Back to Belgium Grants

Final Report

Name of the researcher	Raul Garcia-Patron Sanchez
Selection Year	2013
Host institution	Université Libre de Bruxelles
Supervisor	Professor Nicolas Cerf
Period covered by this report	from 01/03/2014 to 30/09/2015
Title of the project	Quantum Information Processing with Photons

1. Objectives of the proposal

The research project *Quantum Information Processing with Photons* was designed to advance the theoretical understanding of quantum information processing with photons. The science of developing novel technology applications based on the fundamental quantum mechanical properties of optical systems.

Building on my previous experience in the field, ranging from the study of secret key distribution over optical links to the more fundamental aspects of quantum mechanics, such as it non-local behaviour, we designed a research project divided into three different axes: quantum cryptography, quantum communication and quantum computation.

Quantum Key Distribution (QKD) is a quantum technology that allows the distribution of secret key between two partners in an untrusted environment. QKD can be considered the most successful quantum technology to date, currently achieving the distribution of secret key over optical-fibre links of few hundred kilometres. In this project we focused on a family of protocols based in the use of coherent states of light. Their main advantage is that they can be implemented with standard telecom components, that they are compatible with wavelength division multiplexing, and they can reach high repetition rates, facilitating their integration into real-world telecommunication networks. The main objectives where threefold. First of all, complete the security analysis on continuous-variables quantum key distribution protocols based on coherent states on the finite-size regime, which is important for realistic field-implementation. More precisely we wanted to prove the security of this family of protocols against an eavesdropper that implements attacks that are invariant over permutations of the signal light pulses, a subset of attacks that we previously proved that was sufficient to have complete security [1]. Secondly, because a series of experiments had demonstrated the possibility of hacking attacks on QKD commercial platforms [2], which pose a real challenge to the quantum cryptography community, we wanted to produce a detailed list of side-channels attacks that a potential hacker could use against coherent state based QKD protocols and study them theoretically and experimentally. The last point was to adapt the tools of device-independent quantum key distribution, protocols where the trustworthiness of the apparatus assumption can be relaxed making them resistant against hacking attacks, to the family of protocols based on coherent states.

The main objective of the **quantum communication** part was to solve an old open problem in the field of quantum communication: *what is the ultimate data transmission rate achievable over an optical communication channel for a given input power?* More concretely we were interested on the ultimate data transmission rate achievable over Gaussian Bosonic channels, a good model of single-mode optical communication channel, which can later be used as a building block to estimate the ultimate rate of physical channels such as optical-fibres and free-space links whenever the non-linear effects can be neglected. The second objective of the quantum communication part was to study whether the communication of classical bits can be improved by supplementing the quantum communication channel with a classical feedback (noiseless) channel. In the case of Shannon's Information Theory, the answer is known to be negative [3]. Despite some evidence [4], so far no conclusive examples have been found where classical feedback can improve the capacity of communicating bits over a quantum channel a question we intended to solve during this research project.

The **quantum computation** section of the prôject relates to the fundamental question of whether one can prove that quantum computers are strictly more powerful than classical universal Turing machines, and if so, what exactly makes them more powerful. It turns out that quantum optics provide a very interesting ground for analyzing this question, as shown by Aaronson and Arkhipov with their *boson-sampling* proposal of 2010 [5]. This work provided evidence that sampling the distribution resulting from scattering N bosons over a linear-optical interferometer cannot be simulated efficiently in a Turing machine unless an extremely unlikely conjecture in Theoretical Computer Science is true[1]. The first objective of this las part of the research project was to analyse the hardness of simulation of two variations of the initial boson-sampling proposal, the first replacing the photon-counting detectors by homodyne detection and the second replacing the single-photon sources by Gaussian states while still using photon-counting detectors. Secondly, we wanted to analyse whether Aaronson and Arkhipov's mathematical proof of the hardness of boson-sampling is resilient to a realistic quantum optics implementation with natural noise and imperfections. There is evidence of this being true [6, 7, 8, 9, 10], but no final proof. Finally, we wanted to investigate the existence of new non-trivial set of photonic states, other than Gaussian states, that could be simulated efficiently in a classical computer. The motivation being that enlarging the class of states and operations that can be simulated in a classical computer would result in the discovery of new physics and the proposal of interesting new quantum optics experiments, as it was the case with the development of the theory of Gaussian states.

2. Methodology in a nutshell

The Centre for Quantum Information and Communication at ULB, with its long-standing expertise in quantum information processing with photonic system was the ideal environment for attacking, in collaboration with its members, this set of problems on quantum information processing with photons. The research calendar was designed to work in parallel on the three axes of research of the proposed project during the two years of the BELSPO Return Grant. The research program was designed to achieve a good balance between problems related to realistic implementations of quantum information processing tasks in photonic architectures and open problems of more fundamental interest.

