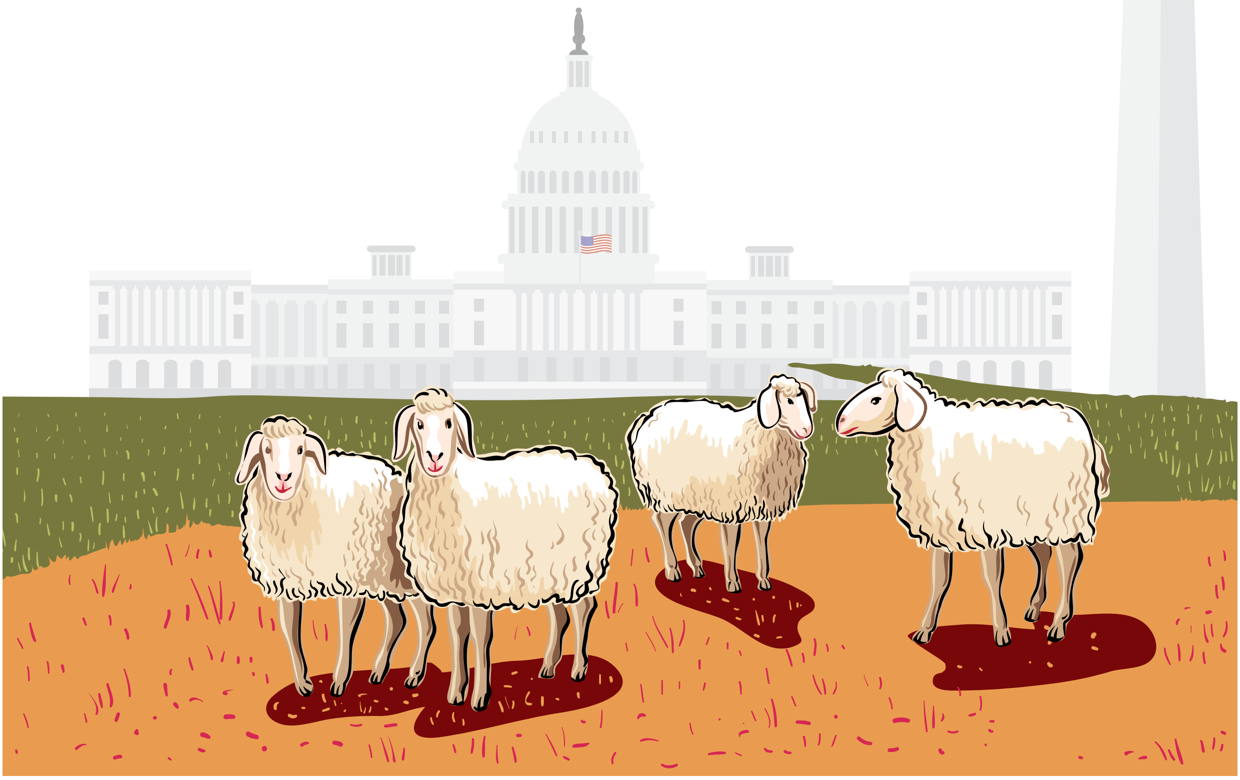
QCrypt

6th INTERNATIONAL CONFERENCE ON QUANTUM CRYPTOGRAPHY



SEPTEMBER 12 – 16, 2016

WASHINGTON, D.C.

2016.qcrypt.net

COMMITTEES

PROGRAM COMMITTEE

Matthias Christandl (*University of Copenhagen*) (*chair*)
Hugo Zbinden (*University of Geneva*) (*vice chair*)
Antonio Acin (*ICFO Barcelona*)
Romain Alléaume (*Télécom ParisTech*)
Ulrik Lund Andersen (*Technical University of Denmark*)
Nicolas Brunner (*University of Geneva*)
Claude Crepeau (*McGill University*)
Frederic Dupuis (*Masaryk University*)
Mikio Fujiwara (*NICT of Japan*)
Warren Grice (*Oak Ridge National Laboratory*)
Iordanis Kerenidis (*University Paris Diderot*)
Masato Koashi (*University of Tokyo*)
Antia Lamas-Linares (*University of Texas/National University of Singapore*)
Carl Miller (*University of Michigan*)
Michele Mosca (*University of Waterloo*)
Maris Ozols (*University of Cambridge*)
Louis Salvail (*University of Montreal*)
Mark Thompson (*University of Bristol*)
Giuseppe Vallone (*University of Padova*)
Feihu Xu (*MIT*)
Qiang Zhang (*University of Science and Technology of China*)

STEERING COMMITTEE

Yi-Kai Liu (*NIST/University of Maryland) (chair)*
Eleni Diamanti (*CNRS, Telecom ParisTech*)
Norbert Lütkenhaus (*IQC, University of Waterloo*)
Masahide Sasaki (*NICT*)
Christian Schaffner (*University of Amsterdam*)
Wolfgang Tittel (*University of Calgary*)
Stephanie Wehner (*QuTech, TU Delft*)

ADVISORY COMMITTEE

Charles H. Bennett (*IBM Research*)
Gilles Brassard (*Université de Montréal*)
Ivan Damgård (*Aarhus University*)
Artur Ekert (*CQT Singapore and Oxford University*)
Nicolas Gisin (*Université de Genève*)
Richard Hughes (*Unaffiliated*)

LOCAL ORGANIZERS

Yi-Kai Liu (*NIST/University of Maryland) (lead organizer*)
Andrew Childs (*University of Maryland*)
Jake Taylor (*NIST/University of Maryland*)

Assisted by the staff of the Joint Center for Quantum Information and Computer Science (QuICS), the University of Maryland Institute for Advanced Computer Studies (UMIACS), and Conferences & Visitor Services (C&VS) at the University of Maryland.

Joint Center for Quantum Information and Computer Science

WELCOME TO QCrypt 2016

Dear Conference Attendees,

Welcome to QCrypt 2016, the 6th International Conference on Quantum Cryptography. This is the first time that QCrypt is being held in the United States, and we are glad to see you all here!

QCrypt is an interesting conference for many reasons. First, quantum cryptography is an excellent example of the power and promise of quantum information science. From its humble beginnings, quantum cryptography has grown to encompass a wide range of topics, including the foundations of cryptography and quantum mechanics; atomic, molecular and optical physics; the engineering of quantum memories and quantum networks; and practical schemes for secure communication in a world with quantum computers. All of these topics can be seen in the scientific program at QCrypt.

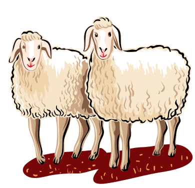
At the same time, science is a human endeavor, and the QCrypt community is an interesting one. This community includes people from many different backgrounds: theorists and experimentalists, physicists and mathematicians, cryptographers and communications engineers. The QCrypt conference is designed to encourage this mixing of disciplines. I think this is fitting because quantum cryptography is itself a product of theoretical insight combined with experimental implementation.

Finally, I would like to say that this conference is the result of many people's efforts. At the organizational level, QCrypt 2016 is being hosted by the Joint Center for Quantum Information and Computer Science (QuICS), a partnership between the University of Maryland and the National Institute of Standards and Technology (NIST). QuICS was founded in 2014, and hosts a growing number of faculty, postdoctoral researchers and graduate students, all working on topics at the intersection of quantum information science, fundamental physics, theoretical computer science, and computer engineering.

At a more personal level, I would like to thank the QCrypt steering committee, the QCrypt program committee, my fellow local organizers at QuICS, the student travel funding committee, the staff of the University of Maryland Institute for Advanced Computer Studies (UMIACS), the staff of the University of Maryland Conference & Visitor Services (C&VS), and our many external contractors for their assistance in planning and hosting this conference. Their contributions were essential to the success of this event.

We hope you enjoy the conference!

Sincerely,
Yi-Kai Liu
Lead local organizer for QCrypt 2016
Chair, QCrypt steering committee, 2015-2016



CONFERENCE OVERVIEW

KEY

- TUTORIAL
- CONTRIBUTED TALK
- INVITED TALK
- SPECIAL EVENT
- POSTER SESSION
- BREAK

MONDAY, SEPTEMBER 12	
9 AM	**Roger Colbeck**, "Device-Independent Random Number Generators"
10:20 AM	Coffee break
10:50 AM	**Mark Wilde**, "Converse Bounds for Private Communication Over Quantum Channels"
11:25 AM	"Simple and Tight Device-Independent Security Proofs"
11:45 AM	"Zero-Knowledge Proof Systems for QMA"
12:05 PM	Lunch
1:40 PM	**Stefano Pirandola**, "Fundamental Limits of Repeaterless Quantum Communications"
2:15 PM	"A Modulator-Free QKD Transmitter"
2:35 PM	"77-Day Field Trial of High Speed Quantum Key Distribution with Implementation Security"
2:55 PM	"Towards Secure QKD with Testable Assumptions on Modulation Devices"
3:15 PM	Coffee break
3:45 PM	**Dirk Englund**, "Photonic Integrated Circuits for Quantum Communications"
4:20 PM	"Observation of Quantum Fingerprinting Beating the Classical Limit"
4:40 PM	"24-Hour Long Relativistic Bit Commitment"
5–5:20 PM	"Quantum Teleportation Over Deployed Fibres and Applications to Quantum Networks"
6–7 PM	QCrypt Public Lecture: **Michele Mosca**, "Cryptography and Cybersecurity in the Quantum Era"

ALL CONFERENCE EVENTS
will be held at the Carnegie Institution for Science,
1530 P St. NW, Washington, D.C. 20005

PLEASE NOTE: All talks will take place in the main auditorium at the Carnegie Institution for Science. Posters are in rooms surrounding the auditorium.

THE CONFERENCE BANQUET
will be held at the Mayflower Hotel,
1127 Connecticut Ave. NW, Washington, D.C. 20036

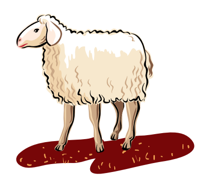
TUESDAY, SEPTEMBER 13	
9:20 AM	**Anne Broadbent**, "How to Verify a Quantum Computation"
10 AM	"Quantum Homomorphic Encryption for Polynomial-sized Circuits"
10:20 AM	Coffee break
10:50 AM	**Jungsang Kim**, "Distributed Quantum Networks Based on Trapped Ions"
11:25 AM	"Rate-Distance Tradeoff and Resource Costs for All-Optical Quantum Repeaters"
11:45 AM	"Continuous Variable Quantum Computing on Encrypted Data"
12:05 PM	Lunch
1:40–2:20 PM	Industry session: **Zachary Dutton, Gregoire Ribordy and Michele Mosca**
2:25 PM	"New Security Notions and Feasibility Results for Authentication of Quantum Data"
2:45 PM	"Continuous-Variable Quantum Key Distribution with a 'Locally' Generated Local Oscillator" "Theoretical Analysis and Proof-of-Principle Demonstration of Self-Referenced Continuous-Variable Quantum Key Distribution" (Combined talks)
3:15 PM	Coffee break
3:45–6 PM	Poster session #1

PLEASE NOTE: All talks will take place in the main auditorium at the Carnegie Institution for Science. Posters are in rooms surrounding the auditorium.

