QCALL
Early-Stage Researchers Conference

16-19 September 2019

Palermo, Italy

Attendee booklet

TOSHIBA

UNIVERSITY OF LEEDS

The electronic version of this booklet can be found at:
https://www.qcall-itn.eu/esrc-2019/program

The open LaTeX template, AMCOS_booklet, used to generate this booklet is available at
https://github.com/maximelucas/AMCOS_booklet

Contents

About

ESRC

The Early-Stage Researchers Conference (ESRC) is a four-day conference on quantum communications, aimed at Master and PhD students as well as early post-doctoral researchers.

The conference will feature five well-known invited speakers, introducing each of the main topics of the conference, and an industrial session. The topics covered by the conference will be:

- Entanglement-based Quantum Communications
- Security of QKD
- Satellite QKD
- MDI-QKD and TF-QKD
- Component technology (Chip-based QKD, detectors, QRNG, etc.)

QCALL

Quantum Communications for ALL (QCALL) is a European Innovative Training Network (project 675662) funded by the Marie Sklodowska Curie Call H2020-MSCA-ITN-2015. QCALL endeavours to take the next necessary steps to bring the developing quantum technologies closer to the doorsteps of end users. QCALL will empower a nucleus of 15 doctoral researchers in this area to provide secure communications in the European continent and, in the long run, to its connections worldwide.

Organizing committee

Innocenzo De Marco	Mirko Pittaluga
Andrew Shields	Mohsen Razavi

Technical committee

Margarida Pereira	Yumang Jing	Davide Rusca
Eleni Diamanti	Zhiliang Yuan	Mikael Afzelius

Program

Here is an overview of the conference program. Detailed information on the sessions and talks follow.

Time	Monday 16/09	Tuesday 17/09	Wednesday 18/09	Thursday 19/09
10:00	Invited Talk: Li Qian	Invited Talk: Daniel Oi	Invited Talk: Charles Ci Wen Lim	Invited Talk: Jake Kennard
10:35	Session 1: MDI and TF-QKD	Session 3: Satellite QKD	Session 4: Security of QKD	Session 5: Component technology
10:55				
11:15	Coffee Break			
11:35	Session 1: MDI and TF-QKD	Session 3: Satellite QKD	Session 4: Security of QKD	Coffee Break
11:55				Session 5: Component technology
12:15		Excursion		
12:35	Lunch		Lunch	Lunch
12:55				
13:15				
13:35				
14:00	Invited Talk: Wolfgang Tittel		Industry Talks	END
14:20				
14:35	Session 2: Entanglement-based Qcomms			
14:55				
15:15	Coffee Break			
15:35	Session 2: Entanglement-based Qcomms			
16:05			Coffee break	
16:25	Poster Session		Industry Panel	
16:35				
16:55				
17:15				
17:35				
17:55				
18:15				
18:35				
18:55				
19:15				
19:35				
21:00 onwards	Film Festival	Social Dinner		

Timetable

INV: Invited Speaker, CTR: Contributed Talk, ESR: QCALL ESR Talk, IND: Industry Talk.

Monday, 16 September 2019

9:00–10:00	**Registration**		
10:00–10:35	INV	**Li Qian** University of Toronto (Canada)	Auto-compensating TF-QKD over fiber
10:35–10:55	ESR	**Federico Grasselli** Heinrich-Heine-Universität Düsseldorf (Germany)	Conference key agreement with single-photon interference
10:55–11:15	ESR	**Mirko Pittaluga** Toshiba Research Europe Ltd, Cambridge (UK)	Experimental QKD beyond the repeaterless secret key capacity
11:15–11:35	**Coffee break**		
11:35–11:55	ESR	**Guillermo Currás Lorenzo** University of Leeds (UK)	Tight finite-key security for TF-QKD
11:55–12:15	CTR	**Álvaro Navarrete** Universidade de Vigo (Spain)	Asymmetric TF-QKD
12:15–12:35	ESR	**Róbert Trényi** Universidade de Vigo (Spain)	Beating the repeaterless bound with adaptive MDI-QKD
12:35–14:00	**Lunch**		
14:00–14:35	INV	**Wolfgang Tittel** QuTech Delft (Netherlands)	Towards Quantum repeaters
14:35–14:55	CTR	**Ittoop Vergheese Puthoor** Heriot-Watt University, Edinburgh (UK)	Quantum digital signatures using MDI scheme
14:55–15:15	ESR	**Yumang Jing** University of Leeds (UK)	QKD over quantum repeaters with repetition codes
15:15–15:35	**Coffee break**		
15:35–15:55	ESR	**Antonio Ortu** Université de Genève (Switzerland)	A solid state quantum memory for quantum repeaters
15:55–16:15	CTR	**Olena Kovalenko** Univerzita Palackého, Olomouc (Czech Republic)	Compensating the cross talk in continuous-variable multimode entanglement distribution
16:15–18:30	**Poster session**		

