Dear Conference Attendee,

Welcome to QCrypt 2018, the 8th International Conference on Quantum Cryptography. This is the first time that QCrypt is being held in China. We are glad to see you all here, and we hope you enjoy your time in our beautiful and modern city, Shanghai.

Quantum cryptography aims to achieve security from fundamental physical principles, such as the quantum no-cloning theorem and the Heisenberg’s uncertainty principle. In the last few years, significant progress has been made in the theoretical understanding of quantum cryptography, and its technological feasibility has been demonstrated experimentally. Quantum cryptography is regarded as one of the most promising candidates for a future quantum technology. The annual conference on quantum cryptography (QCrypt) is a conference for students and researchers working on all aspects of quantum cryptography. The main goals of the conference are to represent the previous year’s best results and to support the building of a research community in quantum cryptography.

Quantum communication is becoming an increasingly hot topic. For instance, the first quantum science satellite Micius was launched on 16th August 2016 by the Chinese Academy of Sciences (CAS), which has enabled quantum cryptography over a record-breaking distance of 1200 km. China has built the world’s longest quantum cryptography backbone fiber network, from Beijing to Shanghai, with 32 nodes in total over a distance exceeding 2000 km. Furthermore, several quantum initiatives have taken place around Europe, UK, USA and the world, aiming to create a coherent government, industry and academic quantum technology community to help develop and support the emerging new quantum technology markets.

This conference is the result of many people’s efforts. QCrypt 2018 is being hosted mainly by the CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China (USTC). This center was founded by Prof. Jian-Wei Pan, 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, and computer engineering. We want to thank the QCrypt steering committee, the QCrypt program committee, our fellow local organizers, 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!

Xiongfeng Ma, Feihu Xu, Jun Zhang and Qiang Zhang,
Local Organizing Committee, QCrypt 2018

Committees

Program committee

Antonio Acin (ICFO)
Virginia d'Auria (Institut de Physique de Nice (INPhYNI))
Kai-Min Chung (Academia Sinica)
Roger Colbeck (University of York) (Chair)
Eleni Diamanti (CNRS, Sorbonne Université)
Frederic Dupuis (CNRS, LORIA, Université de Lorraine)
Andrew Forbes (University of the Witwatersrand)
Mikio Fujiwara (National Institute of Information and Communications Technology)
Tobias Gehring (Technical University of Denmark)
Stacey Jeffery (CWI and QuSoft)
Thomas Jennewein (University of Waterloo)
Marc Kaplan (VeriQloud)
Iordanis Kerenidis (CNRS, Paris Centre for Quantum Computing)
Prem Kumar (Northwestern University)
Anthony Leverrier (Inria Paris)
Xiongfeng Ma (TsingHua University)
Serge Massar (Université libre de Bruxelles)
Christoph Marquardt (Max Planck Institute for the Science of Light) (Co-Chair)
Carl Miller (NIST / University of Maryland)
Christoph Pacher (Austrian Institute of Technology)
Christopher Portmann (ETH Zurich)
Or Sattath (Ben-Gurion University)
Florian Speelman (QMATH, University of Copenhagen)
Masahiro Takeoka (National Institute of Information and Communications Technology, Japan)
Harald Weinfurter (LMU Munch)
Feihu Xu (University of Science and Technology of China)

Steering committee

Anne Broadbent (University of Ottawa) (Co-Chair)
Marcos Curty (University of Vigo)
Akihisa Tomita (Hokkaido University)
Yi-Kai Liu (NIST / University of Maryland)
Norbert Lütkenhaus (IQC, University of Waterloo)
Christian Schaffner (University of Amsterdam, CWI, QuSoft)
Hugo Zbinden (U Geneva, Switzerland)
Qiang Zhang (University of Science and Technology of China) (Chair)

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)
Michele Mosca (IQC, University of Waterloo)
Jian-Wei Pan (University of Science and Technology of China)

Local organizing committee

Xiongfeng Ma (Tsinghua University)
Feihu Xu (University of Science and Technology of China)
Jun Zhang (University of Science and Technology of China)
Qiang Zhang (University of Science and Technology of China) (Local Chair)

CONFERENCE OVERVIEW

KEY

🟪 TUTORIAL
🟫 CONTRIBUTED TALK
🟦 INVITED TALK
🟩 SPECIAL EVENT
🟨 POSTER SESSION
⬜ BREAK

Monday, August 27	
8:45	Welcoming Remark
9:00	**Christoph Marquardt**, "Free space quantum communication"
10:20	Coffee Break
10:50	**Juan Yin**, "Entanglement-based QKD from Micius"
11:25	**Sebastian Philipp Neumann**, "Q^{3}Sat: Quantum communications uplink to a 3U CubeSat – feasibility & design"
11:45	**Jeongwan Jin**, "Genuine time-bin-based quantum key distribution over a turbulent depolarizing free-space channel"
12:05	Lunch
13:40	**Thomas Vidick**, "A cryptographic test of quantumness and certifiable randomness from a single quantum device"
14:15	**Philippe Lamontagne**, "Secure certification of mixed quantum states and application to two-party randomness generation"
14:35	**Siddhartha Das**, "Entanglement and secret-key-agreement capacities of bipartite quantum interactions and read-only memory devices"
14:55	**Christian Majenz**, "Quantum-secure message authentication via blind-unforgeability"
15:15	Coffee Break
15:45	**Yang Liu**, "Device-independent quantum random number generation"
16:05	**Lijiong Shen**, "Randomness extraction from CHSH violation without fair sampling assumptions with a continuous wave source"
16:25	**Tobias Gehring**, "Vacuum fluctuations quantum random number generator with non-iid samples" Merged with **Marco Avesani**, "Secure heterodyne-based quantum random number generator at 17 Gbps"
16:45-18:00	Poster Session (cold food and drinks are available)
Evening	Public Lecture by Andrew Yao

Tuesday, August 28	
9:00	**Renato Renner**, "Finite size effect in QKD"
10:20	Coffee Break
10:50	**Stephanie Wehner**, "Quantum software and quantum network"
11:25	**Yang-Fan Jiang**, "Entanglement swapping over 100 km optical fiber with independent entangled photon-pair sources"
11:45	**Ignatius William Primaatmaja**, "Characterising the behaviour of classical-quantum broadcast networks"
12:05	Group Photo &Lunch
14:00	Free Afternoon & Lab Tour
Evening	Volunteer Cruise Tour or Chinese Acrobat Performance

KEY

🟪 TUTORIAL
🟫 CONTRIBUTED TALK
🟦 INVITED TALK
🟩 SPECIAL EVENT
🟨 POSTER SESSION
⬜ BREAK

ALL CONFERENCE EVENTS

will be held at the Shanghai International Conference Center, Shanghai, China

PLEASE NOTE: All talks will take place in the International Hall at the Shanghai International Conference Center, 3rd Floor. Posters are in Yellow River Hall which is surrounding the International Hall.