---

[1] The mentioned conjecture is the collapse of the Polynomial Hierarchy to the third level.

3. Results

In December 2013, few months before the start of my BELSPO return grant, while participating in the *Mathematical Challenges in Quantum Information* program at the Isaac Newton Institute for Mathematical Sciences at Cambridge University, where I was invited as Visiting Fellow from September to December 2013, I managed to solve in collaboration with Vittorio Giovannetti, Alexander Holevo and Nicolas Cerf the longstanding open problem that was the main objective of the quantum communication part of this project, i.e., calculate the ultimate data transmission rate achievable over Gaussian Bosonic channels (Ref. 1 and 2)[2].

This problem had remained open for more than a decade and few well-renowned theoretical physicist had tried to solve it without much success. The crucial part of the proof resided on technical tools developed by myself and collaborators in two consecutives work, the first during my postdoctoral time at the Massachusetts Institute of Technology [11] and the second during my Humboldt Postdoctoral experience at the Max-Planck Institute for Quantum Optics [12]. Interestingly, these tools are rather simple to understand and build on basics properties of Gaussian channels and well-known quantum Shannon's theory results, which properly combined in my previous work opened a new perspective to the problem and lead to its final solution in 2013.

This important result allowed me to close the semester program *Mathematical Challenges in Quantum Information* at the Isaac Newton Institute for Mathematical Sciences (Cambridge, UK) with the talk *A solution of the Gaussian optimizer conjecture,*[3] which presented this result to the scientific community. Since then I have presented this result in several important research institutions, such as Caltech Institute for Quantum Information[4] (April 1, 2014) or the IBM Thomas J. Watson Research Center (NY, April 25, 2014), see section 4 for more details. This important result lead to a publication on the journal Nature Photonics [12], a result that lead to few press releases as detailed in section 4 of this manuscript, among them the last *Case Study* published by the Isaac Newton Institute for Mathematical Sciences[5], a series of documents that are published to "*become a substantial body of evidence to ensure that the Institute can demonstrate its effectiveness to funders and stakeholders*".

After this work I participated on a collaboration together with Bhaskar Roy Bardhan and Professor Mark M Wilde from Louisiana State University (Baton Rouge), and Professor Andreas Winter from Universitat Autònoma de Barcelona that establish the classical capacity of optical quantum channels as a sharp transition between two regimes; one which is an error-free regime for communication rates below the capacity; and the other in which the probability of correctly decoding a classical message converges exponentially fast to zero if the communication rate exceeds the classical capacity (Ref 5). This result builds on my previous result (see paragraph above and Ref. 1 and 2) and is obtained by proving a strong converse theorem for the classical capacity of all phase-insensitive bosonic Gaussian channels. Apart from bolstering the understanding of the classical capacity of these channels this new work opens the path to applications, such as proving the security of noisy quantum storage models of cryptography with optical links. This last work resulted in a publication in the Transaction of Information Theory journal of the IEEE society.

---

[2] We use (Ref. X) to refer to papers on my publications list in section 4 of this report.
[3] https://www.newton.ac.uk/seminar/20131217140015001
[4] http://www.iqim.caltech.edu/seminars/iqi_seminars_2013-14.html
[5] https://www.newton.ac.uk/files/reports/casestudies/quantum.pdf

After completing this two pieces of work I focused on attacking the second problem of the quantum communication section of our project, namely the study whether the communication of classical bits can be improved by supplementing the quantum communication channel with an assisting classical feedback channel. Despite not being fruitful in obtaining an answer to this question, the research lead to a relatively different result that focuses on the distribution of randomness over quantum channels instead of the transmission of information. Information and randomness being different concepts, the capability to distribute them over a channel should be inequivalent resources. More precisely, the capability to distribute a bit of randomness is a weaker resource than the potential to communicate a bit of information over a channel. Nevertheless, in a work in collaboration with Professor Andreas Winter from Universitat Autònoma de Barcelona and Dr. William Matthews from Cambridge University we showed that the capacity of a classical channel to achieve both tasks is the same. In other words, the optimal way of distributing randomness classically is to generate it locally and transmit it through a communication channel. On the other hand, this changes radically in the quantum realm, as we give examples of quantum channels where the capacity of randomness distribution (when assisted by classical feedback) is strictly higher than that of communicating messages. Therefore, there exist protocols that unlock quantum randomness initially hidden inside the channel. The connection with the initial problem proposed in the research proposal resides in that the kind of protocols needed to show this strict separation need assistance by assisting classical feedback communication. This result was presented by myself at the conference TQC2015 that took place in Brussels and QIPC2015 in Leeds and will be soon posted on the arXiv and submitted to a journal, see section 4 for more details.

