discuss the obtained experimental and theoretical results.

* igor.dotsenko@lkb.ens.fr

Supersolidity in the ultracold : when atoms behave as crystal and superfluid at the same time

Francesca Ferlaino[1*]
[1] *Institut für Experimentalphysik, Universität Innsbruck, Innsbruck, Austria, and Institute for Quantum Optics and Quantum Information (IQOQI), Innsbruck*

Over more than two decades, ultracold quantum gases have enabled the observation of fascinating quantum phenomena. Research directions are ever increasing with the development of novel optical-manipulation techniques and the gain of an exquisite control over the inter-particle interactions.

Recently, a novel class of atomic species, possessing an exceptionally strong magnetic dipole moment, has entered the stage (Cr, Dy, Er). This offers new opportunities to study dipolar quantum phenomena, driven by the long-range and anisotropic interaction between particles. I will review the recent developments in atomic dipolar quantum gases from the Innsbruck perspective. In our laboratories, we work with dipolar Bose-Einstein condensates and Fermi gases of either Erbium or Dysprosium, or with dipolar quantum mixtures of both elements.

Particular emphasis will be given on our recent observations of the elusive and paradoxical supersolid state of matter, using both Er and Dy ultracold gases. Such paradoxical phase, in which crystal rigidity and superfluid flow coexist, has intrigued scientists across different disciplines for decades. It now became possible to create supersolidity in the ultracold thanks to the unique interplay between long-range dipolar interactions, contact interactions, and a powerful stabilization mechanism based on quantum fluctuations.

* Francesca.Ferlaino@uibk.ac.at

Spacetime tradeoffs when optimizing large quantum computations

Craig Gidney[1*]
[1] *Google AI Quantum, United States of America*

In quantum computing, tradeoffs between space and time are everywhere. This is especially true in topological codes like the surface code, because the topological features that computations are turned into (like "this spacetime ring is linked with that spacetime ring") don't change when rotated to span over space instead of over time. This tutorial will describe at a high level how computations in the abstract circuit model are embedded into the surface code, the additional costs that this introduces which are normally ignored, how to dial surface code computations between using a lot of time and using a lot of space, and what the limits on these techniques are. The overarching goal of the tutorial is to explain the design decisions and tradeoffs that drove the layout of the adders and QROM reads used in "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits".

* craig.gidney@gmail.com

Quantum Cyber Security : Challenges and Opportunities

Elham Kashefi[1]*
[1] *LIP6, Sorbonne Universié, CNRS, France,*
Personal Chair in Quantum Computing,
School of Informatics, University of Edinburgh, Scotland

Future information and communication networks will certainly consist of both classical and quantum devices, some of which are expected to be dishonest, with various degrees of functionality, ranging from simple routers to servers executing quantum algorithms. Most of the technology required to achieve advanced stages of a quantum internet is still in its infancy, hence it is very hard to predict the potential use cases. Several applications, however, have already been characterized depending on the different stages of a quantum network such as secure delegated quantum computing, quantum key distribution, clock synchronization, leader election, quantum digital signatures, quantum money among others. Such applications promise to impact and transform the society on multiple levels including communication, accessing information and security. Therefore, it would be extremely useful to have a standard framework to describe the protocols that are relevant to the quantum internet such that they become available to the diverse quantum information science community. We take the first step in this direction and call such an initiative : The Quantum Protocol Zoo which consists of an organised collection of protocols that could be implemented (or simulated) in the coming years. In this lecture I present an overview of the field through this new platform of interaction with various communities contributing to it.

* ekashefi@gmail.com

Quantum Information Processing with Spins in Silicon

Jason Petta[1]*
[1] *Princeton University, United States of America*

ontinuous research on electron spin qubits defined in silicon quantum dots has led to increasingly impressive levels of quantum control, with recent demonstrations of high single qubit gate fidelities and >90% two-qubit gate fidelities. Progress has been fueled by an investment in high quality Si/SiGe heterostructures, coupled with the advent of accumulation-mode device designs that are less sensitive to disorder and enable fine control over quantum dot electrons. At Princeton, we have developed a device architecture that allows for the scalable fabrication of one-dimensional silicon spin qubit arrays [1,2]. Devices fabricated on isotopically enriched ^{28}Si quantum wells allow for high fidelity control of four individually addressable spin qubits. Single qubit gate fidelities exceed 99.9% and we demonstrate ac-driven SWAP gates to transfer spin eigenstates with a fidelity of 98% [3]. The high degree of control offered by the device design allows for the transfer of a single electron across a linear array of nine quantum dots in $\sim$50 ns. With more complex control sequences we perform parallel shuttling of two and three electrons through the array [4]. As a demonstration of automated tuning of dot arrays, we use an image analysis toolbox to automate the calibration of virtual gates in these devices [5].

[1] D. M. Zajac *et al.*, Phys. Rev. Appl. **6**, 054013 (2016).
[2] D. M. Zajac *et al.*, Science **359**, 439 (2018).
[3] A. J. Sigillito *et al.*, npj Quantum Inf. **5**, 110 (2019).
[4] A. R. Mills *et al.*, Nat. Commun. **10**, 1063 (2019).
[5] A. R. Mills *et al.*, Appl. Phys. Lett. **115**, 113501 (2019).

I thank G. Burkard, M. Feldman, M. Gullans, A. Mills, A. Mounce, A. Sigillito, and D. Zajac for crucial contributions to this research. Si/SiGe wafers provided by HRL. Funded by ARO grant W911NF-15-1-0149 and the Gordon and Betty Moore Foundation through grant GBMF4535. Devices were fabricated in the Princeton University Quantum Device Nanofabrication Laboratory.

* petta@princeton.edu

Invited Talks

Quantum information processing with mechanical systems

Yiwen Chu[1*]
[1] *ETH Zürich, Switzerland*

Macroscopic mechanical objects are complex solid-state systems that are difficult to observe or control in the quantum regime. However, recent developments in coupling motion to nonlinear quantum systems have opened up the possibility of creating, measuring, and manipulating non-classical mechanical states. I will present our experiments demonstrating a high frequency bulk acoustic wave resonator that is strongly coupled to a superconducting qubit using piezoelectricity, and show how this system allows for quantum control of mechanical motion. I will then discuss prospects for using such systems as new circuit elements for quantum information processing.

* yiwenchu1@gmail.com

Tunable arrays of single Rydberg atoms for quantum simulation of spin models

Thierry Lahaye[1*]
[1] *Laboratoire Charles Fabry (CNRS UMR 8501), Institut d'Optique Graduate School, 2, avenue Augustin Fresnel F-91127 PALAISEAU Cedex - France*

Over the last years we have developed a novel platform for quantum simulation of spin Hamiltonians, using arrays of single atoms held in optical tweezers and excited to Rydberg levels to make them interact. In this talk, I'll explain how we can now create arrays of up to 200 individually-controlled atoms with almost arbitrary geometries in 1,2 and even 3 dimensions, and illustrate the quantum simulation of Ising and XY spin Hamiltonians on a variety of experiments recently performed in our lab.

* thierry.lahaye@institutoptique.fr

MIP* = RE and Tsirelson's problem

Thomas Vidick[1*]
[1] *California Institute of Technology (CALTECH), United States of America*

Boris Tsirelson in 1993 implicitly posed "Tsirelson's Problem", a question about the possible equivalence between two different ways of modeling locality, and hence entanglement, in quantum mechanics.

Recently we gave a negative answer to Tsirelson's Problem and Connes' Embedding Problem by proving a seemingly stronger result in quantum complexity theory. This result is summarized in the equation MIP* = RE between two complexity classes.

In the talk I will present and motivate Tsirelson's problem. I will then describe the ideas from complexity theory that led to the proof of MIP* = RE and how this equality implies a negative resolution of Tsirelson's Problem.

Based on joint work with Ji, Natarajan, Wright and Yuen available as arXiv :2001.04383.

* vidick@caltech.edu

Contributed Talks

Probing mixed-state entanglement with randomized measurements

Benoît Vermersch*
Univ. Grenoble Alpes, CNRS, LPMMC, 38000 Grenoble, France
Center for Quantum Physics, University of Innsbruck, Innsbruck, Austria and
Institute for Quantum Optics and Quantum Information of the Austrian Academy of Sciences, Innsbruck, Austria

Recently, protocols based on statistical correlations of randomized measurements were developed for probing synthetic quantum many-body systems, to access Rényi entropies, many-body state fidelities, out-of-time-ordered correlators (OTOCs) and topological invariants. After a general introduction to randomized measurements, I will first present our theory proposal for measuring entanglement negativity and the corresponding experimental demonstration in a ion chain implementing a Ising model with tunable-range interactions. In particular, I will show how could detect entanglement using the positive-partial transpose (PPT) criterion, and observe entanglement spreading governed by quasi-particles.

* benoit.vermersch@lpmmc.cnrs.fr

Single artificial atoms in silicon emitting at telecom wavelengths

A. Durand[1*†], W. Redjem[1*], T. Herzig[2], A. Benali[3], S. Pezzagna[2], J. Meijer[2], A. Yu. Kuznetsov[4], H. S. Nguyen[5], S. Cueff[5], J.-M. Gérard[6], I. Robert-Philip[1], B. Gil[1], D. Caliste[6], P. Pochet[6], M. Abbarchi[3], V. Jacques[1], A. Dréau[1] and G. Cassabois[1]

[1]*Laboratoire Charles Coulomb, UMR5221, Université de Montpellier and CNRS, 34095 Montpellier, France*
[2]*Division of Applied Quantum Systems, Felix-Bloch Institute for Solid-State Physics, University Leipzig, Linnéstraße 5, 04103 Leipzig, Germany*
[3]*CNRS, Aix-Marseille Université, Centrale Marseille, IM2NP, UMR 7334, Campus de St. Jérôme, 13397 Marseille, France*
[4]*Department of Physics, University of Oslo, NO-0316 Oslo, Norway*
[5]*Institut des Nanotechnologies de Lyon-INL, UMR CNRS 5270, CNRS, Ecole Centrale de Lyon, Ecully, France*
[6]*Department of Physics, IRIG, Univ. Grenoble Alpes and CEA, F-38000 Grenoble, France*

Given its unrivaled potential of integration and scalability, silicon is likely to become a key platform for large-scale quantum technologies. Individual electron-encoded artificial atoms either formed by impurities [1] or quantum dots [2] [3] have emerged as a promising solution for silicon-based integrated quantum circuits. However, single qubits featuring an optical interface needed for large-distance exchange of information [4] have not yet been isolated in such a prevailing semiconductor. In our recent works [5][6], we showed the isolation of several families of single optically-active point defects in a commercial silicon-on-insulator wafer implanted with carbon atoms. These artificial atoms exhibit a bright, linearly polarized single-photon emission in the near-infrared range and even at telecom wavelengths suitable for long-distance propagation in optical fibers. Our results demonstrate that despite its small bandgap (1.1 eV) a priori unfavorable towards such observation [7], silicon can accommodate point defects optically isolable at single scale, like in wide-bandgap semiconductors [8]. This work opens numerous perspectives for silicon-based quantum technologies, from integrated quantum photonics to quantum communications [9] and metrology.

[1] Y. He, S. Gorman, D. Keith, L. Kranz, J. G. Keizer, and M. Simmons, Nature **571**, 371 (2019).
[2] T. Watson, S. Philips, E. Kawakami, D. Ward, P. Scarlino, M. Veldhorst, D. Savage, M. Lagally, M. Friesen, S. Coppersmith, M. Eriksson, and L. Vandersypen, Nature **555**, 633 (2018).
[3] R. Maurand, X. Jehl, D. Kotekar-Patil, A. Corna, H. Bohuslavskyi, R. Laviéville, L. Hutin, S. Barraud, M. Vinet, M. Sanquer, and S. D. Franceschi, Nature Communications **7**, 13575 (2016).
[4] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. Mitchell, M. Markham, D. Twitchen, D. Elkouss, S. Wehner, T. Taminiau, and R. Hanson, Nature **526**, 682 (2015).
[5] W. Redjem*, A. Durand*, T. Herzig, A. Benali, S. Pezzagna, J. Meijer, A. Y. Kuznetsov, H. S. Nguyen, S. Cueff, J.-M. Gérard, I. Robert-Philip, B. Gil, D. Caliste, P. Pochet, M. Abbarchi, V. Jacques, A. Dréau, and G. Cassabois, arXiv :2001.02136 [cond-mat, physics :physics, physics :quant-ph] (2020).
[6] A. Durand, Y. Baron, W. Redjem, T. Herzig, A. Benali, S. Pezzagna, J. Meijer, A. Y. Kuznetsov, J.-M. Gérard, I. Robert-Philip, M. Abbarchi, V. Jacques, G. Cassabois, and A. Dréau, 2010.11068.
[7] J. Weber, W. Koehl, J. Varley, A. Janotti, B. Buckley, C. Van de Walle, and D. Awschalom, Proceedings of the National Academy of Sciences **107**, 8513 (2010).
[8] I. Aharonovich, D. Englund, and M. Toth, Nature Photonics **10**, 631 (2016).
[9] X. Qiang, X. Zhou, J. Wang, C. Wilkes, T. Loke, S. O Gara, L. Kling, G. Marshall, R. Santagati, T. Ralph, J. Wang, J. O'Brien, M. Thompson, and J. Matthews, Nature Photonics **12**, 534 (2018).

* Equal contributions

† alrik.durand@umontpellier.fr

Unscrambling entanglement through a complex medium

Natalia Herrera Valencia[1], Suraj Goel[1,2], Will McCutcheon[1], Hugo Defienne[3,*] and Mehul Malik[1]
[1]*Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh, UK*
[2]*Indian Institute of Technology Delhi, New Delhi, India*
[3]*School of Physics and Astronomy, University of Glasgow, Glasgow, UK*

The transfer of quantum information through a noisy environment is a central challenge in the fields of quantum communication, imaging, and nanophotonics. In particular, high-dimensional quantum states of light enable quantum networks with significantly higher information capacities and noise-robustness as compared with qubits [1]. High-dimensional entanglement can also tolerate large amounts of loss in loophole-free tests of nonlocality, holding immense potential for the realisation of device-independent quantum communication. However, while qubit-entanglement has been distributed over large distances through free-space and fibre, the transport of high-dimensional entanglement is hindered by the complexity of the channel, which encompasses effects such as free-space turbulence or mode-mixing in multi-mode waveguides. Here we demonstrate the transport of six-dimensional spatial-mode entanglement through a two-metre long, commercial multi-mode fibre with 84.43% fidelity [2]. We show how the entanglement can itself be used to measure the transmission matrix of the complex medium, allowing the recovery of quantum correlations that were initially lost [3]. Using a unique property of entangled states, the medium is rendered transparent to entanglement by carefully "scrambling" the photon that did not enter it, rather than unscrambling the photon that did. Our work overcomes a primary challenge in the fields of quantum communication and imaging, and opens a new pathway towards the control of complex scattering processes in the quantum regime.

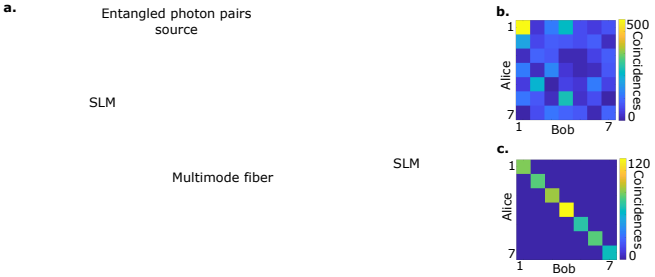


FIGURE 1: **Schematic of the experiment. a**, High-dimensional spatially entangled photon pairs are produced by SPDC in a non-linear crystal. One photon of the pair is sent towards Bob using a 2-m-long commercial MMF, while its twin photon is detected by Alice. Combinations of spatial light modulators (SLM) and single-pixel photodetectors measure coincidences between spatial modes of photons. Alice's SLM is also used to compensate for the complex mode mixing process occurring in the fibre at Bob's end using the transmission matrix of the system previously measured by the entanglement itself. Without such compensation, no particular correlations are found **(b)** between spatial modes of photon pairs because they have been mixed in the multimode fiber. Strong correlations are retrieved when applying the compensation process on Alice's SLM **(c)**.

[1] Erhard, M., Krenn, M., and Zeilinger, A. "Advances in high-dimensional quantum entanglement", Nature Reviews Physics, 1-17. (2020)
[2] Bavaresco, J., Valencia, N. H., Klöckl, C., Pivoluska, M., Erker, P., Friis, N., Mehul, M. and Huber, M. "Measurements in two bases are sufficient for certifying high-dimensional entanglement". Nature Physics, 14(10), 1032-1037. (2018)
[3] Popoff, S. M., Lerosey, G., Carminati, R., Fink, M., Boccara, A. C., and Gigan, S. "Measuring the transmission matrix in optics : an approach to the study and control of light propagation in disordered media", Physical review letters, 104(10), 100601. (2010)
Associated publication : Valencia, N. H., Goel, S., McCutcheon, W., Defienne, H. and Malik, M. "Unscrambling entanglement through a complex medium", Nature Physics, 1-5. (2020)

* Presenter email : hugo.defienne@glasgow.ac.uk

Adiabatic spin-dependent momentum transfer in an SU(N) degenerate Fermi gas

Pierre Bataille[1], Andrea Litvinov[1], Isam Manai[1], John Huckans[2], Fabrice Wiotte[1], Albert Kaladjian[1], Olivier Gorceix[1], Etienne Maréchal[1], Bruno Laburthe-Tolra[1], and Martin Robert-de-Saint-Vincent[1*]

[1] *Laboratoire de Physique des Lasers, CNRS, UMR 7538, Université Sorbonne Paris Nord, F-93430 Villetaneuse, France*

[2] *Department of Physics and Engineering, Bloomsburg University, Bloomsburg, Pennsylvania*

For the study of strongly correlated fermionic systems, ultracold alkaline-earth atoms offer original possibilities with their large ground-state spin and spin-independent collisions (SU(N) symmetry). The nuclear nature of the spins is both a strength and a complication – for example as it prevents the simple use of magnetic forces as in a Stern-Gerlach measurement. Nevertheless, the narrow lines associated with their singlet-to-triplet transitions can be used for novel spin-sensitive manipulations schemes, e.g. effective magnetic fields as in the "Optical Stern-Gerlach" (OSG) scheme [1], and spin-orbit coupling with low levels of spontaneous emission [2].

In our experiment [3], we introduce a spin-orbit coupling scheme where a retro-reflected laser beam selectively diffracts two spin components of a degenerate Fermi gas in opposite directions. Spin sensitivity is provided by sweeping through a magnetic-field sensitive transition : the inter-combination line of strontium 87. The atoms follow adiabatically dark states, which significantly suppresses spontaneous emission. The adiabaticity of the scheme makes it inherently robust. We furthermore demonstrate a generalization of the scheme, and diffract in a single shot four spin states with four different momentum transfers. The spin-orbit coupling is associated with well-defined momentum transfers, set by the two-photon recoil, such that, unlike in OSG, momentum distortion is negligible. Thus, this scheme allows simultaneous measurements of the spin and momentum distributions of a strontium degenerate Fermi gas, opening the path to momentum-resolved spin correlation measurements [4] on SU(N) quantum magnets.

[1] S. Taie et. al., Phys. Rev. Lett. **105**, 190401 (2010).
[2] B. Song et. al., Phys. Rev. A **94**, 061604(R) (2016).
[3] P. Bataille et. al., Phys. Rev. A **102**, 013317 (2020).
[4] G. M. Bruun et. al., Phys. Rev. A **80**, 033622 (2009).

* martin.rdsv@univ-paris13.fr

Strongly correlated materials via embedding methods: solving impurity models with a noisy quantum computer

Pauline Besserve[1,2*] and Thomas Ayral[1]
[1]*Atos Quantum Laboratory, Les Clayes-sous-Bois, France*
[2]*Centre de Physique Théorique, CNRS, Ecole Polytechnique, Institut Polytechnique de Paris, Palaiseau, France*

Modelling materials exhibiting strong electronic correlations is a notoriously difficult task as static mean field treatments are not able to capture typical many-body effects. A powerful way to address such systems are so-called embedding methods, retaining correlations on a few 'impurity' orbitals only. Yet, classical computers still reach their limits in this context as they are faced with either an exponential scaling or the fermionic sign problem.