THE CONFERENCE BANQUET

will be held in Pearl Hall at the Shanghai International Conference Center, 7th floor.

CONFERENCE OVERVIEW

KEY

🟪	TUTORIAL
🟫	CONTRIBUTED TALK
🟦	INVITED TALK
🟩	SPECIAL EVENT
🟨	POSTER SESSION
⬜	BREAK

	Wednesday, August 29
9:00	**Marco Lucamarini**, “Recent porgress in MDI-QKD”
10:20	Coffee Break
10:50	**Pei Zeng**, “Global phase encoding quantum key distribution”
11:10	**Wenyuan Wang**, “Enabling a scalable high-rate measurement-device-independent quantum key distribution network: theory and experiment”
11:30	**Rahul Jain**, “Parallel device-independent quantum key distribution”
11:50	**Alexander Poremba**, “On the power of non-adaptive quantum chosen-ciphertext attacks”
12:10	Lunch
13:40	**Yu-Ao Chen**, “Large scale quantum network in China”
14:15	**Alberto Boaron**, “2.5 GHz clocked quantum key distribution over 379 km”
14:35	**Soeren Wengerowsky**, “In-field entanglement distribution over a 96 km submarine optical fibre”
14:55	**Davide Bacco**, “High-dimensional fiber based quantum key distribution with twisted photons”
15:15	Coffee Break
15:45	**Anna Pappa**, “A comprehensive analysis of quantum E-voting protocols”
16:05	**Or Sattath**, “On the insecurity of quantum Bitcoin mining”
16:25	**Dong Yang**, “Distributed private randomness distillation”
16:45-18:00	Poster Session (only drinks)
Evening	Banquet and After dinner talk by Jian-Wei Pan

	Thursday, August 30
9:00	**Or Sattath**, “Quantum money”
10:20	Coffee Break
10:50	**Stacey Jeffery**, “Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources”
11:25	**Zhengfeng Ji**, “Pseudorandom quantum states”
11:45	**Christian Majenz**, “Unforgeable quantum encryption”
12:05	Lunch
13:40	Industrial Session
Evening	Business Meeting Prize Ceremony and Lightning Talks (cold food and drinks are available before the session)

	Friday, August 31
9:00	**Yu Chen**, “Quantum computation in Google”
9:35	**Léo Colisson**, “On the possibility of classical client blind quantum computing”
9:55	**Nai-Hui Chia**, “On basing one-way permutations on NP-hard problems under quantum reductions”
10:15	Coffee Break
10:50	**Andreas Huelsing**, “Post-quantum cryptography”
11:25	**Dominique Unruh**, “Quantum position-verification in the plane”
11:45	**Fabian Beutel**, “Ultrafast waveguide-integrated single-photon detectors for on-chip QKD detection”

KEY

🟪	TUTORIAL
🟫	CONTRIBUTED TALK
🟦	INVITED TALK
🟩	SPECIAL EVENT
🟨	POSTER SESSION
⬜	BREAK

The Advent of Quantum Computing

Andrew Chi-Chih Yao

Center for Advanced Study, Tsinghua University
Distinguished Professor-At-Large, The Chinese University of Hong Kong
Dean, Institute for Interdisciplinary Information Sciences, Tsinghua University

Monday, 18:00-19:30

In recent years, scientists have made much progress in the theory and implementation of quantum computing. Many even believe that the exciting prospect of building a real quantum computer will likely happen before long. Common curiosity drives one to ask: What advantages might quantum computers hold over traditional ones? What secrets within atoms could be unlocked to produce enormous new power for computing and information processing? In this talk, we will take an in-depth look into the above questions. We will also remark on the present and future of quantum computing.

Andrew Chi-Chih Yao is currently a Professor and the Dean of Institute for Interdisciplinary Information Sciences (IIIS) at Tsinghua University.

Yao used the minimax theorem to prove what is now known as Yao's Principle. He is a member of U.S. National Academy of Sciences, a fellow of the American Academy of Arts and Sciences, a fellow of the American Association for the Advancement of Science, a fellow of the Association for Computing Machinery, and an academician of Chinese Academy of Sciences. His wife, Frances Yao, is also a well-known theoretical computer scientist.
In 1996 he was awarded the Knuth Prize. He received the Turing Award, the most prestigious award in computer science, in 2000, "in recognition of his fundamental contributions to the theory of computation, including the complexity-based theory of pseudorandom number generation, cryptography, and communication complexity".

My past 30 years in quantum world

Jian-Wei Pan

Wednesday evening

Jian-Wei Pan is currently a Professor of Physics of the University of Science and Technology of China (USTC), an Academician of Chinese Academy of Sciences (CAS), and a Fellow of the World Academy of Sciences (TWAS). He serves as the Director of the CAS Centre for Excellence and Innovation in Quantum Information and Quantum Physics, and the Chief Scientist for projects of Micius Quantum Science Satellite and Beijing-to-Shanghai 2000-km Quantum Communication Backbone.

Pan’s work in the field of quantum information and quantum communication has been selected by Nature in “A celebration of Physics” (1999), as “Feature of the year” (2012), and “the science events that shaped the year” (2016, 2017), by Science as “Breakthrough of the year” (1998), by the American Physical Society as “The top physics stories of the year” (1997, 1999, 2004, 2006, 2013), by the Institute of Physics as “Breakthrough of the year” or “Highlights of the year” (1997, 2003, 2004, 2008, 2015, 2017), and by Scientific American as “2016 World Changing Ideas”. Pan has won Fresnel Prize, Quantum Communications Award, Future Prize in Physical Science, Willis E. Lamb Award, and was selected by Nature as “people of the year” in 2017 who “took quantum communication to space and back”.