WEDNESDAY, SEPTEMBER 14	
9 AM	**Vadim Makarov**, "Challenges to Physical Security of Today's Quantum Technologies"
10:20 AM	Coffee break
10:50 AM	**Thomas Jennewein**, "Implementing Free-Space QKD Systems Between Moving Platforms: Polarization vs. Time-Bin Encoding"
11:25 AM	"Quantum-Limited Measurements of Signals from a Satellite in Geostationary Earth Orbit"
11:45 AM	"Time-Bin Encoding Along Satellite-Ground Channels"
12:05 PM	Lunch
Free Afternoon	

KEY

- TUTORIAL
- CONTRIBUTED TALK
- INVITED TALK
- SPECIAL EVENT
- POSTER SESSION
- BREAK



CONFERENCE OVERVIEW

KEY

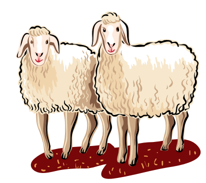
- TUTORIAL
- CONTRIBUTED TALK
- INVITED TALK
- SPECIAL EVENT
- POSTER SESSION
- BREAK

THURSDAY, SEPTEMBER 15	
9 AM	**Bell Test Session:** Ronald Hanson, Krister Shalm, Marissa Giustina and Harald Weinfurter
10:40 AM	Coffee break
11 AM	**Elham Kashefi**, “Verification of Quantum Computing”
12:20 PM	Lunch
1:40 PM	**Hoi-Kwong Lo**, “Battling with Quantum Hackers”
2:15 PM	“Quantum-Proof Multi-Source Randomness Extractors in the Markov Model”
2:35 PM	“On Quantum Obfuscation”
2:55 PM	“Breaking Symmetric Cryptosystems Using Quantum Period Finding”
3:15 PM	Coffee break
3:45–6 PM	Poster session #2
6:30–9:30 PM	Conference Dinner

FRIDAY, SEPTEMBER 16	
9 AM	**Chris Peikert**, “Lattices, Rings, and Cryptography: Theory and Practice”
10:20 AM	Coffee break
10:50 AM	**Dominique Unruh**, “Verification in Quantum Cryptography”
11:25 AM	“Adaptive Versus Non-Adaptive Strategies in the Quantum Setting”
11:45 AM	“Computational Security of Quantum Encryption”
12:05 PM	Lunch
1:40 PM	“Cross-Phase Modulation of a Probe Stored in a Waveguide for Non-Destructive Detection of Photonic Qubits”
2:05 PM	“Information Theoretically Secure Distributed Storage System with Quantum Key Distribution Network and Password Authenticated Secret Sharing Scheme”
2:30 PM	“Integrated Silicon Photonics for Quantum Key Distribution” “Wavelength-Division-Multiplexed QKD with Integrated Photonics” (Combined talks)
2:55 PM	“Laser Damage Creates Backdoors in Quantum Cryptography” “Insecurity of Detector-Device-Independent Quantum Key Distribution” (Combined talks)
3:20 PM	Coffee break
3:45–4:45 PM	Hot Topics Session

KEY

- TUTORIAL
- CONTRIBUTED TALK
- INVITED TALK
- SPECIAL EVENT
- POSTER SESSION
- BREAK



QCrypt PUBLIC LECTURE

Cryptography and Cybersecurity in the Quantum Era

MICHELE MOSCA
University Research Chair and Co-Founder,
Institute for Quantum Computing (IQC), University of Waterloo

MONDAY, 6–7 PM

Cyber technologies and cybersecurity are evolving at an ever-increasing rate, changing apace with social and technological advances.

The emergence of quantum technologies is a critical game-changer that offers new opportunities and challenges for cyber technologies and security.

Quantum computers offer the promise of doing computations previously thought to be impossible, and enabling the solution of important problems for humankind.

However, quantum computers will also break some of the pillars of modern-day cybersecurity. This poses a major challenge for academia, industry and governments, who need to work together to design and deploy new tools that will remain secure in the era of quantum computers.

The flip-side is that quantum information technologies will also enable new tools for helping secure information—tools known as quantum cryptography.

Keynote speaker Michele Mosca will explain the basic ideas behind quantum cryptography and some of the novel applications it enables. He will discuss its impact on the foundations of quantum information science and technology, and its direct, practical applications to society.

MICHELE MOSCA *is a university research chair and co-founder of the Institute for Quantum Computing, University of Waterloo, Canada*

Mosca is globally recognized for his drive to help academia, industry and government prepare their cyber systems to be safe in an era with quantum computers. He is a founding member of the Perimeter Institute for Theoretical Physics and has co-founded evolutionQ Inc. to help organizations evolve their quantum-vulnerable systems and practices to quantum-safe ones.

Mosca obtained his doctorate in mathematics in 1999 from the University of Oxford on the topic of quantum computer algorithms.

Industry Sesssion

ZACHARY DUTTON
Vice President and Lead Scientist, Quantum Information Processing,
Raytheon BBN Technologies

TUESDAY, 1:40 PM

ZACHARY DUTTON *is currently vice president of Quantum Information Processing and a lead scientist at Raytheon BBN Technologies, where he has been since 2007.*

In his recent work, Dutton has worked on a variety of topics in quantum information, including techniques for quantum-enhanced LADAR, joint code-word detection for optical communications, repeater implementations for quantum communications, and quantum computing with superconducting circuits. He has over 50 refereed publications.

In his four years as manager of the Quantum Information Processing business unit, he has grown the staff from 12 to 27 and greatly expanded the size of its cryogenic and optics laboratories. Under his leadership, the group has expanded its capabilities and expertise in a number of areas, including quantum communications, quantum imaging, superconducting circuit-based quantum computing, quantum algorithms, nano-photonics, and cryogenic classical processing.

He received his Bachelor of Arts in physics from U.C. Berkeley in 1996 and his doctorate in theoretical atomic physics from Harvard University in 2002, where he performed seminal work on slow light propagation and electromagnetically induced transparency in atomic Bose-Einstein condensates.

GREGOIRE RIBORDY
Co-Founder and CEO, ID Quantique

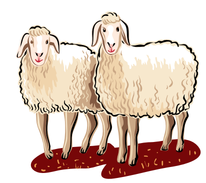
GREGOIRE RIBORDY *has 20 years of experience in various research and development (R&D) and management roles in the field of optical measurements and communication systems.*

He founded ID Quantique in 2001 and has managed the company since then. Prior to this, he was a research fellow at the Group of Applied Physics of the University of Geneva between 1997 and 2001. In this position, he actively developed quantum cryptography technology and is the holder of a number of patents in the field.

Between 1995 and 1996, Ribordy worked for one year in the R&D division of Nikon Corp. in Tokyo.

He is the recipient of several awards such as the 2001 New Entrepreneurs in Technology and Science prize, the 2002 de Vigier award and the Swiss Society for Optics and Microscopy 1999 prize. In 2005, the World Technology Network selected him as one of the most innovative individuals in information technology worldwide.

**Michele Mosca will also participate in the industry session (see left).*



evolution

ICFO The Institute of Photonic Sciences

IDQ FROM VISION TO TECHNOLOGY

INFOSEC GLOBAL

ENTROPY

MPD MICRO PHOTON DEVICES

PicoQuant Unternehmen für optoelektronische Forschung und Entwicklung

Quantum Opus

OEC OptoElectronic Components

qutools

SINGLE QUANTUM Excellence in photon detection

NPJ QUANTUM INFORMATION

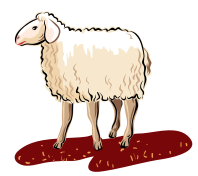
QCrypt thanks all of its sponsors and industry exhibitors for their support and participation.

SCOTT AARONSON
David J. Bruton Centennial Professor of Computer Science, University of Texas at Austin

SCOTT AARONSON*'s research focuses mainly on the capabilities and limits of quantum computers, including quantum lower bounds, quantum proofs and advice, BosonSampling, and quantum money.*

Before coming to the University of Texas at Austin, Aaronson spent nine years as a professor in electrical engineering and computer science at MIT. His first book, "Quantum Computing Since Democritus," was published in 2013 by Cambridge University Press. Aaronson has been honored with the National Science Foundation's Alan T. Waterman Award, the United States PECASE Award, and MIT's Junior Bose Award for Excellence in Teaching.

He received his Bachelor of Science in computer science from Cornell University and his doctorate from U.C. Berkeley. Aaronson completed postdoctoral fellowships at the Institute for Advanced Study in Princeton, New Jersey as well as the University of Waterloo.



Device-Independent Random Number Generators

ROGER COLBECK *University of York*
MONDAY, 9 AM

When executing cryptographic protocols, we usually assume we know how our devices operate, and the success of the protocol relies on this. However, ensuring that devices really operate as intended is far from easy and devices that behave badly may be exploitable by an adversary. This is a particular problem for the task of generating random numbers using quantum mechanics.

In this tutorial, I will discuss protocols that can certify randomness generation based only on the input-output behavior of any devices used, and without needing to model how they produce their outputs (other than that they obey the laws of physics). I will explain the model in detail, before discussing the ideas that go into security proofs.

Challenges to Physical Security of Today's Quantum Technologies

VADIM MAKAROV *University of Waterloo*
WEDNESDAY, 9 AM

I will discuss security threats at the optical implementation layer of quantum communications. Examples of side-channel attacks, countermeasures, and testing the quality of countermeasures will be given.

At our present level of technology, the security-critical part of a quantum communication system is essentially an analog optoelectronic system connected to the optical channel, and is easily accessible by an adversary. Today's implementations sport a surprisingly rich set of imperfections and vulnerabilities, presenting challenges to standardization efforts. This is not surprising in a historical perspective, as our quantum technology today is as rudimentary as the electronic communication and computing were 70 years ago. The history also hints that the technology will improve.

Verification of Quantum Computing

ELHAM KASHEFI *University of Edinburgh*
THURSDAY, 11 AM

Since classical computations cannot scale up to the computational power of quantum mechanics, verifying the correctness of a quantum-mediated computation is challenging. The ability to compute with encrypted data, while hiding the underlying function, has opened a new approach toward verification through the detection of a cheating server that we will review in this tutorial.

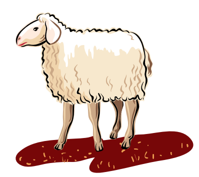
TUTORIALS
MONDAY, WEDNESDAY, THURSDAY AND FRIDAY

Lattices, Rings, and Cryptography: Theory and Practice

CHRIS PEIKERT *University of Michigan*
FRIDAY, 9 AM

Point lattices provide one of the most attractive potential foundations for post-quantum cryptography, i.e., classical systems that are secure against quantum attacks. In addition to powerful objects like fully homomorphic encryption, lattices yield solutions to "everyday" tasks like key exchange and digital signatures. In order to be efficient enough for practical use, such systems typically need to use "algebraically structured" lattices defined over certain polynomial rings.

This tutorial will survey the state-of-the-art in lattice and ring-based cryptography, with a particular focus on theoretical foundations like the (Ring-)SIS/LWE problems and their "worst-case hardness" theorems, classical and quantum cryptanalysis, recent practical implementations, and important open questions and research directions.



Converse Bounds for Private Communication Over Quantum Channels

MARK WILDE *Louisiana State University*
MONDAY, 10:50 AM

We establish several converse bounds on the private transmission capabilities of a quantum channel. The main conceptual development builds firmly on the notion of a private state [Horodecki et al., PRL 94, 160502 (2005)], which is a powerful, uniquely quantum method for simplifying the tripartite picture of privacy involving local operations and public classical communication to a bipartite picture of quantum privacy involving local operations and classical communication. This approach has previously led to some of the strongest upper bounds on secret key rates, including the squashed entanglement and the relative entropy of entanglement.

Here we use this approach along with a "privacy test" to establish a general meta-converse bound for private communication, which has a number of applications. The meta-converse allows for proving that any quantum channel's relative entropy of entanglement is a strong converse rate for private communication. For covariant channels, the meta-converse also leads to second-order expansions of relative entropy of entanglement bounds for private communication rates. For such channels, the bounds also apply to the private communication setting in which the sender and receiver are assisted by unlimited public classical communication, and as such, they are relevant for establishing various converse bounds for quantum key distribution protocols conducted over these channels. We find precise characterizations for several channels of interest and apply the methods to establish several converse bounds on the private transmission capabilities of all phase-insensitive bosonic channels.

This is joint work with Mario Berta and Marco Tomamichel.

Fundamental Limits of Repeaterless Quantum Communications

STEFANO PIRANDOLA *University of York*
MONDAY, 1:40 PM

Quantum communications promises reliable transmission of quantum information, efficient distribution of entanglement, and generation of completely secure keys. For all these tasks there is a crucial question to answer: What are their optimal rates without quantum repeaters?

Our work solves this basic question for any two parties connected by a quantum channel, without any restriction on their classical communication, which can be unlimited and two-way. We design a method which reduces the most general protocol of quantum communication to the computation of a novel quantity, identified as the channel's relative entropy of entanglement. In this way, we bound the ultimate rates that are achievable over the most important bosonic and qubit channels, computing a number of exact formulas for their two-way capacities.

In particular, we determine the fundamental rate-loss scaling which affects any quantum optical communication. By setting these limits, we establish the most general and correct benchmarks for testing the performance of quantum repeaters.