Tuesday, 17 September 2019

10:00–10:35	INV	**Daniel Oi** University of Strathclyde (UK)	Satellite QKD
10:35–10:55	CTR	**Wojciech Zwoliński** Uniwersytet Warszawski (Poland)	Range dependence of an optical pulse position modulation link in the presence of background noise
10:55–11:15	ESR	**Mujtaba Zahidy** Università degli studi di Padova (Italy)	Demonstration of feasibility of free-space quantum key distribution in day-light exploiting 1550 nm wavelength
11:15–11:35	**Coffee break**		
11:35–11:55	CTR	**Lai Zhou** University of Oxford (UK)	Polarization Calibration Scheme in the Practical Handheld Free Space QKD System
11:55–12:15	ESR	**Carlo Liorni** Heinrich-Heine-Universität Düsseldorf (Germany)	Satellite- vs ground-based quantum networks and the role of quantum repeaters
12:45–19:00	**Excursion with packed lunch.** Excursion at the Natural Reserve "Lo Zingaro"		
21:00	**Conference Dinner**		

Wednesday, 18 September 2019

10:00–10:35	INV	**Charles Ci Wen Lim** CQT Singapore (Singapore)	Security of QKD
10:35–10:55	ESR	**Nilesh Vyas** Telecom Paris-Tech, Paris (France)	Key distribution in Quantum Computational Hybrid (QCH) security model with performance beyond QKD
10:55–11:15	ESR	**Margarida Pereira** Universidade de Vigo (Spain)	Implementation security of QKD
11:15–11:35	**Coffee break**		
11:35–11:55	CTR	**Fadri Grünenfelder** Université de Genève (Switzerland)	Implementation of a polarization-based BB84 protocol at 5 GHz repetition rate
11:55–12:15	ESR	**Gaëtan Gras** ID Quantique, Geneva (Switzerland)	Bounding the information leakage in quantum hacking using photon statistics
12:15–12:35	CTR	**Víctor Zapatero Castrillo** Universidade de Vigo (Spain)	QKD secure against malicious providers
12:35–12:55	ESR	**Shouvik Ghorai** Université Pierre et Marie Curie, Paris (France)	Asymptotic Security of Continuous-Variable QKD with a Discrete Modulation
12:55–14:20	**Lunch**		
14:20–14:40	IND	**Ryan Parker** British Telecom (UK)	QKD from the Telco perspective
14:40–15:00	IND	**John Prisco** Quantum XChange, Bethesda MD (USA)	QKD: Defensive weapon to Quantum Computers
15:00–15:20	IND	**Helmut Grießer** ADVA Optical Networking SE, Munich (Germany)	A cost model for QKD in optical telco networks
15:20–15:40	IND	**Félix Bussières** ID Quantique SA, Geneva (Switzerland)	Industry-focused Quantum sensing technologies at IDQ
15:40–16:00	IND	**Andrew Shields** Toshiba Research Europe Ltd, Cambridge (UK)	Quantum Communications R&D in Toshiba
16:05–16:25	**Coffee break**		
16:25–17:45	**Industry Panel Session**		

Thursday, 19 September 2019

10:00–10:35	INV	**Jake Kennard** KETS, Bristol (UK)	Applications of Integrated Quantum Photonics in Cryptography
10:35–10:55	ESR	**Innocenzo De Marco** Toshiba Research Europe Ltd, Cambridge (UK)	A modulator-free QKD transmitter chip
10:55–11:15	CTR	**Asli Dilara Ugurlu** Københavns Universitet, Copenhagen (Denmark)	Suspended Spot-Size Converters for Scalable Single-Photon Devices
11:15–11:35	ESR	**Davide Rusca** Université de Genève (Switzerland)	Fast and practical implementation of self-testing QRNG based on an energy bound
11:35–11:55	**Coffee break**		
11:55–12:15	CTR	**Glib Mazin** Univerzita Palackého, Olomouc (Czech Republic)	Low-latency switchable coupler for photonic routing: Application in deterministic time-bin encoding and loop-based photon counting
12:15–12:35	ESR	**Hamid Tebyanian** Università degli studi di Padova (Italy)	Semi-DI QRNG
12:35–12:55	CTR	**Peter Raymond Smith** Toshiba Research Europe Ltd, Cambridge (UK)	Simple source device-independent continuous-variable QRNG
12:55–13:15	CTR	**Alberto Boaron** Université de Genève (Switzerland)	Long-distance and high-speed QKD with a 2.5 GHz clocked platform
13:15–14:35	**Lunch**		
14:35	**END**		

Monday 16th - Morning

MDI and TF-QKD

Invited Speaker: Li Qian

Li Qian is a professor at Department of Electrical and Computer Engineering, University of Toronto, Canada. Her early research focuses on photonic devices for high-speed optical communications. She was a senior scientist at Corning, Inc., where she led the development of the first commercial extended L-band erbium-doped fiber amplifiers. After joining the faculty at the University of Toronto, she started experimental research in fiber-based quantum cryptosystems in 2005. She and her long-term collaborator, Hoi-Kwong Lo, have demonstrated the first decoy-state QKD system, as well as conducted pioneering research in quantum random number generation and measurement-device-independent QKD systems. She is also well-known for fiber-based entangled photon pair generation, and produced arguably the world's simplest polarization-entangled photon source. The broadband nature of this source enabled the demonstration of a reconfigurable multi-user entanglement-based QKD network.

Auto-compensating twin-field QKD over fiber

Twin-field (TF) QKD (QKD) protocols are known to beat the fundamental rate-loss limit (repeaterless bound) at high loss regimes. However, experimental implementations of TF QKD have been challenging, due to its requirement of phase stability over very long fiber distances. Here, we report a proof-of-principle experimental demonstration of TF-QKD which removes the need to stabilize the phase of the quantum state over kilometers of fiber. A Sagnac loop structure is utilized to automatically compensate the phase fluctuations in fibers linking the various parties. Using decoy states, we demonstrate secret-key generation rates that beat the repeaterless bound when the channel loss is above 40 dB.