INDUSTRY SESSION

Session	Time	Program and Speaker
QKD developer and user panel (13:40-15:15), 95 min. Moderator by N. Gisin (GAP-Optique)	13:40-13:50	10 minutes Introduction by N. Gisin (GAP-Optique)
	13:50-14:20	30 min. talks by 6 panelists Yong Zhao (Quantum CTek) Kelly Richdale (ID Quantique) Momtchil Peev (Huawei) Chongjing Xie (Ali Cloud) Ziyan Zhao (State Grid Corp. of China)
	14:20-15:15	Panel discussion
Coffee Break	15:15-15:45	
Quantum Computer Panel Moderator by Anne Broadbent (U of Otawa)	15:45-15:55	10 min. Introduction by Anne Broadbent (U of Otawa)
	15:55-16:10	15 min. talks by 3 panlists Ruanyao Duan (Baidu) Shengyu Zhang (Tencent) Xiaobo Zhu (USTC/CAS-Alibaba)
	16:10-16:40	30 min. Panel discussion
Post-Quantum Crypto and QKD Standardization Panel (16:40-17:40) :60 min Moderator by M. Sasaki (NICT)	16:40-16:50	10 min. Introduction by Masahide Sasaki (NICT)
	16:50-17:10	20 min. talk by 3 panelists 10min: Jintai Ding (U of Cincinnati) Wei Qi (Chair of QKD subgroup of CCSA China Communication Standard Association) Andrew Shields (Toshiba, Chair of ETSI ISG-QKD)
	17:10-17:40	30 min. Panel disucssion

GENERAL INFORMATION

Business Service

Photocopying and fax service are available at the Business Center, level 2 of Shanghai International Conference Center SHICC Oriental Riverside Hotel, Charges will apply.

Electricity

The electricity in China is generally 220V, 50HZ. Most of hotels in China have both 110V and 220V electrical outlets in the bathrooms, though in guest rooms usually only 220V sockets are available.

Banks, ATM & Currency in China

Nearest Banks: Bank of China (BOC) and Industrial and Commercial Bank of China (ICBC) at Level 1 of the Super Brand Ball (正大广场),
5 minutes' walk from SHICC
ATM: ATM of Bank of China (BOC) at the lobby of SHICC Oriental Riverside Hotel,
Currency in China: Chinese Yuan Renminbi, Code: CNY or RMB,
Symbol: ¥

Parking

There is an underground care park available at SHICC, opens 24 hours, seven days a week, parking rate: RMB 8 per hour.

Smoking Policy

The Shanghai Tobacco Control Regulations in Public Places requires no smoking inside public buildings including hotels and convention centers. Smoking spots are established out of SHICC and all recommended hotels.

Some Friendly Reminders

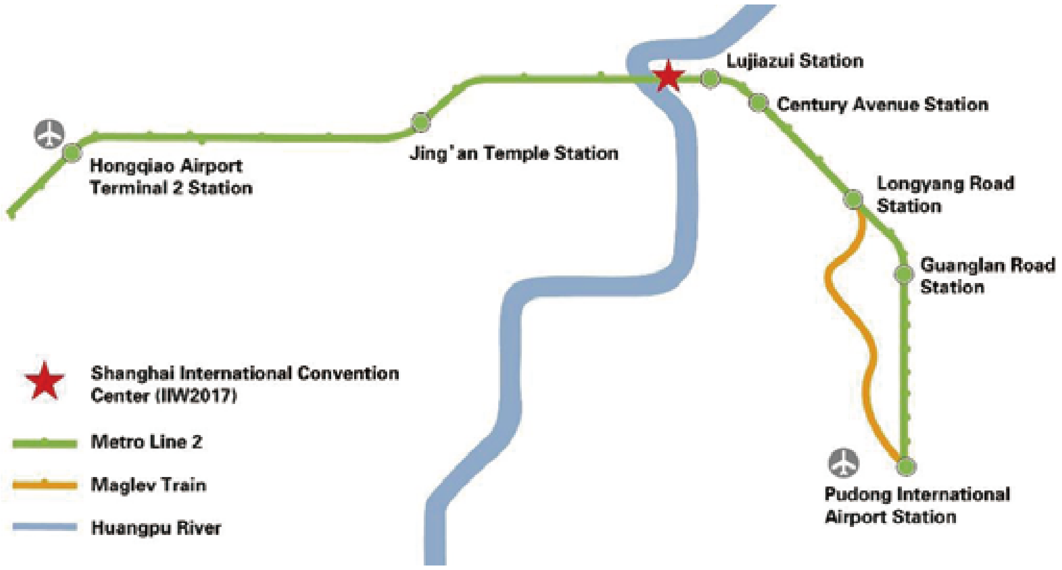
Shanghai can generally be regarded as a safe city with a low rate of violent crime. However, delegates are still advised to take precautions when moving around the city.

Useful Emergency Numbers in China:
Fire: 119
Police: 110
First-aid Ambulance: 120

Phone Numbers of Major Airlines:
China Eastern Airlines (MU): 95530
Shanghai Airlines (FM): 95530
Air China (CA): 95583
China Southern Airlines: 400-669-5539

Shanghai International Convention Center (SHICC)

Address: No. 2727 Binjiang Avenue, Shanghai, P. R. China
Telephone: 86 21 5037 0000 Website: www.shicc.net



Meals and Restaurants

There is a wide selection of different restaurants within walking distance from SHICC, details as follows:

Super Brand Mall (正大广场), 5 minutes' walk from SHICC, different restaurants of both local and international cuisines available from level B2 to level 9, average price ranges from around CNY50 to CNY500 per person.

B2：FOOD OPERA（食代馆）
1F：HOOTERS（猫头鹰美式餐吧), element fresh (新元素), Starbucks (星巴克)
2F：LACESAR（乐凯撒比萨)
5F：Burger King（汉堡王)
6F：Tsui Wah Restaurant（翠华餐厅)

Shanghai IFC Centre (国金中心), 10 minutes' walk from SHICC,different restaurants of both local and international cuisines available from level B2 to level 4, average price ranges from around CNY50 to CNY500 per person.