INVITED TALKS

Photonic Integrated Circuits for Quantum Communications

DIRK ENGLUND *Massachusetts Institute of Technology (MIT)*
MONDAY, 3:45 PM

Photonic integrated circuits (PICs) have become increasingly important in classical communications applications over the past decades, including as transmitters and receivers in long-haul, metro and datacenter interconnect. Many of the same attributes that make PICs attractive for these applications—stability, compactness, high bandwidth, and integration with electronics—also make them appealing for quantum communications.

The first part of this talk will review our recent progress in adapting one of the leading PIC architectures—silicon photonics—for various quantum secure communications protocols. The second part of the talk will consider how photonic integrated circuits technology can extend the reach of quantum communications through all-optical and memory-based quantum repeater protocols.

How to Verify a Quantum Computation

ANNE BROADBENT *University of Ottawa*
TUESDAY, 9:20 AM

Experimental implementations of quantum computers are in their infancy, but already we are faced with the following conundrum: If quantum computers are exponentially more powerful than their classical counterparts, how can we verify the outcome of a quantum computation? In this context, the scientific method of "predict and verify" appears to fail dramatically: these computations are so complex that they are impossible to predict. For a solution to this problem, we turn to theoretical computer science, where it is well established that interaction dramatically increases the power of a verification process.

We thus give a new interactive protocol for the verification of quantum computations in the regime of high computational complexity. Our results are given in the language of quantum interactive proof systems. Specifically, we show that any language in BQP has a quantum interactive proof system with a polynomial-time classical verifier (who can also prepare random single-qubit pure states), and a quantum polynomial-time prover. Here, soundness is unconditional—i.e. it holds even for computationally unbounded provers. Compared to prior work, our technique does not require the encoding of the input or of the computation; instead, we rely on encryption of the input (together with a method to perform computations on encrypted data), and show that the random choice between three types of input (defining a computational run, versus two types of test runs) suffice. Because the overhead is linear, this shows that verification could be achieved at minimal cost. We also present a new soundness analysis, based on a reduction to an entanglement-based protocol.

Distributed Quantum Networks Based on Trapped Ions

JUNGSANG KIM *Duke University*
TUESDAY, 10:50 AM

Construction and operation of a distributed quantum network can enable exciting applications, such as scalable quantum computer and long-distance secure quantum communication systems, but remains a major experimental challenge. Practical realization of a quantum network can be accomplished by the integration of high quality quantum memories and quantum information processing elements with photonic communication channels. Other than identifying physical quantum systems to implement the qubits and logic operations, new protocols for maintaining quantum coherence through a range of quantum operations, classical controllers that keep track of quantum coherence, and new enabling technologies to bridge the hybrid quantum systems are required.

I will describe main challenges and ideas for research directions in enabling practical quantum networks, and discuss examples of relevant research efforts in trapped ion and single photon experiments. Specifically, experimental progress in trapped ion systems in microfabricated traps will be presented.

Implementing Free-Space QKD Systems Between Moving Platforms: Polarization vs. Time-Bin Encoding

THOMAS JENNEWEIN *University of Waterloo*
WEDNESDAY, 10:50 AM

Quantum key distribution (QKD) between moving users is an important step toward realizing a secure network applicable to special use-cases in the field as well as for reaching global distances via quantum satellites. While free-space systems are conceptually similar to fiber-optic systems, the intrinsically variable free-space quantum channel poses unique challenges for the quantum link, including the alignment of reference frames between Alice and Bob, optics and telescopes with active pointing and tracking, blocking background signals, and coping with atmospheric turbulence which makes the beams multi-modal.

Typically, free-space systems have been based on polarization encoding, and I will present our experimental results for transmitting quantum signals from a stationary transmitter to a moving quantum receiver located on a moving truck. I will also present our prototype satellite payload, which has the form-fit-function of the final system, and is currently undergoing outdoor trials.

As a viable alternative to polarization based systems, I will present our recent achievements on implementing time-bin encoded photon analyzers, which demonstrate high interference visibility between time bins despite the highly multi-modicity in spatial and temporal degrees of freedom of the received photons. In conclusion, I will illustrate that time-bin encoding of photons is now applicable to highly multimodal beams, and could lead to interesting advances and applications for quantum communications not possible with polarization encoding.

INVITED TALKS

SPECIAL SESSION ON LOOPHOLE-FREE BELL TESTS

THURSDAY, 9 AM

From the First Loophole-Free Bell Test to a Quantum Internet

RONALD HANSON *Delft University of Technology*
The realization of a highly connected network of qubit registers is a central challenge for quantum information processing and long-distance quantum communication. Diamond spins associated with NV centers are promising building blocks for such a network as they combine a coherent optical interface [1] (similar to that of trapped atomic qubits) with a local register of robust and well-controlled nuclear spin qubits [2].

Here we present our latest progress towards scalable quantum networks, which includes the first loophole-free violation of Bell's inequalities [3,4] and the realization of a robust quantum network memory with nuclear spin qubits using decoherence-protected subspaces [5].

[1] W. Pfaff et al., Science 345, 532 (2014).
[2] J. Cramer et al., Nature Comm. 7, 11526 (2016).
[3] B. Hensen et al., Nature 526, 682 (2015).
[4] B. Hensen et al., Scientific Reports (in press), see also arxiv:1603.05705.
[5] A. Reiserer et al., Phys. Rev. X 6, 021040 (2016).

A Strong Loophole-Free Test of Local Realism and Applications to Randomness

KRISTER SHALM *National Institute of Standards and Technology (NIST)*
Eighty-one years ago, Einstein, Podolsky, and Rosen published a paper with the aim of showing that the wave function in quantum mechanics does not provide a complete description of reality. The Gedankenexperiment showed that quantum theory, as interpreted by Niels Bohr, leads to situations where distant particles, each with their own "elements of reality," could instantaneously affect one another. Such action at a distance seemingly conflicts with relativity. The hope was that a local theory of quantum mechanics could be developed where individual particles are governed by elements of reality, even if these elements are hidden from us. This concept is known as local realism.

In 1964, John Bell, continuing Einstein's line of investigation, showed that the predictions of quantum mechanics are fundamentally incompatible with any local realistic theory. Bell's theorem has profoundly shaped our modern understanding of quantum mechanics, and lies at the heart of quantum information theory. However, all experimental tests of Bell's theorem have had to make assumptions that lead to loopholes.

This past year, a loophole-free violation of Bell's 1964 inequalities, a 'holy grail' in the study of the foundations of quantum mechanics for half a century, was finally achieved by three different groups. Here, we present the loophole-free Bell experiment carried out at the National Institute of Standards and Technology (NIST) that requires the minimal set of assumptions possible. We obtain a statistically significant violation of Bell's inequality using photons that are space-like separated, and therefore forbidden by relativity from communicating. We find that local realism is not compatible with our experimental results. Specifically, we use rigorous statistical methods to reject the null hypothesis that nature obeys local realism with a p-value on the order of 10^-9.

Besides testing local realism, a loophole-free Bell test can be used in a device-independent configuration to extract randomness. I'll also briefly discuss our work at NIST using our loophole-free Bell test setup to extract randomness, as well as our plans to incorporate this source into the NIST randomness beacon.

Significant-Loophole-Free Test of Local Realism with Entangled Photons

MARISSA GIUSTINA *IQOQI/University of Vienna*

Local realism is the worldview in which physical properties of objects exist independently of measurement and where physical influences cannot travel faster than the speed of light. Bell's theorem states that this worldview is incompatible with the predictions of quantum mechanics, as is expressed in Bell's inequalities. Previous experiments convincingly supported the quantum predictions. Yet, every experiment requires assumptions that provide loopholes for a local realist explanation.

Here, we report a Bell test that closes the most significant of these loopholes simultaneously. Using a well-optimized source of entangled photons, rapid setting generation, and highly efficient superconducting detectors, we observe a violation of a Bell inequality with high statistical significance.

Event-Ready Loophole Free Bell Test Using Heralded Atom-Atom Entanglement

HARALD WEINFURTER *Ludwig-Maximilians-Universität München*

Atom-photon entanglement together with entanglement swapping enables an event-ready Bell experiment closing the detection as well as the locality loophole.

Atomic states offer clear advantages for Bell experiments due to the high detection efficiency. In our experiment two entangled atom-photon couples separated by 400 m. line of sight are combined using entanglement swapping. In spite of comparatively low collection efficiency of the photons, we obtain about 1-2 entangled atom pairs per minute. The Bell-state measurement of the entanglement $|\psi^{-}>$ and $|\psi^{+}>$heralds each measurement run. It serves as signal for the observers to start their measurements and to report on their respective results for every run. In this case, a limited detection efficiency is not an issue anymore and enters only in the noise of the experiment. Thus the well-known Clauser-Horn-Shimony-Holt (CHSH) Bell-inequality can be used to obtain high significance with a modest number of events.

Warranting space-like separated observation of the state of the two atoms is enabled by introducing a state dependent ionisation scheme with detection efficiency of the fragments above 95 percent within less than 800 ns. The random number generation is achieved by sampling a telegraph signal and, without any post-processing, exhibits no bias. No correlations are observable for times longer than 100 ns, which altogether makes the two observers truly independent from each other.

In a measurement with a predefined number of 5000 events an overall CHSH S-parameter of $S^{-} = 2.35 \pm 0.047$ was obtained with a p-value of $p = 6.73 \cdot 10^{-7}$, indicating significant disagreement with LHV theories. The question arises whether this experiment can be improved toward device independent key distribution.

INVITED TALKS

Battling with Quantum Hackers

HOI-KWONG LO *University of Toronto*

THURSDAY, 1:40 PM

Quantum hacking threatens the security of practical quantum key distribution (QKD) systems by exploiting their real-life imperfections.

Here, I survey recent practical methods to foil quantum hackers together with their strengths and weaknesses. Device-independent QKD, which is now close to experimental realization, promises ultimate security, but with current technology, it will give a low-key rate at metropolitan distances and can be vulnerable to memory attacks. Measurement-device-independent (MDI)-QKD is automatically immune to all attacks on detectors—the most vulnerable part of a QKD system—and has a high key rate. MDI-QKD has been demonstrated over long distances (e.g. 404 km. of low loss optical fiber and 311 km. of standard optical fiber), as well as in a network setting. With MDI-QKD, the source of a QKD system may become Eve's main interest. Fortunately, encoding flaws can be taken care of by the loss-tolerant protocol. Recently, a loss-tolerant MDI-QKD experiment has been performed, thus addressing both encoding flaws and detector flaws.

Nevertheless, I will argue that significant challenges remain in the security research of practical QKD systems. Those challenges include, for example, quantum random number generation, phase randomization, side channels and covert/subliminal channels. Recent progress on addressing those challenges will also be presented.

Verification in Quantum Cryptography

DOMINIQUE UNRUH *University of Tartu*

FRIDAY, 10:50 AM

In recent years, the computer-aided verification of cryptographic schemes has seen great progress. For example, various state-of-the-art cryptographic schemes were analyzed using the EasyCrypt tool using a probabilistic relational Hoare logic (pRHL). However, existing tools and logics are unsuited for analysis of quantum cryptographic protocols—be it protocols using quantum mechanics or protocols secure against quantum adversaries

In this talk, we explain why pRHL is not sound for quantum cryptography, and show how to lift the ideas from pRHL to the quantum setting.

MONDAY

Simple and Tight Device-Independent Security Proofs

ROTEM ARNON-FRIEDMAN, RENATO RENNER AND THOMAS VIDICK

MONDAY, 11:25 AM

Device-independent (DI) cryptography aims at achieving security that holds irrespective of the quality, or trustworthiness, of the physical devices used in the implementation of the protocol. Such a surprisingly high level of security is made possible due to the phenomena of quantum non-locality. The lack of any a priori characterization of the device used in a DI protocol makes proving security a challenging task. Indeed, proofs for, e.g., DI quantum key distribution (DIQKD) were only achieved recently and result in far from optimal key rates while being quite complex.

In this work we show that a newly developed tool, the "entropy accumulation theorem" of Dupuis et al., can be effectively applied to give fully general proofs of DI security that yield essentially tight parameters for a broad range of DI tasks. At a high level, our technique amounts to establishing a reduction to the scenario in which the untrusted device operates in an identical and independent way in each round of the protocol. This makes the proof much simpler and allows us to achieve significantly better quantitative results for the case of general quantum adversaries.