Contributed Talks

Conference key agreement with single-photon interference

***Federico Grasselli*, Hermann Kampermann, Dagmar Bruss**

Institute for Theoretical Physics III, Heinrich Heine University Düsseldorf, Düsseldorf, Germany

We devise a conference key agreement (CKA) where the users distill the shared secret key through single-photon interference, drawing inspiration from TF-QKD protocols. The CKA is better suited to high-loss scenarios than previous multipartite QKD schemes and employs for the first time a W-class state as its entanglement resource.

Experimental QKD beyond the repeaterless secret key capacity

***Mariella Minder*[1,2], *Mirko Pittaluga*[1,3], *George L. Roberts*[1,2], *Marco Lucamarini*[1], *James F. Dynes*[1], *Zhiliang Yuan*[1], *Andrew J. Shields*[1]**

[1] Toshiba Research Europe Limited, 208 Cambridge Science Park, CB40GZ Cambridge, UK

[2] Department of Engineering, University of Cambridge, Cambridge, UK

[3] School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK

We demonstrate the first experimental overcoming of the repeaterless secret key capacity (PLOB) bound through the implementation of the Twin-Field QKD protocol. We distribute secret keys at record channel losses ($>$ 90 dB).

Tight finite-key security for twin-field QKD

Guillermo Currás Lorenzo[1]***, Marcos Curty***[2]***, Koji Azuma***[3]***, Alvaro Navarrete***[2]***, Mohsen Razavi***[1]

[1] School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK
[2] EI Telecomunicacion, Dept. of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain
[3] NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa, 243-0198, Japan

Protocols based on twin-field QKD (TF-QKD) are predicted to beat the current records in terms of both secret key rate and total achievable distance. A recent simple proposal is perhaps one of the strongest candidates, since it could improve the secret key rate obtainable by almost an order of magnitude with respect to the original protocol while being experimentally easier to implement. However, particularities of its security proof make its extension to the finite-key regime more challenging than that of other protocols. In this work, we overcome these issues and present a finite-key security analysis against coherent attacks, showing that this simple TF-QKD setup can overcome the fundamental bounds on repeaterless QKD links for a block size of just 10^{11} transmitted signals.

Asymmetric twin-field QKD

Federico Grasselli[1]***, Alvaro Navarrete***[2]***, Marcos Curty***[2]

[1] Institute for Theoretical Physics III, Heinrich Heine University Düsseldorf, Düsseldorf, Germany
[2] EI Telecomunicacion, Dept. of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain

We focus on the TF-QKD protocol proposed recently by Curty et al., whose security relies on the estimation of the detection Fock-state statistics through the decoy-state technique. We derive analytical bounds on these statistics assuming independent decoy intensity settings for each party, and we analyze the protocol's performance.

Beating the repeaterless bound with adaptive measurement-device-independent QKD

Robert Trenyi[1]***, Koji Azuma***[2]***, Marcos Curty***[1]

[1] Escuela de Ingenieria de Telecomunicacion, Dept. of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain

[2] NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan

Surpassing the repeaterless bound is a crucial task on the way towards realising long-distance QKD. In this paper, we focus on the protocol proposed by Azuma et al. in [Nature Communications 6, 10171 (2015)], which can beat this bound with idealised devices. We investigate the robustness of this protocol against imperfections in realistic setups, particularly the multiple-photon pair components emitted by practical entanglement sources. In doing so, we derive necessary conditions on the photon-number statistics of the sources in order to beat the repeaterless bound. We show, for instance, that parametric down-conversion sources do not satisfy the required conditions and thus cannot be used to outperform this bound.

Monday 16th - Afternoon

Invited Speaker: Wolfgang Tittel

Wolfgang Tittel is an experimental physicist. He received his PhD from the University of Geneva in 2000 for "Quantum correlation for quantum communication", joined the University of Calgary in 2006 as associate professor, and was promoted to full professor in 2013. Since 2018, he is a professor at the EEMCS Department at the TU Delft, and a staff member at QuTech. Prof Tittel's research was seminal in bringing quantum communication technology out of the laboratory and into the real world using deployed telecommunication fiber. His work has raised, and continues to raise, both scientific and public awareness and appreciation that the new technology is not restricted to contrived laboratory settings. Notable research results include the first demonstration of measurement-device independent QKD, which is of particular interest due to its resilience to quantum hacking, its suitability for building networks, and its upgradability to quantum repeater-based communication links; city-wide quantum teleportation; and the storage and recall of members of entangled photon pairs using rare-earth-ion based quantum memory.

Towards Quantum repeaters

Exploiting the non-classical properties of entangled states as well as quantum memory for light, quantum repeaters allow quantum communication in theory over arbitrarily long distances. After a general introduction of its building blocks, I will describe a quantum repeater architecture based on spectral multiplexing and briefly discuss a specific realization of quantum memory for light using rare-earth-ion doped crystals.