During 2015 I decided, after having solved a longstanding open problem on the ultimate data transmission rate achievable over Gaussian Bosonic channels, to reorient the research objectives of the quantum communication part of the BELSPO grant to a new direction of research. Motivated by the writing of research statement to apply for permanent position and the prospect of applying for research grant that could allow to start a research team, I started to investigate new applications of my previous work on Gaussian Bosonic channels that could be of interest to the community of optical-fiber communication. In May I participated in a conference organized by the Royal Society on *Communication networks beyond the capacity crunch*[6], where I gave a talk on its satellite meeting[7]. This conference focused on the challenges that the community of optical-fibre communication is facing today to increase the communication rate in order to keep up with the expected demand of network traffic. Additionally, during a visit to MIT during the summer 2015 I took the opportunity to visit Réné Essiambre, a world-expert on the physics of non-linear effects on optical fibres and optical communication, working at Bell Labs (Crawford Hill, NJ, USA). Similarly, I had a variety of interactions with experimental groups, such as the *High-Speed Optical Communications Group* and the Technical University of Denmark (Lyngby, 14 April, 2015) or the *Optical Networks Group* from University College London, which organized the Royal Society event I mentioned before. This exposure to the field of optical communication has allowed me to build a set of interesting question that I could work in the future, which resolve around the question of whether quantum technologies could help overcome current challenges in optical communication.

The remaining part of my time during the BELSPO fellowship has been devoted to the third section of the project, i.e., quantum computation over photonic system and more concretely on research connected to the concept of boson-sampling. A fundamental question raised by large-size quantum devices is whether there exists a strict separation in terms of computational power between classical

[6] https://royalsociety.org/events/2015/05/communication-networks/
[7] https://royalsociety.org/events/2015/05/communication-networks-sm/

and quantum computation and if this can be experimentally tested. It was recently argued that photonic circuits may play a relevant role in answering this question through the paradigm of *Boson sampling*[8], a large-size quantum photonic device that makes single-photons interfere through a quantum linear-optics circuit and outputs its photon-number statistics.

Since the initial boson-sampling proposal by Professor Scott Aaronson and his PhD student Alex Arkhipov from Massachusetts Institute of Technology, and revealed in 2010 while I was working there, I have been following closely the evolution of this research area, as it allowed me to combine my interest for computer science with my research on quantum information processing with photons.

During my participation at the semester program *Mathematical Challenges in Quantum Information* at the Isaac Newton Institute for Mathematical Sciences (Cambridge, UK) I participated in an open discussion following a blog post by Professor Scott Aaronson on his world-renowned blog. In my comment I explained how a similar argument for the hardness of boson-sampling can be slightly modified to proof the hardness of classically simulating the exact sampling of Gaussian states on the Fock basis[9], which solves one of the two question of the quantum computation part of my BELSPO project, i.e., the hardness of variants of boson-sampling; More precisely, the one where single-photons sources are replaced by Gaussian states but still send them through a linear-optics interferometer and detected by photon-counting detectors. I also had the opportunity to present this result during a seminar for doctoral students at Paris TelecomTech and will be submitted to the arXiv with additional result in the next months.

In the direction of the second question we wanted to address in the quantum computation part of the project, i.e., analysing how resilient is the hardness of boson-sampling to a realistic quantum optics implementation with natural noise and imperfections, I did some progress during my BELSPO fellowship in a collaboration with Dr. Anthony Leverrier research scientist at INRIA (Paris). In this work we study the only imperfection that had not been addressed so far, the quality of the implementation of the desired unitary transformation representing the linear-interferometer. We analysed how accurate should the implementation be in order for the sampled distribution to be reasonably close to the ideal one (Ref. 3).

Additionally, during the first months of my BELSPO grant I participated, together with 8 leading group of European institutions, in the design of the H2020 European research project *Quantum Simulation on a Photonic Chip* (QUCHIP) focusing on the advance of quantum simulation over photonic integrated chips. The proposal was selected for funding and started in March 2015[10], consisting on a budget of 2,681,713 €, which 120,000 € go to the ULB. This budget allowed me to hire a postdoc, Levon Chakhmakhchyan, which has been working with me on problems related to boson-sampling. Under my supervision, Levon Chakhmakhchyan has designed a quantum-inspired algorithm which exploits tools from quantum optics to develop a novel approach to address an open question in computer science, the estimation of the permanent of Hermitian positive semidefinite matrices. A work that highlights the benefits that further exploration of the connection between the theory of computer science and quantum optics could bring to both communities.