B2：GRANDMA'S HOME (外婆家)、FOOD POD (筷食通)
B1：PizzaExpress (马上诺), DIN TAI FUNG（鼎泰丰)
4F：Hunter Gatherer (悦衡食集), Simply Tai (天泰餐厅), GINZA BAIRIN (银座梅林)

Along the Huangpu River, 5-15 minutes' walk from SHICC, different restaurants, bars and cafeterias, average price ranges from around CNY50 to CNY1000 per person.

BlueFrog (蓝蛙)，Vapiano (新意尚)，PAULANER (宝莱纳)

Registration desk open time

Sunday (August 26th) 13:00-23:00 At 1st floor
Monday 07:30-12:00 13:00-16:00 At 3rd floor
Tuesday 08:30-12:00 At 3rd floor
Wednesday 08:30-12:00 At 3rd floor
Thursday 08:30-12:00 At 3rd floor
Friday 08:30-12:00 At 3rd floor

Instructions for presenters

Presenters should upload their presentations in the speaker ready room at least 1 hour before their session begins.
Running time for the talks is as follows.
Regular: 17 minutes plus 3 minutes questions
Invited: 30 minutes plus 5 minutes questions
Tutorial: 70 minutes plus 10 minutes questions

The ratio of ppt should be 16:9.

Instructions for presenters

All the posters can be put in the poster room for the whole conference period. The posters with the **odd number** will be presented on **Monday** and the presenters should be with your posters. The posters with **even number** will be presented on **Wednesday** session and the presenters should be before your posters.

The size of poster area is 0.9m (width) * 1.2m (height).

Shanghai International Conference Center
Oriental Pearl TV Tower
Shanghai Pudong Gardens
Super Brand Mall
Shanghai IFC Centre
Din Tai Fung
Jade on 36
Fook Lam Moon
South Beauty
Simply Thai Restaurant
Morton's the Steakhouse
Bank of China Tower
Along the Huangpu River
Google

The 2nd floor of the Conference Center provides a simple meal, and there is buffet on the first floor.
There are also some restaurants in Super Brand Mall and International Finance Center.

Recent porgress in MDI-QKD

Marco Lucamarini (Toshiba Cambridge)

Abstract: Since its inception in 2012, Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) has grown into a well-established technique that allows us to overcome all the implementation issues due to imperfect photodetectors as well as the restriction of a trusted-node architecture in a quantum network and that of a limited transmission range in point-to-point QKD.

In this tutorial, I will introduce and review MDI-QKD, from a practical perspective and with special emphasis on the years following 2014, as earlier developments were covered by Joshua Slater's 2014 QCrypt tutorial.

Starting from simple observations on 1st and 2nd-order optical interference, I will move towards quantum-encrypted communications via an intermediate node, essential quantum networks and long-distance experiments, to conclude with the recent "Twin-Field" MDI-QKD protocol that exploits interference between phase-randomised fields to overcome the repeaterless rate-loss bound of QKD.

Free space quantum communication

Christoph Marquardt (Max Planck Institute for the Science of Light)

Finite size effect in QKD

Renato Renner (ETH Zürich)

Abstract: Any real-world cryptographic scheme only runs for a finite time. This finiteness leads to statistical fluctuations, which may be exploited in attacks: An eavesdropper has a non-zero chance of gaining secret information without being detected. This tutorial aims at experimenters (who will learn how much they should worry about the finiteness of their implementations) as well as theorists (who would like to know how to phrase security statements and proofs such that they are applicable to real-world implementations).

TUTORIAL TALKS

Quantum Money

Or Sattath (Ben-Gurion University)

Abstract: The introduction of quantum money (QM), circa 1969 by Stephen Wiesner, was the first time quantum mechanics was used for cryptographic purposes, and it initiated the fields of quantum cryptography and quantum information. The goal of QM is to create "money that it is physically impossible to counterfeit", based on the laws of quantum mechanics (specifically, variants of the no-cloning theorem).

In this tutorial we will review several QM schemes, and discuss different aspects of QM, such as private vs. public verifiability, anonymity, fault tolerance, classical verifiability, and powerful attack vectors to keep in mind when designing a QM scheme. We will also discuss extensions and applications of QM, such as quantum lightning, quantum copy protection and quantum tokens for digital signatures.

Quantum computing with superconducting circuits

Yu Chen (Google/UCSB)

Abstract: More than half a century after its inception, a few great minds of physics, including Richard Feynman, predicted that the laws of quantum mechanics could give rise to a computing paradigm that is far superior to classical computing for certain tasks. Decades have passed, controlling quantum systems well enough to implement even the most primitive computing tasks has still remain as an outstanding challenge. One possible way of making quantum bits (qubits) is based on superconducting integrated circuits. Devices made out of this approach shows quantum properties at the macroscopic level, providing advantages in controlling and connecting qubits. In this talk, I will discuss the prospects and challenges in building a quantum computer based on superconducting integrated circuits. I will also discuss ongoing research activities in Google quantum A.I lab, focusing on building a sizable quantum processor for near-term applications.

Large scale quantum network in China

Large scale quantum network in China

Abstract: Quantum key distribution (QKD) together with one time pad encoding can provide information-theoretical security for communication. Currently, though QKD has been widely deployed in many metropolitan fiber networks, its implementation in a large scale remains experimentally challenging. This talk will provide a review on the experimental efforts towards the goal of global QKD, including the security of practical QKD with imperfect devices, QKD metropolitan and backbone networks over optical fiber.

Post-quantum cryptography

Andreas Hulsing (TU Eindhoven)

Abstract: Post-quantum cryptography is the study of conventional cryptography in the presence of an adversary with access to a quantum computer. In contrast to quantum cryptographic solutions like quantum key exchange it does not require a change in our infrastructure. Instead, the cryptographic mechanisms today can be replaced with post-quantum versions. However, like the cryptographic mechanisms used today the security of post-quantum schemes is based on the conjectured intractability of certain mathematical problems. In this talk I will give an overview of the landscape of schemes submitted to the recent NIST standardization project. I will discuss the underlying problems and summarize the current knowledge about quantum algorithms to solve them. In addition, I will touch on challenges in the area of provable post-quantum security.