Contributed talks

Quantum signatures using measurement-device-independent scheme

Ittoop Vergheese Puthoor[1]***, Ryan Amiri***[1]***, Petros Wallden***[2]***, Marcus Curty***[3]***, Erika Andersson***[1]

[1] Institute of Photonics and Quantum Sciences (IPaQS), Heriot-Watt University, Edinburgh, UK
[2] School of Informatics, University of Edinburgh, UK
[3] Escuela de Ingenieria de Telecomunicacion, Dept. of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain

Digital signatures play an important role in software distribution, modern communication and financial transactions, where it is important to detect forgery and tampering. Here, we demonstrate a signature scheme that is proven to be secure against detector side channel attacks by using the concept of measurement-device-independence.

QKD over quantum repeaters with repetition codes

Yumang Jing, Daniel Alsina Leal, and Mohsen Razavi

School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK

We employ a novel hybrid numerical-analytic approach to study the performance of a QKD system that is run over a quantum repeater with three and five-qubit repetition codes by accounting for various sources of error in the setup. This will enable us to obtain a more accurate picture of the requirements of such systems in practice.

A solid state quantum memory for quantum repeaters

Antonio Ortu, Jean Etesse, Alexey Tiranov, Adrian Holzaepfel, Krzysztof Kaczmarek, Mikael Afzelius

Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1227 Carouge, Switzerland

In this talk, I will introduce a solid state quantum memory based on a europium-doped crystal. With a scheme that combines the atomic frequency comb technique and the DLCZ protocol, this material could be used to generate photon pairs and store entangled states in a quantum repeater for a future optical fiber quantum network.

Compensating the cross talk in continuous-variable multimode entanglement distribution

Olena Kovalenko, Vladyslav C. Usenko, Radim Filip

Department of Optics, Palacky University, 17 listopadu, 771 46 Olomuc, Czech Republic

We consider the effect of linear crosstalk in the multimode entanglement distribution using twin-beam states. We suggest the method of an optimized linear coupling on the remote sides prior to detection. We compare it to methods of entanglement concentration using an optimized Gaussian measurement of one pair of modes.

Tuesday 17th - Morning

Session: Satellite QKD

Invited Speaker: Daniel Oi

Daniel Oi is a Senior Lecturer working on Quantum Information in the Computational Nonlinear and Quantum Optics (CNQO) group at the Department of Physics, University of Strathclyde. His research interests span fundamental aspects of quantum theory, quantum engineering, the theory of quantum computation, and quantum space science and technologies. Prior to joining Strathclyde in 2006, he was a Research Fellow at Sidney Sussex College and the Department of Applied Mathematics and Theoretical Physics, University of Cambridge. He completed his doctorate at the Centre for Quantum Computation, University of Oxford in 2002.

Satellite QKD

Fibre-based QKD range is limited by intrinsic loss and current lack of practical quantum repeaters. Satellite QKD (SatQKD) can provide global quantum secure communication and the success of the Chinese satellite, Micius, has spurred enormous international interest and activity. I shall describe the basic concepts and issues associated with SatQKD.

Contributed talks

Range Dependence of an Optical Pulse Position Modulation Link in the Presence of Background Noise

Wojciech Zwolinski[1]***, Marcin Jarzyna***[2]***, Konrad Banaszek***[1,2]

[1] Faculty of Physics, University of Warsaw, Warsaw, Poland

[2] Centre of New Technologies, University of Warsaw, Warsaw, Poland

We analyzed the information efficiency of a deep-space optical communication link with background noise, employing the pulse position modulation (PPM). We show that complete decoding which uses events with multiple detectors photocounts within one PPM frame, achieves information efficiency scaling as the inverse of the square of the distance. This represents a qualitative enhancement compared to simple decoding omitting multi photocounts events leading to inverse-quartic scaling with the distance.

Demonstration of feasibility of free-space quantum key distribution in day-light exploiting 1550 nm wavelength

Marco Avesani[1]***, Luca Calderaro***[1]***, Matteo Schiavon***[1]***, Andrea Stanco***[1]***, Costantino Agnesi***[1]***, Alberto Santamato***[1]***, Mujtaba Zahidy***[1]***, Alessia Scriminich***[1]***, Giulio Foletto***[1]***, Francesco Vedovato***[1]***, Giuseppe Vallone***[1,2]***, Paolo Villoresi***[1]

[1] Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Padova, Italy

[2] Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, Padova, Italy

Here we report the results of our experiment with a QKD system based on efficient BB84 protocol at 1550 nm, performed in day-light over a 145 m channel in the urban area of the city of Padova. We achieved more than 30 kbps of secret key after finite-size security analysis with a QBER of less than 2% during the test. A global scale quantum network will allow secure communication between parties over intercontinental distances. Realizing it requires advancements in space-based quantum links, which is a promising solution for long-distance communication, but are yet to reach their fiber-based counterparts in terms of performance. A free-space system that fulfills criteria such as compatibility with fiber-based networks and daylight operation paves the way for implementing such a global network.

Polarization Calibration Scheme in the Practical Handheld Free Space Quantum Key Distribution System

Lai Zhou[1]***, David Lowndes***[2]***, Vincent Lee***[1]***, Grahame Faulkner***[1]***, Dominic O'Brien***[1]

[1] Department of Engineering Science, University of Oxford, Oxford, UK
[2] Department of Electrical and Electronic Engineering, Bristol University, Bristol, UK

The paper proposes a polarization calibration scheme suitable for use in a free-space QKD link between moving terminals, such as handheld devices. Simulation results are presented.

