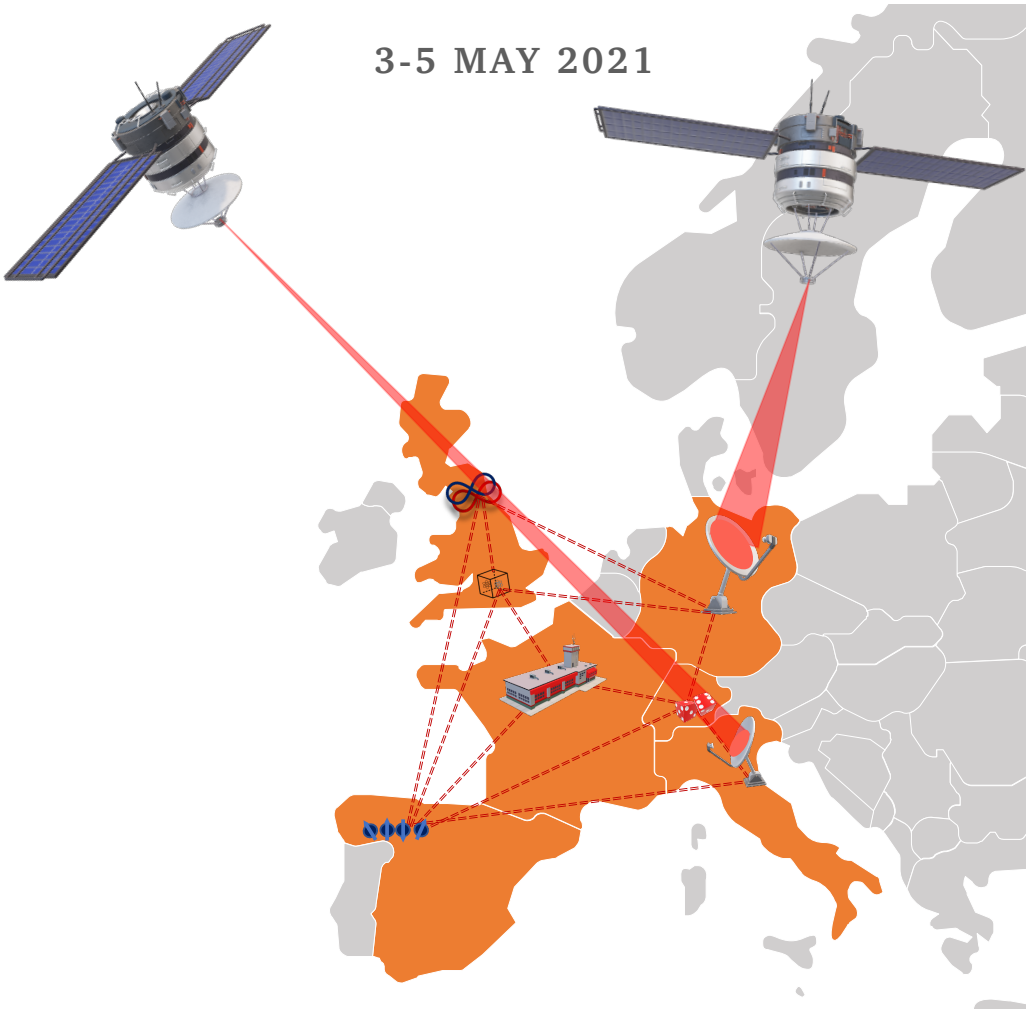
QCALL FINAL SYMPOSIUM ON ADVANCES IN QUANTUM COMMUNICATIONS

3-5 MAY 2021



Content

Time (CET)	Monday, 3 May	Tuesday, 4 May	Wednesday, 5 May
	Session I: Novel Techniques in Quantum Secure Communications 1 Chair: Marcos Curty, University of Vigo	Session III: Novel Techniques in Quantum Secure Communications 2 Chair: Romain Alléaume, Telecom Paris	Session V: Quantum Repeaters Chair: Mohsen Razavi, University of Leeds
14:00-14:30	Recent progress in practical quantum key distribution **Xiang-Bin Wang** *Tsinghua University*	Ultimate limits of the quantum Internet **Stefano Pirandola** *University of York*	Trapped-ion interfaces for quantum networks **Tracy Northup** *University of Innsbruck*
14:30-15:00	Device-independent protocols from computational assumptions **Tony Metger** *ETH Zürich*	Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution **Eneet Kaur** *University of Waterloo*	Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes **Liang Jiang** *University of Chicago*
15:00-15:20	Using random sampling theory to prove the finite-key security of non-standard QKD protocols **Guillermo Curras Lorenzo** *University of Leeds*	Continuous-variable quantum money with classical verification **Shouvik Ghorai** *Sorbonne University*	Quantum key distribution over quantum repeaters with encoding **Yumang Jing** *University of Leeds*
15:20-15:40	Bridging the gap between theory and practice of QKD **Margarida Pereira** *University of Vigo*	Everlasting secure key agreement in a quantum computational time-lock security model **Nilesh Vyas** *Telecom Paris*	A long-lived quantum memory for quantum repeaters **Antonio Ortu** *University of Geneva*
15:40-16:15	Break	Break	Break
	Session II: Device-Independent Cryptography and Quantum Random Number Generators Chair: Dagmar Bruss, University of Dusseldorf	Session IV: Experimental Quantum Key Distribution Chair: Eleni Diamanti, Sorbonne University	Session VI: Satellite and Near-term QKD Systems Chair: Hugo Zbinden, University of Geneva
16:15-16:45	Higher rates for device-independent randomness expansion **Roger Colbeck** *University of York*	Frequency conversion of single photons to 1550 nm enabling quantum communication protocols **Beatrice da Lio** *University of Copenhagen*	Satellite quantum key distribution & the QEYSSat mission **Katanya Kuntz** *University of Waterloo*