In this work, we investigate a hybrid quantum-classical approach using a Noisy Intermediate-Scale Quantum (NISQ) computer to sort out the ground state properties of these impurity models. Such a hybrid impurity solving scheme is used to study the Hubbard model at equilibrium via embedding methods.

We prepare approximations to the impurity ground states with a shallow parametrized circuit ansatz. The best parametrization is obtained using the Variational Quantum Eigensolver (VQE) algorithm, minimizing the expectation value of the impurity Hamiltonian over circuit instances. We simulate the realistic execution of state-of-the-art hybrid embedding schemes and go beyond impurity sizes reached in previous studies leveraging Atos' simulator, the Quantum Learning Machine. Device parameters are chosen to mirror the performances of a current superconducting backend, and our model accounts for a large variety of noise sources: shot noise, decoherence along the circuit, gate errors and readout error. An error mitigation technique is incorporated to the computation. Under these realistic conditions, we gain quantitative insight into the challenge of scaling up the impurity size: the necessary tradeoff between escaping prohibitive error levels through limited circuit depths on the one hand, and reaching sufficient ground state expressibility at the expense of large circuit depths on the other hand.

* pauline.besserve@atos.net

A SNAIL Travelling Wave Parametric Amplifier

Arpit Ranadive[1], Martina Esposito[1], Luca Planat[1], Edgar Bonet[1],
Cécile Naud[1], Olivier Buisson[1], Wiebke Guichard[1], Nicolas Roch[1]*
[1] *Université Grenoble Alpes, CNRS, Grenoble INP, Institut Néel, 38000 Grenoble, France*

Superconducting parametric amplifiers can provide quantum noise limited amplification of weak microwave signals and constitute a remarkable resource for quantum technologies and quantum information science [1].
We present the experimental demonstration of a novel Travelling Wave Parametric Amplifier (TWPA) composed of an array of superconducting nonlinear asymmetric inductive elements (SNAILs). The asymmetry in the SNAILs allows to change the sign of the Kerr non-linearity by tuning an external magnetic flux. As predicted by Bell & Samolov [2], we demonstrate the use of Kerr sign reversal to obtain the phase matching condition for four wave mixing amplification with no need of gap engineering in the dispersion relation.
In contrast to previously demonstrated TWPAs [3–5], the absence of gaps in transmission allows continuous amplification band with significantly lower gain ripples. Also, it provides in-situ tunability of the amplification band over an unprecedented large dynamic range (gain larger than 15 dB is observed in the entire 4-12 GHz range) by simply changing the pump frequency. The latter constitute a notable advantage with respect to previous state of the art TWPAs [3–6] where the pump frequency is constrained by the dispersion engineering approach. We achieve near quantum limited amplification with up to 4 GHz bandwidth and -98 dBm saturation at 20 dB gain.
We will present the design, fabrication and the gain/noise characterization of the SNAIL TWPA and discuss the advantages of our novel phase-matching approach for applications in circuit-QED.

[1] J. Aumentado, Superconducting parametric amplifiers : The state of the art in josephson parametric amplifiers, IEEE Microwave Magazine **21**, 45 (2020).
[2] M. T. Bell and A. Samolov, Traveling-Wave Parametric Amplifier Based on a Chain of Coupled Asymmetric SQUIDs, Phys. Rev. Applied **4**, 10.1103/PhysRevApplied.4.024014 (2015).
[3] B. Ho Eom, P. K. Day, H. G. Leduc, and J. Zmuidzinas, A wideband, low-noise superconducting amplifier with high dynamic range, Nature Physics **8**, 623 (2012), arXiv :1201.2392.
[4] C. Macklin, K. O'Brien, D. Hover, M. E. Schwartz, V. Bolkhovsky, X. Zhang, W. D. Oliver, and I. Siddiqi, A near – quantum-limited Josephson traveling-wave parametric amplifier, Science **350**, 307 (2015).
[5] L. Planat, A. Ranadive, R. Dassonneville, J. Puertas Martínez, S. Léger, C. Naud, O. Buisson, W. Hasch-Guichard, D. M. Basko, and N. Roch, Photonic-Crystal Josephson Traveling-Wave Parametric Amplifier, Physical Review X **10**, 10.1103/PhysRevX.10.021021 (2020).
[6] M. Malnou, M. R. Vissers, J. D. Wheeler, J. Aumentado, J. Hubmayr, J. N. Ullom, and J. Gao, A three-wave mixing kinetic inductance traveling-wave amplifier with near-quantum-limited noise performance, arXiv :2007.00638 (2020), arXiv :2007.00638v1.

* arpit.ranadive@neel.cnrs.fr

Limitations in quantum computing from resource constraints

Marco Fellous Asiani[1], Jing Hao Chai[2], Robert S. Whitney[3], Alexia Auffèves[1], Hui Khoon Ng[4,2,5]
[1] *Institut Néel, Grenoble, France*
[2] *Centre for Quantum Technologies, National University of Singapore, Singapore*
[3] *Laboratoire de Physique et Modélisation des Milieux Condensés, Université Grenoble Alpes and CNRS, BP 166, 38042 Grenoble, France.*
[4] *Yale-NUS College, Singapore*
[5] *MajuLab, International Joint Research Unit UMI 3654, CNRS, Université Côte d'Azur, Sorbonne Université, National University of Singapore, Nanyang Technological University, Singapore*

Fault-tolerant quantum computation is the only known route to large-scale, accurate quantum computers. Fault tolerance schemes prescribe how, by investing more physical resources and scaling up the size of the computer, we can keep the computational errors in check and carry out more and more accurate calculations. Underlying all such schemes is the assumption that the error per physical gate is independent of the size (number of qubits/gates) of the quantum computer. This, unfortunately, is not reflective of current quantum computing experiments [1], [2] where the error typically grows with computer size. Here, we examine the general consequences of this fact on fault-tolerant quantum computation. We then focus on the example being when constraints on available physical resources result in physical error rates that grows as the computer grows. In all those cases, fault tolerance schemes can no longer reduce computational error to an arbitrarily small number, even if one starts below the so-called fault tolerance noise threshold. Instead, there is a minimum attainable computational error, beyond which further growth of the computer in an attempt to reduce the error becomes counter-productive. We discuss simple, but rather generic, situations in which this effect can arise, one example being when the available energy to perform the gates is assumed to be limited, and we highlight the areas of future developments needed for experiments to overcome this limitation.

[1] C. Monroe. J. Kim. Scaling the ion trap quantum processor. Science 339, 1164–1169 (2013).

[2] Ikonen, J., Salmilehto, J. & Möttönen, M. Energy-efficient quantum computing. npj Quantum Inf 3, 17 (2017).

Cavity Protected Polaritons in a Cold Atom Ensemble

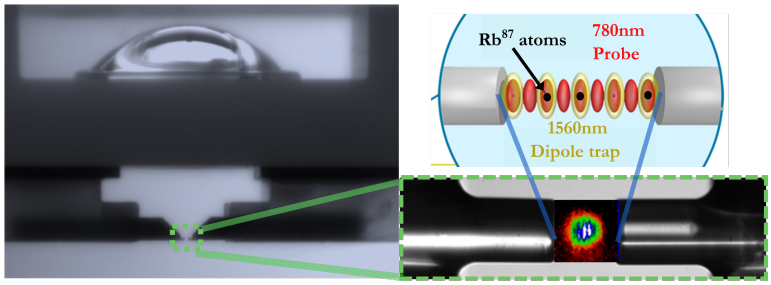
Pierre-Antoine Bourdel[1], Mohamed Baghdad[1], Sylvain Schwartz[1], Francesco Ferri[1], Jakob Reichel[1] and Romain Long[1]
[1] *Laboratoire Kastler Brossel, ENS-Université PSL, CNRS, Sorbonne Université, Collège de France, 24 rue Lhomond, 75005 Paris, France*

Controlling and characterizing entanglement in large quantum systems is an exciting challenge of modern physics. Along this line, we have built a CQED platform where cold rubidium atoms are strongly coupled to a fiber-based Fabry-Perot cavity under a high-numerical aperture lens. The coupling between the atomic qubits and the cavity generates multiparticle entanglement, while the microscope is meant to allow for single-qubit manipulation and readout. To achieve maximal and homogeneous coupling of the atomic ensemble to the 780nm cavity mode, we use an intracavity lattice trap at 1560nm.

Because of the strong differential lightshifts induced by the 1560nm light, our qubit ensemble has a very large frequency inhomogeneous broadening. Thus, when probing the atoms-cavity coupled system, we could expect to detect multiple eigenfrequencies. Instead we observe two very narrow polariton peaks, as if we probed a frequency-homogeneous system. This effect, called cavity protection, occurs for strong collective coupling of the atoms to the cavity [1][2][3]. It was experimentally observed in the microwave domain with spin nitrogen vacancy centers [4] and in the optical domain with rare earth ions in crystals [5].

Here, we report the first significant reduction, by a factor of 5, of the width of the polaritons with respect to their width in absence of cavity protection. Moreover, because we achieve strong coupling at the single qubit level, we characterize finely the transition from the unprotected regime to the cavity-protected regime by varying the number of atoms at a mesoscopic scale (a few tens), several orders of magnitude lower than previous experiments. This allows us to capture the essence of cavity protection : for increasing collective coupling, the number of states coupled to the cavity field gradually decreases. In the protected regime, only the two bright polaritonic states are coupled to the cavity, preserving the coherence of the coupled system.

Finally, using the high sensitivity of the light-shifted atomic frequency to the 1560nm dipole trap power, we modulate the polariton frequencies very efficiently. We thus demonstrate a frequency modulated Rabi splitting, which increases the number of available frequencies of the system while still being cavity protected. This could have applications for quantum memories and quantum communications.



Left : Fiber Fabry-Perot cavity, high-numerical aperture lens, 6 mm above the cavity.
Bottom-right : zoom on the cavity, superimposed with an aborption image of the cloud of atoms inside the cavity.
The distance between the two fibers is of 135 μm.

[1] R. Houdré *et al*, Phys. Rev. A, **53**, 2711 (1996).
[2] I. Diniz *et al*, Phys. Rev. A, **84**, 063810 (2011).
[3] Z. Kurucz, Phys. Rev. A, **83**, 053852 (2011)
[4] S. Putz *et al*, Nature Phys., **10**, 720 (2014)).
[5] T. Zhong *et al*, Nat Comm., **8**, 14107 (2017).

Scalable device-independent certification of many-body entanglement using statistical inference

Tommaso Roscilde[1], Irénée Frérot[2*]
[1]*Laboratoire de Physique, Ecole Normale Supérieure de Lyon, Lyon (France)*
[2]*Institute of Photonic Sciences (ICFO), Barcelona (Spain)*

Many-body entanglement is the basis of the fundamental quantum advantage potentially offered by future devices, such as many-body quantum sensors, quantum processors and quantum simulators. A scalable and robust certification of entanglement is therefore central to the assessment of quantum devices. The most reliable approach in this context is the device-independent one, relying uniquely on the input settings and on the output of the quantum device, and fundamentally based on the violation of Bell inequalities. Devising relevant Bell inequalities which are violated by entangled many-body quantum states is generically considered to be a hard problem, scaling exponentially in the number of degrees of freedom.

Here we present a variational algorithm which, given a set of quantum data (typically correlation functions for the output elements of the quantum device), builds explicitly the local-variable theory by solving a so-called “inverse Ising problem", namely by finding the best approximation to the quantum data via the Boltzmann equilibrium state of an Ising model (in the case of binary outputs - easily generalizable to other classical statistical physics models in the case of richer outputs). If the local-variable theory fails to reproduce the quantum data within their precision, then the method outputs explicitly the Bell inequality which is maximally violated by a linear combination of the quantum data, thereby detecting non-locality. This data-driven approach has by construction a computational cost scaling polynomially with system size, and it is therefore fully scalable.

We demonstrate its effectiveness by discovering new Bell inequalities violated by paradigmatic quantum states with an arbitrary number of qubits, of central relevance for the quantum simulation of quantum magnetism - namely the low-temperature states of quantum Heisenberg antiferromagnets in arbitrary spatial dimensions [1].

[1] I. Frérot and T. Roscilde, arXiv :2004.07796 (2020).

* tommaso.roscilde@ens-lyon.fr

How to hack 2 048 RSA code with 8 100 qubits and a multimode memory with 2 hours storage time ?

Élie Gouzien* and Nicolas Sangouard
Institut de physique théorique, CEA, CNRS, Université Paris-Saclay, 91191, Gif-sur-Yvette, France

The RSA cryptosystem is widely used for securing Internet communications. Its security relies on the difficulty to factor a number N written with n bits and product of two similar sized prime numbers. In particular, the complexity of best known classical factorization algorithm, the general number field sieve, is supra-polynomial, of the order of $2^{\left[(64/9)^{1/3}+o(1)\right]n^{1/3}(\log n)^{2/3}}$. On the contrary, Shor's algorithm and its variants allow factorizing N with complexity of the order $O\left(n^3\right)$ [1, 2]. The exponential speedup given by the Shor's algorithm makes it unique and since multiplying even large integers is computationally easy, the outcome of this algorithm can be checked. Hacking RSA with a newly implemented quantum computer would not only show a strong form of quantum supremacy but would also be useful to confirm the proper functioning of this quantum computer.

Since Shor's initial article [1], a lot of progress have been accomplished both on the algorithmic and hardware parts [2–5]. Recently, efforts have been dedicated to facilitate its implementation with superconducting qubits laid on 2D grid [6–8], leading to the result that it should be feasible to factor 2 048 bits RSA numbers with a 2D grid of 20 millions superconducting qubits in 8 hours [9].

Inspired by the classical computing architectures, we here study the potential of an architecture combining a relatively small processor with a large multimode quantum memory. Such an architecture allows loading only few qubits into the processor at a given time, hence reducing its size. It also increases the coherence time of untouched qubits which reduces the requirements on error correction. Full connectivity can also be reached by loading arbitrary qubits into the processor, thus allowing us to use faster algorithm and, more important, to choose an error correction code allowing fault-tolerant implementation of a universal set of gates, hence avoiding magic states distillation and gate teleportation that are needed in standard 2D surface codes. By using Ekerå and Håstad's variant of Shor's algorithm [2], windowed arithmetic circuits [3], coset representation of integers for the modular additions [10] and 3D gauge colour codes [11–13], we show that factorizing a 2 048 bits RSA numbers would be possible with a 2D grid of 8 100 superconducting qubits and a multimode quantum memory with 2 hours storage time in 176 days.

[1] P. W. Shor, in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (IEEE Comput. Soc. Press, 1994) pp. 124–134.
[2] M. Ekerå and J. Håstad, in *Post-Quantum Cryptography*, Lecture Notes in Computer Science, Vol. 10346, edited by T. Lange and T. Takagi (Springer International Publishing, 2017) pp. 347–363, 1702.00249.
[3] C. Gidney, "Windowed quantum arithmetic," (2019), 1905.07682.
[4] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt, Science **351**, 1068 (2016), 1507.08852.
[5] M. Kjaergaard, M. E. Schwartz, J. Braumüller, P. Krantz, J. I.-J. Wang, S. Gustavsson, and W. D. Oliver, Annual Review of Condensed Matter Physics **11**, 369 (2020), 1905.13641.
[6] C. Gidney and A. G. Fowler, "Flexible layout of surface code computations using autoccz states," (2019), 1905.08916.
[7] A. G. Fowler and C. Gidney, "Low overhead quantum computation using lattice surgery," (2019), 1808.06709.
[8] C. Gidney and A. G. Fowler, Quantum **3**, 135 (2019), 1812.01238.
[9] C. Gidney and M. Ekerå, "How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits," (2019), 1905.09749.
[10] C. Gidney, "Approximate encoded permutations and piecewise quantum adders," (2019), 1905.08488.
[11] H. Bombín, New Journal of Physics **17**, 083002 (2015), 1311.0879.
[12] H. Bombín, Physical Review X **5**, 031043 (2015), 1404.5504.
[13] A. M. Kubica, *The ABCs of the Color Code: A Study of Topological Quantum Codes as Toy Models for Fault-Tolerant Quantum Computation and Quantum Phases Of Matter*, Ph.D. thesis (2018).

* elie.gouzien@cea.fr

Computational advantage from quantum superposition of multiple temporal orders of gates

Márcio M. Taddei[1], Jaime Cariñe[2,3,4], Daniel Martínez[2,3], Tania García[2,3], Nayda Guerrero[2,3], **Alastair A. Abbott**[5], Mateus Araújo[6], Cyril Branciard[7], Esteban S. Gómez[2], Stephen P. Walborn[2,3], Leandro Aolita[1], Gustavo Lima[2,3]

[1]*Instituto de Física, Federal University of Rio de Janeiro, Rio de Janeiro, Brazil*
[2]*Departamento de Física, Universidad de Concepción, Concepción, Chile*
[3]*Millennium Institute for Research in Optics, Universidad de Concepción, Concepción, Chile*
[4]*Departamento de Ingeniería Eléctrica, Universidad Católica de la Santísima Concepción, Concepción, Chile*
[5]*Department of Applied Physics, University of Geneva, Geneva, Switzerland*
[6]*Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Vienna, Austria*
[7]*Univ. Grenoble Alpes, CNRS, Grenoble INP, Institut Néel, Grenoble, France*

Quantum mechanics allows for processes where two or more events take place in a quantum superposition of different temporal orders. This possibility leads to the exotic phenomenon of causal indefiniteness [1], which is not only of interest from a foundational perspective, but also opens up new possibilities for quantum information processing. In standard quantum computational models, for example, the gate ordering is assumed to be fixed, and computations without definite gate orders do not fit within this paradigm. The best known example of a causally indefinite circuit is the celebrated quantum N-switch, S_N, which coherently applies a different permutation of N given gates on a target quantum system conditioned on the state of a control quantum system [2, 3]. S_N has been identified as a resource for a number of exciting information-theoretic tasks. For instance, for $N = 2$, it allows one to deterministically distinguish pairs of commuting versus anti-commuting unitaries [4].

The quantum N-switch is known to provide a quadratic advantage in a particular oracle problem over all known circuits with fixed gate order [3]. However, the formulation of this problem requires the target-system dimension that grows (super-)exponentially in N, making it experimentally intractable. In fact, all experimental realizations of the quantum N-switch reported thus far have treated only simplest case of $N = 2$ gate orders (see, e.g., [5]).

In this contribution, we introduce a novel algorithm that exploits the quantum N-switch and experimentally demonstrate it for $N = 4$ unitary gates [6]. Specifically, we develop a problem, which we name the Hadamard promise problem, that the quantum switch can solve efficiently and which, in contrast to previously reported problems, can be demonstrated with a qubit target system for all N. We show that the quantum N-switch provides a quadratic advantage in query complexity over all known algorithms exploiting circuits with fixed gate orders, and develop theoretical techniques to bound the probability of success of causally definite circuits for a given number of permissible queries. The algorithm is thus not only an interesting computational primitive on its own but also a practical tool to benchmark experimental realizations of S_N.

To demonstrate the practicability of the algorithm we implement it with a quantum N-switch of $N = 4$ gates using modern multi-core optical-fiber technology. The 4 gates are implemented on the target polarization qubits using programmable liquid-crystal devices, and the spatial degree of freedom of a single photon is used as the control system. We obtain an average success probability for the algorithm, over different sets of gates, of $p_{\text{succ}} \approx 0.95$, higher than the optimal probability of success obtainable with 4 queries using a quantum circuit with a causally definite gate order. Our results represent the first demonstration of the quantum N-switch for N larger than 2, as well as of its efficiency for phase estimation problems involving multiple unknown gates.