Satellite- vs ground-based quantum networks and the role of quantum repeaters

Carlo Liorni, Hermann Kampermann and Dagmar Bruss

Institute for Theoretical Physics III, Heinrich Heine University Düsseldorf, Düsseldorf, Germany

Satellite-based optical links represent a very appealing alternative to fiber networks, when long distances are addressed. The losses introduced by such channels in different weather conditions are modeled, to precisely infer the key rates achievable by QKD protocols. Their performances in different configurations are then compared to ground-based implementations.

Wednesday 18th - Morning

Session: Security of QKD

Invited Speaker: Charles Ci Wen Lim

Charles Ci Wen Lim is an Assistant Professor in Electrical and Computer Engineering and a Fellow at the Centre for Quantum Technologies at NUS (Singapore). After graduating from Nanyang Polytechnic, he studied physics at NUS and went on to earn his PhD at the University of Geneva. He is a 2019 National Research Foundation Fellow. In 2019, he received a Quantum Engineering Programme grant to work on quantum cryptography and communication.

Security of QKD

In this presentation, I will cover the recent security proof techniques of QKD, focusing on new numerical methods for calculating the (non-asymptotic) secret key rates of prepare-and-measure QKD, measurement-device-independent (MDI-QKD), and device-independent (DI-QKD).

Contributed talks

Key distribution in a Quantum Computational Hybrid security model with performance beyond QKD

Nilesh Vyas, Romain Alléaume

LTCI, Télécom Paris, Institut Polytechnique de Paris, 46 rue Barrault, 75013 Paris, France

We define the Quantum Computational Hybrid (QCH) security model as: we assume there exist some encryption, that cannot be broken during a time shorter than t_{comp} and conversely assume that any quantum memory fully decoheres within a time t_{coh}, much smaller than t_{comp}. We propose an explicit key distribution protocol in which Alice sends qudit state to Bob, thereby encoding $\log(d)$ bits of x in basis chosen among a full set of $(d+1)$ MUBs. This enables to perform secure key distribution with many photons per channel use. As a consequence, the key rate of our protocol can significantly outperform the performance limits of QKD, when operated over a large number of modes.

Implementation security of QKD

Margarida Pereira[1]***, Marcos Curty***[1]***, Kiyoshi Tamaki***[2]

[1] Escuela de Ingenieria de Telecomunicacion, Dept. of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain

[2] Graduate School of Science and Engineering for Research, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan

In this work, we extend the security analysis of the generalised loss-tolerant protocol [M. Pereira el al, arXiv: 1902.02126 (2019)] to the finite-key regime. By simulating the secret key rate for flawed and leaky sources, we show that the resulting performance is robust against general imperfections. Our work constitutes an important step forward towards bridging the gap between the theory and the practice of QKD.

Implementation of a polarization-based BB84 protocol at 5 GHz repetition rate

Fadri Grünenfelder, Alberto Boaron, Davide Rusca, Anthony Martin, Hugo Zbinden

Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1227 Carouge, Switzerland

We present a high-speed implementation of a polarization-based QKD protocol. We use a modified version of the original BB84 protocol with three polarization states. As a source we employ phase-randomized weak coherent laser pulses and we prevent photon-number-splitting attacks by implementing the 1-decoy method.

Bounding the information leakage in quantum hacking using photon statistics

***Gaetan Gras*[1,2]*, Davide Rusca*[2]*, Hugo Zbinden*[2]*, Felix Bussieres*[1]

[1] ID Quantique SA, CH-1227 Carouge, Switzerland

[2] Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1227 Carouge, Switzerland

We present a countermeasure against detector control attacks based on the photon statistics measured by Bob. With this countermeasure, we can estimate an upper bound on the information leaked through this kind of attack.

QKD secure against malicious providers

Victor Zapatero, Marcos Curty

EI Telecomunicaciòn, Departamento de Teorìa de la Señal y Comunicaciones, Universidad de Vigo E-36310, Spain

In QKD, all the legitimate users' devices are honest by hypothesis, implicitly implying that all the hardware providers are trustworthy. This assumption is not justified and it compromises the security. Recently, a solution was proposed to restore security in a setting with a limited number of malicious devices, and in this work we show its feasibility in practical QKD protocols.

Asymptotic Security of Continuous-Variable QKD with a Discrete Modulation

Shouvik Ghorai[1]***, Philippe Grangier***[2]***, Eleni Diamanti***[1]***, Anthony Leverrier***[3]

[1] LIP6, CNRS, Sorbonne Universite, Paris, France

[2] Laboratoire Charles Fabry, IOGS, CNRS, Universite Paris Saclay, F91127 Palaiseau, France

[3] Inria Paris, France

We establish a lower bound on the asymptotic secret key rate of continuous-variable QKD with a discrete modulation of coherent states. The bound is valid against collective attacks and is obtained by formulating the problem as a semidefinite program. We illustrate our general approach with the quadrature-phase-shift-keying modulation scheme and show that distances over 100 km are achievable for realistic values of noise. We also discuss the application to more complex quadrature-amplitude-modulation schemes. This result opens the way to establishing the full security of continuous-variable protocols with a discrete modulation, and thereby to the large-scale deployment of these protocols for QKD.