---

[8] S. Aaronson, A. Arkhipov, *The Computational Complexity of Linear Optics*, STOC '11

[9] http://www.scottaaronson.com/blog/?p=1579#comment-92082

[10] http://www.quchip.eu/

Previously, I mentioned that motivated by the writing of research statement to apply for permanent position and the prospect of applying for research grant that could allow to start a research team, I started to investigate new applications of my work on quantum communication realized during my BELSPO fellowship. In parallel I did a similar brainstorming for the area of research concerning quantum computation over integrated photonic circuits, which allowed me to build a set of interesting question that I could work in the future and that has already being fruitful in helping me secure funding from the Wiener-Anspach foundation to implement a two-year research program in collaboration with the quantum optics group of Professor Ian Walmsley from Oxford University.

Due to time constraint it has been very difficult for me to make progress on the first part of the BELSPO project related to quantum key distribution. After seeing that: (i) the first objective of the QKD part of the project, i.e., the completion of the security analysis on continuous-variables quantum key distribution protocols based on coherent states on the finite-size regime, was concluded by Dr. Anthony Leverrier research scientist at INRIA (Paris) [13]; (ii) that a series of works were already addressing the second point of my project, i.e., a detailed list of side-channels attacks by a potential hacker; (iii) the uncertainty of obtaining a positive result on the third point of the project; i.e., device-independent quantum key distribution with coherent states; I decided to focus all my time and energy on the two other parts of the project, which resulted in very fruitful result, as presented above.

Additionally, during the time of my BELSPO fellowship I had the opportunity to co-supervise the PhD student Michael Jabbour. This supervision lead to a publication in collaboration with Professor Nicolas Cerf where we analysed the conditions under which local operations and classical communication enable entanglement transformations between bipartite pure Gaussian states (Ref. 4). A set of necessary and sufficient conditions had been found for the interconversion between such states that is restricted to Gaussian local operations and classical communication [14]. Here, we exploited majorization theory in order to derive more general (sufficient) conditions for the interconversion between bipartite pure Gaussian states, showing the surprising fact that there are transformation between Gaussian states that need to go beyond Gaussian operations is more pervasive than initially thought.

4. Valorisation/Diffusion (including Publications, Conferences, Seminars, Missions abroad...)

Publications During the nineteen months of BELSPO fellowship I had the opportunity to publish five manuscripts that since then have led to 110 citations according to Google Scholar, among them one on Nature Photonics. The first column indicates the order number of the publication; second, the information on the manuscript; third, the number of citations according to Google Scholar.

#	Paper	Citat.
5	Strong converse for the classical capacity of all phase-insensitive bosonic Gaussian channels Bhaskar Roy Bardhan, Raul Garcia-Patron, Mark M. Wilde, Andreas Winter IEEE Trans. Inf. Theory 61, 1842 (2015)	6

4	Interconversion of pure Gaussian states using non-Gaussian operations MG Jabbour, R García-Patrón, NJ Cerf Phys. Rev. A 91, 012316 (2015), **Editor's suggestion**	1
3	Analysis of circuit imperfections in BosonSampling Anthony Leverrier, Raúl García-Patrón Quantum Information and Computation 15, 0489 (2014)	22
2	**Ultimate classical communication rates of quantum optical channels** V. Giovannetti, R. Garcia-Patron, N. J. Cerf, A. S. Holevo **Nature Photonics** 8, 796 (2014)	**49**
1	A solution of the Gaussian optimizer conjecture V. Giovannetti, A. S. Holevo, R. Garcia-Patron Commun. Math. Phys, advance online publication (27 Aug 2014)	32

Conferences and seminars After solving an old open problem in quantum optical communication (result Ref. 20-21 that concludes a designed roadmap presented in a Hot Topic Talk at the 11th Int. Conf. QCMC in Vienna, Austria, July 2012), I presented this result to the scientific community at the *Isaac Newton Institute for Mathematical Sciences* (Cambridge, UK), during the talk *A solution of the Gaussian optimizer conjecture*[11], closing the semester program *Mathematical Challenges in Quantum Information* (December 17, 2013). In 2014 I had the opportunity to presented this result in several universities and research centers, such as Caltech Institute for Quantum Information[12] (April 1, 2014), IBM Thomas J. Watson Research Center (NY, April 25, 2014), Massachusetts Institute of Technology (April 23, 2014) and Institute for Quantum Computing[13] (Waterloo (Canada) April 28, 2014).