[1] O. Oreshkov, F. Costa, and Č. Brukner, Nature Communications **3**, 1092 (2012), arXiv:1105.4464.
[2] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Physical Review A **88**, 022318 (2013).
[3] M. Araújo, F. Costa, and Č. Brukner, Physical Review Letters **113**, 250402 (2014).
[4] G. Chiribella, Physical Review A **86**, 040301(R) (2012).
[5] K. Goswami and J. Romero, AVS Quantum Sci **2**, 037101 (2020).
[6] M. M. Taddei, J. Cariñe, D. Martínez, T. García, N. Guerrero, A. A. Abbott, M. Araújo, C. Branciard, E. S. Gómez, S. P. Walborn, L. Aolita, and G. Lima, (2020), arXiv:2002.07817 [quant-ph].

Fundamental Quantum Aspects (FQA)

Fast high fidelity qubit readout of a transmon molecule using longitudinal coupling

Remy Dassonneville[1], Tomás Ramos[2,3], Vladimir Milchakov[1], Luca Planat[1], Etienne Dumur[1], Farshad Foroughi[1], Javier Puertas[1], Sebastian Leger[1] Karthik Bharadwaj[1], Jovien Delaforce[1], Cecile Naud[1], Wiebke Hash-Guichard[1], Juanjo Garcia Ripoll[2], Nicola Roch[1], and Olivier Buisson[1],*

[1]*Univ.Grenoble-Alpes, CNRS, Grenoble INP, Institute Neel, 38000 Grenoble, France*

[2]*Instituto de Fısica Fundamenta ,IFF-CSIC Calle Serrano 113b, 28006 Madrid, Spain*

[3]*DAiTA Lab, Facultad de Estudios Interdisciplinarios, Universidad Mayor, Santiago, Chile*

The most common technique of qubit readout in cQED relies on the transverse dispersive coupling between a qubit and a microwave cavity. However, despite important progresses, implementing fast high fidelity readout remains a major challenge. Indeed, inferring the qubit state is limited by the trade-off between speed and accuracy due to Purcell effect and unwanted transitions induced by readout photons in the cavity. To overcome this we introduce a transmon molecule based on two transmons coupled by a large inductance, which is inserted inside a 3D-cavity.

The full system presents one transmon –used as qubit– with a large direct crossKerr(longitudinal) coupling to a non-linear readout resonator, called polaron mode. This polaron mode results from the hybridization between the microwave cavity and the second mode of the transmon molecule circuit. The direct cross-Kerr coupling is a key point of our readout scheme since it protects the qubit from Purcell effect. We will present qubit readout performance with fidelity as high as 95.7% in 120ns and discuss the quantum non-demolition properties of this novel readout.

[1] R. Dassonneville, T. Ramos, and V. Milchakov, "Fast High-Fidelity Quantum Nondemolition Qubit Readout via a Non-perturbative Cross-Kerr Coupling", Phys. Rev. X. **10**, 011045 (2020).

* vladimir.milchakov@neel.cnrs.com

A Gödelian Hunch from Quantum Theory - IQFA Quantum Abstract

Hippolyte Dourdent[1]*
[1]*Institut Néel, CNRS, Univ. Grenoble-Alpes, 38000 Grenoble, France*

Quantum theory does not only defy common sense. It also defies classical logic, i.e. our common language and semantic. In this sense, quantum theory is more paradoxical than other physical theories. Still, classical logic itself is not immune to paradoxes, as self-referring propositions can lead to pathologies such as the well-known Liar paradox "This sentence is false." Because it features an over-determination - if the sentence is true then it is false, if it is false then it is true - the "Liar" leads to undecidability, the impossibility to decide whether the sentence is true or false. Analogs have been famously used in the foundations of mathematical logic, from Russell's paradox to Gödel's incompleteness theorem.

But is Nature itself paradoxical ? Does the world really feature intrinsically strange phenomena that cannot be grasped with our words, whether it is a non-local behaviour or parallel worlds ? In [1], Szangolies coined the expression "Gödelian hunch" to describe "the idea that the origin of the peculiarities surrounding quantum theory lie in phenomena related, or at least similar, to that of incompleteness in formal systems." What if the paradoxical nature of quantum theory could find its source in some undecidability analog to the one emerging from the Liar ? In this work [2], we argue for such quantum Gödelian hunch. Quantum paradoxes are not physical, but arise from a lack of "metaphysical distancing". This idea is illustrated via two case studies : quantum contextuality as an instance of the Liar-like logical structure of quantum propositions ; and the measurement problem as a self-referential problem.

Quantum contextuality results from a theorem established by Kochen and Specker [3], which shows that a quantum measurement cannot reveal a pre-existing value of a measured property independently of the measurement context. In a topological generalization of this result [4], the logical structure of quantum contextuality is compared to sequences of cyclically referring statements, "Liar cycles", which, associated with a truth predicate, lead to a logical contradiction. As an example, the Hardy paradox [5] can be shown to entail such a Liar-like logical structure.

The measurement problem is often presented as a tension between the linear and deterministic evolution of the wave-function following the Schrödinger equation and the projection postulate. Nevertheless, the problem was also analyzed as emerging from a self-referential logical error. I will introduce the notion of "meta-contextuality" as a Liar-like feature underlying this analysis for the measurement problem, the related Wigner's friend thought experiment and a recent paradox by Frauchiger and Renner [6]. These paradoxes are avoided by interpretations, such as Rovelli's relational quantum mechanics [7], that feature meta-contextuality, i.e. acknowledge the need for a distinction between meta-theoretical and theoretical objects when one uses quantum theory.

Finally, this quantum Gödelian hunch opens a discussion on the emergence of time itself from self-contradiction.

Third prize winner in the FQXi Essay Contest 2020.

[1] J. Szangolies, "Epistemic Horizons and the Foundations of Quantum Mechanics", Found Phys **48**, 1669–1697 (2018).
[2] H. Dourdent, "A Gödelian Hunch", arXiv :2005.04274 [quant-ph] (2020).
[3] S. Kochen, E. Specker, "The Problem of Hidden Variables in Quantum Mechanics", J. of Math. and Mech. **1**, 59-87 (1967).
[4] S. Abramsky, S. Mansfield, R.S. Barbosa, "The Cohomology of Non-Locality and Contextuality", EPTCS **95**, 1-14 (2012).
[5] L. Hardy, "Nonlocality for two particles without inequalities for almost all entangled states", Phys. Rev. Lett. **71**, 1665 (1993).
[6] D. Frauchiger, R. Renner, "Quantum theory cannot consistently describe the use of itself", Nat Commu **9**, 3711 (2018).
[7] C. Rovelli, "Relational Quantum Mechanics", Int. J. of Theor. Phys. **35**, 1637 (1996).

* hippolyte.lazourenko-dourdent@neel.cnrs.fr

Excitation using longitudinal acoustic phonons of a solid-state fibred single photon source

M. BILLARD[1,2*], S.E. THOMAS[2], F. PASTIER[1], M. ESMANN[2], A. BRIEUSSEL[1], V. GIESZ[1], N. SOMASCHI[1], O. KREBS[2] and P. SENELLART[2*]

[1] *Quandela, 10 Boulevard Thomas Gobert, 91120 Palaiseau, France*

[2] *Centre de Nanosciences et de Nanotechnologies (C2N), 10 Boulevard Thomas Gobert, 91120 Palaiseau, France*

Over the last decade, the constant improvement in performance of solid-state single photon sources has established them as a prime candidate for quantum optics experiments where high flux of pure single photons is required [1]. Individual quantum dots (QD) coupled to optical micropillar cavities are now able to produce a high rate stream of pure and indistinguishable single photons [2, 3] required for applications such as quantum computing [4, 5] or long-distance communications [6]. The growing interest in commercially available single photon sources motivated the development of techniques to get practical bright emitters. In this context, we worked on fibred sources and on the QD emission properties under longitudinal acoustic phonon excitation regime [7–9]. In these conditions, efficient sources harness the power of state-of-the-art QD devices, while also improving the ease-of-use for non-expert users.

Here, we present the use of longitudinal acoustic phonon excitation regime to get bright polarised single photons sources [10]. By exciting a linear dipole with a detuned laser, we demonstrated a polarisation purity of 99.4%±0.7%. Since the laser is spectrally filtered, all the emitted photons are collected. This overcomes the intrinsic limitation due to the cross-polarisation selection required in resonant fluorescent experiments. In comparison with this excitation regime, we demonstrated a relative reduction of the excited state probability by around 15%. Nevertheless, the first lens brightness reached 51%±1%. Eventually, with a purity of 93.9%±0.1% and an indistinguishability of 91.5%±0.3%, this excitation regime enables to get a bright source of single and indistinguishable photons.

The need to have a practical bright source also motivated the development of low losses and high stability optical systems. The current confocal microscope to use the source in free-space and under LA-phonon assisted excitation has then a total transmission about 45% and is mechanically stable over several days. Thus, it is already available for the use of single-photon sources commercialized by Quandela. To provide a complete plug-and-play single photon source, without needing a low-vibration cryostat and an optical table, we are working on a fibred source where a single-mode fiber is attached to a single pillar [11, 12]. A new version of the system has been developed and the first results are promising. We have already proven an efficiency as high as in the free-space excitation and new developments are underway to improve the process. The way to fixed precisely the fibre above a pillar is still in progress and compact cryostat are under study to cool the source at least at 40K. The next Quandela product will be a bright fibred single photon source in a compact, stable, and "plug and play" system which fit in racks.

[1] B. Lounis et al., Rep. Prog. Phys. **68**, 1129-1179 (2005).
[2] N. Somaschi, et al., Nature Photonics **10**, 340–345 (2016)
[3] H. Ollivier, et al., ACS Photonics 7,1050-1059 (2020)
[4] S. Slussarenko, et al., Appl. Phys. Rev. 6, 041303 (2019).
[5] J. Wang, J., et al., Nature Photonics 14, 273284 (2020)
[6] K. Takemoto, et al., Scientific Reports 5, 14383 (2015)
[7] A. Barth et al., Phys. Rev. B 94 (2016)
[8] M. Cosacchi, et al., Phys. Rev. Lett. 123, 017403 (2019)
[9] C. Gustin, et al., Advanced Quantum Technologies 3, 1900073 (2020)
[10] S.E. Thomas, et al., https://arxiv.org/abs/2007.04330v2 (2020)
[11] K. Żołnacz, et al., Optics Express, 27, 19 (2019)
[12] H.J. Snijders, et al., Phys. Rev. Applied 9, 031002 (2018)

* marie.billard@quandela.com

Non-locality and Entanglement Detection with Mermin polynomials for Grover's algorithm and Quantum Fourier Transform*

Henri de Boutray[1,2], Hamza Jaffali[1,2], Frédéric Holweck[1,3], Alain Giorgetti[1,2] & Pierre-Alain Masson[1,2]
[1]*Univ. Bourgogne Franche-Comté (UBFC)*
[2]*Institut FEMTO-ST (UMR 6174 - CNRS/UBFC/UFC/ENSMM/UTBM)*
[3]*Laboratoire Interdisciplinaire Carnot de Bourgogne (ICB, UMR 6303)*

The non-locality and thus the presence of entanglement of a quantum system can be detected using Mermin polynomials. This gives us a means to study non-locality evolution during the execution of quantum algorithms. We first consider Grover's quantum search algorithm, noticing that states during the execution of the algorithm reach a maximum for an entanglement measure when close to a predetermined state, which allows us to search for a single optimal Mermin operator and use it to evaluate non-locality through the whole execution of Grover's algorithm. The Quantum Fourier Transform is also studied with Mermin polynomials. A different optimal Mermin operator is searched for at each execution step, since in this case nothing hints us at finding a predetermined state maximally violating the Mermin inequality.

* Corresponding author: henri.de_boutray@univ-fcomte.fr.

This work is supported by the French Investissements d'Avenir program, project ISITE-BFC (contract ANR-15-IDEX-03), and by the EIPHI Graduate School (contract ANR-17-EURE-0002). The computations have been performed on the supercomputer facilities of the Mésocentre de calcul de Franche-Comté.

A Qubit Route to the Psychological Arrow of Time and Beyond

Robert S. Whitney[1]*
[1] *Laboratoire de Physique et Modélisation des Milieux Condensés (UMR 5493), Université Grenoble Alpes and CNRS, Maison des Magistères, BP 166, 38042 Grenoble, France.*

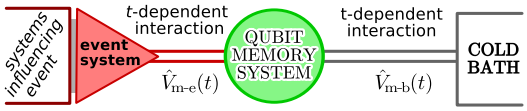
THE PSYCHOLOGICAL ARROW OF TIME

Stephen Hawking [1, 2] defined the psychological arrow of time as pointing from a past *that we can remember* to an unknown future. Even though physical laws do not distinguish between past and future, he proposed that this arrow of time follows from entropy increasing with time t (second law of thermodynamics). I present a qubit model of a memory which fully portrays this [3]. I solve the qubit dynamics under a time-dependent Schrodinger equation which is symmetric under $t \to -t$, and show that it can remember its past but not its future. Crucially a Landauer erasure of information [4] is found to be necessary to prepare the qubit to act as a memory. In other words, there is no memory without forgetting (information erasure), and forgetting require entropy production. It is this that creates a psychological arrow of time, and forces it to point in the direction of entropy increase.

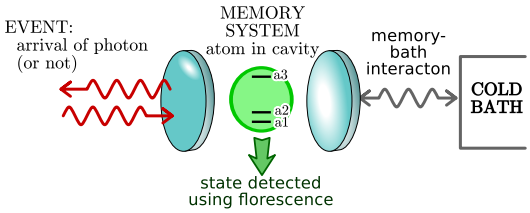
AND BEYOND — to rare fluctuations in which the qubit remembers the future!

Fluctuation theorems (Crooks equality [5], etc) tell us that small systems have fluctuations during which usual processes are reversed, and entropy reduces with time. So does a system record/remember future events during such fluctuations? I study the qubit's behaviour during fluctuations in which entropy is reduced [3]. I find that then (and only then) the qubit *remembers future events!* However, by analysing the probabilities of these fluctuations, I show that the future memories can equally be thought of as thermally-induced errors which *coincidentally* give the correct answer for an event before it occurs. Thus, future memories during entropy-reducing fluctuations cannot be used to predict the future at either the microscopic or macroscopic scale.

(a) Schematic of the thought experiment



(b) Photon-atom version of the experiment, based on Ref. [6].



[1] S. W. Hawking, "The direction of time," New Scientist **115**, 46 (9 July 1987).
[2] Hawkings argument was later developed in detail in; D. H. Wolpert, "Memory systems, computation, and the second law of thermodynamics," Int. J. Theor. Phys. **31**, 743 (1992).
[3] R.S. Whitney, *Manuscript in preparation*.
[4] R. Landauer, "Irreversibility and Heat Generation in the Computing Process," IBM J. Res. Dev. **5**, 183 (1961).
[5] G. E. Crooks, "Entropy production fluctuation theorem and the nonequilibrium work relation for free energy differences," Phys. Rev. E **60**, 2721 (1999).
[6] A. Reiserer, S. Ritter, and G. Rempe, "Nondestructive Detection of an Optical Photon," Science **342**, 1349 (2013).

* robert.whitney@grenoble.cnrs.fr

Wigner distribution on a double-cylinder phase space for studying quantum error-correction protocol

Nicolas Fabre [1], Arne Keller[1], and Perola Milman[1*]
[1] *Laboratoire Matériaux et Phénomènes Quantiques, Sorbonne Paris Cité, Université de Paris, CNRS UMR 7162, 75013 Paris, France*

We introduce a quasi-probability phase space distribution with two pairs of azimuthal-angular coordinates. This representation is well adapted to describe quantum systems with discrete symmetry. Quantum error correction of states encoded in continuous variables using translationally invariant states is studied as an example of application. We also propose an experimental scheme for measuring such distribution [1].

[1] N. Fabre, A. Keller, and P. Milman, Wigner Distribution on a Double-Cylinder Phase Space for Studying Quantum Error-Correction Protocols, Phys. Rev. A **102**, 022411 (2020).

* nclsfabre1@gmail.com

Mechanical and relaxation-based detection of dipolar-interactions between spins in diamond

Clément Pellet-Mary[1], Maxime Perdriat[1], Paul Huillery[1], and Gabriel Hétet[1*]
[1]*Laboratoire de Physique de l'Ecole Normale Supérieure,*
ENS, Université PSL, CNRS, Sorbonne Université,
Université de Paris, F-75005 Paris, France.
[*] *gabriel.hetet@phys.ens.fr*

The electronic spin of the negatively charged nitrogen vacancy center (NV^-) is employed both for applications and fundamental research, thanks to its good coherence properties, long lifetimes and most importantly their ability to be optically polarized. We have recently found new ways to use these properties of NV centers in order to study the dipolar interactions between ensemble of spins in diamond, including NV centers as well as other spin defects.

On the one hand, we have observed cross-relaxations (CR) between NV centers and other defects (see Fig. 1), namely VH^- [1], War1 (first defect found by EPR at the university of Warwick, still chemically unknown) and ^{13}C-NV pair. None of these defects had been observed through CR before. This observation is a first step toward hyper-polarization of new spin defects in diamond.

On the other hand, we have used a levitating diamond [2] to measure the torque applied by the NV centers on the diamond when two classes of NV with different orientation are brought into resonance (see Fig. 2) because of the dipolar-mediated modification of the T_1 of NV in dense ensembles[3]. This demonstration paves the way toward the mechanical detection of other spin impurities in diamond, as well as the observation of the Einstein-de Haas effect with paramagnetic systems[4].

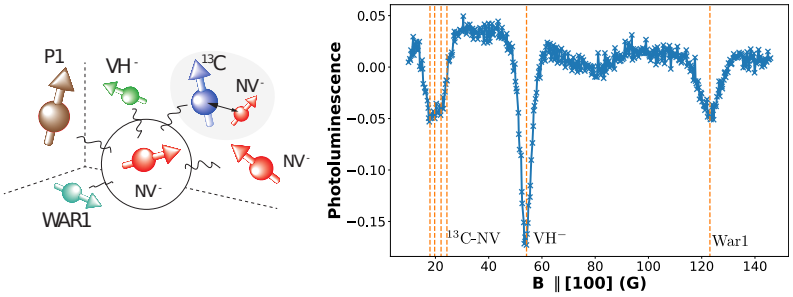


Figure 1 : *Relaxation-based detection of dipolar interaction.* **Left** : Sketch of the various spins interacting. **Right** : Photoluminescence change while scanning the magnetic field along the crystalline [100] direction. Three dips are observed for the CR with ^{13}C-NV, VH^- and War1.

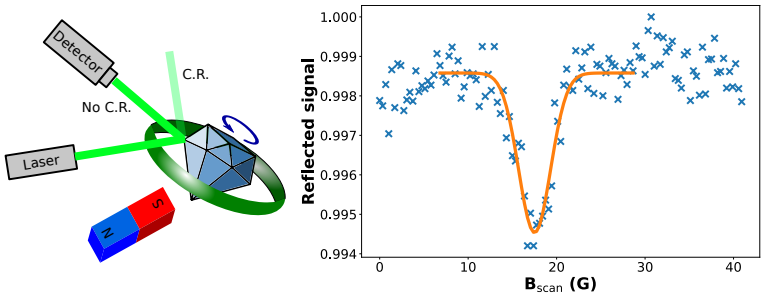


Figure 2 : *Mechanical detection of dipolar interactions.* **Left** : Sketch of the experimental setup. **Right :** Angular position of the diamond while scanning B_{Scan} without a microwave. The rotation of the diamond at 17 G corresponds to the resonance between two classes of NV.

[1] Glover, C., et al. Physical review letters 90.18 (2003) : 185507.
[2] Delord, T., et al. Nature 580.7801 (2020) : 56-59.
[3] Choi, J., et al. Physical review letters 118.9 (2017) : 093601.
[4] Zangara, P.R., et al. Physical Review B 100.23 (2019) : 235410.