As concrete applications we give simple and modular security proofs for DIQKD and randomness expansion protocols based on the CHSH inequality. For both tasks we establish essentially optimal key rates and noise tolerance that are much higher than what was known before. Our results considerably decrease the gap between theory and experiments, thereby marking an important step towards practical DI protocols and their implementations.

Zero-Knowledge Proof Systems for QMA

ANNE BROADBENT, ZHENGFENG JI, FANG SONG AND JOHN WATROUS

MONDAY, 11:45 AM

Prior work has established that all problems in NP admit classical zero-knowledge proof systems, and under reasonable hardness assumptions for quantum computations, these proof systems can be made secure against quantum attacks. We prove a result representing a further quantum generalization of this fact, which is that every problem in the complexity class QMA has a quantum zero-knowledge proof system. More specifically, assuming the existence of an unconditionally binding and quantum computationally concealing commitment scheme, we prove that every problem in the complexity class QMA has a quantum interactive proof system that is zero-knowledge with respect to efficient quantum computations.

Our QMA proof system is sound against arbitrary quantum provers, but only requires an honest prover to perform polynomial-time quantum computations, provided that it holds a quantum witness for a given instance of the QMA problem under consideration. The proof system relies on a new variant of the QMA-complete local Hamiltonian problem in which the local terms are described by Clifford operations and standard basis measurements. We believe that the QMA-completeness of this problem may have other uses in quantum complexity.

A Modulator-Free QKD Transmitter

ZHILIANG YUAN, BERND FRÖHLICH, MARCO LUCAMARINI, GEORGE ROBERTS, JAMES DYNES AND ANDREW SHIELDS

MONDAY, 2:15 PM

Quantum key distribution (QKD) is a powerful method for guaranteeing the confidentiality of future communication networks. It has progressed from laboratories to real-world implementations and is gradually being integrated into existing optical networks.

However, its commercial success still requires significant innovations that will make the technology more robust and affordable. As a step toward this goal, we propose and demonstrate a novel light source that can generate pulses modulated in phase without the aid of an external phase modulator. This allows to considerably reduce the source driving voltage and to reliably control the phase randomization of the emitted pulses. By changing the electrical signals only, a diverse range of QKD protocols can easily be accommodated. This development makes QKD devices substantially more compact, versatile and energy-efficient—features that are essential for widespread adoption.

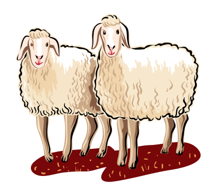
77-Day Field Trial of High Speed Quantum Key Distribution with Implementation Security

ALEXANDER DIXON, JAMES DYNES, MARCO LUCAMARINI, BERND FRÖHLICH, ANDREW SHARPE, ALAN PLEWS, SIMON TAM, ZHILIANG YUAN, YOSHIMICHI TANIZAWA, HIDEAKI SATO, SHINICHI KAWAMURA, MIKIO FUJIWARA, MASAHIDE SASAKI AND ANDREW SHIELDS

MONDAY, 2:35 PM

Quantum key distribution's central and unique claim is information theoretic security. However, there is an increasing awareness that the security of real QKD systems rely not only on theoretical security proofs, but also on how closely the system matches the theoretical models and resists known attacks. These hacking or side channel attacks exploit physical devices which do not necessarily behave precisely as the theory expects. As a result, there is a need to demonstrate QKD systems providing both theoretical and implementation based security.

We report here a QKD system which has been designed to provide these features of resistance to real security issues, component monitoring and failure detection—important not only from a security point of view, but also for reliable and robust operation. Alongside the increased security confidence level, the system operates with a high and stable secure key rate due to newly developed active stabilization, averaging 210 kbps and producing 1.33 Tbits of secure key data over 77 days in a telecom network.



Towards Secure QKD with Testable Assumptions on Modulation Devices

AKIHIRO MIZUTANI, YUICHI NAGAMATSU, MARCOS CURTY, HOI-KWONG LO, KOJI AZUMA, RIKIZO IKUTA, TAKASHI YAMAMOTO, NOBUYUKI IMOTO AND KIYOSHI TAMAKI

MONDAY, 2:55 PM

In order to realize secure communication in practice, one serious problem is to establish practical security proofs to bridge the gap between theory and practice.

Currently, source devices become the only region exploitable by a potential eavesdropper (Eve). Therefore, it is urgently required to establish security proofs based on practical source devices for realizing secure communication in practice.

In this work, we have accommodated two dominant imperfections in the source devices, i.e., phase modulation and intensity fluctuation errors. For both imperfections, we made potentially experimentally testable assumptions, and proved the security against coherent attacks in the finite-key regime.

As a result of our security proof, even under a realistic phase modulation and intensity fluctuation errors, we show that long distance secure communication is possible with reasonable times of signal transmission. Our result constitutes a significant step toward realizing secure quantum communication with practical devices.

Observation of Quantum Fingerprinting Beating the Classical Limit

JIANYU GUAN, FEIHU XU, HUALEI YIN, WEI-JUN ZHANG, SI-JING CHEN, XIAO-YAN YANG, LI LI, LI-XING YOU, TENG-YUN CHEN, ZHEN WANG, QIANG ZHANG AND JIANWEI PAN

MONDAY, 4:20 PM

Quantum communication promises the remarkable advantage of an exponential reduction in the transmitted information over classical communication to accomplish distributed computational tasks. However, to date, demonstrating this advantage in a practical setting continues to be a central challenge.

Here, we report an experimental demonstration of a quantum fingerprinting protocol that for the first time surpasses the ultimate classical limit to transmitted information. Ultra-low noise superconducting single-photon detectors and a stable fiber-based Sagnac interferometer are used to implement a quantum fingerprinting system that is capable of transmitting less information than the classical proven lower bound over 20 km. standard telecom fiber for input sizes of up to two Gbits. The results pave the way for experimentally exploring the advanced features of quantum communication and open a new window of opportunity for research in communication complexity.

CONTRIBUTED TALKS (continued)

24-Hour Long Relativistic Bit Commitment

EPHANIELLE VERBANIS, RAPHAËL HOULMANN, GIANLUCA BOSO, FELIX BUSSIÈRES, ANTHONY MARTIN AND HUGO ZBINDEN

MONDAY, 4:40 PM

We report on the first implementation of a relativistic bit commitment protocol sustained for 24 hours using high-speed optical communication and FPGA-based processing between standard computers. Our commitment time is more than six orders of magnitude longer than what was previously achieved, and we show that it could be extended even further.

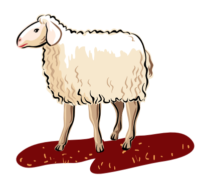
Quantum Teleportation Over Deployed Fibres and Applications to Quantum Networks

VENKATA RAMANA RAJU VALIVARTHI, MARCEL-LI GRIMAU PUIGIBERT, QIANG ZHOU, GABRIEL H. AGUILAR, VARUN VERMA, FRANCESCO MARSILI, SAE WOO NAM, DANIEL OBLAK AND WOLFGANG TITTEL

MONDAY, 5 PM

If a photon interacts with a member of an entangled photon pair via a so-called Bell-state measurement (BSM), its state is teleported over arbitrary distances (in principle) onto the second member of the pair. Starting in 1997, this puzzling prediction of quantum mechanics has been demonstrated many times. However, with just one very recent exception, only the photon that received the teleported state—if any—traveled far, while the photons partaking in the BSM were always measured close to where they were created.

Here, using the Calgary Fibre Network, we report quantum teleportation from a telecommunication-wavelength photon, interacting with another telecommunication photon after both have traveled over several kilometers in beeline, onto a photon at 795 nm. wavelength. This improves the distance over which teleportation takes place from 818 m. to 6.2 km. Our demonstration establishes an important requirement for quantum repeater-based communications and constitutes a milestone on the path to a global quantum Internet.



TUESDAY

Quantum Homomorphic Encryption for Polynomial-sized Circuits

YFKE DULEK, CHRISTIAN SCHAFFNER AND FLORIAN SPEELMAN

TUESDAY, 10 AM

We present a new scheme for quantum homomorphic encryption that is compact and allows for efficient evaluation of arbitrary polynomial-sized quantum circuits. Building on the framework of Broadbent and Jeffery [BJ15] and recent results in the area of instantaneous non-local quantum computation [Spe15], we show how to construct quantum gadgets that allow perfect correction of the errors that occur during the homomorphic evaluation of T gates on encrypted quantum data. Our scheme can be based on any classical (leveled) fully homomorphic encryption (FHE) scheme and requires no computational assumptions besides those already used by the classical scheme.

The size of our quantum gadget depends on the space complexity of the classical decryption function, which aligns well with the current efforts to minimize the complexity of the decryption function.

Our scheme (or slight variants of it) offers a number of additional advantages such as ideal compactness, the ability to supply gadgets "on demand," circuit privacy for the evaluator against passive adversaries, and a three-round scheme for blind delegated quantum computation, which puts only very limited demands on the quantum abilities of the client.

Rate-Distance Tradeoff and Resource Costs for All-Optical Quantum Repeaters

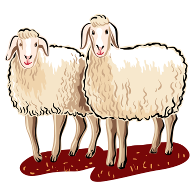
MIHIR PANT, HARI KROVI, DIRK ENGLUND AND SAIKAT GUHA

TUESDAY, 11:25 AM

We present a resource-performance tradeoff of an all-optical quantum repeater that uses photon sources, linear optics, photon detectors and classical feed forward at each repeater node, but no quantum memories.

We show that the quantum-secure key rate has the form R(t) = Dt^s bits per mode, where t is the end-to-end channel's transmissivity, and the constants D and s are functions of various device inefficiencies and the resource constraint, such as the number of available photon sources at each repeater node. Even with lossy devices, we show that s < 1 is possible to attain, and in turn to outperform the maximum key rate attainable without quantum repeaters, R_direct(t) = -log_2(1-t) bits per mode for t<<1, beyond a certain total range L, where t~e^{-aL} in optical fiber.

We also propose a suite of modifications to a recently-proposed all-optical repeater protocol that ours builds upon, which lower the number of photon sources required to create photonic clusters at the repeaters so as to outperform R_direct(t), from ~10^11 to ~10^6 photon sources per repeater node. We show that the optimum separation between repeater nodes is independent of the total range L, and is around 1.5 km. for assumptions we make on various device losses. Our results shed light on the tradeoff between resource requirements and the end-to-end key rate achieved using any specific repeater architecture.



CONTRIBUTED TALKS (continued)

Continuous Variable Quantum Computing on Encrypted Data

KEVIN MARSHALL, CHRISTIAN S. JACOBSEN, CLEMENS SCHAFERMEIER, TOBIAS GEHRING, CHRISTIAN WEEDBROOK AND ULRIK L. ANDERSEN

TUESDAY, 11:45 AM

In today's era of cloud and distributed computing, protecting a client's privacy is a task of the highest priority. Performing computations in the cloud on encrypted data rather than on plain text is a promising tool to achieve this goal.

Here, we report about a continuous variable protocol for performing computation on encrypted data on a quantum computer. We theoretically investigate the protocol and present a proof-of-principle experiment implementing displacements and squeezing gates. We demonstrate losses of up to 10 km. both ways between the client and the server and show that security can still be achieved.

Our approach offers a number of practical benefits, which can ultimately allow for the potential widespread adoption of this quantum technology in future cloud-based computing networks.

New Security Notions and Feasibility Results for Authentication of Quantum Data

SUMEGHA GARG, HENRY YUEN AND MARK ZHANDRY

TUESDAY, 2:25 PM

We give a new class of security definitions for authentication in the quantum setting. Our definitions capture and strengthen several existing definitions, including superposition attacks on \emph{classical} authentication, as well as full authentication of quantum data. We argue that our definitions resolve some of the shortcomings of existing definitions.

We then give several feasibility results for our strong definitions. As a consequence, we obtain several interesting results, including: the classical Carter-Wegman authentication scheme with 3-universal hashing is secure against superposition attacks, as well as adversaries with quantum side information; quantum authentication where the entire key can be reused if verification is successful; conceptually simple constructions of quantum authentication; and a conceptually simple QKD protocol.