Verifier-on-a-Leash: new schemes for verifiable delegated quantum computation, with quasilinear resources

Stacey Jeffery (CWI)

Abstract: The problem of reliably certifying the outcome of a computation performed by a quantum device is rapidly gaining relevance. We present two protocols for a classical verifier to verifiably delegate a quantum computation to two non-communicating but entangled quantum provers. Our protocols have near-optimal complexity in terms of the total resources employed by the verifier and the honest provers, with the total number of operations of each party, including the number of entangled pairs of qubits required of the honest provers, scaling as O(g log g) for delegating a circuit of size g. This is in contrast to previous protocols, which all require a prohibitively large polynomial overhead. Our first protocol requires a number of rounds that is linear in the depth of the circuit being delegated, and is blind, meaning neither prover can learn the circuit being delegated. The second protocol is not blind, but requires only a constant number of rounds of interaction. Our main technical innovation is an efficient rigidity theorem which allows a verifier to test that two entangled provers perform measurements specified by an arbitrary m-qubit tensor product of single-qubit Clifford observables on their respective halves of m shared EPR pairs, with a robustness that is independent of m. Our two-prover classical-verifier delegation protocols are obtained by combining this rigidity theorem with a single-prover quantum-verifier protocol for the verifiable delegation of a quantum computation, introduced by Broadbent.

A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device

Thomas Vidick (Caltech)

Abstract: In the talk I will describe a protocol for producing certifiable randomness from a single untrusted quantum device. The randomness is certified to be statistically close to uniform as long as the quantum device is computationally bounded during the execution of the protocol. This holds even when the randomness is measured from the point of view of any computationally unbounded quantum adversary, that may share entanglement with the quantum device.

The protocol relies on the existence of post-quantum secure trapdoor claw-free functions, and introduces a new primitive for constraining the power of an untrusted quantum device. The primitive can be instantiated based on the hardness of the learning with errors (LWE) problem.

The randomness protocol can also be used as the basis for an efficiently verifiable quantum supremacy proposal, thus answering an outstanding challenge in the field.

Quantum software and quantum network

Stephanie Wehner (Qutech/TU Delft)

Entanglement-based QKD from Micius

Juan Yin (USTC)

Free-space quantum communication with satellites opens a promising avenue for the global secure quantum network and the large-scale test of quantum foundations. The world's first quantum science satellite "Micius" was launched on August 16th 2016. And it has successfully completed the three scientific goals in the following year after launch. In addition, we demonstrated satellite-relayed quantum secured communication between China and Europe at locations separated by 7600 km. Recently, based on the distributed entangled photons, we also realized the entanglement-based QKD between the satellite and the ground, and the remote state preparation between two ground stations, etc. Here we will introduce these latest experimental progresses on the satellite-based quantum communication with Micius. Our work paves the way to the global-scale quantum network.

Lightning Talks

organized by

Charles Bennett (IBM Research)

Gilles Brassard (University of Montreal)

Monday, August 27
11:25-11:45

Q^{3}Sat: Quantum communications uplink to a 3U CubeSat – feasibility & design

Sebastian Philipp Neumann, Siddarth Koduru Joshi, Matthias Fink, Thomas Scheidl, Roland Blach, Carsten Scharlemann, Sameh Abouagaga, Daanish Bambery, Erik Kerstel, Mathieu Barthelemy and Rupert Ursin

Abstract: We have performed a detailed analysis of such a CubeSat mission (“Q³Sat”), finding that cost and complexity can be reduced by sending the photons from ground to satellite, i.e. using an uplink. We have also created a preliminary design of such a 3U CubeSat including a detailed size, weight and power budget and a CAD to account for the assembly of the components. Our feasibility study shows that it is possible to achieve quantum communication over thousands of kilometers via a single trusted node, using a relatively cheap and easy-to-construct CubeSat. The uplink design allows to keep the more sensitive, computation-intensive and expensive devices on ground. The experiment proposed by us therefore poses a comparably low-threshold quantum space mission. The proposed CubeSat can also be used for fundamental experiments such as Bell tests, clock synchronization, light pollution measurements and earth/atmosphere observation at the beacon wavelengths.

11:45-12:05

Genuine time-bin-based quantum key distribution over a turbulent depolarizing free-space channel

Jeongwan Jin, Jean-Philippe Bourgoin, Ramy Tannous, Sascha Agne, Christopher Pugh, Katanya Kuntz, Brendon Higgins and Thomas Jennewein

Abstract: Although time-bin encoding is often preferred for the realization of quantum network components in optical fibers, it is usually considered impractical for free-space transmission as the analysis of time-bin quantum states is hindered by turbulence-induced effects and optical misalignments. Here, we demonstrate quantum key distribution using time-bin-encoded photons over a 1.2 km free-space channel by employing recently-developed optical compensation techniques at the receiver. The measured total throughput of our time-bin qubit receiver from input to output multimode-fiber coupling is 81 %. Despite turbulence and depolarization effects in the channel, we measure an average quantum bit error ratio down to 4.99 % for the time-bin encoded photons and generate secure key. Hence, our demonstration could lead to new approaches for practical free-space quantum communication, and extends the use of fiber-based time-bin quantum devices to free space.

14:15-14:35

Secure certification of mixed quantum states and application to two-party randomness generation

Philippe Lamontagne, Frédéric Dupuis, Serge Fehr and Louis Salvail

Abstract: We present a general class of mixed state certification protocols, which overcomes two challenges in the analysis of this protocol: First, defining what we mean when we say that the sampling works is not trivial. Second, the fact that the prover might not necessarily want to provide the state that gives him the best chance of passing the test, even if he has it. We show that any protocol that fits this class, and that satisfies the simple criteria of being invariant under permutations and performing well on i.i.d. states, allows us to control the post-sampling state in a meaningful way. A positive consequence of this modular analysis is that previous results on pure state certification also fit our framework, and thus fall under a special case of our analysis. We also apply our analysis to the coin flipping protocol, where one party produces coin tosses in the form of EPR pairs and the other party verifies them using our sampling protocol, allows two distrusting parties to produce a common high-entropy source, where the entropy is an arbitrary small fraction below maximum (except with negligible probability).