Breaking simple quantum position verification protocols with little entanglement

Andrea Olivo[1,2], Ulysse Chabaud[3], André Chailloux[1] and Frédéric Grosshans[3]
[1]*Inria, Paris, France*
[2]*LPGP, CNRS, Université Paris-Saclay, Orsay, France*
[3]*Sorbonne Université, CNRS, LIP6, Paris, France*

In this work, we study a cryptographic primitive known as position verification (PV), the quantum version of which (QPV) was introduced in 2010 independently by multiple works [3, 5]. Secure implementations of PV, if they exist, aim to provide some *prover* P with the possibility of certifying to a third party (the *verifier* V) its location in space. One of PV's applications is the authentication of a physical channel where the prover's position is used as the only token, avoiding the need of public-key authentication schemes whose security in a post-quantum world is still a major open question. PV has been shown to be insecure in the classical setting, even under computational assumptions. A coalition of colluding adversaries can mimic the honest prover's actions by copying and sharing the data sent by the verifiers while satisfying the timing constraint. It is then natural to ask how the situation changes if we allow the verifier's challenges to be quantum states, as they cannot be faithfully copied. The problem is interesting in its own right, as it sits at the subtle interplay between quantum constraints on measurements and relativistic effects. The design of generic attacks to QPV led to a technique with exponential entanglement cost, instantaneous nonlocal quantum computation (INQC) [1]. Security proofs for QPV have proven to be elusive, with the notable exception of a hash-function based protocol [9], and linear-entanglement lower bounds for the protocol class we analyze [6, 8]. On the other hand, the entanglement requirement has been reduced to polynomial for many classes of structured protocols (see, e.g. [2, 7]). The focus of our work is to explore the security against small entangled adversaries of a class of experimentally simple protocols, a variation on the BB84-inspired protocols where the polarisation angle θ is not a multiple of $\frac{\pi}{4}$. These protocols with non-Clifford angles have already been introduced [3] to defeat teleportation based attacks, and their security partly characterized in previous work [4]. We provide :

— A definition of the attack model (in quantum circuit representation) that encompasses a wider class of attacks for adversaries sharing a maximally entangled pair of d-level systems.
— A no-go proof for $d = 2$ and $d = 3$ (equivalent to the one in [4]) by introducing a possibly more intuitive graphical representation of the attacker's Hilbert space.
— A thorough numerical exploration of exact attacks up to $d = 12$ by reducing the problem to finding solutions of a nonlinear system of polynomial equations, giving new INQC attacks for many θ using much smaller entangled states than previous techniques [2].
— A numerical analysis of non-exact attacks for $d \leq 5$, by allowing the attackers a probability of failure p_{err} that we seek to minimize, finding that with just two ebits per verifier's qubit $\min\{p_{\text{err}}\}$ is upper bounded by $\simeq 5 \cdot 10^{-3}$. An extension of the protocol where the verifier is allowed more than two basis choices is similarly explored.

The full preprint can be found at `arxiv.org/abs/2007.15808`.

[1] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner. Position-based quantum cryptography : Impossibility and constructions. *SIAM Journal on Computing*, 43(1) :150–178, 2014.
[2] A. Gonzales and E. Chitambar. Bounds on instantaneous nonlocal quantum computation. *IEEE Transactions on Information Theory*, 66(5) :2951–2963, 2020.
[3] A. Kent, W. J. Munro, and T. P. Spiller. Quantum tagging : Authenticating location via quantum information and relativistic signaling constraints. *Phys. Rev. A*, 84 :012326, Jul 2011.
[4] H.-K. Lau and H.-K. Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Phys. Rev. A*, 83 :012322, Jan 2011.
[5] R. A. Malaney. Location-dependent communications using quantum entanglement. *Phys. Rev. A*, 81 :042319, Apr 2010.
[6] J. Ribeiro and F. Grosshans. A tight lower bound for the BB84-states quantum-position-verification protocol. 2015.
[7] F. Speelman. Instantaneous non-local computation of low T-depth quantum circuits. Volume 61 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 9 :1–9 :24.
[8] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15 :103002, October 2013.
[9] D. Unruh. Quantum position verification in the random oracle model. Volume 8617 of *Lecture Notes in Computer Science*, pages 1–18. Springer Berlin Heidelberg, August 2014.

Detecting the origins of quantum heat in a circuit QED system

Dániel Szombati[1], Jérémy Stevens[1], Nathanaël Cottet[1], Stefan Zeppetzauer [1], Quentin Ficheux [1], Sébastien Jezouin [1], Cyril Elouard [2], Maria Maffei [3], Alexia Auffèves [3], Andrew Jordan [2], Audrey Bienfait [1], and Benjamin Huard [1*]

[1] *Univ Lyon, ENS de Lyon, Univ Claude Bernard,CNRS, Laboratoire de Physique, F-69342 Lyon, France*

[2] *Department of Physics and Astronomy, University of Rochester, Rochester, NY 14627, USA*

[3] *Université Grenoble Alpes, CNRS, Grenoble INP, Institut Néel, 38000 Grenoble, France*

The field of thermodynamics was born with the intent to convert the kinetic energy of the random velocity of thermalized particles, i.e. heat, into useful work. Using a similar analogy, a central goal of quantum thermodynamics consists in harnessing the randomness of the quantum measurement backaction and converting it into work. A two level system (TLS) with energy separation E brought into superposition, once measured, will randomly collapse into one of its two energy eigenstates, thus resulting in a final state whose energy can vary by E. Energy conservation principles dictate that this energy E, gained or lost by the TLS post measurement, must be exchanged with the environment. Due to the spontaneous nature of this energy exchange enabled by the measurement backaction, it is dubbed quantum heat. Here, using a circuit QED transmon system in the dispersive limit, we aim to measure and quantify the origins of quantum heat. The role of the environment is played by the excitation pulse which brought the TLS into superposition in the first place. Although the pulse is entangled to the TLS following their interaction, the amount of correlations between the pulse and the TLS is too small to enable the observation of a backaction of the pulse measurement on the TLS. Our results pave the way for further quantum thermodynamics experiments, such as a quantum Maxwell's demon functioning as a true quantum heat engine.

* benjamin.huard@ens-lyon.fr

Quantum Entanglement and the Lorentz Group

Zeno Toffano[1,2], Alberto Ottolenghi[3*]
[1]*Telecom Dept., CentraleSupélec, Gif-sur-Yvette, France*
[2]*Laboratoire des Signaux et Systèmes, CNRS, Université Paris-Saclay, France*
[3]*Honorary Fellow, University College London (UCL), United Kingdom*

The Lorentz metric represented by the diagonal matrix $\boldsymbol{G} = \mathrm{diag}(1,-1,-1,-1)$ acts on Minkowski space-time quadrivectors. In the language of Quantum Information the operator $\boldsymbol{G}$ can be viewed as an entangling gate this because it acts in a similar way as the Controlled-Z gate on the computational basis of a 2-qubit separable quantum vector. The entangling power corresponds to the fact that the resulting vector, considered as a 2-qubit vector, cannot be put into a Kronecker product of two 1-qubit vectors. For example considering a uniform positive normalized input vector, which is separable, one has the transformation :

$$\boldsymbol{G} \cdot \tfrac{1}{2}(1,1,1,1)^T = \tfrac{1}{2}(1,-1,-1,-1)^T$$

It can be easily verified that in this case the resulting output vector is completely entangled, for example by calculating the associated quantum concurrence which equals to 1.

One can represent the generators of the Lorentz group by 4×4 matrices. An example is given by the Lorentz rotation matrix $\boldsymbol{Z}(\phi)$ [1] :

$$\boldsymbol{Z}(\phi) = \exp(-i\phi \boldsymbol{J}_3) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\phi & -\sin\phi \\ 0 & 0 & \sin\phi & \cos\phi \end{pmatrix} \; , \; \boldsymbol{J}_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix} = \boldsymbol{\Pi}_1 \otimes \boldsymbol{\sigma}_y$$

The matrix $\boldsymbol{J}_3$ is the associated Lorentz group generator. $\boldsymbol{J}_3$ can be expressed as the Kronecker product of the qubit logical-1 projector $\boldsymbol{\Pi}_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ with the Pauli matrix $\boldsymbol{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and consequently the operator $\boldsymbol{Z}(\phi)$ in a qubit representation acts as a control gate on the unitary double angle rotation operator $\boldsymbol{R}_y(2\phi) = \exp(\text{-}i\phi\boldsymbol{\sigma}_y)$ around the Oy axis. This can be highlighted by developing the exponential and using the idempotent property of the projector and the involution property of the Pauli matrix :

$$\boldsymbol{Z}(\phi) = \exp(-i\phi(\boldsymbol{\Pi}_1 \otimes \boldsymbol{\sigma}_y)) = \boldsymbol{\Pi}_0 \otimes \boldsymbol{I}_2 + \boldsymbol{\Pi}_1 \otimes \boldsymbol{R}_y(2\phi)$$

where $\boldsymbol{\Pi}_0 = \boldsymbol{I}_2 - \boldsymbol{\Pi}_1 = |0\rangle\langle 0|$ is the qubit logical-0 projector. The form can be compared with the more-known entangling gate Control-NOT which can be expressed also as a function of projectors :

$$\boldsymbol{C}_{NOT} = \boldsymbol{\Pi}_0 \otimes \boldsymbol{I}_2 + \boldsymbol{\Pi}_1 \otimes \boldsymbol{\sigma}_x = \boldsymbol{\Pi}_0 \otimes \boldsymbol{I}_2 + \boldsymbol{\Pi}_1 \otimes i\boldsymbol{R}_x(\pi)$$

which is a control gate on the unitary Pauli operator $\boldsymbol{\sigma}_x = \boldsymbol{X}$ (the NOT gate) and corresponds geometrically to a reflection or equivalently a rotation around the Ox axis of angle π multiplied by the imaginary number i.

The following questions arise : is there a link between the Lorentz space-time structure and entanglement ? Do they have a common origin ? These questions could be related with the lack of mechanical understanding of the nature of a relativistic spinor. Spinors are often identified with qubits, for example the complex 1-qubit column vector $|\psi\rangle = (\psi_1, \psi_2)^T$ transforms under left-multiplication with matrices in the $SU(2)$ special-unitary group like a 1-spinor [2] and Dirac 2-spinors can be associated with 2-qubit states. The physics related to the information content of the Lorentz group is often overlooked, not being considered for actual applications in Quantum Information. Spinor algebra arises by the Lorentz invariance constraint in the quantum Hilbert space framework and conversely spinor algebra implies Lorentz invariance. Therefore the Lorentz group can be considered as a bridging algebraic structure between Quantum Information and Relativity Theory. Also the logic content of the associated linear algebra structures [3] could provide a new perspective to further explore this matter.

[1] Bakal, S ; Kim. Y. S. ; Noz, M. E., "Physics of the Lorentz Group", IOP Publishing, Bristol, UK. 2015.

[2] Havel, T.F. and Doran, C.J.L., "Geometric algebra in quantum information processing", in Quantum Computation and Information, Ed. Lomonaco, S.J. and Brandt, H.E., Contemp. Math., Volume 305, 2002.

[3] Toffano, Z. ; Dubois, F. "Adapting Logic to Physics : The Quantum-Like Eigenlogic Program", Entropy, 22, 139, 2020.

* zeno.toffano@centralesupelec.fr ; alberto.ottolenghi@hotmail.com

Storage and release of light in subradiant excitations of a dense atomic cloud

Igor Ferrier-Barbut*
Université Paris-Saclay, Institut d'Optique Graduate School,
CNRS, Laboratoire Charles Fabry, 91127, Palaiseau, France.

The description of the interaction between a single two-level atom and radiation is well established and underpins several milestones of modern physics. The response of the system is characterized by a resonance frequency and a decay rate. This picture is modified when considering more than one emitter. Light-induced interactions modify dramatically the response of the ensemble and the behavior of the system becomes collective. Several phenomena arising from collective effects have been observed in atomic systems, in particular subradiance was recently observed in a dilute cloud of cold atoms [1]. Engineering subradiant states has drawn an increasing attention recently. For instance, the opportunity to store an excitation in an atomic medium for a long time has inspired proposals to use subradiance for quantum memories, and the sensitivity of subradiant states to external fields could be a promising route for quantum metrology.

I report here on the study of subradiant collective decay in a dense ensemble of cold ^{87}Rb atoms [2]. Thanks to the high densities reached in our clouds, we explore for the first time collective effects in this strongly interacting regime where the interatomic distances are much smaller than the probing wavelength. We observe a subradiant decay and investigate its dependence on the cloud parameters, observing scalings that reveal long-range interactions. Moreover, we implement an experimental procedure that allows to release the excitation stored in these long-lived modes in a directional pulse of light. This technique is a first step for the realization of devices for light storing and quantum memories based on subradiance.

[1] W. Guerin, M. O. Araújo, & R. Kaiser, *Phys. Rev. Lett.* **116**, 083601 (2016).
[2] G. Ferioli *et al.,* in preparation.

* igor.ferrier-barbut@institutoptique.fr

Effect of filtering on the generation of Schrödinger cat-like states from a pulsed multimode squeezing

Mohamed Faouzi MELALKIA[1,*], Jean ETESSE[1], Sébastien TANZILLI[1], and Virginia D'AURIA[1*]
[1] *Université Côte d'Azur, Institut de Physique de Nice (INPHYNI), CNRS UMR 7010, Parc Valrose, 06108 Nice Cedex 2, France*

Light is a perfect candidate to carry out quantum information for applications to quantum computation [1], communication [2] and metrology [3]. Information can be encoded using observables with discrete spectrum (or DV for discrete variable encoding) [4] as well as with continuous spectrum observables (or CV for continuous variable encoding) [5]. One of the most used states to encode a CV qubit is the so called optical Schrödinger cat state, i.e. a superposition of two coherent states with the same amplitude and opposite phases $|\alpha\rangle + e^{i\varphi}|-\alpha\rangle$. Approximation of these states, named Schrödinger kittens, have been generated in an heralded fashion by subtraction of one or two photons from a degenerate single mode squeezed vacuum states. Experiments have been conducted in continuous wave regime [6] generally using optical parametric oscillators as well as in the pulsed regime [7].

The quality of Schrödinger kittens generated with this strategy, however, suffers from the impurity of the squeezing in the wave-packet of the heralded state. In the CW regime, it is shown theoretically and experimentally [8] that a narrowband filtering of the heralding photon increase the purity of the generated state. We extend this study so as to describe also the pulsed regime where the squeezed vacuum state is in general spectrally multimode [9]. We calculate and numerically simulate the state generated when subtracting a photon from an arbitrary multimode pulsed squeezed vacuum state. In addition, we investigate its homodyne detection by considering an arbitrary pulsed local oscillator. The fidelity between the heralded state and a perfect single mode photon subtracted squeezed state decreases when the number of modes excited in the multimode squeezed vacuum increases. We show how to increase this fidelity by using a narrowband filter in the heralding path. In addition, we demonstrate that the optimal local oscillator is the one which matches perfectly the fundamental dominant mode of the multimode squeezed vacuum state. This study quantifies the effect of spectral filtering on the quality of the generated state using a multimode approach that can be applied to a wide variety of situations. We believe that it will have a major impact on realisation of non-Gaussian states in an heralded fashion.

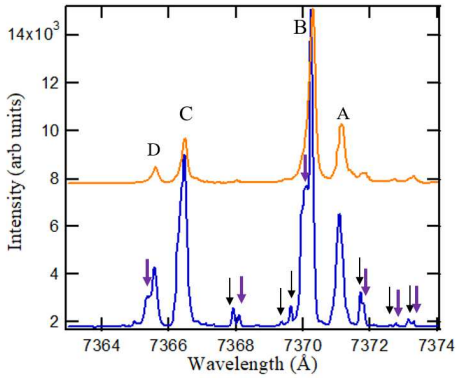
[1] J. L. O'Brien, "Optical quantum computing". Science, **318**, 1567-1570(2007).
[2] N. Gisin, and R. Thew, "Quantum communication", Nature photonics, **1**, 165-171(2007).
[3] V. Giovannetti, S. Lloyd, and L. Maccone, "Advances in quantum metrology", Nature photonics, **5**, 222(2011).
[4] M. A. Nielsen, and I. L. Chuand, "Quantum Computation and Quantum Information", Cambridge University Press, 2010.
[5] D. Gottesman, A. Kitaev, and J. Preskill, "Encoding a qubit in an oscillator", Physical Review A, **64**, 012310(2001).
[6] K. Wakui, H. Takahashi, A. Furusawa, et al, "Photon subtracted squeezed states generated with periodically poled $KTiOPO_4$", Optics Express, **15**, 3568-3574(2007).
[7] A. Ourjoumtsev, R. Tualle-Brouri, J. Laurat, et al, "Generating optical Schrödinger kittens for quantum information processing", Science, **312**, 83-86(2006).
[8] W. Asavanant, K. Nakashima, Y. Shiozawa, et al, "Generation of highly pure Schrödinger's cat states and real-time quadrature measurements via optical filtering", Optics Express, **25**, 32227-32242(2017).
[9] W. Wasilewski, A. I. Lvovsky, K. Banaszek, et al, "Pulsed squeezed light : Simultaneous squeezing of multiple modes", Physical Review A, **73**, 063819(2006).

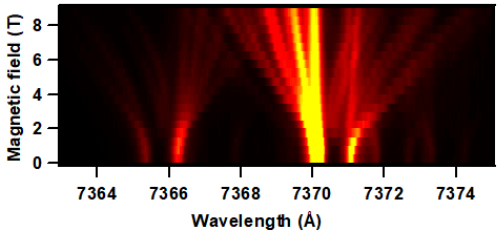
* mohamed.melalkia@univ-cotedazur.fr

SiV $^-$ colour centres in nanodiamonds with excellent spectral properties for quantum information

Mackrine Nahra[1], Lucien Besombes[2], Valery Davydov [3], Viatcheslav Agafonov[4] and Christophe Couteau[1]*
[1]*Laboratory Light, nanomaterials & nanotechnologies - L2n, University of Technology of Troyes (UTT) & CNRS ERL 7004, Troyes, France*
[2]*Institut Néel, CNRS, Univ. Grenoble Alpes and Grenoble INP, 38000 Grenoble, France*
[3]*L.F . Vereshchagin Institute for High Pressure Physics , Russian Academy of Sciences, Troitsk, 142190 Moscow, Russia*
[4]*GREMAN , UMR CNRS CEA 7347, Université de Tours, 37200 Tours, France*

Multiple emitters producing indistinguishable single photons are required for quantum optics technologies. However, typically, solid-state quantum emitters such as quantum dots, defects in 2D materials, defects in solid emit distinguishable single photons. This necessitates the use of optical cavities or electric field tuning of the transition frequency. In low strain bulk diamond, multiple SiV centres can produce indistinguishable single photons [1]. We present work where SiV centrss in nanodiamonds were prepared by the high pressure high temperature method (HPHT) [2], exhibiting excellent spectral properties at 4K, comparable to their bulk counterpart. We observe an improved inhomogeneous ensemble linewidth below the ground state splitting and stable optical transitions. We measured a linewidth of around 6 GHz. It is narrower than previously reported SiV centres in bulk diamond and as well as for any linewidth reported SiV$^-$ in nanodiamonds under off resonant excitation.These properties means that theses quantum emitters are insensitive to perturbations of the dielectric environment thanks to the SiV inversion symmetry and are suitable for emitting indistinguishable photons which is seeked for interfacing several emitters in a quantum network [3]. These results also demonstrate that direct HPHT synthesis technique is capable of producing nanodiamonds with high crystalline quality.
Furthermore, we applied a magnetic field up to 9 T so that we experimentally studied the Zeeman interaction of an ensemble of SiV centres in the same nanodiamonds sample treated with hydrogen at 500 °C for two different emitters labelled emitter 1 and emitter 2. Emitter 2 also presents ^{29}Si silicon isotopes which present a nuclear spin $I = 1/2$ (blue spectrum).





[1] L. J. Rogers, K. D. Jahnke, *et al.* , " Multiple intrinsically identical single-photon emitters in the solid state", Nature communications, 5, **1**, 1−6 (2014).
[2] V. A. Davydov, A. Rakhmanina, *et al.*, "Production of nano- and microdiamonds with si-v and nv luminescent centers at high pressures in systems based on mixtures of hydrocarbon and fluorocarbon compounds", JETP letters, 99, **10**, 585−589 (2014).
[3] K. Li, Y. Zhou, *et al.*, "Non blinking emitters with nearly lifetime−limited linewidths in cvd nanodiamonds", Physical Review Applied, 6, **2**, 024010 (2016).