Continuous-Variable Quantum Key Distribution with a "Locally" Generated Local Oscillator

BING QI, PAVEL LOUGOVSKI, RAPHAEL POOSER, WARREN GRICE, MILJKO BOBREK, CHARLES CI WEN LIM AND PHILIP G. EVANS

TUESDAY, 2:45 PM

Continuous-variable quantum key distribution (CV-QKD) protocols based on coherent detection have been studied extensively in both theory and experiment. While the existing security proofs of CV-QKD are based on the assumption that the local oscillator (LO) for coherent detection is trustable, this assumption cannot be justified in most practical implementations of CV-QKD, where both the quantum signal and the LO are generated from the same laser at the sender's side and propagate through an insecure quantum channel.

To close the above gap between theory and experiment, we proposed an intradyne CV-QKD scheme where the LO is generated from an independent laser source at the receiver's end (Phys. Rev. X 5, 041009, 2015). This scheme not only removes the security issues related to an untrusted LO, but also greatly simplifies QKD implementation. We demonstrate the above scheme in a coherent communication system constructed by a spool of 25 km. single mode fiber and two independent commercial laser sources operated at free-running mode. The observed phase-noise variance is 0.04 (rad^2), which is small enough to enable secure key distribution. This technology also opens the door for other quantum communication protocols, such as measurement-device-independent (MDI) CV-QKD

Here, using the Calgary Fibre Network, we report quantum teleportation from a telecommunication-wavelength photon, interacting with another telecommunication photon after both have traveled over several kilometers in beeline, onto a photon at 795 nm. wavelength. This improves the distance over which teleportation takes place from 818 m. to 6.2 km. Our demonstration establishes an important requirement for quantum repeater-based communications and constitutes a milestone on the path to a global quantum Internet.

Note: This talk is combined with the following talk.

Theoretical Analysis and Proof-of-Principle Demonstration of Self-Referenced Continuous-Variable Quantum Key Distribution

CONSTANTIN BRIF, DANIEL SOH, PATRICK COLES, NORBERT LUTKENHAUS, RYAN CAMACHO, JUNJI URAYAMA AND MOHAN SAROVAR

This work presents the theoretical analysis and proof-of-principle demonstration of a new continuous-variable quantum key distribution (CV-QKD) protocol, self-referenced CV-QKD. This protocol eliminates the need for transmission of a high-power local oscillator between the communicating parties. Instead, each signal pulse is accompanied by a reference pulse (or a pair of twin reference pulses), used to align Alice's and Bob's measurement bases.

We quantify the expected secret key rates by expressing them in terms of experimental parameters and present a proof-of-principle, fiber-based experimental demonstration of the protocol. Our analysis of the secret key rate fully takes into account the inherent uncertainty associated with the quantum nature of the reference pulse(s) and quantifies the limit at which the theoretical key rate approaches that of the respective conventional protocol that requires local oscillator transmission. The self-referenced protocol greatly simplifies the hardware required for CV-QKD, especially for potential integrated photonics implementations of transmitters and receivers, with minimum sacrifice of performance. As such, it provides a pathway towards scalable integrated CV-QKD transceivers, a vital step toward large-scale QKD networks.

WEDNESDAY

Quantum-Limited Measurements of Signals from a Satellite in Geostationary Earth Orbit

DOMINIQUE ELSER, KEVIN GÜNTHNER, IMRAN KHAN, BIRGIT STILLER, ÖMER BAYRAKTAR, CHRISTIAN R. MÜLLER, KAREN SAUCKE, DANIEL TRÖNDLE, FRANK HEINE, STEFAN SEEL, PETER GREULICH, HERWIG ZECH, BJÖRN GÜTLICH, INES RICHTER, ROLF MEYER, CHRISTOPH MARQUARDT AND GERD LEUCHS

WEDNESDAY, 11:25 AM

Quantum communication has been implemented in metropolitan area networks around the world. Optical satellite communication lends itself to interconnect such metropolitan networks over global distances. For this purpose, existing Laser Communication Terminals (LCTs) can be upgraded to quantum key distribution (QKD) application. We have performed first satellite measurement campaigns to validate this approach.

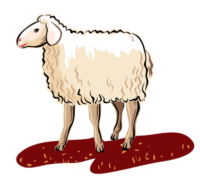
Time-Bin Encoding Along Satellite-Ground Channels

GIUSEPPE VALLONE, DANIELE DEQUAL, MARCO TOMASIN, FRANCESCO VEDOVATO, MATTEO SCHIAVON, VINCENZA LUCERI, GIUSEPPE BIANCO AND PAOLO VILLORESI

WEDNESDAY, 11:45 AM

Time-bin encoding is an extensively used technique to encode a qubit in quantum key distribution (QKD) along optical fibers. Despite its success in fibers QKD (in particular in the "plug-and-play" systems), time-bin encoding was never implemented in long-distance free-space QKD.

Here we demonstrate that time-bin interference at the single photon level can be observed along free-space channels and in particular along satellite-ground channels. To this purpose, we used a scheme similar to the "plug-and-play" systems: a coherent superposition between two wavepackets is generated on ground, sent on space and reflected by a rapidly moving satellite at a very large distance with a total path length up to 5000 km. The beam returning on ground is at the single photon level and we measured the interference between the two time-bins. We will demonstrate that the varying relative velocity of the satellite with respect to the ground introduces a modulation in the interference pattern that can be predicted by special relativistic calculations. Our results attest the viability of time-bin encoding for quantum communications in space.



THURSDAY

Quantum-Proof Multi-Source Randomness Extractors in the Markov Model

ROTEM ARNON-FRIEDMAN, CHRISTOPHER PORTMANN AND VOLKHER SCHOLZ

THURSDAY, 2:15 PM

Randomness extractors, widely used in classical and quantum cryptography as well as in device independent randomness amplification and expansion, are functions which generate almost uniform randomness from weak sources of randomness.

In the quantum setting, one must take into account the quantum side information held by an adversary, which might be used to break the security of the extractor. In the case of seeded extractors, the presence of quantum side information has been extensively studied. For multi-source extractors, one can easily see that high conditional min-entropy is not sufficient to guarantee security against arbitrary side information, even in the classical case. Hence, the interesting question is under which models of side information multi-source extractors remain secure.

In this work we suggest a natural model of side information, which we call the Markov model, and prove that any multi-source extractor remains secure in the presence of quantum side information of this type (albeit with weaker parameters). This improves on previous results in which more restricted models were considered and the security of only some types of extractors were shown.

On Quantum Obfuscation

GORJAN ALAGIC AND BILL FEFFERMAN

THURSDAY, 2:35 PM

Encryption of data is fundamental to secure communication. Beyond encryption of data lies obfuscation, i.e., encryption of functionality. It has been known for some time that the most powerful classical obfuscation, so-called "black-box obfuscation," is impossible. In this work, we initialize the rigorous study of obfuscating programs via quantum-mechanical means. We prove quantum analogues of several foundational results in obfuscation, including the aforementioned black-box impossibility result.

In its most powerful "quantum black-box" instantiation, a quantum obfuscator would turn a description of a quantum program f into a quantum state R_f , such that anyone in possession of R_f can repeatedly evaluate f on inputs of their choice, but never learn anything else about the original program. We formalize this notion of obfuscation, and prove an impossibility result: such obfuscation is only possible in a setting where the adversary never has access to more than one obfuscation (of either the same program, or of different programs). Our proof involves a novel and recently developed technical idea: chosen-ciphertext-secure encryption for quantum states. In addition, we show that some applications of obfuscation still appear possible in spite of our impossibility result. These include encryption for quantum states, quantum fully-homomorphic encryption, and quantum money.

We also define quantum versions of indistinguishability obfuscation and best-possible obfuscation. We then show that these notions are equivalent, and that their perfect and statistical variants are impossible to achieve. The remaining (i.e., computational) variant would still have an application of interest: witness encryption for QMA.

Breaking Symmetric Cryptosystems Using Quantum Period Finding

MARC KAPLAN, GAËTAN LEURENT, ANTHONY LEVERRIER AND MARÍA NAYA-PLASENCIA

THURSDAY, 2:55 PM

Due to Shor's algorithm, quantum computers are a severe threat for public key cryptography. This motivated the cryptographic community to search for quantum-safe solutions. On the other hand, the impact of quantum computing on secret key cryptography is much less understood.

In this paper, we consider attacks in the quantum chosen plaintext model, in which an adversary can query an oracle implementing a cryptographic primitive in a quantum superposition of different states. The adversary is then very powerful, but recent results show that it is nonetheless possible to design secure cryptosystems.

We introduce new applications of a quantum procedure called Simon's algorithm (the simplest quantum period finding algorithm) in order to attack symmetric cryptosystems in this model. Following previous works in this direction, we show that several classical attacks based on finding collisions can be dramatically sped up using Simon's algorithm: finding a collision requires $\Omega(2n/2)$ queries in the classical setting, but when collisions happen with some hidden periodicity, they can be found with only $O(n)$ queries in the quantum model.

We obtain attacks with very strong implications. First, we show that the most widely used modes of operation for authentication and authenticated encryption (e.g. CBC-MAC, PMAC, GMAC, GCM and OCB) are completely broken in this security model. Our attacks are also applicable to many CAESAR candidates: CLOC, AEZ, COPA, OTR, POET, OMD and Minalpher.

Second, we show that slide attacks can also be sped up using Simon's algorithm. This is the first exponential speed up of a classical symmetric cryptanalysis technique in the quantum model.

FRIDAY

Adaptive Versus Non-Adaptive Strategies in the Quantum Setting

FRÉDÉRIC DUPUIS, SERGE FEHR, PHILIPPE LAMONTAGNE AND LOUIS SALVAIL

FRIDAY, 11:25 AM

We prove a general relation between adaptive and non-adaptive strategies in the quantum setting, i.e., between strategies where the adversary can or cannot adaptively base its action on some auxiliary quantum side information. Our relation holds in a very general setting, and is applicable as long as we can control the bit-size of the side information, or, more generally, its “information content.”

Since adaptivity is notoriously difficult to handle in the analysis of (quantum) cryptographic protocols, this gives us a very powerful tool: as long as we have enough control over the side information, it is sufficient to restrict ourselves to non-adaptive attacks.

We demonstrate the usefulness of this methodology with two examples. The first is a quantum bit commitment scheme based on 1-bit cut-and-choose. Since bit commitment implies oblivious transfer (in the quantum setting) and oblivious transfer is universal for two-party computation, this implies the universality of 1-bit cut-and-choose, and, thus, solves the main open problem of [10]. The second example is a quantum bit commitment scheme proposed in 1993 by Brassard et al.

It was originally suggested as an unconditionally secure scheme, back when this was thought to be possible. We partly restore the scheme by proving it secure in (a variant of) the bounded quantum storage model.

In both examples, the fact that the adversary holds quantum side information obstructs a direct analysis of the scheme, and we circumvent it by analyzing a non-adaptive version, which can be done by means of known techniques, and applying our main result.

Computational Security of Quantum Encryption

GORJAN ALAGIC, ANNE BROADBENT, BILL FEFFERMAN, TOMMASO GAGLIARDONI, MICHAEL ST. JULES AND CHRISTIAN SCHAFFNER

FRIDAY, 11:45 AM

Quantum-mechanical devices have the potential to transform cryptography. Most research in this area has focused either on the information-theoretic advantages of quantum protocols or on the security of classical cryptographic schemes against quantum attacks. In this work, we initiate the study of another relevant topic: the encryption of quantum data in the computational setting.

In this direction, we establish quantum versions of several fundamental classical results. First, we develop natural definitions for private-key and public-key encryption schemes for quantum data. We then define notions of semantic security and indistinguishability and, in analogy with the classical work of Goldwasser and Micali, show that these notions are equivalent. Finally, we construct secure quantum encryption schemes from basic primitives. In particular, we show that quantum-secure one-way functions imply IND-CCA1-secure symmetric-key quantum encryption, and that quantum-secure trapdoor one-way permutations imply semantically-secure public-key quantum encryption.