14:35-14:55

Entanglement and secret-key-agreement capacities of bipartite quantum interactions and read-only memory devices

Stefan Baeuml, Siddhartha Das and Mark Wilde

Abstract: In this extended abstract, we present our work on two basic building blocks of bipartite quantum protocols, namely, the generation of maximally entangled and secret key via bipartite quantum interactions. In particular, we provide a non-trivial, effciently computable upper bound on the positive-partial-transpose-assisted (PPT-assisted) quantum capacity of bidirectional quantum channels, thus addressing a question that has been open for almost two decades. In addition, we provide an upper bound on the private capacity of bidirectional quantum channels assisted by local operations and classical communication (LOCC). As an application, we introduce a cryptographic protocol, which we call private reading of a classical digital memory.

14:55-15:15

Quantum-secure message authentication via blind-unforgeability

Gorjan Alagic, Christian Majenz, Alexander Russell and Fang Song

Abstract: In this work, we study authentication of classical information in the quantum-secure model. Here, the adversary is granted quantum query access to the signing algorithm of a message authentication code (MAC) or digital signature, and is tasked with producing valid forgeries. In the purely classical setting, the security model focuses on "fresh" forgeries, i.e., forgeries distinct from previous adversarial queries to the oracle; this ensures that the security definition is not vacuous and captures the natural intuition. In the setting where the function may be queried in superposition, however, it's unclear how to meaningfully reflect this critical constraint that a forgery was "unqueried" without ruling out natural, intuitive attacks.

15:45-16:05

Device-independent quantum random number generation

Yang Liu, Qi Zhao, Ming-Han Li, Jian-Yu Guan, Yanbao Zhang, Bing Bai, Wei-Jun Zhang, Wen-Zhao Liu, Cheng Wu, Xiao Yuan, Hao Li, Zhen Wang, Lixing You, Jun Zhang, Xiongfeng Ma, Jingyun Fan, Qiang Zhang and Jian-Wei Pan

Abstract: Device-independent quantum random number generation (DIQRNG) based on the loophole free violation of Bell inequality offers a final solution to generate unpredictable randomness without any device assumption. Here, we report a fully functional DIQRNG experiment against the most general quantum adversaries. We construct a robust experimental platform that realizes Bell inequality violation with entangled photons with detection and locality loopholes closed simultaneously. We performed devices independent random number generation based on the platform. Using a large Toeplitz matrix (137.90 Gb × 62.469 Mb) hashing, our DIQRNG experiment generates 6.2469×10^7 quantum-certified random bits in 96 hours (or 181 bits/s) with uniformity within 10^{-5}.

16:05-16:25

Randomness extraction from CHSH violation without fair sampling assumptions with a continuous wave source

Lijiong Shen, Jianwei Lee, Thinh Le Phuc, Jean-Daniel Bancal, Alessandro Cere, Thomas Gerrits, Adriana E. Lita, Sae Woo Nam, Valerio Scarani and Christian Kurtsiefer

Abstract: Certified private randomness can be extracted by a system that show a violation of a Bell inequality. The randomness extraction rate depends on the observed violation and on the repetition rate of the Bell test. Photonic systems generally show a smaller violation, but thanks to their higher repetition it is possible to obtain higher randomness generation rate. We demonstrate a detection loophole-free Bell violation using a photonic system based on a continuous wave source, and show that it allows to increase the randomness generation rate compared to pulsed systems.

16:25-16:45

Vacuum fluctuations quantum random number generator with non-iid samples

JTobias Gehring, Arne Kordts, Dino Solar Nikolic, Nitin Jain, Cosmo Lupo, Stefano Pirandola, Thomas Bochmann Pedersen and Ulrik Lund Andersen

Abstract: Impacting security. Quantum random number generators (QRNGs) promise perfectly unpredictable random numbers based on quantum physical processes instead of deterministic algorithms producing numbers which only appear to be random. Up to now all QRNGs assume the measured samples to be uncorrelated. With real-life detector electronics this is challenging or even impossible to achieve and will require at least additional digital signal post-processing. In this work we experimentally realize a quantum random number generator based on vacuum fluctuations which does not require the samples to be i.i.d. We demonstrate an unprecedented real-time random number generation rate of 9 GBit/s using a Toeplitz randomness extractor implemented in a FPGA and certify their security with a metrological approach based on system characterization. Our approach offers a number of practical benefits and will therefore find widespread applications in quantum random number generators.

Secure heterodyne-based quantum random number generator at 17 Gbps

Marco Avesani, Davide G. Marangon, Giuseppe Vallone and Paolo Villoresi

Abstract: Random numbers are commonly used in many different fields, ranging from simulations in fundamental science to security applications. In some critical cases, as Bell's tests and cryptography, the random numbers are required to be both secure and to be provided at an ultra-fast rate. However, practical generators are usually considered trusted, but their security can be compromised in case of imperfections or malicious external actions. In this work we introduce an efficient protocol which guarantees security and speed in the generation. We propose a novel source-device-independent protocol based on generic Positive Operator Valued Measurements and then we specialize the result to heterodyne measurements. The security of the generated numbers is proven without any assumption on the source, which can be even fully controlled by an adversary. Furthermore, we experimentally implemented the protocol by exploiting heterodyne measurements, reaching an unprecedented secure generation rate of 17.42 Gbit/s, without the need to take into account finite-size effects. Our device combines simplicity, ultrafast-rates and high security with low cost components, paving the way to new practical solutions for random number generation

Tuesday, August 28
11:25-11:45

Entanglement swapping over 100 km optical fiber with independent entangled photon-pair sources

Yangfan Jiang, Qichao Sun, Yali Mao, Li-Xing You, Wei Zhang, Wei-Jun Zhang, Xiao Jiang, Teng-Yun Chen, Hao Li, Yi-Dong Huang, Xian-Feng Chen, Zhen Wang, Jingyun Fan, Qiang Zhang and Jian-Wei Pan

Abstract: To date, there is no report on entanglement swapping with independent sources over 100-km optical fiber nor that with suspended optical fiber. We aim to implement the entanglement swapping in an intercity quantum network with independent entanglement sources. In our experiment, the total transmission loss of the optical fiber link is about 20 dB higher than previous field tests with independent sources. Our results show that realizing entanglement swapping between two cities is technically feasible, even if more suspended fiber is used. Moreover, the configuration of our experiment allows the space-like separation between any two measurements of those performed in the three nodes (Alice, Bob and Charlie), and various of time-space relation can be achieved by combining both coiled optical fiber and deployed optical fiber.