16:45-17:05	Practical semi-self testing randomness generation based on quantum state's indistinguishably **Hamid Tebyanian** *University of Padova*	Dual-band phase stabilisation technique for long distance quantum communications **Mirko Pittaluga** *Toshiba Research Europe Ltd*	Recent developments in practical BB84 QKD **Mujtaba Zahidy** *University of Padova*
17:05-17:25	Entropy bounds for multipartite device-independent cryptography **Federico Grasselli** *University of Dusseldorf*	Countermeasure against quantum hacking using detection statistics **Gaëtan Gras** *ID Quantique*	Performance of the coherent-one-way quantum key distribution protocol **Róbert Trényi** *University of Vigo*
17:25- 17:45	Fast and practical quantum key distribution **Davide Rusca** *University of Geneva*	Photonic integration of a directly phase-modulated source for quantum key distribution **Innocenzo De Marco** *Toshiba Research Europe Ltd*	Intercontinental communication through space-borne quantum repeaters **Carlo Liorni** *University of Dusseldorf*
18:00- 19:00	Free Evening Discussions 1 Breakout Rooms	Industry Panel: Starting a quantum company Chair: Félix Bussières, ID Quantique	Free Evening Discussions 2 Breakout Rooms

Invited Speakers

- Xiang-Bin Wang, Tsinghua University
- Eneet Kaur, University of Waterloo
- Roger Colbeck, University of York
- Beatrice da Lio, University of Copengagen
- Stefano Pirandola, University of York
- Liang Jiang, University of Chicago
- Tracy Northup, Innsbruck University
- Katanya Kuntz, University of Waterloo
- Tony Metger, ETH Zürich
- Innocenzo De Marco,Toshiba Research Europe Ltd
- Mirko Pittaluga,Toshiba Research Europe Ltd
- Nilesh Vyas, Telecome Paris Tech
- Gaëtan Gras, IDQ
- Margarida Pereira, University of Vigo
- Guillermo Currás Lorenzo, University of Leeds
- Mujtaba Zahidy, University of Padova
- Yumang Jing, University of Leeds
- Carlo Liorni, University of Dusseldorf
- Antonio Ortu, University of Geneva
- Róbert Trényi, University of Vigo
- Shouvik Ghorai, Université Pierre et Marie CURIE
- Federico Grasselli, University of Dusseldorf
- Davide Rusca, University of Geneva
- Hamid Tebyanian, University of Padova

Industry panelists

- Richard Murray, Orca Computing
- Carmen Palacios-Berraquero, Nu quantum
- Carlos Abellan, QuSide