CONTRIBUTED TALKS (continued)

Cross-Phase Modulation of a Probe Stored in a Waveguide for Non-Destructive Detection of Photonic Qubits

CHETAN DESHMUKH, NEIL SINCLAIR, KHABAT HESHAMI, DANIEL OBLAK, CHRISTOPH SIMON AND WOLFGANG TITTEL

FRIDAY, 1:40 PM

Non-destructive detection of photonic qubits is an enabling technology for quantum information processing and quantum communication. For practical applications such as quantum repeaters and networks, it is desirable to implement such detection in a way that allows some form of multiplexing as well as easy integration with other components such as solid-state quantum memories.

Here we propose an approach to non-destructive photonic qubit detection that promises to have all the mentioned features. Mediated by an impurity-doped crystal, a signal photon in an arbitrary time-bin qubit state modulates the phase of an intense probe pulse that is stored during the interaction. A proof-of-principle experiment with macroscopic signal pulses has been able to demonstrate the expected cross-phase modulation as well as the ability to preserve the coherence between temporal modes. Our findings open the path to a new key component of quantum photonics based on rare-earth-ion doped crystals.

Information Theoretically Secure Distributed Storage System with Quantum Key Distribution Network and Password Authenticated Secret Sharing Scheme

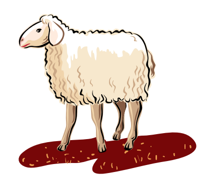
MIKIO FUJIWARA, ATSUSHI WASEDA, RYO NOJIMA, SHIHO MORIAI, WAKAHA OGATA AND MASAHIDE SASAKIL

FRIDAY, 2:05 PM

A quantum key distribution (QKD) allows two users to share random numbers with the unconditional security based on the fundamental laws of physics. By combining a QKD with one-time pad encryption (OTP), communication with unconditional security can be realized.

A QKD system, however, does not guarantee the security of stored data. Shamir’s (k, n)-threshold secret sharing (SS) scheme in which the data are split into n pieces (shares) for storage and at least k pieces of them must be gathered for reconstruction, provides information theoretical security. Therefore, a combination of a QKD system and SS scheme is a combination for secure data transmission and storage. However, assumed is authentication must be perfectly secure, which is not trivial in practice.

Here we propose a totally information theoretically secure distributed storage system based on a user-friendly single-password-authenticated secret sharing scheme and secure transmission using quantum key distribution, and demonstrate it in the Tokyo metropolitan area (≤90 km).



Integrated Silicon Photonics for Quantum Key Distribution

PHILIP SIBSON, JAKE KENNARD, STASJA STANISIC, CHRIS ERVEN AND MARK THOMPSON

FRIDAY, 2:30 PM

Integrated photonics provides a compact and robust platform to implement complex photonic circuitry, and with silicon, in particular, offers extreme levels of miniaturization in a CMOS-compatible technology.

Here we demonstrate integrated silicon photonic devices for polarization and time-bin encoded quantum key distribution protocols. These GHz clocked devices use a combination of slow but ideal thermo-optic phase shifters and fast but non-ideal carrier-depletion phase modulators to transmit BB84 states. This work experimentally demonstrates the feasibility of QKD transmitters for high-speed QKD based on CMOS-compatible silicon photonic integrated circuits.

Note: This talk is combined with the following talk.

Wavelength-Division-Multiplexed QKD with Integrated Photonics

PHILIP SIBSON, CHRIS ERVEN AND MARK THOMPSON

This work experimentally demonstrates Wavelength-Division-Multiplexed QKD with integrated photonics for high-rate QKD. We use two GHz rate indium phosphide transmitters and a silicon oxynitride receiver with integrated wavelength de-multiplexing and two reconfigurable receivers for multi-protocol QKD. The increase in rates and the ability to scale up these circuits opens the way to new and advanced integrated quantum communication technologies and larger adoption of quantum-secured communications.

Laser Damage Creates Backdoors in Quantum Cryptography

SHIHAN SAJEED, SARAH KAISER, POOMPONG CHAIWONGKHOT, MATHIEU GAGNE, JEAN-PHILIPPE BOURGOIN, CARTER MINSHULL, MATTHIEU LEGRE, THOMAS JENNEWEIN, RAMAN KASHYAP AND VADIM MAKAROV

FRIDAY, 2:55 PM

Implementations of quantum communication (QC) protocols are assumed to be secure as long as implemented devices are perfectly characterized and all side channels are identified and closed. We show that this assumption is not always true.

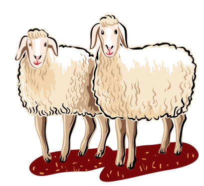
We introduce a laser-damage attack that can, on-demand, create deviations in the behavior of the implemented devices from the characterized one. We test it on two different and perfectly characterized implementations of quantum key distribution and coin-tossing protocols and successfully create deviations to render the system insecure. Our results show that in order to provide unconditional security, quantum cryptography protocols need to be supported by additional testing and countermeasures against laser damage.

Note: This talk is combined with the following talk.

Insecurity of Detector-Device-Independent Quantum Key Distribution

ANQI HUANG, SHIHAN SAJEED, SHIHAI SUN, FEIHU XU, VADIM MAKAROV AND MARCOS CURTY

It is time to close the gap between theory and practice in quantum key distribution (QKD). To bridge this gap, detector-device-independent QKD (ddiQKD) has recently been proposed. However, from our analysis, this protocol is not as secure as expected. The main contributions of this work are two-fold. First, we show that, in contrast to mdiQKD, the security of ddiQKD cannot be based on post-selected entanglement alone as assumed. Second, we argue that ddiQKD is actually insecure under detector side-channel attacks.



POSTER SESSIONS

TUESDAY AND THURSDAY • 3:45–6 PM

Quantum-Aware Software Defined Networks

ALEJANDRO AGUADO, VICENTE MARTIN, DIEGO LOPEZ, MOMTCHIL PEEV, JESUS MARTINEZ-MATEO, JOSE LUIS ROSALES, FERNANDO DE LA IGLESIA, MIGUEL GOMEZ, EMILIO HUGUES-SALAS, ANDREW LORD, REZA NEJABATI AND DIMITRA SIMEONIDOU

TUESDAY

A General Framework for Quantum Secret Sharing Protocols with Ditter Measurements

ZOÉ AMBLARD AND FRANCOIS ARNAULT

TUESDAY

Imperfect Oblivious Transfer

RYAN AMIRI, PETROS WALLDEN AND ERIKA ANDERSSON

THURSDAY

Estimating the Cost of Generic Quantum Pre-Image Attacks on SHA-2 and SHA-3

MATTHEW AMY, OLIVIA DI MATTEO, VLAD GHEORGHIU, MICHELE MOSCA, ALEX PARENT AND JOHN SCHANCK

THURSDAY

Simple Implementation of Quantum Key Distribution Based on Single-Photon Bell-State Measurement”

XUEBI AN, WEN-YE LIANG, ZHEN-QIANG YIN, WEI CHEN, SHUANG WANG AND ZHENG-FU HAN

TUESDAY

Multi-user Quantum Key Distribution with Entangled Photons from a Semiconductor Chip”

CLAIRE AUTEBERT, JULIEN TRAPATEAU, ADELINE ORIEUX, ARISTIDE LEMAITRE, CARMEN GOMEZ-CARBONNEL, ELENI DIAMANTI, ISABELLE ZAQUINE AND SARA DUCCI

THURSDAY

Differential Phase-Time Quantum Key Distribution Protocol

DAVIDE BACCO, JESPER BJERGE CHRISTENSEN, MARIO A. USUGA CASTANEDA, YUNHONG DING, KARSTEN ROTTWITT AND LEIF KATSUO OXENLØWE

TUESDAY

Equiangular Quantum Key Distribution in More Than 2 Dimensions

RADHAKRISHNAN BALU, PAUL KOPROWSKI AND KASSO OKOUDJOU

THURSDAY

Quantum Key Distribution Using Multiple Gaussian Focused Beams

BOULAT BASH, NIVEDITA CHANDRASEKARAN, JEFFREY SHAPIRO AND SAIKAT GUHA

TUESDAY

Testing of the Time-Frequency QKD-Protocol Over Different Transmission Channels

FABIAN BEUTEL, JASPER RÖDIGER, NICOLAS PERLOT, OLIVER BENSON AND RONALD FREUND

TUESDAY

Detector-Device-Independent QKD: Security Analysis and Fast Implementation

ALBERTO BOARON, BORIS KORZH, RAPHAEL HOULMANN, GIANLUCA BOSO, CHARLES CI WEN LIM, ANTHONY MARTIN AND HUGO ZBINDEN

TUESDAY

Measurement-Device-Independent Randomness Generation with Arbitrary States

FELIX BISCHOF, HERMANN KAMPERMANN AND DAGMAR BRUSS

THURSDAY

Popescu-Rohrlich Correlations Imply Efficient Instantaneous Nonlocal Quantum Computation

ANNE BROADBENT

TUESDAY

Cavity Integrated Quantum Key Distribution

DARIUS BUNANDAR, NICHOLAS HARRIS, ZHESHEN ZHANG, CATHERINE LEE, RAN DING, TOM BAEHR-JONES, MICHAEL HOCHBERG, JEFFREY SHAPIRO, FRANCO WONG AND DIRK ENGLUND

TUESDAY

Metrology for Quantum-Secured Communications

VIACHESLAV BURENKOV, DAVID SZWER, PRAVIN PATEL, CHRISTOPHER CHUNNILALL AND ALASTAIR SINCLAIR

THURSDAY

Finite-Key-Size Effect in Commercial Plug-and-Play QKD System

POOMPONG CHAIWONGKHOT, SHIHAN SAJEED, LARS LYDERSEN AND VADIM MAKAROV

THURSDAY

Optimal Quantum Algorithm for Polynomial Interpolation

ANDREW CHILDS, WIM VAN DAM, SHIH-HAN HUNG AND IGOR SHPARLINSKI

TUESDAY

Highly Efficient Optical Quantum Memory with Long Coherence Time in Cold Atoms
YOUNG-WOOK CHO, G. T. CAMPBELL, J. L. EVERETT, J. BERNU, D. B. HIGGINBOTTOM, M. T. CAO, J. GENG, N. P. ROBINS, P. K. LAM AND B. C. BUCHLER

TUESDAY

Software for Numerical Calculation of Key Rates
PATRICK COLES, JIE LIN, ADAM WINICK, YANBAO ZHANG, ERIC METODIEV, SHOUZHEN GU, ELECTRA ELEFTHERIADOU, FILIPPO MIATTO AND NORBERT LUTKENHAUS

THURSDAY

Kilometer Transmission Range Quantum Digital Signatures
ROBERT COLLINS, ROSS DONALDSON, RYAN AMIRI, MIKIO FUJIWARA, TOSHIMORI HONJO, KAORU SHIMIZU, KIYOSHI TAMAKI, MASAHIRO TAKEOKA, PETROS WALLDEN, VEDRAN DUNJKO, MASAHIDE SASAKI, ERIKA ANDERSSON, JOHN JEFFERS AND GERALD BULLER

THURSDAY

Free-Space Quantum Signatures Using Heterodyne Measurements
CALLUM CROAL, MATTHEW THORNTON, CHRISTIAN PEUNTINGER, BETTINA HEIM, IMGRAN KHAN, CHRISTOPH MARQURDT, GERD LEUCHS, PETROS WALLDEN, ERIKA ANDERSSON AND NATALIA KOROLKOVA

THURSDAY

Quantum Secure Direct Communication Using Differential Quadrature Phase-shift Quantum Key Distribution
RANARA LOUISE DAMASCENO, ANTÔNIO GEOVAN GUERRA AND RUBENS VIANA

TUESDAY

Software-Defined Classical Metadata Control Channel for Quantum Network Applications
VENKAT DASARI, RONALD SADLIER, RYAN PROUT, BRIAN WILLIAMS AND TRAVIS HUMBLE

THURSDAY

Phase Stabilization of Deployed Telecom Fiber Links for Entanglement Distribution
P. BEN DIXON, MATT GREIN, CATHERINE LEE, RYAN MURPHY, MARK STEVENS, DIRK ENGLUND AND SCOTT HAMILTON

THURSDAY

Forgetting Boosts the Private Capacity
DAVID ELKOUSS AND SERGII STRELCHUK

TUESDAY

Distribution of Graph States via Quantum Routers with Network Coding
MICHAEL EPPING, HERMANN KAMPERMANN AND DAGMAR BRUSS