11:45-12:05

Characterising the behaviour of classical-quantum broadcast networks

Yukun Wang, Ignatius William Primaatmaja, Antonios Varvitsiotis and Charles Ci Wen Lim

Abstract: It is well known that transmitting classical information over quantum networks can significantly improve communication rates and achieve secure communication. These quantum advantages crucially rely on the network's innate ability to distribute classical correlations reliably and securely. To this end, it is of significant interest to understand how classical information propagates in quantum networks. Here, we report a computational toolbox that is able to characterise the stochastic matrix of any classical-quantum network, assuming only the inner-product information of the quantum code states. The toolbox is hence highly versatile and can analyse a wide range of quantum network protocols, including those that employ infinite-dimensional quantum states. To demonstrate the feasibility and efficacy of our toolbox, we use it to reveal new results in multipartite quantum distributed computing and quantum cryptography. Taken together, these findings suggest that our method may have important implications for quantum network information theory and the development of new quantum technologies.

Wednesday, August 29
10:50-11:10

Global phase encoding quantum key distribution

Pei Zeng, Hongyi Zhou and Xiongfeng Ma

Abstract: Here, we propose a global-phase-encoding quantum key distribution (GPE-QKD) scheme that can surpass the linear key rate bound. Unlike the former single-photon based QKD protocols, we employ more practical coherent state sources. The two communication parties each prepares a coherent state and they encode the key information on the global phase of the two states. Meanwhile, by developing an optical-mode-based security proof, we show that the key rate of the proposed scheme scales with the square root of the transmittance, R = O(\sqrt(\eta)). Furthermore, the proposed global-phase-encoding scheme is immune to all possible detection attacks.

11:10-11:30

Enabling a scalable high-rate measurement-device-independent quantum key distribution network: theory and experiment

Wenyuan Wang, Hui Liu, Teng-Yun Chen, Feihu Xu and Hoi-Kwong Lo

Abstract: The key goal of our work is to design and demonstrate a software solution that enables high key generation rate in a general scalable MDI-QKD network with arbitrary losses for various channels. We propose and experimentally implement an asymmetric MDI-QKD protocol, which can provide substantially higher key rate than all previous protocols. Using a self-stabilized time-bin phase encoding MDI-QKD system, we demonstrate as much as 10 to 300 times higher key rate than previous protocols over different lengths of standard fiber spools up to 100 km. Moreover, our protocol enables a much larger region of possible combinations of channels. Our work completely removes the requirement of symmetric channels in MDI-QKD, which provides a powerful and robust solution for a scalable and reconfigurable MDI-QKD network where users can be added/deleted dynamically.

11:30-11:50

Parallel device-independent quantum key distribution

Rahul Jain, Carl Miller and Yaoyun Shi

Abstract: A prominent application of quantum cryptography is the distribution of cryptographic keys with unconditional security. Recently, such security was extended by Vazirani and Vidick (Physical Review Letters, 113, 140501, 2014) to the device-independent (DI) scenario, where the users do not need to trust the integrity of the underlying quantum devices. The protocols analyzed by them and by subsequent authors all require a sequential execution of N multiplayer games, where N is the security parameter. In this work, we prove unconditional security of a protocol where all games are executed in parallel. Besides decreasing the number of time-steps necessary for key generation, this result reduces the security requirements for DI-QKD by allowing arbitrary information leakage of each user's inputs within his or her lab. To the best of our knowledge, this is the first parallel security proof for a fully device-independent QKD protocol. Our protocol tolerates a constant level of device imprecision and achieves a linear key rate.

11:50-12:10

On the power of non-adaptive quantum chosen-ciphertext attacks

Gorjan Alagic, Stacey Jefferey, Maris Ozols and Alexander Poremba

Abstract: Large-scale quantum computing is a significant threat to classical cryptography. We consider classical symmetric-key encryption in such a model: the adversary has quantum oracle access to encryption and decryption, but the latter is restricted to non-adaptive queries only. Using a bound on quantum random-access codes, we show that the standard PRF- and PRP-based encryption schemes are QCCA1-secure when instantiated with a quantum-secure PRF (pseudorandom function) or PRP (psuedorandom permutation), respectively. We revisit the standard symmetric-key IND-CPA-secure learning with errors (LWE) encryption scheme in this model and show that leaking just one quantum decryption query (and no other queries or leakage of any kind) leads to a full key recovery with constant success probability. Likewise, leaking just one quantum encryption query, where the adversary is allowed to instantiate the randomness register, also leads to complete key recovery. By contrast, a classical decryption (respectively encryption) query can produce at most one bit (respectively log q bits) of the (n log q)-bit key.

14:15-14:35

2.5 GHz clocked quantum key distribution over 379 km

Alberto Boaron, Boris Korzh, Gianluca Boso, Davide Rusca, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Claire Autebert, Félix Bussières, Ming-Jun Li, Daniel Nolan, Anthony Martin and Hugo Zbinden

Abstract: We present a system with 2.5 GHz pulse rate which is at the same time simple and efficient, and push QKD further to its limits. We improve the secret key rate (SKR) by more than one order of magnitude compared to the state-of-theart experiments at distances above 200km and perform a record breaking secret key exchange over 379 km. We use a protocol based on time-bin encoding with decoy state method. We employ only three quantum states and two decoy levels. The SKR is obtained by performing a complete security analysis, taking into account finite-statistics effects.

14:35-14:55

In-field entanglement distribution over a 96 km submarine optical fibre

Soeren Wengerowsky, Siddarth Koduru Joshi, Fabian Steinlechner, Julien R. Zichi, Sergiy M. Dobrovolsky, René van der Molen, Johannes W. N. Los, Val Zwiller, Marijn A. M. Versteegh, Alberto Mura, Davide Calonico, Massimo Inguscio, Hannes Hübel, Anton Zeilinger, André Xuereb and Rupert Ursin

Abstract: We present the distribution of polarisation-entangled photons between Malta and Sicily using a 96 km-long submarine telecommunications as a quantum channel. We were able to observe around 260 photon pairs per second, with a polarisation visibility above 86%. Our experiment demonstrates the feasibility of using deployed submarine telecommunications optical fibres as long-distance quantum channels for polarisation-entangled photons.This opens up possibilities for future experiments and technological applications using existing infrastructure.