Free evening discussion 1 candidates

- Sk Sazim, IP, Slovak Academy of Sciences
- Gleb Mazin, Palacký University in Olomouc
- Swati Singh, Dayalbagh Educational Institute
- Dino Solar Nikolic, Alea Quantum Technologies/DTU
- Dilip Krishnaswamy, Reliance Jio Infocomm
- Neel Kanth Kundu, Hong Kong University of Science and Technology
- Ali Amerimehr, RFA Co, Ltd.
- Federico Centrone, Sorbonne Université

Free evening discussion 2 candidates

- Peter Freiwang, LMU Munich
- Omid Golami, University of Calgary
- Soumya Das, Indian Statistical Institute
- Seong Su Park, ETRI
- Radel Ben-Av, HIT
- Shish Kaushik, CiRQuIT Quantum Research
- Shradhanjali Sahu, University of Leeds
- Anil Prabhakar, IIT Madras

Monday, 3 May 2021

Xiang-Bin Wang, Tsinghua University

Recent progress in practical quantum key distribution

We shall present the four-intensity protocol of MDIQKD and the sending-or-not-sending (SNS) TFQKD. With the joint constraints and Full optimization, the four-intensity MDIQKD protocol can produce a high key rate. The protocol has been applied in many experiments, e.g., the long distance MDI-QKD, the free-space MDIQKD, the on-chip MDIQKD, and so on. The SNS-TFQKD protocol has the unique advantage of fault tolerance of large mis-alignment error and also the high key rate with finite-key effects since the traditional theory of decoy-state method directly applies. So far, the SNS protocol has been successfully implemented in the experiment of 509 km QKD, the field test of 511 km QKD, the experiment of 522 km QKD and 600 km QKD.

Tony Metger, ETH Zürich

Device-independent protocols from computational assumptions

Device-independent protocols use untrusted quantum devices to achieve a cryptographic task. Such protocols are typically based on Bell inequalities and require the assumption that the quantum device is composed of separated non-communicating components. We present protocols for self-testing and device-independent quantum key distribution (DIQKD) that are secure even if the components of the quantum device can exchange arbitrary quantum communication. Instead, we assume that the device cannot break a standard post-quantum cryptographic assumption. This allows us to leverage recently introduced cryptographic tools (Brakerski et al., FOCS 2018; Mahadev, FOCS 2018) to give a classical user a high degree of control over an untrusted quantum device. Importantly, the computational assumption only needs to hold during the protocol execution and only applies to the (adversarially prepared) device in possession of the (classical) user, while the adversary herself remains unbounded. The output of the protocol, e.g. a secret key in the case of DIQKD, is information-theoretically secure.

Guillermo Curras Lorenzo, University of Leeds

Using random sampling theory to prove the finite-key security of non-standard QKD protocols

Quantum key distribution (QKD) protocols that rely on two mutually unbiased encoding bases, such as standard BB84, admit a trivial finite-key security analysis based on random sampling theory. Namely, in these protocols, the observed bit-error rate in a given basis provides a random sample for the phase-error rate in the other basis, and this fact can be used to obtain simple and tight security bounds. Protocols that do not rely on mutually unbiased encoding bases do not admit this simple security analysis, and their finite-key security proofs have often relied on Azuma's inequality, which typically results in significantly lower secret-key rates. In a recent work, we have shown that, if the users probabilistically assign tags to their detected emissions, the finite-key security of some of these protocols also admits a reduction to a random sampling problem. As an example, we apply our results to prove the finite-key security of the three-state loss-tolerant protocol, in both its prepare-and-measure and measurement-device-independent versions, obtaining considerably better secret-key rates than previous analyses based on Azuma's inequality. This talk presents the results of https://arxiv.org/abs/2101.12603.

Margarida Pereira, University of Vigo

Bridging the gap between theory and practice of QKD

Even though quantum key distribution (QKD) has made a tremendous progress in the last years, there are still a number of open challenges that need to be addressed before it can be widely used for securing our everyday communications. On the theoretical front, one important challenge is to establish implementation security, rather than theoretical security. Typical security proofs of QKD rely on unrealistic assumptions and ignore inherent device imperfections. For example, it is common to assume that the emitted states are perfectly encoded and that the user's devices do not leak any unwanted information, which is very hard to ensure in practical implementations. Problematically, this gap between theory and practice of QKD could be exploited by an eavesdropper. Namely, unaccounted device flaws are effectively side channels that could allow an eavesdropper to learn some secret information without being detected, thus compromising the security of QKD. Here, we review recent results that significantly reduce this gap, providing a clear path to prove the security of QKD with arbitrarily flawed devices, while guaranteeing high secret-key rates in some parameter regimes.