TUESDAY

Scheme for Practical Server-Client COW-QKD Based on Auto-Compensated Fiber Interferometer
IGNACIO HERNÁN LÓPEZ GRANDE AND MIGUEL ANTONIO LAROTONDA

THURSDAY

Efficient Characterization of Multi-Qubit States and their Application to Demonstrate Measurement Only Blind Quantum Computing
CHIARA GREGANTI, MARIE-CHRISTINE ROEHSNER, STEFANIE BARZ, TOMOYUKI MORIMAE, MORDECAI WAEGELL AND PHILIP WALTHER

THURSDAY

Differential Phase Shift QKD Protocol with Small Number of Random Delays
YUKI HATAKEYAMA, AKIHIRO MIZUTANI, NOBUYUKI IMOTO AND KIYOSHI TAMAKI

THURSDAY

Design of the Bhattacharyya Parameter of Polar Codes for Quantum Key Distribution
TIANJIAN HE, GAN WANG, ZHENGYU LI, YAXIONG LIU, TIAN LIU, XIANG PENG AND HONG GUO

THURSDAY

Free-Space Quantum Cryptography in a Turbulent Atmosphere
ALEXANDER HILL, BRADLEY CHRISTENSEN AND PAUL KWIAT

THURSDAY

Coexistence Scheme for Entanglement Based QKD in a Wavelength Multiplexed PON
FLORIAN HIPP, MICHAEL HENTSCHEL, SLAVISA ALEKSIC, ANDREAS POPPE AND HANNES HÜBEL

TUESDAY

Device-Independent Secret Key Rates for Quantum Repeater Setups
TIMO HOLZ, HERMANN KAMPERMANN AND DAGMAR BRUSS

TUESDAY

An Advanced Eve of QKD: Breaking a Security Assumption and Hacking a Black Box
ANQI HUANG, SHIHAN SAJEED, POOMPONG CHAIWONGKHOT, MATHILDE SOUCARROS, MATTHIEU LEGRE AND VADIM MAKAROV

TUESDAY

Field Implementation of Continuous-variable Quantum Key Distribution Network in Shanghai
DUAN HUANG, PENG HUANG, TAO WANG, HUASHENG LI, YINGMING ZHOU AND GUIHUA ZENG

TUESDAY

Single Quadrature Continuous Variable Quantum Key Distribution with a Local Local Oscillator
TIMUR ISKHAKOV, CHRISTIAN JACOBSEN, MIKKEL PEDERSEN, TOBIAS GEHRING AND ULRIK ANDERSEN

TUESDAY

High-Dimensional Quantum Key Distribution with Decoy States Using Discrete-Variable Time-Frequency States
NURUL ISLAM, CLINTON CAHALL, ANDRES ARAGONESES, CHARLES LIM, MICHAEL ALLMAN, VARUN VERMA, SAE WOO NAM, JUNGSANG KIM AND DANIEL GAUTHIER

TUESDAY

Key Rate Enhancement Using Qutrit States for Uncharacterized Quantum Key Distribution
YONGGI JO AND WONMIN SON

THURSDAY

Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics
JONATHAN JOGENFORS

THURSDAY

Robust Quantum Key Distribution Systems Using a Dual-Parallel Modulator
YU KADOSAWA, KENSUKE NAKATA, AKIHISA TOMITA, KAZUHISA OGAWA AND ATSUSHI OKAMOTO

THURSDAY

Encoding Secret Information in Measurement Settings
AMIR KALEV AND SYED ASSAD

THURSDAY

Quantum Password Authentication Against Man-in-the-Middle Attack
EVGUENI KARPOV

TUESDAY

Security of Differential Quadrature Phase Shift Quantum Key Distribution
SHUN KAWAKAMI, TOSHIHIKO SASAKI AND MASATO KOASHI

TUESDAY

Practical Long-Distance Quantum Key Distribution Using Concatenated Entanglement Swapping
AEYSHA KHALIQUE AND BARRY C. SANDERS

TUESDAY

Continuous-Variable Quantum Communication at 10 GHz and Compatible with Telecom Networks
IMRAN KHAN, BIRGIT STILLER, KEVIN JAKSCH, KEVIN GÜNTHNER, CHRISTIAN PEUNTINGER, JONAS GEYER-RAMSTECK, DOMINIQUE ELSER, CHRISTOPH PACHER, CHRISTOPH MARQUARDT AND GERD LEUCHS

THURSDAY

Security Improvements of B92 QKD Systems Using Multi-Qubit Scheme Against Unambiguous State Discrimination Attack
HEASIN KO, BYEONG-SEOK CHOI, JOONG-SEON CHOE AND CHUN-JU YOUN

TUESDAY

Experimental Realization of a Relativistic QKD System with One-Way Quantum Communication
KONSTANTIN KRAVTSOV, IGOR RADCHENKO, SERGEI KULIK AND SERGEI MOLOTKOV

TUESDAY

Mismatched Measurements and Quantum Key Distribution
WALTER KRAWEC

TUESDAY

Continuous Variable Quantum Key Distribution with Displaced Coherent State
RUPESH KUMAR, XINKE TANG, RAMEEZ ASIF, ADRIAN WONFOR, RICHARD PENTY, SEB SAVORY AND IAN WHITE

TUESDAY

QKD Authentication and Detector Hack Protection with Secret Basis Shift
YURY KUROCHKIN, ALEXEY FEDOROV, VASILY USTIMCHIK, ANTON LOSEV, ALAN KANAPIN, ALEXANDER SOKOLOV, ALEXANDER MILLER AND VLADIMIR KUROCHKIN

THURSDAY

CVsim: A Novel CV-QKD Simulation Tool
FABIAN LAUDENBACH, CHRISTOPH PACHER, CHI-HANG FRED FUNG, MOMTCHIL PEEV, ANDREAS POPPE AND HANNES HÜBEL

THURSDAY

Security of Continuous-Variable Quantum Key Distribution with Coarse-Grained Detector
ZHENGYU LI, YICHEN ZHANG, CHRISTIAN WEEDBROOK AND HONG GUO

TUESDAY

Measurement-Device-Independent Quantum Coin Tossing
ZHAO LIANGYUAN, YIN ZHENQIANG, WANG SHUANG, CHEN WEI, CHEN HUA, GUO GUANGCAN AND HAN ZHENGFU

TUESDAY

Laser Annealing Heals Radiation Damage in Single-photon Avalanche Photodiodes
JIN GYU LIM, ELENA ANISIMOVA, THOMAS JENNEWEIN AND VADIM MAKAROV

TUESDAY

Superadditivity of a Reverse Private Capacity in Quantum Channels
KYONGCHUN LIM, CHANGHO SUH AND JUNE-KOO KEVIN RHEE

TUESDAY

---

502 Gbits/s Quantum Random Number Generation with Simple and Compact Structure
JINLU LIU, JIE YANG, ZHENGYU LI, WEI HUANG AND BINGJIE XU

TUESDAY

Experimental Quantum Data Locking
YANG LIU, ZHU CAO, CHENG WU, DAIJI FUKUDA, LIXING YOU, JIAQIANG ZHONG, TAKAYUKI NUMATA, SIJING CHEN, WEIJUN ZHANG, SHENG-CAI SHI, CHAO-YANG LU, ZHEN WANG, XIONGFENG MA, JINGYUN FAN, QIANG ZHANG AND JIAN-WEI PAN

THURSDAY

QKD Information Leakage Due to Blackflashes in Single Photon Avalanche Photodiodes
COLIN LUALDI, DANIEL STACK AND STEPHEN PAPPAS

TUESDAY

Physical Components Modeling in Quantum Key Distribution Towards Security Analysis
XILONG MAO, YAN LI, YAN PENG AND BAOKANG ZHAO

THURSDAY

Source-Device-Independent Ultra-Fast Quantum Random Number Generation
DAVIDE MARANGON, GIUSEPPE VALLONE AND PAOLO VILLORESI

THURSDAY

Performance of Parallelization of the Open Source AIT QKD Software R10 for QKD Post Processing
OLIVER MAURHART, CHRISTOPH PACHER AND MANUEL WARUM

TUESDAY

In-line Quantum Repeaters
FILIPPO MIATTO AND NORBERT LUTKENHAUS

THURSDAY

Quantum Error-Correcting Codes for a Bosonic Mode
MARIOS H. MICHAEL, MATTI SILVERI, R. T. BRIERLEY, VICTOR V. ALBERT, JUHA SALMILEHTO, LIANG JIANG AND S. M. GIRVIN

THURSDAY

Randomness in Nonlocal Games Between Mistrustful Players
CARL MILLER AND YAOYUN SHI

TUESDAY

Quantum Steering and CHSH-Type Nonlocality of Quantum Vortex State Under Thermal Environment
DEVENDRA K. MISHRA, MANISH K. GUPTA, HWANG LEE AND JONATHAN P. DOWLING

TUESDAY

Visualization of Qutrit States
VINOD MISHRA

TUESDAY

Robustness of Round-Robin Differential-Phase-Shift Quantum-Key-Distribution Protocol Against Source Flaws
AKIHIRO MIZUTANI, NOBUYUKI IMOTO AND KIYOSHI TAMAKI

THURSDAY

Practical Implementation of MDI-QKD with Plug-and-Play Architecture
SUNG MOON, SANG-WOOK HAN AND YONG-SU KIM

TUESDAY

Security of the Bennett 1992 Quantum Key Distribution Protocol Estimating Eavesdropper's Information Without the Bit Error Rate
TOSHIYUKI NAKAMURA, KENSUKE NAKATA, AKIHISA TOMITA, KAZUHISA OGAWA AND ATSUSHI OKAMOTO

TUESDAY

Finite-key Analysis for Time-Energy High-Dimensional Quantum Key Distribution
MURPHY YUEZHEN NIU, FEIHU XU, FABIAN FURRER AND JEFFREY H. SHAPIRO

TUESDAY

Quantum Homomorphic Encryption from Quantum Codes
YINGKAI OUYANG, SI-HUI TAN AND JOSEPH FITZSIMONS

THURSDAY

On-Chip Detection and Modulation for Continuous-Variable Quantum Key Distribution
MAURO PERSECHINO, MELISSA ZIEBELL, PAUL CROZAT, ANDRÉ VILLING, DELPHINE MARRIS-MORINI, LAURENT VIVIEN, ELENI DIAMANTI AND PHILIPPE GRANGIER

THURSDAY

Toward Feasible Long-Distance Quantum Communications Systems
NICOLO LO PIPARO, MOHSEN RAZAVI AND WILLIAM MUNRO

THURSDAY

Towards the Deployment of Quantum Key Distribution Systems in a Software Defined Networking Environment
ALASDAIR PRICE, ALEJANDRO AGUADO, EMILIO HUGUES-SALAS, PAUL HAIGH, PHILIP SIBSON, JAUME MARHUENDA, JAKE KENNARD, JOHN RARITY, MARK THOMPSON, REZA NEJABATI,
DIMITRA SIMEONIDOU AND CHRIS ERVEN

THURSDAY

Measurement-Device-Independent Quantum Digital Signatures
ITTOOP PUTHOOR, RYAN AMIRI, PETROS WALLDEN, MARCOS CURTY AND ERIKA ANDERSSON

THURSDAY

Parameter Optimization in a Three-Party Measurement-Device-Independent Quantum Key Distribution System
YUCHENG QIAO, ZHENGYU LI, GAN WANG, XIANG PENG AND HONG GUO

THURSDAY

Studying the Effects of Atmospheric Propagation on QKD Using a Scintillation Playback System
WILLIAM RABINOVICH, RITA MAHON, MARK BASHKANSKY AND JOHN REINTJES

THURSDAY

Device-Independence for Two-Party Cryptography and Position Verification
JÉRÉMY RIBEIRO, PHUC THINH LE, JĐDRZEJ KANIEWSKI, JONAS HELSEN AND STEPHANIE WEHNER

TUESDAY

Proposing a Quantum Simulator for Integer Factorization
JOSE LUIS ROSALES AND VICENTE MARTIN-AYUSO

TUESDAY

Applicability of a Post-Quantum Signature in a QKD Public Channel
ROBERTO ROSCINO, KEVIN LAYAT, BRUNO HUTTNER, GRÈGOIRE RIBORDY AND DARIO CASELUNGHE