* mackrine.nahra@utt.fr

Quantum Communication & Cryptography (QCOM)

Loss-tolerant and error-corrected Bell measurement on logical qubits encoded with tree graph states.

Paul Hilaire[1*], Edwin Barnes[1], Sophia E. Economou[1], and Fréderic Grosshans[2,3*]
[1] *Department of Physics, Virginia Tech, Blacksburg, Virginia 24061, USA*
[2] *Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université, 4 place Jussieu, 75005 Paris, France*
[3] *Laboratoire Aimé Cotton, CNRS, Université Paris-Sud, ENS Cachan, Université Paris-Saclay, 91405 Orsay Cedex*

Using linear optics, a two-photon Bell state measurement (BSM) only succeeds with a probability of at best 50% [1] (see Fig. 1(a)). This limits the performances of many quantum repeater (QR) protocols that use these photonic BSMs either for quantum teleportation or for entanglement swapping. QRs also require loss-tolerance to transfer information at a higher rate than direct fiber transmission and error-correction. A loss-tolerant and error-corrected BSM would therefore enable efficient all-photonic QR schemes.

By using either ancillary photonic qubits [2] or nonlinear interaction with atoms [3, 4], it is possible to overcome the 50% limit but these solutions are neither loss-tolerant nor fault-tolerant. To achieve so, we need to logically encode the photonic qubits and thus to perform a logical BSM. Here, we propose to use a photonic tree graph state which is a logical encoding that can be efficiently produced with a few matter qubits [5]. We develop two logical BSM schemes, denoted "static" and "dynamic", that are both loss-tolerant and error-corrected. In the static protocol (Fig. 1(b)), each photonic qubit of a tree graph state is measured with its corresponding qubit of the second tree via standard two-photon BSM which can be implemented with static linear optics. The dynamic protocol (Fig. 1(c)) requires feedforward and yields better performances by dynamically choosing to realize either two-photon BSM or single-qubit measurements depending on previous measurement outcomes.

These results can be directly applied to an all-photonic QR protocol that is fault-tolerant, a feature that was lacking in the original proposal [6].

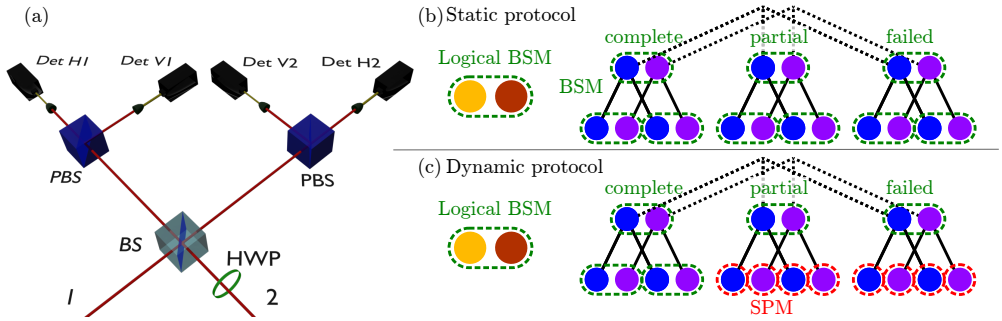


FIGURE 1. (a) Optical setup for two-photon BSM. (b, c) Logical BSM at the logical level (left pannel) and at the physical level (right pannel) for the static (b) and the dynamic (c) protocols. (SPM : single photon measurements.)

[1] N. Lütkenhaus, J. Calsamiglia, and K.A. Suominen, Phys. Rev. A **59**, 3295 (1999).
[2] W.P. Grice, Phys. Rev. A, **84**, 042331 (2011)
[3] Y.-H. Kim, S.P. Kulik, and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001)
[4] S. Lloyd, M. S. Shahriar, J. H. Shapiro, and P. R. Hemmer Phys. Rev. Lett. **87**, 167903 (2001)
[5] D. Buterakos, E. Barnes, and S.E. Economou, Phys. Rev. X **7**, 041023 (2017)
[6] K. Azuma, K. Tamaki H.-K. Lo, Nature Communications **6**, 6787 (2015)

* paulhilaire@vt.edu

Composable Security for Multipartite Entanglement Verification

Raja YEHIA[1], Eleni DIAMANTI[1], Iordanis KERENIDIS[2*]
[1]*LIP6, CNRS, Sorbonne Université, 75005 Paris, France*
[2]*IRIF, CNRS, Université de Paris, 75013 Paris, France*

Abstract. We present a multipartite entanglement verification protocol for n parties consisting only in local quantum operations and authenticated classical communication once a state is shared among them and providing composable security against a malicious source. It can be used as a secure subroutine in the Quantum Internet to test if a source is sharing quantum states that are at least ϵ-close to the GHZ state before performing a communication or computation protocol. Using the Abstract Cryptography framework, we can readily compose our basic protocol in order to create a composably secure multi-round protocol enabling honest parties to obtain a state close to a GHZ state or an abort signal, even in the presence of a noisy or malicious source.
Link to ArXiv paper : The full paper can be found on https ://arxiv.org/abs/2004.07679.

Extended Abstract : Our work extends the work from [1], where the authors develop and analyze a n-party entanglement verification protocol consisting only of classical communication and local quantum operations. One of the parties, called the *Verifier*, has a central role in the protocol : she sends instructions to all parties and broadcasts the output of the verification. The identity of the Verifier as well as the event that the verification actually takes place is randomized to allow for repetition of the protocol in a possibly dishonest setting. We assume that the parties have access to trusted common random sources. We use the Abstract Cryptography framework, where one defines an ideal resource and a concrete resource and the goal is to prove that they are indistinguishable in the presence of malicious parties.

Ideal resource. Our ideal resource, called $\mathcal{MEV}_C$, is meant to be used repetitively by n parties to know if a source is sharing states that are close to the GHZ state. They collectively send a start signal to $\mathcal{MEV}_C$ while the source sends a classical description of a n qubit state ρ. $\mathcal{MEV}_C$ then produces either a bit $C = 0$ and the state ρ shared among the parties or a bit $C = 1$ and a verification bit b_{out} that depends on how close ρ is from the GHZ state. See Fig. 1 for 3 parties.

Concrete resource. We call $\mathcal{R}$ the resource constructed by a state generator resource composed in series to a collection of n quantum channel resources and in parallel to n classical channel resources, and two multiparty trusted common random oracles $\mathcal{O}_C$ and $\mathcal{O}_v$. Moreover we call $\pi_{[n]} = \{\pi_i\}_{i=1}^n$ the protocols of each party and π_S the protocol of an honest source. Together they form our concrete resource $\pi_{[n]}\mathcal{R}\pi_S$. See Fig. 2 for a 3-party example and the paper for formal definitions.

Results and Contribution for QTurn : We prove indistinguishability between $\mathcal{MEV}_C$ and $\pi_{[n]}\mathcal{R}\pi_S$ in the Abstract Cryptography framework [2, 3] resulting in the composable security of the multipartite entanglement verification protocol in a distributed setting with faulty devices. We also define a practical resource for verified GHZ distribution in a quantum network. Our work first provides a practical introduction to composable frameworks, which are increasingly used in modern cryptography, and then proves rigorously the composability of the protocol. As a consequence, multipartite entanglement verification can be thought as a secure resource in the distributed setting and can be readily used as a subroutine of more complex protocols in a near-term Quantum Internet. In our work, we show an example of such construction by presenting a multi-round resource that has practical use for many Quantum Internet near-term protocols. A photonic implementation of the protocol has already been realized that shows the feasibility of the protocol with current state-of-the-art experimental capabilities [4].

[1] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, "Multipartite entanglement verification resistant against dishonest parties," *Physical Review Letters*, vol. 108, 12 2011.
[2] U. Maurer and R. Renner, "Abstract cryptography," *In Innovations In Computer Science*, 2011.
[3] U. Maurer and R. Renner, "From indifferentiability to constructive cryptography (and back)," in *Theory of Cryptography*, (Berlin, Heidelberg), pp. 3–24, Springer Berlin Heidelberg, 2016.
[4] W. McCutcheon, A. Pappa, B. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. Rarity, and M. Tame, "Experimental verification of multipartite entanglement in quantum networks," *Nature Communications*, vol. 7, p. 13251, 11 2016.

* raja.yehia@lip6.fr

FIGURES

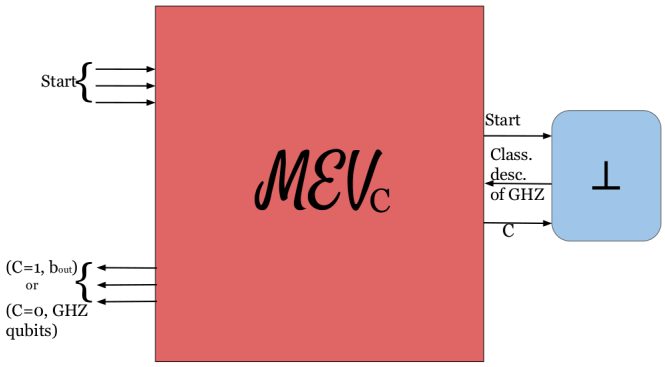


FIGURE 1. The ideal filtered $\mathcal{MEV}_C\perp$ resource for $n = 3$ parties. On the left are the parties interfaces that are used by the parties to collectively send the start signal and receive the output. On the right is the source interface, filtered by $\perp$ in the honest case that blocks any input and sends specific messages to the resource.

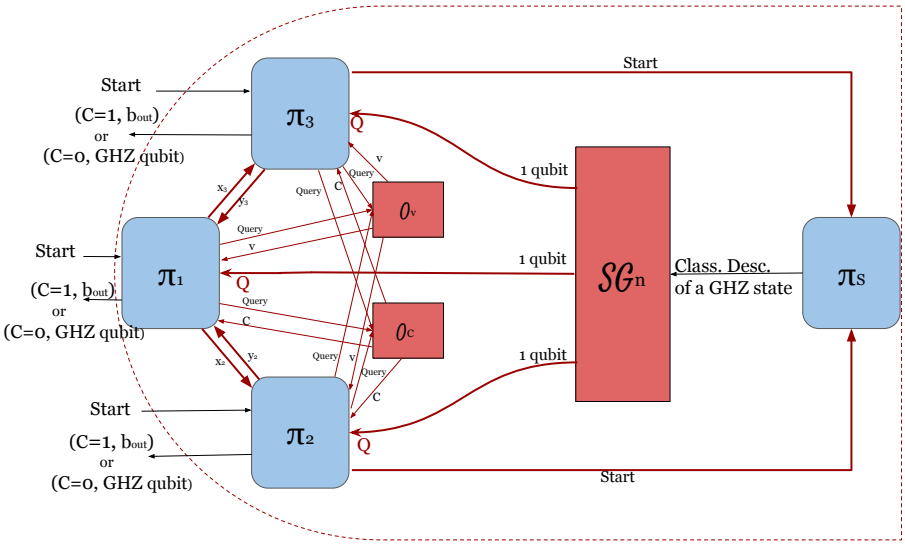


FIGURE 2. The $\pi_{[n]}\mathcal{R}\pi_S$ resource included within the dotted red line for $n = 3$ parties wishing to test a source, when party 1 is chosen to be the Verifier. We represent resources in red and converters in blue. We recall the timeline of the protocol : (1) all the π_i send a start signal to π_S that sends a classical description of a GHZ state to the $\mathcal{SG}_n$ resource. (2) Upon reception of the qubit, they send a query to $\mathcal{O}_C$ and get C. (3) If $C = 0$ output a GHZ qubit and if $C = 1$ the parties query $\mathcal{O}_v$ and get v (here party 1). (4) The Verifier sends instructions $X = \{x_i\}_{i=1}^n$ (here $\{x_2, x_3\}$) to others parties, get outcomes $Y = \{y_i\}_{i=1}^n$ (here $\{y_2, y_3\}$) and computes and broadcasts b_{out}.

Robust self-testing of the singlet

Xavier Valcarce[1]* and Pavel Sekatski[2], Julian Zivy[1], Jean-Daniel Bancal[1] and Nicolas Sangouard[1]
[1]*Université Paris-Saclay, CEA, CNRS, Institut de physique théorique, 91191, Gif-sur-Yvette, France*
[2]*Departement Physik, Universität Basel, Klingelbergstrasse 82, 4056 Basel, Switzerland*

With the exponential growth of quantum technologies, there is the need of protocols certifying that quantum information is maintained faithfully and processed accurately. This is crucial to ensure the security of some quantum technologies as quantum key distribution [1], delegated quantum computing [2] or quantum random number generator [3]. Furthermore, such protocols are a key component to ensure the accurate information processing of quantum computer elements [4].

Device-independent certification, also known as self-testing [5], is a method to infer the underlying physics of a quantum device in a black-box scenario. It is based on non-local correlations, or nonlocality [6], appearing between the outcomes of local incompatible measurements performed on a subsystem of a state. A family of tool to detect nonlocality are the well-known Bell inequalities. The most-studied and simplest one of them is the CHSH inequality. It applies when two parties share a state and perform each out of two dichotomic measurements. From the statistic of these outcomes, the CHSH score is computed. When this score is higher than 2 we are in a nonlocal regime. More interestingly, when this score is the maximum quantum value, $2\sqrt{2}$, we can deduce that the two parties are sharing a maximally entangled two-qubit state – a *singlet* state, up to local unitaries [7]. We say that CHSH self-test the singlet.

In practice, imperfections occur which ultimately lead to a non-maximal CHSH score. However, we can still use the CHSH score to deduce something about the shared state structure. In [8] it was shown that for all CHSH score above ≈ 2.11, we can certify that the measured state has a non-trivial fidelity with respect to the singlet. Conversely, a state with a trivial singlet fidelity, up to local unitaries, achieving a CHSH score of 2.0014 was discovered. Hence, there exist a threshold CHSH score between these value from which self-testing the singlet is possible. In a recent publication presented in this poster, we provide some insight on this threshold. In particular, we have demonstrated the existence of a state with a CHSH score of ≈ 2.05 not satisfying self-testing criteria [9].

A CHSH score of 2.11 is not trivial to attain experimentally. In a recent effort [10], presented in this poster, we came with a new self-testing protocol based on *generalized* CHSH operator. We directly exploit the available information of the outcomes statistics to perform better self-testing. This is, the extracted singlet fidelity of the measured state to the singlet is certified to be higher than in the CHSH case. Furhtermore, when a CHSH score below 2.11 is obtained from imbalanced correlators, our protocol might be used to device-independently extract a singlet state. In some cases, self-testing becomes possible even in an equivalent $2 + \varepsilon$ CHSH score.

[1] A. Ekert and R. Renner, "The ultimate physical limits of privacy," *Nature*, vol. 507, pp. 443–447, Mar. 2014.
[2] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, "Verification of quantum computation : An overview of existing approaches," *Theory of Computing Systems*, vol. 63, pp. 715–808, July 2018.
[3] A. Acín and L. Masanes, "Certified randomness in quantum physics," *Nature*, vol. 540, pp. 213–219, Dec. 2016.
[4] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, "Certifying the building blocks of quantum computers from bell's theorem," *Physical Review Letters*, vol. 121, nov 2018.
[5] I. Šupić and J. Bowles, "Self-testing of quantum systems : a review," *Quantum*, vol. 4, p. 337, Sept. 2020.
[6] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, pp. 195–200, Nov. 1964.
[7] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, "Device-independent state estimation based on bell's inequalities," *Physical Review A*, vol. 80, dec 2009.
[8] J. Kaniewski, "Analytic and nearly optimal self-testing bounds for the clauser-horne-shimony-holt and mermin inequalities," *Physical Review Letters*, vol. 117, Aug. 2016.
[9] X. Valcarce, P. Sekatski, D. Orsucci, E. Oudot, J.-D. Bancal, and N. Sangouard, "What is the minimum CHSH score certifying that a state resembles the singlet?," *Quantum*, vol. 4, p. 246, Mar. 2020.
[10] X. Valcarce, J. Zivy, N. Sangouard, and P. Sekatski, "Self-testing two-qubit maximally entangled states from generalized chsh inequalities," *To be published*, 2020.

* xavier.valcarce@ipht.fr

Nonlinear quantum optics with Rydberg atoms in an optical cavity

Julien Vaneecloo[1],* Merlin Enault-Dautheribes[1], Sébastien Garcia[1], and Alexei Ourjoumtsev[1†]
[1] *Quantum Photonics team, Institut de Physique - Collège de France,*
11 place Marcelin Berthelot, 75231 Paris, France

We present an experimental platform that combines an ultracold rubidium ensemble with a medium-finesse cavity to shape and control interactions between optical photons. Those photon-photon interactions are obtained by probing the atomic cloud in a ladder Electromagnetically Induced Transparency scheme (EIT, figure 1a) to map Rydberg excitations onto photons [1]. In this context, the optical response of the medium is very sensitive to the number of excitations propagating through the cavity due to a blockade phenomenon caused by the strong dipolar interactions between Rydberg atoms.

The inhomogeneous broadening of the Rydberg linewidth is a crucial parameter that set the transparency and the size of the blockade volume. We recently managed to reduce this broadening below $100\,\mathrm{kHz}$ by mean of degenerate Raman sideband cooling [2] to reach a temperature of $1\,\mu\mathrm{K}$. At this temperature, the Doppler contribution is negligible and it becomes possible to probe the ensemble directly inside the dipole trap as the differential light shift is significantly reduced. Currently, we observe strong anti-bunching at zero delay (figure 1b) for the 100S Rydberg state with a thousand atoms trapped in a Gaussian rms radius of $6\,\mu\mathrm{m}$ within a blockade sphere, corresponding to a regime where only one photon at a time can be transmitted by the resonator [3]. This result, associated with the level of transmission in EIT, demonstrates that we have created strong photon-photon interactions with low loss.

The control of this Rydberg polariton state [4] will thereby enable us to perform several quantum optics experiments with the deterministic generation of non-Gaussian states or the creation of a two-photon phase gate.

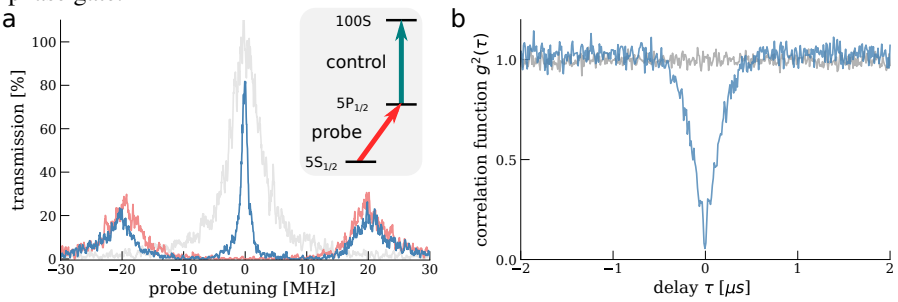


FIGURE 1: a-The transmission spectrum : bare cavity resonance in grey, atom-cavity coupling in red and Electromagnetically Induced Transparency in blue when control field is on, see inset. b- The correlation function features strong anti-bunching at zero delay in the Rydberg blockade regime (blue) compared to the empty cavity (grey), a proof that only single photons are emitted.

[1] Murray, C., and Thomas Pohl. "Quantum and nonlinear optics in strongly interacting atomic ensembles." Advances in Atomic, Molecular, and Optical Physics. Vol. 65. Academic Press, 2016. 321-372.
[2] Kerman, Andrew J., et al. "Beyond optical molasses : 3D Raman sideband cooling of atomic cesium to high phase-space density." Physical review letters 84.3 (2000) : 439.
[3] Peyronel, Thibault, et al. "Quantum nonlinear optics with single photons enabled by strongly interacting atoms." Nature 488.7409 (2012) : 57-60.
[4] Dudin, Y. O., et al. "Observation of coherent many-body Rabi oscillations." Nature Physics 8.11 (2012) : 790-794.