Roger Colbeck, University of York

Higher rates for device-independent randomness expansion

I will present some recent work that leads to improved rates for device-independent randomness expansion. I will discuss the key factors leading to the improvements and compare the new rates with those from previous analyses. Taking parameters from a recent experimental implementation of randomness expansion, the new techniques increase the rate such that where expansion previously took around 20hrs it would now be possible in about a minute. The talk will be based on https://arxiv.org/abs/2103.07504 .

Hamid Tebyanian, University of Padova

Practical Semi-self Testing Randomness Generation Based on Quantum State's Indistinguishability

I will present a proof-of-principle time-bin encoding semi-DI QRNG experiments based on the prepare-and-measure scheme. The experimental setup is easy-to-implement comprises commercially available off-the-shelf (COTS) components at the telecom wavelength (1550 nm), granting a high entropy source. This experiment's single and easy-to-verify assumption is bounding the prepared pulses' energy. Reliant on this single postulate and the input-output correlation, we lower bound the guessing probability and compute the conditional min-entropy, which determines the amount of genuine randomness. Moreover, we present a generalized form of semidefinite programming (SDP) for this semi-DI protocol, optimizing the conditional min-entropy for multiple input-outcome.

Federico Grasselli, University of Dusseldorf

Entropy bounds for multipartite device-independent cryptography

When the outcomes of a set of parties measuring their local quantum systems exhibit non-local correlations by violating a Bell inequality, one can infer that such outcomes are secret to some extent. This is at the core of the security of many device-independent (DI) protocols, such as DI conference key agreement. We quantify the amount of secret randomness in the parties' outcomes by analytically computing their conditional von Neumann entropies as a function of the Bell violation, for different Bell inequalities.

Davide Rusca, University of Geneva

Fast and practical quantum key distribution

In the last few decades many protocols have been developed in the domain of quantum key distribution. The first one presented, BB84, remains of interest for the community given its good performances and simplicity of implementation. In our work we simplified the experimental requirements for this protocol to the minimum using only three preparation states and two decoy intensities. In this presentation we are going to focus on pushing to the limit the repetition rate of our experiment and, in doing so, we characterize all the possible sources of imperfection that appear and that could be an hindrance to the security of the original protocol.

Tuesday, 4 May 2021

Stefano Pirandola, University of York

Ultimate limits of the quantum Internet

We examine the ultimate rates for quantum and private communication that are achievable over a quantum network with arbitrary topology. We discuss the capacities under different types of routing of the quantum systems (single-path and multi-path). We also discuss the performance of quantum networks over the globe and comparing their optimal performance with respect to the use of satellites.

Eneet Kaur, University of Waterloo

Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution

We consider discrete-modulation protocols for continuous-variable quantum key distribution (CVQKD) that employ a modulation constellation consisting of a finite number of coherent states and that use a homodyne or a heterodyne-detection receiver. We establish security proof for collective attacks in the asymptotic regime, and we provide a formula for an achievable secret-key rate. The main constituents of our approach include approximating a complex, isotropic Gaussian probability distribution by a finite-size Gauss-Hermite constellation, applying entropic continuity bounds, and leveraging previous security proofs for Gaussian-modulation protocols. As an application of our method, we calculate secret-key rates achievable over a lossy thermal bosonic channel. We show that the rates for discrete-modulation protocols approach the rates achieved by a Gaussian-modulation protocol as the constellation size is increased.

Shouvik Ghorai, Sorbonne University

Continuous-Variable Quantum Money with Classical Verification

Quantum money exploits the no-cloning property of quantum mechanics to generate unforgeable tokens, banknotes, and credit cards. We propose a continuous-variable private-key quantum money scheme with classical verification. The motivation behind this protocol is to facilitate the process of practical implementation. Previous classical verification money schemes use single-photon detectors for verification, while our protocols require coherent detection. Our money scheme exploits a set of coherent states, where we encode information on its quadratures. We analyze the correctness and security parameters of the money scheme for a varying ensemble size of 4N. We note that the loss tolerance of the scheme improves with an increase in ensemble size. Our analysis shows that CV money schemes with 13% loss tolerance are feasible. It opens up a new door to more practically feasible quantum money schemes.