Wednesday 18th - Afternoon

Industry session

QKD from the Telco Perspective

Ryan Parker

British Telecommunications Plc, UK

This talk will cover the past and current QKD (QKD) research undertaken by BT – this will include experimental research, and challenges faced by industry, as well as the business and commercial case for QKD, such as terrestrial and satellite-based use-cases and techno-economic analysis.

QKD: Defensive Weapon to Quantum Computers

John Prisco

Quantum XChange, 7700 Old Georgetown Road, Bethesda MD, USA

Quantum computers will fundamentally change how organizations secure their most sensitive data. As technology heavyweights like IBM and Google race for quantum supremacy, nation-state actors and cybercriminals are stockpiling encrypted data now, to be deciphered later by quantum computers. This means that critical SSL-protected data is vulnerable to exploitation. Organizations need a well-articulated, quantum-risk plan to ensure business continuity.

A cost model for QKD in optical telco networks

Helmut Grießer

ADVA Optical Networking SE, Munich, Germany

Fiber based optical communication is the workhorse of the Internet, providing cost-efficient data transport over huge distances. These networks rely heavily on optical amplification, and adapting them for QKD (QKD) does increase the cost of data transmission. We present a cost model for enabling QKD in fiber networks.

Industry-focused Quantum sensing technologies at IDQ

Félix Bussières

ID Quantique SA, CH-1227 Carouge, Switzerland

In this talk, I will review some the latest industrial applications of quantum sensing developed by IDQ, including high-performance OTDRs for the Ariane 6 launcher, quantum lidar for autonomous vehicles and remote gas sensing.

Quantum Communications R&D in Toshiba

Andrew J. Shields

Toshiba Research Europe Ltd, Cambridge, UK

In this talk I will review some of the research at Toshiba in extending the limits of quantum communication technology to higher key rates, longer distances and lower cost, as well as our recent deployments of the technology in Europe, US and Japan.

Thursday 19th

Component technology

Invited Speaker: Jake Kennard

Jake Kennard is a co-founder and director of KETS Quantum Security. Based in Bristol, UK, KETS provide commercial integrated, on chip quantum secured encryption technologies – from quantum random number generators to full QKD systems. Prior to this he was a Senior Research Associate at the Quantum Engineering Technology Labs at the University of Bristol & the Quantum Communications Hub, where his research focused on developing on-chip quantum technologies and their implementations in networks. Jake holds a PhD in Quantum Photonics also from the University of Bristol, where he primarily specialised in applications of diamond color centres.

Applications of Integrated Quantum Photonics in Cryptography

Integrated photonics are a versatile, robust and scalable platform in which to implement quantum technologies. Here we present a number of core technologies with applications in cryptography; namely QKD systems, integrated Quantum Random Number Generators and on-chip homodyne detectors, including latest demonstrations and real world implementations.

Contributed talks

Chip-based QKD system

Innocenzo De Marco[1,2]***, Taofiq K. Paraiso***[1]***, Thomas Roger***[1]***, Davide G. Marangon***[1]***, Mirko Sanzaro***[1]***, Marco Lucamarini***[1]***, Zhiliang Yuan***[1]***, Andrew J. Shields***[1]

[1] Toshiba Research Europe Limited, 208 Cambridge Science Park, CB40GZ Cambridge, UK
[2] School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK

We demonstrate the operation of a chip-based QKD system based on optical injection locking. This allows for direct phase modulation and eliminates the need for an optical phase modulator, rendering our system more stable and less power consuming.

Suspended Spot-Size Converters for Scalable Single-Photon Devices

Asli D. Ugurlu[1]***, Henri Thyrrestrup***[1]***, Ravitej Uppu***[1]***, C. Ouellet-Plamondon***[1]***, Rüdiger Schott***[2]***, Andreas D. Wieck*** [2]***, Arne Ludwig***[2]***, Peter Lodahl***[1]***, Leonardo Midolo***[1]

[1] Center for Hybrid Quantum Networks (Hy-Q), Niels Bohr Institute, University of Copenhagen, Blegdamsvej 17, 2100-DK Copenhagen, Denmark
[2] Lehrstuhl für Angewandte Festkörperphysik, Ruhr-Universität Bochum, Universitätsstrasse 150, D-44780 Bochum, Germany

We demonstrate an adiabatic inverted taper spot-size converter for the end-fire coupling of suspended Gallium Arsenide waveguides to lensed fibres. The presented out-coupler plays a key role for building efficient and scalable quantum photonic networks.

Fast and practical implementation of self-testing QRNG based on an energy bound

Davide Rusca[1]***, Thomas van Himbeeck***[2,3]***, Anthony Martin***[1]***, Jonatan Bohr Brask***[1,4]***, Hamid Tebyanian***[5]***, Stefano Pironio***[2,3]***, Nicolas Brunner***[1]***, Hugo Zbinden***[1]

[1] Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1227 Carouge, Switzerland

[2] Laboratoire d'Information Quantique, Université Libre de Bruxelles, 1050 Bruxelles, Belgium

[3] Centre for Quantum Information & Communication, Université Libre de Bruxelles, Belgium

[4] Department of Physics, Technical University of Denmark, Fysikvej, Kongens Lyngby 2800, Denmark

[5] Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Padova, Italia

We implement a simple and fast self-testing QRNG experiment. Our scheme requires an extra natural assumption compared to the completely Device-Dependent approach, namely that the mean number of photons of the signal optical modes is bounded. The scheme is self-testing, as it allows the user to verify in real-time the correct functioning of the setup, hence guaranteeing the continuous generation of certied random bits. The scheme is based on a prepare-and-measure setup, which we implement in a fiber experiment. The randomness generation rate is 112.5 Mbits/s, comparable to commercial solutions.