* julien.vaneecloo@college-de-france.fr
† alexei.ourjoumtsev@college-de-france.fr

Integrated quantum photonics with silicon vacancy centers in silicon carbide

Charles Babin[1],* Daniil M. Lukin[2], Rainer Stöhr[1], Naoya Morioka[1], Tobias Linkewitz[1], Vadim Vorobyov[1], Melissa A. Guidry[2], Alexander D. White[2], Timo Görlitz[1], Di Liu[1], Yu-Chen Chen[1], Matthias Niethammer[1], Jelena Vučković[2], Jörg Wrachtrup[1], and Florian Kaiser[1†]

[1] *3rd Institute of Physics, University of Stuttgart and Institute for Quantum Science and Technology IQST, Pfaffenwaldring 57, 70569 Stuttgart, Germany*

[2] *E. L. Ginzton Laboratory, Stanford University, Stanford, CA 94305, USA*

Solid-state color centers promise chip-based quantum technologies. Fascinating opportunities emerge by linking atom-like optical transitions and long-lived electron and nuclear spin qubit clusters [1]. Recent research demonstrated that "immortal solid-state spin qubits" based on Shor's nine-qubit error correction code are realistically within reach [2]. To efficienctly entangle such qubits, it is now well-accepted that scaling beyond the basic two-qubit scenario requires boosting the efficiencies of the related spin-photon interfaces, e.g. using cavity quantum electrodynamics (cQED). However, despite considerable efforts, the development of a scalable solid-state cQED platform has remained extraordinarily challenging for the commonly-used diamond platform [3]. Here, we show our latest exciting results on developing an integrated spin-photonics platform based on silicon vacancy (V_{Si}) centers in semiconductor silicon carbide (SiC). In particular, we will highlight three major achievements:

1) We generate spin-controlled multi-photon states for the first time in SiC. Hong-Ou-Mandel type experiments revealed more than 90% interference contrast [4], thus demonstrating the potential of V_{Si} centers in SiC as a spin-photonics platform.

2) Any scalable spin-photonics platform needs to provide local tuning mechanisms to account for unavoidable nanofabrication errors. We show that V_{Si} centers in SiC can be straightforwardly Stark-shift tuned across 200 GHz without degradation of the optical properties. Also, by modulating the energy level scheme faster than the excited state lifetime, we create spectrally-engineered Floquet states, which can be used to compensate linewidth mismatches of multiple emitters [5].

3) We present the latest advancements on the development of an integrated SiC platform. We use Helium ion and proton implantation to create single V_{Si} centers with sub-diffraction limited spatial resolution. Additionally, we confine single V_{Si} centers in triangular-shaped SiC nanophotonic waveguides. Remarkably, for both cases the spin and optical properties of single emitters remained surprisingly robust, essentialy identical to defects deep in the bulk material. Most importantly, we show that those results are reproducible across multiple crystals originating from different growth processes.

Our results highlight the tremendous potential of the SiC nanophotonics platform. Combining our work with recently demonstrated integrated quantum nonlinear photonics in SiC [6] could enable on-chip wavelength conversion. In summary, we believe that the SiC nanophotonics platform has matured significantly in the last years, making it the prime candidate for realizing a scalable chip-based quantum spin-photonics applications.

[1] D. D. Awschalom, R. Hanson, J. Wrachtrup and B. B. Zhou, "Quantum technologies with optically interfaced solid-state spins", Nat. Photonics **12**, 516-527 (2018).

[2] C. E. Bradley et al. "A Ten-Qubit Solid-State Spin Register with Quantum Memory up to One Minute", Phys. Rev. X **9**, 031045 (2019).

[3] E. Janitz et al., "Cavity quantum electrodynamics with color centers in diamond", Optica **7**, 1232-1252 (2020).

[4] N. Morioka et al., "Spin-controlled generation of indistinguishable and distinguishable photons from silicon vacancy centres in silicon carbide", Nat. Commun **11**, 2516 (2020).

[5] D. M. Lukin et al. "Spectrally reconfigurable quantum emitters enabled by optimized fast modulation", npj Quantum Inf. **6**, 80 (2020).

[6] M. A. Guidry et al. "Optical parametric oscillation in silicon carbide nanophotonics", Optica **7**, 1139-1142 (2020).

* c.babin@pi3.uni-stuttgart.de

† f.kaiser@pi3.uni-stuttgart.de

QKD attack rating : all attacks are equal, but some attacks are more equal than others

Rupesh Kumar[1], Francesco Mazzoncini[2], Hao Qin[3] and Romain Alléaume[2*]
[1]*Quantum Communications Hub, Department of Physics, University of York, Heslington, United Kingdom.*
[2]*Télécom Paris-LTCI, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France.*
[3]*CAS Quantum Network Co., Ltd No. 99 Xiupu Rd, Pudong New District, Shanghai 201315, China.*

Theoretical security proofs constitute a strong conceptual framework to capture the security properties of QKD protocols, based on a model. QKD implementations may, however, not fully comply with the model used in the security proof, leading to security vulnerabilities and the possibility to launch side-channel attacks. Hence, to guarantee a very high-security level for QKD, forward-looking methods and standards in quantum cryptography implementation security shall be adopted, following a methodology similar to the ones used to certify the security of classical crypto-systems, such as the Common Criteria (CC) [1].

Inspired by CC, we introduce a metric called Attack Potential to QKD, that aims to evaluate the total effort required to successfully mount an attack. To illustrate the relevance of this approach, we applied this metric to two different attack strategies [2] on a working CV-QKD experimental set-up. The first strategy relies on inducing detector saturation by performing a large coherent displacement [3]. This strategy is experimentally challenging and therefore translates into a high attack rating. We also analyze e a second attack strategy that simply consists of saturating the detector with an external laser [4]. The low rating we obtain indicates that this attack constitutes a primary threat to practical CV-QKD systems.

The introduction of an attack rating methodology in the context of QKD brings fresh perspectives. It has the ability to strengthen the security rationale associated with QKD system design and to accelerate the evolution towards a quantum industry capable of manufacturing QKD devices with high-security assurance. Theoretical and practical security of a given QKD system may, indeed, significantly differ, notably when practical security is limited by engineering constraints. This calls to reconsider the absolute security claims sometimes associated with QKD and to adopt a more balanced viewpoint, taking implementation complexity into consideration. Although increasing theoretical security should not constitute the ultimate objective, it provides a fundamental upper bound that we aim to raise, and also to be able to match as closely as possible in practice. This novel viewpoint underlines the necessity to combine theoretical security considerations with vulnerability analysis based on attack ratings, in order to guide the design and engineering of practical QKD systems towards the highest possible security standards. Moreover, Attack Potential can be used as a metric in order to balance the effort invested at QKD system design stage and at the countermeasure development stage to thwart attacks, allowing to prioritize the attacks that constitute the most serious threats in practice. In conclusion, adapting existing criteria from IT security to the context of quantum cryptography represents a significant challenge. The use of attack ratings is likely to represent a fundamental step towards strengthening cyber security infrastuctures by the integration of high-assurance quantum cryptographic devices.

[1] "Common methodology for information technology security evaluation", version 3.1, revision 5 (2017). URL https ://www.ssi.gouv.fr/uploads/2015/01/cemv3.1r5.pdf.
[2] R. Kumar, F. Mazzoncini, H. Qin and R. Alléaume, "Experimental vulnerability analysis of QKD based on attack ratings", arXiv :2010.07815, (2020).
[3] H. Qin, R. Kumar and R. Alléaume, "Quantum hacking : Saturation attack on practical continuous-variable quantum key distribution", Physical Review A **94**,(2016).
[4] H. Qin, R. Kumar and R. Alléaume, "Homodyne-detector-blinding attack in continuous variable quantum key distribution", Phys. Rev. A **98**, (2018).

* mazzoncini@telecom-paris.fr

Everlasting Secure Key Agreement with performance beyond QKD in a Quantum Computational Hybrid security model (arXiv :2004.10173)

Nilesh Vyas* and Romain Alléaume
Télécom Paris, LTCI, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France

Extending the functionality and overcoming the performance limitation under which QKD can operate requires either quantum repeaters or new security models. Investigating the latter option, we introduce the **Quantum Computational Hybrid** (QCH) security model, where we assume that computationally secure encryption may only be broken after time much longer than the coherence time of available quantum memories. This model can be seen as a combination of time-release encryption [1] with the noisy quantum memory model [3].

Using the QCH security model we develop a new quantum cryptographic framework, that we call, "**Quantum Computational Time-lock**" (QCT). We propose an explicit d-dimensional key agreement protocol, that we call, "**MUB-Quantum Computational Timelock**" (MUB-QCT), where a bit is encoded on a qudit state using a full set of $d+1$ mutually unbiased bases (MUBs) and a family of pair-wise independent permutation. To prove the security, we first show that the eavesdropping reduces to performing an immediate measurement followed by post-measurement decoding [2]. Secondly, following construction of quantum to classical randomness extractor based on full set of MUBs [5], we calculate the upper bound on Eve's accessible information. We prove that when sending one copy of quantum state per channel use, $I_{acc}(X;E) \leq \mathcal{O}(1/d)$. When Alice sends m copies per channel use, Eve's accessible information, when restricted to perform only copy-by-copy individual attacks, is $I_{acc}(X;E)_m \leq \mathcal{O}(m/d)$, enabling secure key distribution with input states containing up to $O(d)$ photons. Thus, the MUB-QCT construction has the potential to provide a radical shift to the performance and practicality of quantum key distribution.

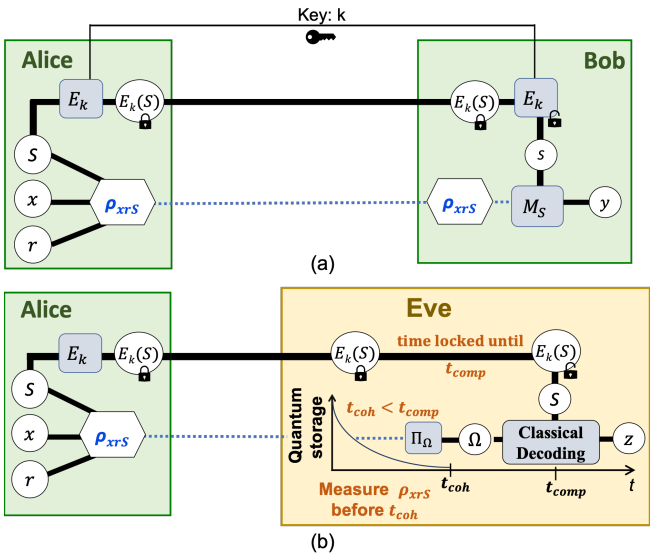


FIGURE 1. A general overview of a QCT construction. (a) Protocol between authorized Alice and Bob. (b) Protocol between authorized Alice and Eve.

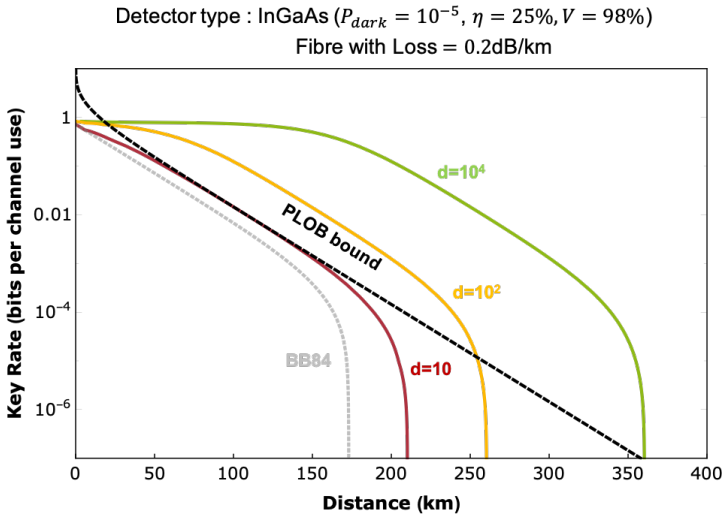


FIGURE 2. Plot of key rate per channel use as a function of distance for, Typical QKD Field Deployment (standard fiber, InGaAs single-photon detectors) [6]. The plots are given for different values of d (number of modes) and are obtained by maximizing the key rate against the mean photon number m.

[1] D. Unruh. (pp. 129-146), Eurocrypt 2014. Springer.
[2] D. Gopal, and S. Wehner. Phys. Rev. A 82, 022326 (2010).
[3] S. Wehner, *et al*. Phys. Rev. Lett., 100(22), 220502.
[4] Cosmo Lupo. Entropy, 17(5), 3194-3204 (2015).
[5] M. Berta, *et al*. IEEE Transactions on Information Theory, vol. 60, no. 2, pp. 1168-1192, Feb. 2014.
[6] L. C. Comandar *et al.* Appl. Phys. Lett. 104, 021101 (2014).

*nilesh.vyas@telecom-paris.fr

Broad diversity of near-infrared single-photon emitters in silicon

A. Durand,[1] Y. Baron,[1,*] W. Redjem,[1] T. Herzig,[2] A. Benali,[3] S. Pezzagna,[2] J. Meijer,[2] A. Yu. Kuznetsov,[4] J.-M. Gérard,[5] I. Robert-Philip,[1] M. Abbarchi,[3] V. Jacques,[1] G. Cassabois,[1] and A. Dréau[1]

[1]*Laboratoire Charles Coulomb, UMR5221, Université de Montpellier and CNRS, 34095 Montpellier, France*
[2]*Division of Applied Quantum Systems, Felix-Bloch Institute for Solid-State Physics, University Leipzig, Linnéestraße 5, 04103 Leipzig, Germany*
[3]*CNRS, Aix-Marseille Université, Centrale Marseille, IM2NP, UMR 7334, Campus de St. Jérôme, 13397 Marseille, France*
[4]*Department of Physics, University of Oslo, NO-0316 Oslo, Norway*
[5]*Department of Physics, IRIG-PHELIQS, Univ. Grenoble Alpes and CEA, F-38000 Grenoble, France*

The boom of silicon in semiconductor technologies was closely tied to the ability to control its density of lattice defects [1]. After being regarded as detrimental to the crystal quality in the first half of the 20^{th} century [2], point defects have become an essential tool to tune the electrical properties of this semiconductor, leading to the development of a flourishing silicon industry [1]. At the turn of the 21^{st} century, progress in Si-fabrication and implantation processes has triggered a radical change by enabling the control of these defects at the single level [3]. This paradigm shift has brought silicon into the quantum age, where individual dopants are nowadays used as robust quantum bits to encode and process quantum information [4]. These individual qubits can be efficiently controlled and detected by all-electrical means [4], but have the drawback of either being weakly coupled to light [5] or emitting in the mid-infrared range [6] unsuitable for optical fiber propagation. In order to isolate matter qubits that feature an optical interface enabling long-distance exchange of quantum information while benefiting from well-advanced silicon integrated photonics [7], one strategy is to investigate defects in silicon that are optically-active in the near-infrared telecom bands [8–10].

In our recent work [11], we report the detection of individual emitters in silicon belonging to seven different families of optically-active point defects. These fluorescent centers are created by carbon implantation of a commercial silicon-on-insulator wafer usually employed for integrated photonics. We analyse their photoluminescence spectrum, dipolar emission and optical relaxation dynamics at 10K. For a specific family, we show a constant emission intensity at saturation from 10K to temperatures well above the 77K-liquid nitrogen temperature. Given the advanced control over nanofabrication and integration in silicon, these novel artificial atoms are promising candidates for Si-based quantum technologies [7].

[1] Yutaka Yoshida and Guido Langouche, "Defects and Impurities in Silicon Materials", Quant. Inf. J., volume **916** of Lecture Notes in Physics. Springer Japan, Tokyo, (2015).

[2] Hans J. Queisser and Eugene E. Haller, "Defects in Semiconductors: Some Fatal, Some Vital", Science **281**, 945-950 (1998).

[3] Andrea Morello, Jarryd J. Pla, Floris A. Zwanenburg et al., "Single-shot readout of an electron spin in silicon", Nature **467**, 687-691 (2010).

[4] Y. He, S. K. Gorman, D. Keith, "A two-qubit gate between phosphorus donor electrons in silicon", Nature **571**, 371 (2019).

[5] M. Steger, K. Saeedi, M. L. W. Thewalt et al., "Quantum Information Storage for over 180 s Using Donor Spins in a ^{28}Si 'Semiconductor Vacuum'", Science **336**, 1280-1283 (2012).

[6] Kevin J. Morse, Rohan J. S. Abraham, Adam DeAbreu et al., "A photonic platform for donor spin qubits in silicon", Science Advances **3**, e1700930 (2017).

[7] Joshua W. Silverstone, Damien Bonneau, Jeremy L. O'Brien and Mark G. Thompson, "Silicon Quantum Photonics", IEEE Journal of Selected Topics in Quantum Electronics **22**, 390-402 (2016).

[8] L. Bergeron, C. Chartrand, A. T. K. Kurkjian et al., "A silicon-integrated telecom photon-spin interface", arXiv: 2006.08793 (2020).

[9] Lorenz Weiss, Andreas Gritsch, Benjamin Merkel and Andreas Reiserer, "Erbium dopants in silicon nanophotonic waveguides", arXiv: 2005.01775 (2020).

[10] W. Redjem, A. Durand, T. Herzig et al., "Single artificial atoms in silicon emitting at telecom wavelengths", arXiv: 2001.02136 (2020).

[11] A. Durand, Y. Baron, W. Redjem et al., "Broad diversity of near-infrared single-photon emitters in silicon", arXiv: 2010.11068 (2020).

* yoann.baron@umontpellier.fr

Covert continuous-variable quantum key distribution

Raphaël Aymeric[1], David Faisin [2], and Romain Alléaume[1,3*]
Télécom Paris, LTCI, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France

Quantum Key Distribution (QKD) [1, 2] is a protocol harnessing fundamental quantum mechanics and classical post-processing to share a secret key between two parties, Alice and Bob, with information-theoretical security. This security contrasts with most cryptographic applications which are secure with computational security, $i.e.$ they are based on problems that are hard to solve in terms of number of computer operations. For keys obtained via QKD, a malevolent third party, Eve, has asymptotically no better strategy than randomly guessing the key exchanged by Alice and Bob which is particularly interesting for solutions which require extreme security such as communications between governmental facilities.

Nonetheless, Eve is in no way prevented from *knowing* that a key is distilled between Alice and Bob and this can be an issue. Eve can use this knowledge to launch a potential side-channel attack, or even guess their intentions. Extreme security should also require Eve cannot know whether Alice and Bob are distilling a secret key via any given QKD protocol, $i.e$ their communication should be *covert*.

Previous work on covert communications exploit some channel noise to hide the signal, and a square-root law [3] has been derived stating that $O(\sqrt{n})$ bits can be covertly transmitted in $O(n)$ channel uses. The purpose of this work is to investigate the performance of CV-QKD protocols under the constraint of covert signals. Unsurprisingly, such protocols are drastically limited for two reasons. First, hiding the QKD states requires channel noise which is detrimental to the key rate. Second, the $1/\sqrt{n}$ scaling of the signal power -from which stems the square-root law- means that only a limited amount of signals can be sent before the key rate becomes negative.

An original solution to increase the performance of such protocols is what we call *block-coherent* encoding. This technique consists in splitting individual QKD pulses over multiple modes, indexed by a shared secret S_{AB} between Alice and Bob, before transmission over the channel. Upon reception Bob uses his knowledge of S_{AB} to rebuild the original signal thus leading to a coherent gain on the total signal power which scales as the square-root of the number of modes used in the encoding. Such encodings can be implemented in the spectral domain with spread-spectrum techniques [4] or in the temporal domain with a dedicated interferometer.

In addition, we explore two relaxed security models which permit to circumvent the $1/\sqrt{n}$ scaling of the signal power. In the first model Alice can control a portion of the channel noise. She can therefore substitute her signal to the noise while avoiding detection. In the second model, Eve is assumed to have some uncertainty on the total channel noise, thus Alice can avoid detection by sending signals which are low intensity compared to Eve's uncertainty. We argue both models present realistic applications. For instance, if the Alice-Bob link is located on WDM channels generating Raman noise before Alice and on the Alice-Bob link, it is sound to assume Alice can have some control over the Raman noise generated upstream, by placing spectral filters on the quantum channel wavelength for instance. Also, Eve will have uncertainty on the channel noise power when a jammer generates varying random noise without any form of coordination with Alice. When combined with block-coherent encoding, both models enable covert CV-QKD in the asymptotic regime of infinite signals and in practical scenarios.