Outreach of research My recent work solving an old open problem in quantum optical communication (see Ref. 20-21 in the publication list) has received attention in the specialized media, such as *Laser Focus World*[14] and the Belgian science journalism site Daily Science[15]. The Isaac Newton Institute published a *Case Study*[16] that presents this result. Similarly, the Max-Planck Institute for Quantum Optics also edited a press release[17]. The Belgian research council FNRS also published an article on its newsletter as the science magazine Athena edited by the Federation Wallonie-Bruxelles[18].

5. Future prospects for a permanent position in Belgium

The main objective of the BELSPO fellowship grants being to facilitate the return to Belgium of talented researchers in order of help them to find a permanent position in the country, I am happy to announce that October 1st 2015 the I started my new job as tenured FNRS research associate (*chercheur qualifié* FNRS).I would like to thank BRLSPO for giving me the opportunity, through its return grant, to start an independent research program that resulted in obtaining a permanent position at Université Libre de Bruxelles.

---

[11] https://www.newton.ac.uk/seminar/20131217140015001
[12] http://www.iqim.caltech.edu/seminars/iqi_seminars_2013-14.html
[13] https://uwaterloo.ca/institute-for-quantum-computing/events/raul-garcia-patron-ultimate-communication-capacity-quantum
[14] http://www.laserfocusworld.com/articles/2014/09/gaussian-encoding-guarantees-ultimate-capacity-of-optical-communication-channels.html
[15] http://dailyscience.be/2014/10/07/le-bruit-de-la-lumiere-limite-les-telecommunications-optiques/
[16] https://www.newton.ac.uk/files/reports/casestudies/quantum.pdf
[17] http://www.mpq.mpg.de/4990732/14_09_24
[18] FNRS newsletter 99, page 40, December 2014, ATHENA 305, page 42, November 2014

6. Miscellaneous (Bibliography)

[1] Security of continuous-variable quantum key distribution against general attacks
A. Leverrier, R. García-Patrón, R. Renner and N. J. Cerf
Phys. Rev. Lett. 110, 030502 (2013)

[2] Full-field implementation of a perfect eavesdropper on a quantum cryptography system
I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer and V. Makarov
Nat. Commun. 2, 349 (2011)

[3] Elements of Information Theory
T. M. Cover and J. A. Thomas
(Wiley, Hoboken)

[4] Inequalities and Separations among Assisted Capacities of Quantum Channels
C. H. Bennett, I. Devetak, P. W. Shor, J. A. Smolin,
Phys. Rev. Lett. 96, 150502 (2006)

[5] The Computational Complexity of Linear Optics
S. Aaronson and A. Arkhipov
Proceedings of ACM STOC 2011, pages 333-342, arXiv:1011.3245 (2010)

[6] Boson Sampling on a Photonic Chip
J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M.Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys, J. C. Gates, B. J. Smith, P.G.R. Smith, I. A. Walmsley
Science, 339, 798 (2012)

[7] Photonic Boson Sampling in a Tunable Circuit
M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. Ralph, A.G. White
Science, 339, 794 (2012)

[8] Experimental Boson Sampling
M. Tillmann, B. Dakić, R. Heilmann, S. Nolte, A. Szameit, P. Walther
arXiv:1212.2240 (2012)

[9] Experimental Boson Sampling in arbitrary integrated photonic circuits
A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvao, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, F. Sciarrino
arXiv:1212.2783 (2012)

[10] Error tolerance of the Boson-Sampling model for linear optics quantum computing
P. P. Rohde and T. C. Ralph
Phys. Rev. A 85, 022332 (2012)

[11] Majorization Theory Approach to the Gaussian Channel Minimum Entropy Conjecture
R. García-Patrón, C. Navarrete-Benlloch, S. Lloyd, J. H. Shapiro and N. J. Cerf
Phys. Rev. Lett. 108, 110505 (2012)

[12] The Holy Grail of Quantum Optical Communication
R. García-Patrón
Hot Topic Talk at the 11th Int. Conf. Quantum Communication, Measurement and Computing (QCMC), Vienna, Austria, July 2012 http://qcmc2012.org/2012/06/hot-topic-talks-selected/

[13] Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States
Anthony Leverrier
Phys. Rev. Lett. 114, 070501 (2015)

[14] Entanglement transformations of pure Gaussian states
G. Giedke, J. Eisert, J.I. Cirac, M.B. Plenio
Quant. Inf. Comput. 3, 211 (2003)

5. Signatures

Researcher Dr. Raul Garcia-Patron Sanchez

Supervisor Professor Nicolas J. Cerf