Low-latency switchable coupler for photonic routing: Application in deterministic time-bin encoding and loop-based photon counting

Vojtech Svarc, Martina Novakova, Glib Mazin, Miroslav Jezek

Department of Optics, Palacky University, 17 listopadu, 771 46 Olomuc, Czech Republic

We report a 2x2 photonic coupler with arbitrary splitting ratio switchable by a low-voltage electronic signal. Using the reported coupler, we demonstrate for the first time the perfectly balanced time-multiplexed device for photon-number-resolving detectors and the active preparation of a photonic temporal qudit state up to four time bins.

Semi-DI Quantum Random Number Generator

Hamid Tebyanian[1], ***Marco Avesani***[1], ***Giuseppe Vallone***[1,2], ***Paolo Villoresi***[1,2]

[1] Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Padova, Italy
[2] Istituto di Fotonica e Nanotecnologie - CNR, Via Trasea 7 - 35131 Padova, Italia

Randomness is a central feature of quantum mechanics and an invaluable resource for both classical and quantum technologies. Typically the number of random bits that can be certified is bounded by the dimension of the measured quantum system. First I show that, using Positive Operator Valued Measurement (POVM), is possible to arbitrarily increase the number of certified bits for any fixed dimension. Moreover, the use of POVM makes it possible to certify the randomness without any assumption on the source. We experimentally demonstrate our method with a compact and simple Quantum Random Number Generator that employs qubits and POVM up to 6 outcomes. Next, I present our latest work on semi-DI QRNG based on energy assumptions.

Simple source device-independent continuous-variable quantum random number generator

Peter Raymond Smith[1,2], ***Davide G. Marangon***[1], ***Marco Lucamarini***[1], ***Zhiliang Yuan***[1], ***Andrew J. Shields***[1]

[1] Toshiba Research Europe Limited, 208 Cambridge Science Park, CB40GZ Cambridge, UK
[2] Department of Engineering, University of Cambridge, Cambridge, UK

We introduce a protocol for a novel source device independent continuous-variable quantum random number generator, in which we exploit a phase-randomized local oscillator to bound the min-entropy and extract true randomness from a completely uncharacterized input. Our proof of principle implementation achieves an equivalent rate of 270 Mbit/s.

Long-distance and high-speed QKD with a 2.5 GHz clocked platform

Alberto Boaron[1], ***Davide Rusca***[1], ***Gianluca Boso***[1], ***Raphael Houlmann***[1], ***Fadri Grunenfelder***[1], ***Cedric Vulliez***[1], ***Misael Caloz***[1], ***Matthieu Perrenoud***[1], ***Gaetan Gras***[1], ***Claire Autebert***[1], ***Felix Bussieres***[1], ***Ming-Jun Li***[1], ***Daniel Nolan***[2], ***Anthony Martin***[1], ***Hugo Zbinden***[1]

[1] Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1227 Carouge, Switzerland
[2] Corning Incorporated, Corning, NY, 14831, United States

We use a 2.5 GHz clocked QKD system to perform long-distance and high-speed QKD. Taking benefit from superconducting detectors optimized for each operation regime we achieve state-of-the-art performance.

List of Posters

Device-independent secret key rate from optimized Bell inequality violation
Sarnava Datta, *Heinrich-Heine-Universität Düsseldorf (Germany)*

Squeezing-enhanced QKD over atmospheric channels
Ivan Derkach, *Univerzita Palackého, Olomouc (Czech Republic)*

Towards a cavity-assisted highly efficient photonic quantum memory in Pr3+:Y2SiO5
Stefano Duranti, *ICFO, Barcelona (Spain)*

Analysis and Simulation of Photon Pair Properties and Device Imperfections in Phase-Time Coding QKD
Erik Fitzke, *Technische Universität Darmstadt (Germany)*

A theoretical framework for PUFs and QR-PUFs
Giulio Gianfelici, *Heinrich-Heine-Universität Düsseldorf (Germany)*

Secure practical indoor optical wireless communications using QKD
Vincent Lee, *University of Oxford (UK)*

Parameter regimes for surpassing the PLOB bound with error-corrected qudit repeaters
Daniel Miller, *Heinrich-Heine-Universität Düsseldorf (Germany)*

Test of a Time-bin Entanglement-based QKD System in a Commercial Optical Link
Oleg Nikiforov, *Technische Universität Darmstadt (Germany)*

High speed Integrated QKD system
Rebecka Sax, *Université de Genève (Switzerland)*

Suspended Spot-Size Converters for Scalable Single-Photon Devices
Asli D. Ugurlu, *Københavns Universitet, Copenhagen (Denmark)*

List of Participants

Invited speakers

Daniel Oi	University of Strathclyde (UK)
Charles Ci Wen Lim	CQT Singapore (Singapore)
Li Qian	University of Toronto (Canada)
Wolfgang Tittel	QuTech (Netherlands)
Jake Kennard	KETS, Bristol (UK)

Industrial speakers

Helmut Grießer	ADVA (Germany)
Ryan Parker	BT (UK)
John Prisco	Quantum XChange (USA)