[1] Charles H. Bennett and Gilles Brassard. Quantum cryptography : Public key distribution and coin tossing. *Theoretical Computer Science*, 560 :7 – 11, 2014.

[2] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88 :057902, 2002.

[3] Gheorghe A. Patel M. et al. Bash, B. Quantum-secure covert communication on bosonic channels. *Nat Commun*, 6(8626), 2015.

[4] Marvin K. Simon, Jim K. Omura, Robert A. Scholtz, and Barry K. Levitt. *Spread Spectrum Communications Handbook (Revised Ed.)*. McGraw-Hill, Inc., USA, 1994.

* raphael.aymeric@telecom-paris.fr

Quantum Sensing & Metrology (QMET)

Number-Resolved Photocounter for Propagating Microwave Mode

Rémy Dassonneville[1], **Réouven Assouly**[1], Pierre Rouchon[2]and Benjamin Huard[1*]
[1]*Univ Lyon, ENS de Lyon, Univ Claude Bernard, CNRS, Laboratoire de Physique,F-69342 Lyon, France*
[2]*Centre Automatique et Systèmes, Mines-ParisTech, PSL Research University, 60 bd Saint-Michel, 75006 Paris, France. QUANTIC team, INRIA de Paris, 2 rue Simone Iff, 75012 Paris, France.*

The first detectors of propagating microwave photons have been realized using superconducting circuits a decade ago[1]. However a number-resolved photocounter is still missing. We demonstrate a single-shot counter for propagating microwave photons that can resolve up to 3 photons. It is based on a pumped Josephson Ring Modulator that can catch an arbitrary propagating mode by frequency conversion and store its quantum state in a stationary memory mode. A transmon qubit then counts the number of photons in the memory mode using a series of binary questions. Using measurement based feedback, the number of questions is minimal and scales logarithmically with the maximal number of photons. The detector features a detection efficiency of 0.96 ± 0.04, and a dark count probability of 0.030 ± 0.002 for an average dead time of $4.5\,\mu s$. To maximize its performance, the device is first used as an *in situ* waveform detector from which an optimal pump is computed and applied. Depending on the number of incoming photons, the detector succeeds with a probability that ranges from $(54 \pm 2)\,\%$ to 99%.[2]

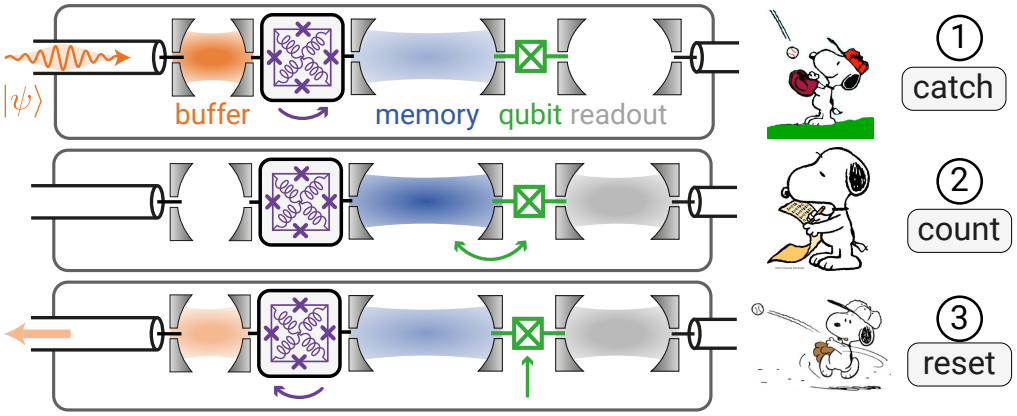


FIG. 1. Schematic view of the catch-count-release protocol used to count the number of photons present in a propagating mode

[1] Y. F. Chen, D. Hover, S. Sendelbach, L. Maurer, S. T. Merkel, E. J. Pritchett, F. K. Wilhelm, and R. McDermott, Microwave Photon Counter Based on Josephson Junctions, Phys. Rev. Lett. **107**, 217401 (2011)

[2] R. Dassonneville, R. Assouly, P. Rouchon and B. Huard, Number-Resolved Photocounter for Propagating Microwave Mode, Phys. Rev. Applied **14**, 044022 (2020)

* benjamin.huard@ens-lyon.fr

Multimode squeezing with a Travelling Wave Parametric Amplifier

Martina Esposito[1], Arpit Ranadive[1], Luca Planat[1], Dorian Fraudet[1], Vincent Jouanny[1], Sébastien Leger[1], Cécile Naud[1], Olivier Buisson[1], Wiebke Guichard[1], Nicolas Roch[1]*
[1]*Université Grenoble Alpes, CNRS, Grenoble INP, Institut Néel, 38000 Grenoble, France*

Quantum states of light consisting of many entangled modes (multimode entangled states) provide a powerful quantum resource and have been proposed as a platform for universal quantum computing with continuous variables (CV) [1].
Photonic multimode CV quantum states have been experimentally demonstrated at optical frequencies [2–4] but they are still not established in the microwave regime, where one can take advantage of much higher non-linear interactions without introducing dissipation. Nonlinear superconducting circuits based on Josephson junctions, like Josephson parametric amplifiers (JPA), can be tailored to behave as sources of multimode entangled radiation in the microwave regime [5].
It has been demonstrated that Josephson parametric amplifiers based on resonant structures, resonant JPAs, can successfully generate entangles states in the form of two-mode squeezing [6, 7], however the extension to a higher number of entangled modes is limited by the narrow bandwidth of these devices (typically tens of MHz). Travelling wave parametric amplifiers (TWPAs) allow nonlinear interactions on a much larger bandwidth, several GHz, and have been proposed as promising candidates for engineering multimode entangled states [5].
The demonstration of two-mode squeezing with a TWPA device is a necessary step towards engineering squeezed states with a large number of entangled modes. We will present preliminary experimental results on the generation of two-mode squeezed states with a Josephson TWPA composed of an array of superconducting nonlinear asymmetric inductive elements (SNAILs) and discuss the extension of our approach for the generation of large multimode entangled states.

[1] O. Pfister, Journal of Physics B: Atomic, Molecular and Optical Physics **53** (2020), 10.1088/1361-6455/ab526f.
[2] M. Chen, N. C. Menicucci, and O. Pfister, Phys. Rev. Lett. **112**, 120505 (2014).
[3] Y. Cai, J. Roslund, G. Ferrini, F. Arzani, X. Xu, C. Fabre, and N. Treps, Nature Communications **8**, 15645 (2017).
[4] W. Asavanant, Y. Shiozawa, S. Yokoyama, B. Charoensombutamon, H. Emura, R. N. Alexander, S. Takeda, J. ichi Yoshikawa, N. C. Menicucci, H. Yonezawa, and A. Furusawa, Science **366**, 373 (2019).
[5] A. L. Grimsmo and A. Blais, npj Quantum Information **3**, 20 (2017).
[6] E. Flurin, N. Roch, J. D. Pillet, F. Mallet, and B. Huard, Phys. Rev. Lett. **114**, 1 (2015).
[7] C. Eichler, D. Bozyigit, C. Lang, M. Baur, L. Steffen, J. M. Fink, S. Filipp, and A. Wallraff, Physical Review Letters **107**, 1 (2011), arXiv:1101.2136.

* martina.esposito@neel.cnrs.fr

Repeated Error Correction for Quantum Metrology

Nathan Shettell[1,2],* William Munroe[3], Damian Markham[1,4], and Kae Nemoto[2,4]
[1]*Laboratoire d'Informatique de Paris 6, CNRS, Sorbonne Université, 4 place Jussieu, 75005 Paris, France*
[2]*National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan*
[3]*NTT Basic Research Laboratories & Research Center for Theoretical Quantum Physics, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa, 243-0198, Japan*
[4]*Japanese-French Laboratory for Informatics, CNRS, National Institute for Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan*

The objective of quantum metrology is to determine high precision estimates of unknown parameters. Because entanglement allows one to create non-classical correlations between the quantum probes, one is able to develop estimation strategies that achieve a quadratic gain in precision over the best classical strategies. However, in a realistic setting, quantum metrology is faced with many obstacles ; one of the most difficult to overcome is noise. It becomes increasingly difficult to distinguish the effects of a signal versus the effects of noise [1] ; significantly reducing the achievable precision.

One of the proposed solutions to counter the effects of noise is to incorporate quantum error correction techniques within the quantum metrology scheme. It was shown that if the noise and signal satisfy an orthogonality conditioned, then the Heisenberg limit may be recovered by repeatedly performing error correction [2, 3]. Unfortunately, the necessary conditions to recover the Heisenberg limit are unattainable with current quantum technologies. For example i) instantaneous error correction with an infinitesimal wait time between applications, ii) the availability of noiseless ancilla, and iii) error correction performed with perfect fidelity.

In our study we explore a model with discrete applications of error correction ; illustrated in Figure 1. We keep current technological limitations in mind and focus on a specific error correction model : a parity check with an ancillary qubit. As expected, we show that the duration of time which the Heisenberg limit can be achieved is extended, but cannot not be achieved indefinitely. We discuss the limitations of general error correction strategies for quantum metrology. Lastly, we benchmark the factors of today's quantum technologies which need to be improved upon such that one can reliably achieve a Heisenberg limit level of precision.

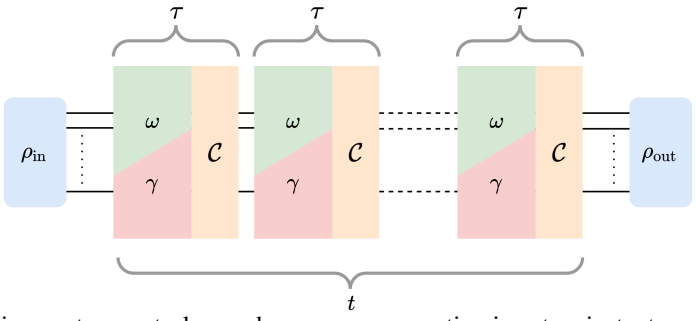


FIG. 1 : In a realistic quantum metrology scheme, error correction is not an instantaneous process, and that the wait time between error correction is not infinitesimally small. We account for this by setting a finite time τ between applications of error correction ; during which the evolution of the input state, ρ_{in}, is influenced by the signal ω and the noise γ. This process is repeated t/τ times. The final quantum state ρ_{out} is used for parameter estimation.

[1] B. M. Escher, R. L. de Matos Filho, and L. Davidovich. "General framework for estimating the ultimate precision limit in noisy quantum-enhanced metrology." Nat. Phys. 7.5 : 406-411 (2011).
[2] S. Zhou, M. Zhang, J. Preskill, and L. Jiang. "Achieving the heisenberg limit in quantum metrology using quan-tum error correction." Nat. Commun., vol. 9,no. 1, pp. 1–11, (2018).
[3] R. Demkowicz-Dobrzański, J. Czajkowski, and P. Sekatski. "Adaptive quantum metrology under general markovian noise." Phys. Rev. X, vol. 7, no. 4, p. 041009 (2017).

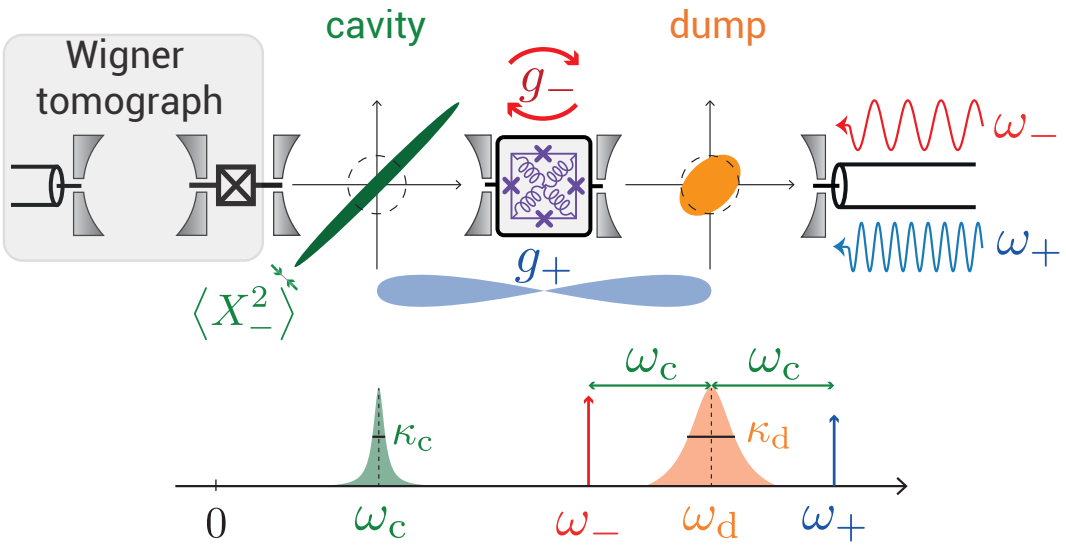
* nathan.shettell@lip6.fr

Stabilization of squeezing beyond 3 dB in a microwave resonator by reservoir engineering.

Rémy Dassonneville[1], Réouven Assouly[1], Théau Peronnin[1], Aashish Clerk[2], Audrey Bienfait[1], and Benjamin Huard[1*]
[1]*Univ Lyon, ENS de Lyon, Univ Claude Bernard, CNRS, Laboratoire de Physique,F-69342 Lyon, France*
[2]*Pritzker School of Molecular Engineering, University of Chicago, Chicago, IL 60637, USA*

Squeezed states, whose fluctuations on one quadrature are below the zero point fluctuations (ZPF) at the expense the other, are an instrumental resource for quantum sensing and information processing. Squeezing is usually generated by parametrically pumping a resonator. While any amount of squeezing can theoretically be obtained for the outgoing field, the intraresonator squeezing is limited to 3 dB below the ZPF. Indeed, input-output relations impose that the intraresonator fluctuations result from the average of the ingoing ZPF and outgoing squeezed fluctuations. Using reservoir engineering techniques [2], the 3 dB limit has recently been overcome in a mechanical resonator [1]. However, a proof of principle is still missing for electromagnetic modes.

In this work, we use two parametric pumps and a dump mode to engineer an effective coupling to an artificial squeezed reservoir. We perform in-situ Wigner tomography of the squeezed microwave mode using an ancillary superconducting qubit. We measure intraresonator squeezing as high as 6.73 +-0.03 dB, going well beyond the 3 dB limit. Interestingly, the non-classicality of the squeezed state is demonstrated using photon number statistics.



[1] C. U. Lei, et al, "Quantum Nondemolition Measurement of a Quantum Squeezed State Beyond the 3 dB Limit", Phys. Rev. Lett. **117** (2016).

[2] A. Kronwald, et al, "Arbitrarily large steady-state bosonic squeezing via dissipation", Phys. Rev. A **88** (2013).

* remy.dassonneville@ens-lyon.fr

Detecting spins with a microwave photon counter

Emanuele Albertinale[1], Léo Balembois[1], Eric Billaud[1], Vishal Rajan[1], Daniel Flanigan[1], Thomas Schenkel[2], Daniel Estève[1], Denis Vion[1], Patrice Bertet[1], Emmanuel Flurin[1]
[1]*Quantronics group, SPEC, CEA, CNRS, Université Paris-Saclay, CEA Saclay 91191 Gif-sur-Yvette Cedex, France,* [2]*Accelerator Technology and Applied Physics Division, Lawrence Berkeley National Laboratory, Berkeley, California 94720, USA*

Operational single photon counters at microwave frequencies have been developed recently. Here we plug such a single microwave photon counter [1] to the output of a superconducting micro-resonator, itself coupled to an ensemble of bismuth donor electron spins in silicon at millikelvin temperatures in the Purcell regime [2]. We report the direct observation of the microwave photons emitted by the spins, during their energy relaxation following a pi pulse. Moreover by changing the area of the exciting pulse we were able to measured Rabi oscillations in the variation of the total number of detected photons. Finally we report the direct observation of the photons emitted from the spin ensemble in a Hahn echo experiment.

[1] R. Lescanne, S. Deléglise, E. Albertinale, U. Réglade, T. Capelle, E. Ivanov, T. Jacqmin, Z. Leghtas, and E. Flurin, "Irreversible qubit-photon coupling for the detection of itinerant microwave photons," *Physical Review X*, vol. 10, no. 2, p. 021038, 2020.

[2] A. Bienfait, J. Pla, Y. Kubo, X. Zhou, M. Stern, C. Lo, C. Weis, T. Schenkel, D. Vion, D. Esteve, *et al.*, "Controlling spin relaxation with a cavity," *Nature*, vol. 531, no. 7592, pp. 74–77, 2016.

Optical control of an individual Cr atom : towards a spin qubit for nano-mechanical systems

V. Tiwari[1], K. Makita[2], M. Arino[2], M. Morita[2], T. Crozes[1], E. Bellet-Amalric[3], S. Kuroda[2], H. Boukari[1] and L. Besombes[1*]
[1] *Univ. Grenoble Alpes, CNRS and Grenoble INP, Institut Néel, 38000 Grenoble, France*
[2] *University of Tsukuba, Institute of Material Science, Tsukuba 305-8573, Japan*
[3] *Univ. Grenoble Alpes and CEA,IRIG-PHELIQS, 38000 Grenoble, France*

Spin in solids are promising *qubits* for various quantum technologies including quantum sensing and quantum computing. However, long-distance spin-spin coupling is difficult to achieve. One possible route is phonon-assisted spin-spin coupling in a mechanical resonator and surface acoustic waves (SAW) are proposed for long-range coupling in a wide range of *qubits* [1]. This will require spin *qubits* with a large spin to strain coupling. A variety of magnetic atoms (Mn, Fe, Co, Cr, etc.) can be incorporated in conventional semiconductors offering a large choice of localized electronic spins, nuclear spins as well as orbital angular momentums. Magnetic atoms with non zero orbital momentum are expected to present a large spin to strain coupling. This arises form the modification of the crystal field and spin-orbit coupling.

When a magnetic atom is inserted in a semiconductor quantum dot (QD), it can be addressed optically. This is in particular the case of Chromium that, when incorporated as Cr^{2+} in a CdTe/ZnTe QD, provides an electronic spin S=2 and an orbital momentum L=2 [2]. It has been shown that the $S_z = \pm 1$ spin states of Cr^{2+} form a spin *qubit* that could be efficiently coupled to in-plane strain.

We analyse here the effect of optically generated non-equilibrium phonons on the spin dynamics of a single Cr^{2+} ion inserted in a CdTe/ZnTe QD. Using a three pulses optical pumping experiment we demonstrate that the measured spin relaxation strongly depends on the optical excitation condition. We show that a tunable spin-lattice coupling dependent on the optically generated non-equilibrium phonon can explain the observed dynamics. We found excitation conditions where the Cr^{2+} spin states $S_z = \pm 1$ can be populated by non-resonant excitation, efficiently prepared by resonant optical pumping an conserved in the dark during a few μs [3]. This paves the way towards the coherent mechanical driving of the $\{+1; -1\}$ Cr^{2+} spin *qubit* with the strain field of SAW in the GHz range.

We demonstrate that efficient SAW transducers can be realized on these non-piezoelectric II-VI QD samples and that the emission of a QD can be used as an efficient sensor for the dynamical strain field of SAW. The energy of QDs is modulated by SAW in the GHz range and leads to characteristic broadening of time-integrated PL spectra. The dynamic modulation of the QD PL energy can also be detected in the time domain using phase-locked time domain spectroscopy. This technique is in particular used for monitoring complex local acoustic fields resulting from the superposition of two or more SAW pulses in a cavity. Under magnetic field, the dynamic spectral tuning of a single QD by SAW can be used to generate single photons with alternating circular polarization controlled in the GHz range [4].