Nilesh Vyas, Telecom Paris

Everlasting Secure Key Agreement in a Quantum Computational Time-lock security model

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 Time-lock (QCT) 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 with the noisy quantum memory model. Using the QCT security model, 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 permutations. To prove the security, we first show that eavesdropping reduces to performing an immediate measurement followed by post-measurement decoding. Secondly, following the construction of quantum to classical randomness extractor based on the full set of MUBs, Eve's mutual information is bounded as O(1=d). As a result, MUB-QCT offers : high resilience to error (up to 50% for large d) ; MDI-type security as security is independent of channel monitoring, and does not require to trust measurement devices. Under restricted scenario MUB-QCT protocol also allows the possibility to do secure key distribution with input states containing up to O(d) photons, which implies a significant performance increase, characterized by a O(d) multiplication of key rates.

Beatrice da Lio, University of Copenhagen

Frequency conversion of single photons to 1550 nm enabling quantum communication protocols

Quantum communication applications require high speed indistinguishable single photons at telecom wavelengths, to exploit the low loss transmission window of optical fibers and hence allow long distance communication links. However, high performance quantum dot single photon sources have been demonstrated emitting in the wavelength range of 900-980 nm. In this talk, I will present our recent work on quantum frequency conversion of single photons from a bright quantum dot emitting at 942 nm to 1550 nm. The overall end-to-end efficiency was measured to be 40.9%, and high single photon purity was demonstrated with a second order correlation function value of g2(0)=0.029 after conversion.

Mirko Pittaluge, Toshiba Research Europe Ltd

Dual-band phase stabilisation technique for long distance quantum communications

We discuss the characteristics and the advantages of using a dual-band phase stabilisation technique for phase-sensitive quantum communications. We examine how this technique can extend the current range of fibre-based Quantum Key Distribution by discussing experimental results obtained with a Twin Field QKD setup.

Gaëtan Gras, ID Quantique

Countermeasure against quantum hacking using detection statistics

In the last few years, detector blinding attacks have been proposed and could potentially threaten the security of quantum key distribution systems. Even though such attacks are technically challenging to implement, it is important to consider countermeasures to avoid information leakage. We present a countermeasure against these kinds of attacks based on the use of multipixel detectors. Thanks to this method, we are able to estimate an upper bound on the information Eve could have obtained on the key exchanged. Finally, we show that a multipixel detector based on superconducting nanowire single-photon detectors can fulfill all the requirements for our countermeasure to be effective.

Innocenzo de Marco, Toshiba Research Europe Ltd

Photonic integration of a directly phase-modulated source for Quantum Key Distribution

Deployment of quantum key distribution systems will rely on devices that are cheap, compact and scalable. In this talk I will describe the photonic integration of a light source that is well-suited for this, as it is able to generate signal states for a variety of different protocols without the need for unbalanced interferometers or phase modulators, which would add to the complexity of the system.

Wednesday, 5 May 2021

Tracy Northup, University of Innsbruck

Trapped-ion interfaces for quantum networks

Future quantum networks offer a route to quantum-secure communication, distributed quantum computing, and quantum-enhanced sensing. A current challenge across all experimental platforms is how to move beyond proof-of-principle realizations to the efficient, faithful distribution of quantum states over scalable networks. I will present ongoing work on nodes for quantum networks based on trapped ions in optical cavities, focusing in particular on a connection between remote trapped-ion systems in Innsbruck. We will then consider how to extend such links to multi-node networks.

Liang Jiang, University of Chicago

Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes

We propose a novel architecture of quantum-error-correction-based quantum repeaters that combines the techniques used in discrete and continuous-variable quantum information [1]. Specifically, we propose to encode the transmitted qubits in a concatenated code consisting of two levels. On the first level we use a continuous-variable GKP code which encodes the qubit in a single bosonic mode. On the second level we use a small discrete-variable code, encoding a logical qubit in as few as four or seven physical qubits. We find that the combination of using the two types of repeaters enables us to achieve performance needed in practical scenarios with a significantly reduced cost with respect to an architecture based solely on multi-qubit repeaters. [1] Rozpędek, F., Noh, K., Xu, Q., Guha, S. & Jiang, L. Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes. arXiv:2011.15076 (2020).