THURSDAY

Realistic Parameter Regimes for a Sequential Single-Node Quantum Repeater
FILIP ROZPĐDEK, KENNETH GOODENOUGH, JEREMY RIBEIRO, VALENTINA CAPRARA VIVOLI, ANDREAS REISERER, DAVID ELKOUSS AND STEPHANIE WEHNER

TUESDAY

Modeling and Studying Measurement Device-Independent Quantum Key Distribution Systems
MATTHEW RUSSELL, LOGAN MAILLOUX, MICHAEL GRIMAILA AND DOUGLAS HODSON

THURSDAY

Quantum Key Distribution Protocol with Slow Basis Change
TOSHIHIKO SASAKI, KIYOSHI TAMAKI AND MASATO KOASHI

THURSDAY

Experimental Realization of Equiangular Three State Quantum Key Distribution
MATTEO SCHIAVON, GIUSEPPE VALLONE AND PAOLO VILLORESI

TUESDAY

Shortcuts to Quantum Network Routing
EDDIE SCHOUTE, LAURA MANCINSKA, TANVIRUL ISLAM, IORDANIS KERENIDIS AND STEPHANIE WEHNER

THURSDAY

Pilot-Assisted Local Oscillator Synchronisation for CV-QKD
BERNHARD SCHRENK AND HANNES HÜBEL

THURSDAY

Integrated Photon Pair Source Based on SOI Micro-Ring Resonators
BERNHARD SCHRENK, FABIAN LAUDENBACH, PAUL MÜLLNER, DAIVID FOWLER, RAINER HAINBERGER AND HANNES HÜBEL

TUESDAY

Nonlocal Correlations of Entangled Two-Qudit States Using Energy-Time Entangled Photons
SACHA SCHWARZ, BÄNZ BESSIRE, ALBERTO MONTINA, STEFAN WOLF, YEONG-CHERNG LIANG AND ANDRÉ STEFANOV

TUESDAY

Measurement Uncertainty Relations for Finite Observables
RENÉ SCHWONNEK, DAVID REEB AND REINHARD F. WERNER

THURSDAY

Opportunistic Quantum Network Coding Based on Quantum Teleportation
TAO SHANG, GANG DU AND JIAN-WEI LIU

TUESDAY

Quantum Homomorphic Signature
TAO SHANG, XIAO-JIE ZHAO, CHAO WANG AND JIAN-WEI LIU

TUESDAY

A Novel Readout System for Free-running Negative Feedback Avalanche Diodes to Significantly Suppress Afterpulsing Effect
NIGAR SULTANA AND THOMAS JENNEWEIN

TUESDAY

An Overview of the Quantum Communication Project at NIST
XIAO TANG, OLIVER SLATTERY, LIJUN MA, PAULINA KUO, ALAN MINK AND BARRY HERSHMAN

TUESDAY

Practical Challenges in Classical Coherent Receivers for Detecting High Speed CV-QKD Signals
XINKE TANG, RAMEEZ ASIF, RUPESH KUMAR, ADRIAN WONFOR, SEB SAVORY, IAN WHITE AND RICHARD PENTY

TUESDAY

High-Speed Implementation of Privacy Amplification in Quantum Key Distribution
RIRIKA TAKAHASHI, YOSHIMICHI TANIZAWA AND ALEXANDER DIXON

TUESDAY

Practically Verifiable Blind Quantum Computation with Error Tolerance
YUKI TAKEUCHI, KEISUKE FUJII, TOMOYUKI MORIMAE AND NOBUYUKI IMOTO

THURSDAY

Weak Value Assisted Quantum Key Distribution
JAMES TROUPE AND JACOB FARINHOLT

THURSDAY

Collapse-Binding Commitments in the Standard Model
DOMINIQUE UNRUH

TUESDAY

Quantum Security of the Fiat-Shamir Transform
DOMINIQUE UNRUH

TUESDAY

Towards Macroscopic Quantum Key Distribution
VLADYSLAV USENKO, KIRILL SPASIBKO, LASZLO RUPPERT, MARIA CHEKHOVA, RADIM FILIP AND GERD LEUCHS

TUESDAY

Proof-of-Principle Study of Self-Coherent Continuous-Variable Quantum Key Distribution
LUIS TRIGO VIDARTE, ADRIEN MARIE, ROMAIN ALLÉAUME AND ELENI DIAMANTI

THURSDAY

Efficient Rate-Adaptive Reconciliation for Continuous-Variable Quantum Key Distribution
XIANGYU WANG, YICHEN ZHANG, ZHENGYU LI, BINGJIE XU, SONG YU AND HONG GUO

THURSDAY

Amplifying the Randomness of Weak Sources Correlated with Devices
HANNA WOJEWODKA, FERNANDO G.S.L. BRANDAO, ANDRZEJ GRUDKA, KAROL HORODECKI, MICHAL HORODECKI, PAWEL HORODECKI, MARCIN PAWLOWSKI AND RAVISHANKAR RAMANATHAN

TUESDAY

Experimental Fast Quantum Random Number Generation Using High-Dimensional Entanglement with Semi-Self-Testing
FEIHU XU, JEFFREY SHAPIRO AND FRANCO WONG

THURSDAY

Software Defined Quantum Key Distribution Network
ZHE YAN

THURSDAY

Secure Quantum Key Distribution Against Pattern Effects of Optical Pulse Intensities
KEN-ICHIRO YOSHINO, MIKIO FUJIWARA, KENSUKE NAKATA, AKIHISA TOMITA AND AKIO TAJIMA

TUESDAY

Composable Security Analysis for Continuous Variable Measurement-Device-Independent Quantum Key Distribution
YICHEN ZHANG, ZHENGYU LI, SONG YU AND HONG GUO

THURSDAY

Application of Virtual Photon Subtraction in Two-Way Continuous-Variable Quantum Cryptography
YIJIA ZHAO, YI-CHEN ZHANG, ZHENGYU LI, SONG YU AND HONG GUO

TUESDAY

NOTES

QCrypt CHARTER

(revised, February 25, 2016)

GOAL OF THE CONFERENCE

The annual conference on quantum cryptography (QCrypt) is a conference for students and researchers working on all aspects of quantum cryptography. This includes theoretical and experimental research on the possibilities and limitations of secure communication and computation with quantum devices, how security can be preserved in the presence of a quantum computer, and how to achieve long distance quantum communication. The conference includes, but is not limited to, research on quantum key distribution.

It is the goal of the conference to represent the previous year's best results on quantum cryptography, and to support the building of a research community.

FORMAT OF THE CONFERENCE

In order to achieve this goal, the conference features both invited and contributed talks, selected by the steering committee and program committee, respectively. In addition, the steering committee invites up to five focus tutorials, one preceding each day, with the goal to ease communication between the different subfields.

In addition, QCrypt features a poster session and an industry exhibit. To further connections to industry, QCrypt also includes an industry session consisting of a panel discussion or short presentation. To share latest advances, QCrypt includes a hot topic session, in which very recent (post-deadline) and high-quality research results are selected and presented. To inform the public, QCrypt typically includes a talk for the general public outside the normal conference program.

QCrypt also features a room that is open for working groups in quantum information. QCrypt is a community event, and participants are highly encouraged by contributing to the program by hosting their own organized sessions in the working group room. There are no restrictions on what this room may be used for, provided all QCrypt attendees can participate and reasonable time will be available to different working groups. Rooms can be booked at the QCrypt Wiki http://qcrypt.wikia.com, which also provides room for the organization of working groups.

In line with the goal of showcasing the best results each year from all subfields, the conference has no published proceedings. Yet, contributed talks are highly competitive. QCrypt welcomes the submission of any interesting and important result, while allowing researchers from a wide range of disciplines to pursue publication in any venue appropriate to their field. For authors who want to put their abstracts to public, and to cite their presentations in QCrypt later, the local organizing committee offers an opportunity to upload such abstracts in an electronic form in the conference web site. Oral presentations in QCrypt are recorded as videos. If presenters give permission, recorded videos as well as their presentation slides are uploaded to the conference web site.

STEERING COMMITTEE

The steering committee (SC) is responsible for shaping the medium- and long-term course of the conference series and for making sure that the conference maintains a high scientific and organisational standard. In particular, the SC has the responsibility to select the main organiser, venue and program chairs for the next conference. The SC has eight members who serve for four years with two members being replaced each year. The selection of new members is made by the SC during the previous year. The SC chair is selected among the SC members, and is responsible for the external relations of the conference.

To ease communication between the SC and the local organization, a member of the local organizing committee must take part in the SC for at least the year before and during the conference.

The conference usually takes place over one week (Monday to Friday) in August or September. The venue is decided by the steering committee who tries to ensure a suitable rotation of continents wherever possible. The SC will solicit applications to host the conference approximately two years in advance.
The SC selects the invited speakers. At most half of the talk time of the conference can be given to invited speakers. The remaining talk time is reserved for contributed talks. SC members cannot be invited speakers, but are allowed to submit and present contributed papers.

The SC reviews submissions to the hot topic session, and selects hot topic papers which present very recent and high-quality research results.

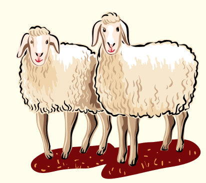
PROGRAM COMMITTEE

The role of the program committee (PC) is to select the contributed talks. The PC is chaired by one theorist and one experimentalist, of which one will be the primary chair and one the co-chair. The PC chairs are selected by the SC. With input from the SC, the PC chairs select and recruit the PC members of typically 10 or more people representing the broad range of subfields in quantum cryptography. SC members may not simultaneously serve on the PC. PC members are allowed to submit papers and to present contributed papers. PC members must declare a conflict of interest on submissions to which they contributed so that they are not involved in discussing these papers in the PC.

Talks are reviewed and selected based on scientific excellence. The two PC chairs make final a selection from the scientifically excellent talks to create a balanced and interesting program, encouraging broad participation and representation of topics in QCrypt.

ADVISORY COMMITTEE

The advisory committee (AC) advises the SC on the long-term direction of the conference series. The AC has at most 10 members covering a broad range of geographical locations and scientific expertise. The advisory committee is regularly informed by the SC about the progress of the conference organisation and gives input on future decisions, for instance on invited speakers and sponsorship contributed talks. AC members can be invited speakers, and are allowed to submit and present contributed papers



QCrypt CHARTER (continued)

STUDENT PAPER PRIZE

Since 2011, QCrypt features a prize for the best student submission. A submission is eligible for the student prize if and only if the main author(s) is/are a student(s) at the time of the submission and will present the work at QCrypt, and further a significant portion of the work (at least 60 percent) must have been done by said student(s), including the majority of the key ideas. Eligibility can only be indicated at the time of submission. The student(s) are responsible for notifying all authors that the paper was nominated for the student prize, and all authors have 14 days following submission to voice any disagreements about the paper's nomination to the PC chair. The PC chair is free to ask for any clarifications regarding the students' contributions at any time.

The PC will select up to three submissions for a shortlist for the best student paper prize. A final decision is made during QCrypt following a short interview of the student(s) by members of the PC. Being shortlisted for the best student award is a competitive distinction even if the student(s) are not chosen for the best student paper award.

The PC is free to make one best student award to theory and one to experiment in the same year, should students on the shortlist come from both areas.

PREVIOUS QCrypt CONFERENCES

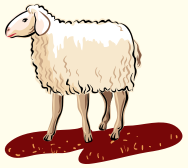
1st QCrypt CONFERENCE
SEPTEMBER 12 – 16, 2011
Zurich, Switzerland

2nd QCrypt CONFERENCE
SEPTEMBER 10 – 14, 2012
Singapore

3rd QCrypt CONFERENCE
AUGUST 5 – 9, 2013
Waterloo, Canada

4th QCrypt CONFERENCE
SEPTEMBER 1 – 5, 2014
Paris, France

5th QCrypt CONFERENCE
SEPTEMBER 28 – OCTOBER 2, 2015
Tokyo, Japan



QuICS would like to thank the following sponsors for their support of QCrypt:

THANKS

MICROSOFT RESEARCH

JOINT CENTER FOR
QUANTUM INFORMATION
AND COMPUTER SCIENCE

QCrypt 2016 is hosted by the Joint Center for Quantum Information and Computer Science (QuICS), a partnership between the University of Maryland and the National Institute of Standards and Technology (NIST).