Finally, we show that the probability of finding single Cr^{2+} is limited by the fluctuation of charge state of Cr. Cr^{+} with a $3d^5$ configuration (S=5/2, L=0) is indeed observed in the optical spectra of some QDs. This negatively charged excited state of the Cr is stabilized by the ferromagnetic exchange interaction with the spin of a confined heavy-hole. We will show that the resulting hole-Cr^{+} complex forms a stable ferromagnet with a spin memory in the 20 μs range at zero magnetic field and we will discuss some possible applications of this new nano-magnet.

[1] M.J.A. Schuetz, E.M. Kessler, G. Giedke, L.M.K. Vandersypen, M.D. Lukin, J.I. Cirac, "Universal quantum transducers based on SAW", Phys. Rev. X **5**, 031031 (2015).
[2] A Lafuente-Sampietro, H Utsumi, H Boukari, S Kuroda, L Besombes, "Individual Cr atom in a QD : Optical addressability and spin-strain coupling", Phys. Rev. B **93**, 161301(R) (2016).
[3] V. Tiwari, K. Makita, M. Arino, M. Morita, S. Kuroda, H. Boukari, L. Besombes, "Influence of nonequilibrium phonons on the spin dynamics of a single Cr atom", Phys. Rev. B **101**, 035305 (2020).
[4] V. Tiwari, K. Makita, M. Arino, M. Morita, T. Crozes, E. Bellet-Amalric, S. Kuroda, H. Boukari, L. Besombes, "Radio-frequency stress induced modulation of CdTe/ZnTe quantum dots", J. Appl. Phys. **127**, 234303 (2020).

* vivekanand.tiwari@neel.cnrs.fr

Quantum-enhanced interferometry in pulsed regime

Romain Dalidet[1], Anthony Martin[1], Laurent Labonté[1], Sebastien Tanzilli[1]
[1]*Université Côte d'Azur, CNRS, Institut de physique de Nice, France*

Measurement of optical properties such as crystal non-linearity, birefringence or absorption has been at the art of metrology since the last decades. The growth of accuracy and precision gave rise to numerous technologies in various fields, from pulsed laser source to tomography [1]. Chromatic dispersion (Group Velocity Dispersion), *i.e* the dependence of the group velocity of light in a medium as a function of the wavelength, plays a crucial role in fiber communication and pulse shaping. GVD has been extensively measured using both classical and quantum light theory. Unfortunately few works have been reported to directly measure higher order dispersion such as Third Order Dispersion (TOD). Recent work based on NOON state generation has led to state-of-the-art GVD measurement [2]. However, the measurement is limited to one value, forbidding experimental access to third and higher-order dispersion coefficients. Here, we report a numerical study showing that this limitation can be surpassed in pulsed regime while keeping the unprecedent precision. The coincidence rate of NOON states passing through a Mach-Zehnder interferometer (Fig.1) is :

$$P_c \propto cos^2(\phi) \approx cos^2\Big(L \sum \frac{k_{s,i}^{(n)} \Delta\omega_{s,i}^n}{n!}\Big) \tag{1}$$

Here, $k_{s,i}^{(n)}$ is the n-th derivative of the wave vector for signal and idler photons at the degenerate wavelength, $\Delta\omega$ is the frequency offset and L is the length of the sample under test. In the continuous regime, $\Delta\omega_s = -\Delta\omega_i$ and odd-order dispersion terms vanish. Conversely, in pulsed regime, odd-orders do not vanish anymore as the last property is not always verified.

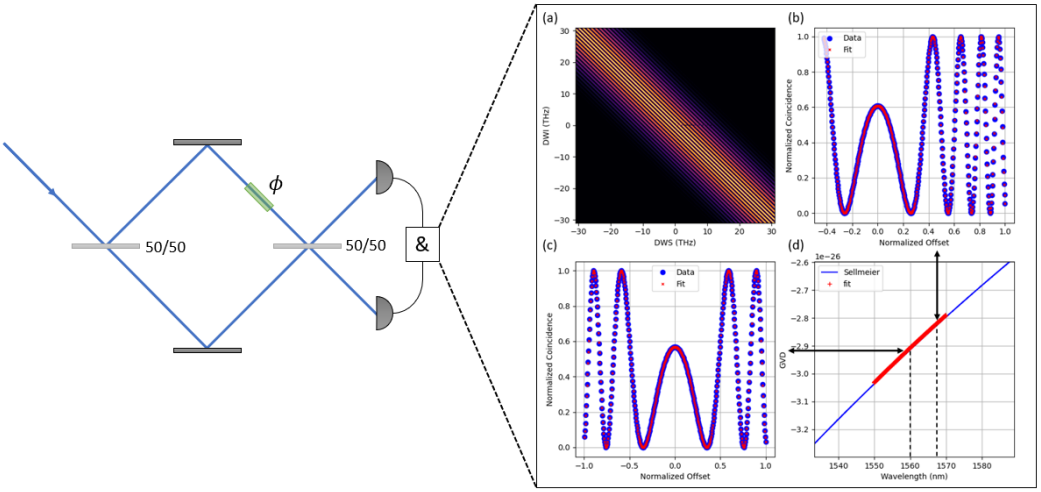


Fig. 1 : Left : Mach-Zehnder interferometer, inducing a relative phase difference ϕ. Right : a) Typical JSI measured. b) and c) Extracted diagonals at $\lambda = 1567$ and 1560 nm respectively. d) Extracted GVD from which TOD can be calculated.

We use the Joint Spectral Intensity (JSI) which represents the spectral correlations of the photon pairs. At the output of the interferometer (Fig.1), the measured JSI stands as the coherent superposition of the standard JSI associated to the photons pairs and the JSI from the pairs passing through the sample under test, leading to interference pattern from which the GVD can be extracted. Indeed, every diagonals correspond to a continuous case with a different pump wavelength, from which the GVD can be extracted. We benchmark our approach by inferring the GVD and TOD of fused silica over a 20nm range (Fig.1.d). We find the TOD precision to be less than 1% over the entire spectral range.

[1] Palmieri et al. npj Quantum Inf 6, 20 (2020).

[2] Kaiser et al. Light Sci Appl 7, 17163 (2018).

Quantum Processing, Algorithm, & Computing (QPAC)

Fast differentiable evolution of quantum states under Gaussian transformations

Yuan Yao and Filippo M. Miatto
Institut Polytechnique de Paris and
Télécom Paris, LTCI, 19 Place Marguerite Perey 91120 Palaiseau, France

I. INTRODUCTION

Parametrized optical quantum circuits process quantum information by propagating quantum states of light through a sequence of parametrized optical transformations [1]. Working in the optical domain has several advantages such as no low temperature or vacuum requirements, and the possibility of building compact devices via integrated optics [2].

A possible way to achieve a universality is by combining Gaussian transformations (such as beam splitters, squeezers, displacements, phase shifters) and non-Gaussian ones (such as the Kerr gate) [3]. Such circuits can already be trained via Machine Learning techniques [4]. However, current methods can quickly become very demanding in terms of computational resources, and this makes it challenging to apply them to the design of devices that make use of several optical modes.

II. METHODS

In a previous work [5], we introduced a recursive, differentiable algorithm to compute the transformation matrix associated with each gate. This algorithm was approximately 2 orders of magnitude faster than previous methods [6]. In our current research, we designed a new algorithm that directly computes the output state without the need to compute the transformation matrix. Our algorithm is differentiable thanks to the differentiability of the recurrence relation on which it relies.

III. RESULTS

If we train a circuit on a pure state input, our new algorithm is exponentially faster in the number of optical modes M, as the number of tensor elements that need to be computed is lower by a factor $\mathcal{O}(1/2^M)$ with respect to having to compute the whole transformation tensor. Moreover, back-propagated gradient tensors have the shape of the state, rather than the shape of the transformation tensor, which is a square root improvement that benefits circuits with respect to their depth.

IV. DISCUSSION

The outstanding challenge is that if the input state is mixed, we would have to run it on each significant eigenstate, thus getting a performance hit proportional to the rank of the state. However, in early numerical benchmarks we have noticed no impact, probably thanks to automatic code vectorisation.

[1] G. R. Steinbrecher, J. P. Olson, D. Englund, and J. Carolan, npj Quantum Inf. **5**, 1 (2019).
[2] A. Politi, J. C. Matthews, M. G. Thompson, and J. L. O'Brien, IEEE J. Sel. Top. Quantum Electron. **15**, 1673 (2009).
[3] S. Lloyd and S. L. Braunstein, in *Quantum information with continuous variables* (Springer, 1999) pp. 9–17.
[4] L. Banchi, N. Quesada, and J. M. Arrazola, Phys. Rev. A **102**, 012417 (2020).
[5] F. M. Miatto and N. Quesada, "Fast optimization of parametrized quantum optical circuits," (2020), arXiv:2004.11002 [quant-ph].
[6] N. Killoran, T. R. Bromley, J. M. Arrazola, M. Schuld, N. Quesada, and S. Lloyd, Phys. Rev. Research **1**, 033063 (2019).

Cavity-photon induced state transitions in a coupled Fluxonium qubit system

Jeremy Stevens[1], Alexis Jouan[1], Nathanael Cottet[1,2], Long Nguyen[3], Aaron Somoroff[3], Quentin Ficheux[3], Audrey Bienfait[1], Vladimir Manucharyan[3], Benjamin Huard[1*]
[1] *École Normale Supérieure de Lyon, France*
[2] *Yale University, USA*
[3] *University of Maryland, USA*

Superconducting qubits are a subject of intense research as a platform for scalable quantum computing. While transmon qubits have received a lot of attention, the less ubiquitous Fluxonium qubit has been shown to have long lifetimes and gates unlimited by level anharmonicity [**?**]. Despite this, little research has been put into studying multi-Fluxonium devices. Here, one of the difficulties is understanding how their rich level structure can make them prone to measurement photons inducing transitions out of the qubit subspace [**?**]. We present a systematic study of a system comprising two capacitively coupled Fluxonium qubits sharing the same read-out cavity. By tracking the state dependent transmission of the read-out pulse, we determine the transition rates from state i to state j of the coupled system using a forward-backward analysis [**?**] to characterize these cavity induced transitions. By varying the flux bias of the system and the population of the cavity, we characterize the fidelity of this read-out.

[1] L.B. Nguyen et al., Phys. Rev. X 9 041041, 2019
[2] D. Sank et al., Phys. Rev. Lett. 117 190503, 2016
[3] T. Rybarczyk et al., Physical Review A 91 062116, 2015

* jeremy.stevens@ens-lyon.fr

Twenty millisecond electron-spin coherence in an erbium doped crystal

Miloš Rančić[1], Marianne Le Dantec[1], Emmanuel Flurin[1], Denis Vion[1], Daniel Esteve[1], Patrice Bertet[1], Philippe Goldner[2], Thierry Chanelière[3], Sylvain Bertaina[4], Sen Lin[5], Ren Bao Liu[5*]

[1]*Quantronics Group, SPEC, CEA Saclay, Saclay, France*

[2]*Chimie ParisTech, PSL University, Paris, France*

[3]*Institut Néel, Univ. Grenoble Alpes, Grenoble, France*

[4]*IM2NP, Faculté des Sciences et Techniques, Marseille, France*

[5]*Department of Physics and The Hong Kong Institute of Quantum Information Science and Technology, The Chinese University of Hong Kong, Hong Kong, China*

Rare-earth-ions are interesting physical systems because they have long lived states and record coherence times for both the optical and nuclear transitions [1, 2]. Rare Earths with an odd number of electrons are also paramagnetic, with an electronic transition that can be studied by standard Electron Paramagnetic Resonance (EPR) spectroscopy at GHz frequencies. For such transitions, coherence times up to 2 ms have been measured at temperatures greater than 100 mK [3]. In this talk, I will present our recent EPR results in 50 ppm and 10 ppb Er^{3+} doped $CaWO_4$. These measurements were recorded in a previously unstudied temperature regime for this material : sub-Kelvin temperature down to 10 mK, using a superconducting micro-resonator and a superconducting parametric amplifier [4, 5]. We observe the longest recorded Hahn-echo decay for an electronic spin transition in a rare earth doped material, up to 20 milliseconds. With two and three pulse echo measurements, we are further able to probe the ultra-slow spin dynamics at these low temperatures and compare our results with theoretical predictions of spin-spin and spin-lattice relaxation.

[1] Bottger, T., Thiel, C. W., Cone, R. L. and Sun, Y. "Effects of magnetic field orientation on optical de-coherence in Er3+ :Y2SiO5", Phys. Rev. B **79**, 115104 (2009).

[2] Zhong, M. et al. "Optically addressable nuclear spins in a solid with a six hour coherence time". Nature **517**, 177-180 (2015).

[3] Li, P. et al. "Hyperfine Structure and Coherent Dynamics of Rare-Earth Spins Explored with Electron-Nuclear Double Resonance at Subkelvin Temperatures" Phys. Rev. Appl **13**, 024080 (2020).

[4] Haikka, P., Kubo, Y., Bienfait, A., Bertet, P. and Molmer, K. "Proposal for detecting a single electron spin in a microwave resonator", Phys. Rev. A **95**, (2017).

[5] Bienfait, A. et al. "Reaching the quantum limit of sensitivity in electron spin resonance", Nat. Nanotechnol. **11**, 253-257 (2015).

* milos.rancic@cea.fr

6 Index of Authors

Author Index

7 List of Participants

List of participants

- Abadillo-Uriel Jose Carlos
- Abbasi Zargaleh Soroush
- Abbott Alastair
- Abroug Neil
- Aggarwal Anuj
- Albertinale Emanuele
- Alibart Olivier
- Amanti Maria
- Anthore Adrien
- Appas Félicien
- Arnault François
- Auffèves Alexia
- Ayari Anthony
- Aymeric Raphaël
- Ayral Thomas
- Babin Charles
- Baboux Florent
- Bancal Jean-Daniel
- Baron Yoann
- Bassi Marion
- Bauer Michel
- Bauerle Christopher
- Belabas Nadia
- Benito Maria
- Bertet Patrice

- Bertrand Benoit
- Besserve Pauline
- Bettonte Gabriella
- Bienfait Audrey
- Billard Marie
- Billaud Eric
- Billiot Gerard
- Bonnin Alexis
- Bourdel Pierre-Antoine
- Bourlet Nicolas
- Bouscal Adrien
- Bredariol Grilo Alex
- Bresque Léa
- Brune Michel
- Brunel Floriane
- Cailliau Florian
- Campagne-Ibarcq Philippe
- Camus Philippe
- Carette Titouan
- Cenni Marina
- Chabaud Ulysse
- Chanelière Thierry
- Charbonnier Jean
- Charles Henri-Pierre
- Chen Antoine
- Chomaz Philippe
- Chu Yiwen
- Cohen Mathis
- Collange Caroline
- Contamin Lauriane
- Coste Nathan
- Couteau Christophe

- D'auria Virginia
- Dalidet Romain
- Dalyac Constantin
- Dassonneville Rémy
- David Jean-Baptiste
- De Boutray Henri
- De Forges De Parny Laurent
- De Franceschi Silvano
- Defienne Hugo
- Degiovanni Pascal
- Demarty Marine
- Denys Aurélie
- Desjardins Pierre
- Desprez Frédéric
- Diamanti Eleni
- Dixit Anvesh
- Dotsenko Igor
- Dourdent Hippolyte
- Doutre Florent
- Dréau Anaïs
- Ducci Sara
- Dumur Étienne
- Durand Alrik
- Durt Thomas
- Dutta Biplab
- El Homsy Victor
- Eremeev Vitalie
- Esposito Martina
- Esteve Daniel
- Etesse Jean
- Ezratty Olivier
- Ezzouch Rami

- Fabre Nicolas
- Fainsin David
- Febvre Pascal
- Fedrici Bruno
- Fellous Marco
- Ferlaino Francesca
- Ferrero Michel
- Ferrier-Barbut Igor
- Filipovic Jovana
- Francesconi Saverio
- Frerot Irénée
- Gaignard Maxime
- Galland Christophe
- Gamrat Christian
- Garbe Louis
- Garcia Sébastien
- Gidney Craig
- Giorgetti Alain
- Girit Çağlar
- Goffman Marcelo
- Goldner Philippe
- Gorceix Olivier
- Goswami Ashutosh
- Gouveia Arnaldo
- Gouzien Élie
- Greneche Jean-Marc
- Gu Xuemei
- Guerin Stephane
- Guthmuller Eric
- Hansen Hubert
- Henner Théo
- Henry Antoine

- Hetet Gabriel
- Hilaire Paul
- Horodecki Pawel
- Hua Xin
- Huard Benjamin
- Jacquinot Hélène
- Jonval Maxime
- Joulain Karl
- Kaali Srinivasan
- Kadri Hachem
- Kashefi Elham
- Keller Arne
- Kemlin Vincent
- Kerstel Erik
- Kilber Natalie
- Klaus Lauritz
- Klemt Bernhard
- Kouadou Tiphaine
- Koukiou Flora
- Krebs Olivier
- Labonté Laurent
- Lafforgue Louis
- Lafoucriere Jacques-Charles
- Lagarrigue Alek
- Lahaye Thierry
- Lamic Baptiste
- Lanco Loïc
- Le Dantec Marianne
- Lefloch François
- Lemonde Pierre
- Lim Caroline B.
- Liu Yujia

- Long Romain
- Louise Stéphane
- Loulidi Faedi
- Mansfield Shane
- Martin Anthony
- Martinez I Diaz Biel
- Marulanda Acosta Valentina
- Massé Gaël
- Masson Pierre-Alain
- Maussang Kenneth
- Mazzoncini Francesco
- Mehdi Elham
- Melalkia Mohamed Faouzi
- Meyer Uta
- Milchakov Vladimir
- Morel Adrien
- Mothe Raphaël
- Mounier Eric
- Nahra Mackrine
- Nechita Ion
- Niegemann David
- Niquet Yann-Michel
- Nurizzo Martin
- Olivier Segolene
- Olivo Andrea
- Ottolenghi Alberto
- Ourjoumtsev Alexei
- Paul Hermouet
- Pelet Yoann
- Pellet-Mary Clément
- Peronnin Théau
- Perruchot Francois

- Petta Jason
- Peyruchat Léo
- Picholle Eric
- Planat Luca
- Poizat Jean-Philippe
- Ponchon Thibault
- Pothier Hugues
- Ranadive Arpit
- Rancic Milos
- Rath Aniket
- Ravets Sylvain
- Raymond Arnault
- Réouven Assouly
- Reymond Georges
- Robert-De-Saint-Vincent Martin
- Roch Nicolas
- Rodriguez Ramiro
- Roeland Ganaël
- Roscilde Tommaso
- Rouabah Taha
- Rouchon Pierre
- Roussel Benjamin
- Rouvière Clémentine
- Sabonis Deividas
- Salas-Montiel Rafael
- Samson Diana
- Sangouard Nicolas
- Sansavini Francesca
- Sauder Greg
- Scherübl Zoltán
- Schuhmann Jérémie
- Schwartz Sylvain

- Shettell Nathan
- Shukla Vishakha
- Stevens Jeremy
- Szombati Daniel
- Tanzilli Sébastien
- Thibault Xavier
- Thomas Candice
- Tiwari Vivekanand
- Toffano Zeno
- Tosi Leandro
- Trigo Vidarte Luis
- Urbina Cristian
- Valcarce Xavier
- Van Den Bossche Mathias
- Vaneecloo Julien
- Vermersch Benoit
- Vidick Thomas
- Vincent Estelle
- Vinet Maud
- Vion Denis
- Vyas Nilesh
- Walschaers Mattia
- Wang Junliang
- Wen Yutian
- Whitney Robert
- Yacoub Verena
- Yao Yuan
- Yavkin Boris
- Yehia Raja
- Yu Cécile
- Zanon Thomas
- Zaquine Isabelle
- Zihlmann Simon
- Zivy Julian

http://gdriqfa.cnrs.fr/

IQFA'11 is organized at Université Grenoble Alpes

by IQFA's Scientific Committee and the members of the Institut Néel.

With the financial supports and help of