QCALL ESRs

Carlo Liorni	Heinrich-Heine-Universität Düsseldorf (Germany)
Federico Grasselli	Heinrich-Heine-Universität Düsseldorf (Germany)
Gaëtan Gras	ID Quantique, Geneva (Switzerland)
Nilesh Vyas	Telecom Paris-Tech, Paris (France)
Innocenzo De Marco	Toshiba Research Europe Limited, Cambridge (UK)
Mirko Pittaluga	Toshiba Research Europe Limited, Cambridge (UK)
Margarida Pereira	Universidade de Vigo (Spain)
Róbert Trényi	Universidade de Vigo (Spain)
Hamid Tebyanian	Università degli studi di Padova (Italy)
Mujtaba Zahidy	Università degli studi di Padova (Italy)
Antonio Ortu	Université de Genève (Switzerland)
Davide Rusca	Université de Genève (Switzerland)
Shouvik Ghorai	Université Pierre et Marie Curie, Paris (France)
Guillermo Currás Lorenzo	University of Leeds (UK)
Yumang Jing	University of Leeds (UK)

QCALL Supervisors

Félix Bussières	ID Quantique, Geneva (Switzerland)
Andrew Shields	Toshiba Research Europe Limited, Cambridge (UK)
Marcos Curty	Universidade de Vigo (Spain)
Mikael Afzelius	Université de Genève (Switzerland)
Mohsen Razavi	University of Leeds (UK)
Sanaz Sigaroudi	University of Leeds (UK)

External Participants

Iyad Suleiman	Danmarks Tekniske Universitet, Copenhagen (Denmark)
Daniel Miller	Heinrich-Heine-Universität Düsseldorf (Germany)
Giulio Gianfelici	Heinrich-Heine-Universität Düsseldorf (Germany)
Sarnava Datta	Heinrich-Heine-Universität Düsseldorf (Germany)
Ittoop Vergheese Puthoor	Heriot-Watt University, Edimburgh (UK)
Stefano Duranti	ICFO, Barcelona (Spain)
Asli D. Ugurlu	Københavns Universitet, Copenhagen (Denmark)
Erik Fitzke	Technische Universität Darmstadt (Germany)
Oleg Nikiforov	Technische Universität Darmstadt (Germany)
Peter Raymond Smith	Toshiba Research Europe Limited, Cambridge (UK)
Álvaro Navarrete	Universitade de Vigo (Spain)
Víctor Zapatero Castrillo	Universitade de Vigo (Spain)
Xing Chen	Universität Stuttgart (Germany)
Alberto Boaron	Université de Genève (Switzerland)
Fadri Grünenfelder	Université de Genève (Switzerland)
Rebecka Sax	Université de Genève (Switzerland)
Yupeng Gong	University of Cambridge (UK)
Lai Zhou	University of Oxford (UK)
Vincent Lee	University of Oxford (UK)
Glib Mazin	Univerzita Palackého, Olomouc (Czech Republic)
Ivan Derkach	Univerzita Palackého, Olomouc (Czech Republic)
Olena Kovalenko	Univerzita Palackého, Olomouc (Czech Republic)
Wojciech Zwoliński	Uniwersytet Warszawski (Poland)

Useful Information

Venue

The conference will be held at the Addaura Hotel in Mondello, a neighbourhood in Palermo, Italy. **Coffee breaks and lunches** will be offered **in front of the main entrance of the conference hall**. The **poster session** will be held on Monday afternoon.

Wi-Fi will be available during the conference:

- **SSID:** Addaura_Hotel
- **Password:** Addaura1

Social events

Excursion An excursion is planned on Tuesday at the Natural Reserve "Lo Zingaro". This was the first natural reserve set up in Sicily in May 1981, located almost completely in the municipal territory of San Vito Lo Capo. It stretches along some seven kilometers of unspoilt coastline of the Gulf of Castellammare and its mountain chain, the setting of steep cliffs and little bays.

Conference dinner The conference dinner will be held at "Alle Terrazze" restaurant, Viale Regina Elena, 90149 Palermo, Italy.

Mondello - Places of interest

We have highlighted some of the (many) points of interest in Mondello and Palermo in Google Maps. Feel free to visit the city in your free time and explore the surroundings. You can visit this link (`http://bit.ly/QCALL_ESRC`) or scan the QR code on the right to access the map.

Contacts

Here is a list of contacts you may need. Remember the European Emergency Number is **112**. Calling this number will put you in contact with a centre rerouting your call to the right institution.

Below you can find a list of contacts for information about the event:

- **Addaura Hotel:** (+39) 091 6842222
- **Restaurant "Alle Terrazze":** (+39) 091 6262903
- **Organising committee (email):** esr.conf@qcall-itn.eu

Partner Institutions

QCALL - Quantum Communications for All is a European Innovative Training Network (project 675662) funded by the Marie Skłodowska Curie Call H2020-MSCA-ITN-2015.

Full Partners

UNIVERSITY OF LEEDS

TOSHIBA

IDQ

TELECOM ParisTech

HEINRICH HEINE UNIVERSITÄT DÜSSELDORF

UNIVERSITÉ DE GENÈVE

UNIVERSITÀ DEGLI STUDI DI PADOVA

UNIVERSITE PIERRE & MARIE CURIE
LA SCIENCE A PARIS

UNIVERSIDADE DE VIGO

Supporting Partner Organisations