Yumang Jing, University of Leeds

Quantum key distribution over quantum repeaters with encoding

We propose a postselection technique, based on quantum error detection, for quantum key distribution (QKD) systems that run over quantum repeaters with encoding. We fully study the effect of different terms, components, and system imperfections on the secret key generation rate of the QKD system, and how one can use the information obtained during entanglement swapping and decoding stages to maximize the rate.

Antonio Ortu, University of Geneva

A long-lived quantum memory for quantum repeaters

In recent years, experimental demonstrations showed how rare earth-doped solid-state crystals are capable of storing, coherently and on-demand, states of light at the single photon level and entanglement of photon-spin pairs to be used as building blocks for future quantum repeaters. By improving on our previous work on a Eu:YSO based quantum memory, we show how even longer storage times can be obtained, while preserving a good signal to noise ratio and multimode capability.

Katanya Kuntz, University of Waterloo

Satellite Quantum Key Distribution & the QEYSSat Mission

I will discuss Quantum Key Distribution (QKD) and how it can be combined with satellites to make a secure global quantum network. I will give a high-level overview of the current 'Quantum Space Race,' and Canada's upcoming QEYSSat mission, the Quantum Encryption and Science Satellite, as well as my role as the QEYSSat Science Team Coordinator. I will explain how to generate secure keys between two Quantum Ground Stations using a satellite, such as QEYSSat, as a trusted node.

Mujtaba Zahidy, University of Padova

Recent developments in practical BB84 QKD

Practical quantum key distribution, in free-space or fiber, requires a meticulous effort to achieve stable, resilient key generation rate with low QBER and hence, high practical security. These efforts should focus on reducing the errors in preparation, perfect transmission of qubits, and cancelling the sources of noise at measurement. Here, we shall cover a series of endeavors in order to achieve a stable key generation in free-space as well as fiber-based QKD with practical examples in deployed fiber. I will cover new techniques to generate mutually unbiased basis used in polarization-based BB84, sharing a time reference between entities in QKD, polarization drift compensation, free-space to fiber injection, and finally, parallel classical communication. The result of a series of experiments will be presented.

Robert Trenyi, University of Vigo

Performance of the coherent-one-way quantum key distribution protocol

Multi-photon pulses emitted by practical laser sources limit the performance of quantum key distribution (QKD) due to the photon-number splitting (PNS) attack. The coherent-one-way (COW) QKD protocol was proposed to rule out the possibility of the PNS attack while it was believed to be able to provide a secret key rate that scales linearly with the system's transmittance with a relatively simple experimental setup. Here we disprove this expectation by providing an upper bound on its secret key rate that scales at most quadratically with the system's transmittance via considering an intercept-resend type of attack. This makes the COW scheme inappropriate for long-distance QKD. Moreover, we also show that so far all implementations of the COW protocol appearing in scientific literature are actually insecure.

Carlo Liorni, University of Dusseldorf

Intercontinental communication through space-borne quantum repeaters

In this work we propose to combine quantum repeaters and satellite-based links, into a scheme that allows to achieve entanglement distribution over global distances with a small number of intermediate untrusted nodes. We perform a comparison with other repeater chain architectures and show that our scheme, even though more technically demanding, is superior in many situations of interest. We analyse strengths and weaknesses of the proposed scheme, discuss exemplary orbital configurations and study the impact of changing some crucial parameters. The integration of satellite-based links with ground repeater networks can be envisaged to represent the backbone of the future Quantum Internet.

Organising and Technical Programme Committee:

Eleni Diamanti, CNRS and Sorbonne University
Dagmar Bruß, University of Dusseldorf
Romain Alleaume, Telecom Paris
Félix Bussières, ID Quantique
Mohsen Razavi, University of Leeds
Federico Grasselli, University of Dusseldorf
Gaëtan Gras, ID Qunatique
Hamid Tebyanian, University of Padova

More information..... www.qcall-itn.eu/qfs

Contact us..... qfs@qcall-itn.eu

MARIE CURIE ACTIONS