14:55-15:15

High-dimensional fiber based quantum key distribution with twisted photons

Davide Bacco, Daniele Cozzolino, Beatrice Da Lio, Kasper Ingerslev, Yunhong Ding, Kjeld Dalgaard, Poul Kristensen, Michael Galili, Karsten Rottwitt, Siddharth Ramachandran and Leif Oxenloewe

Abstract: In this work I am going to talk about high-dimensional fiber based quantum key distribution with twisted photons. As we all know that two essential challenges of QKD systems are short propagation distances and the low transmittable bit rates. A fundamental way to overcome these issues is using high-dimensional quantum states, as the high-dimensional states provides increased information capacity and higher robustness against channel noise. However, the generation, transmission and detection of high-dimensional quantum states is very challenging, and only a few experimental realizations have been achieved for HD QC protocols. Using the orbital angular momentum of light is promising. We experimentally demonstrate the first transmission of high-dimensional quantum states, encoded in four OAM modes and their superstition, over a 1.2KM long OAM fiber, by implementing a real-time decoy-state HD QKD protocol, demonstrating the highest secret key rate and the longest transmission distance presented to date.

15:45-16:05

A comprehensive analysis of quantum E-voting protocols

Myrto Arapinis, Elham Kashefi, Nikolaos Lamprou and Anna Pappa

Abstract: Recent advances at Google, IBM, as well as at a number of research groups indicate that quantum computers will soon be reality. Motivated by the ever more realistic threat quantum computers pose to existing classical cryptographic protocols, researchers have developed several schemes to resist “quantum attacks”. In particular, for electronic voting, several e-voting schemes relying on properties of quantum mechanics have been proposed. However, each of these proposals comes with a different and often not well-articulated corruption model, has different objectives, and is accompanied by security claims which are never formalized and are at best justified only against specific attacks. In this paper, we systematize and evaluate the security of suggested e-voting protocols based on quantum technology. We examine what the claims of these works are concerning privacy, correctness and verifiability, and if they are correctly attributed to the proposed protocols. In all non-trivial cases, we provide specific quantum attacks that violate these properties. We argue that the cause of these failures lies in the absence of formal security models and in a more general lack of reference to the existing cryptographic literature.

16:05-16:25

On the insecurity of quantum Bitcoin mining

Or Sattath

Abstract: Classically, a Bitcoin fork occurs rarely, when two miners find a block almost at the same time: only if both miners are unaware of the other’s block, due to propagation time effects. The situation differs dramatically when quantum miners use Grover’s algorithm. Suppose Alice receives Bob’s new block. To maximize her revenue, she should stop applying Grover iterations and measure her state. Her hope is that her block (rather than Bob’s) would become part of the longest chain. This strong correlation between the miners’ actions, and the fact that they all measure their state at the same time, may lead to more forks. This is known as a security risk for Bitcoin. We propose a mechanism which, we conjecture, prohibits this form of quantum mining, and circumvents the high rate of forks.

16:25-16:45

Distributed private randomness distillation

Dong Yang, Karol Horodecki and Andreas Winter

Abstract: We develop the resource theory of private randomness extraction in the distributed and device-dependent scenario. We begin by introducing the notion of independent bits (ibits), which are bipartite states that contain ideal private randomness for each party, and motivate the natural set of the allowed free operations. As the main tool of our analysis, we introduce Virtual Quantum State Merging (VQSM), which is essentially the flip side of Quantum State Merging, without the communication. We focus on the bipartite case and find the rate regions achievable in different settings. Perhaps surprisingly, it turns out that local noise can boost randomness extraction. As a consequence of our analysis, we resolve a long-standing problem by giving an operational interpretation for the reverse coherent information capacity in terms of the number of private random bits obtained by sending quantum states from one honest party (server) to another one (client) via an eavesdropped quantum channel.

Thursday, August 30
11:25-11:45

Pseudorandom quantum states

Zhengfeng Ji, Yi-Kai Liu and Fang Song

Abstract: We propose the concept of pseudorandom quantum states, which appear random to any quantum polynomial-time adversary. This offers a computational approximation to perfectly random quantum states (analogous to cryptographic pseudorandom generators), as opposed to statistical notions of quantum pseudorandomness that have been studied previously, such as quantum t-designs (analogous to t-wise independent distributions).

Under the assumption that quantum-secure one-way functions exist, we present efficient constructions of pseudorandom states, showing that our definition is achievable. We then prove several basic properties of pseudorandom states, which show the utility of our definition. First, we show a cryptographic no-cloning theorem: no efficient quantum algorithm can create additional copies of a pseudorandom state, when given polynomially-many copies as input. Second, as expected for random quantum states, we show that pseudorandom quantum states are highly entangled on average. Finally, as a main application, we prove that any family of pseudorandom states naturally gives rise to a private-key quantum money scheme.

11:45-12:05

Unforgeable quantum encryption

Gorjan Alagic, Tommaso Gagliardoni and Christian Majenz

Abstract: In this work, we instead consider encryption schemes: the non-interactive and more efficient approach which dominates the classical Internet. Our goal is to achieve, in the quantum setting, the basic features of Internet encryption: (i.) a small key suffices for transmitting a large amount of data, (ii.) keys can be exchanged over public channels, and (iii.) security guarantees are extremely strong. Previous work has shown how to achieve (i.) and (ii.), but only for a limited form of quantum secrecy. Authentication or adaptive chosen-ciphertext security for such schemes has not been considered. In fact, at the time of writing, there is not even a definition for two-time quantum authentication. The aim of this work is to address this problem.

Friday, August 31
9:35-9:55

On the possibility of classical client blind quantum computing

Alexandru Cojocaru, Leo Colisson, Elham Kashefi and Petros Wallden

Abstract: In this work I will talk about the possibility of classical client blind quantum computing. The idea of quantum internet has come into being with the development of quantum technologies, which can be implemented with a collection of protocols. The development of quantum hardware has increased the computational capacity of quantum servers to be linked in such a network. This raised the necessity of privacy preserving functionalities such as the research developed around quantum computing on encrypted data. However, a reliable long-distance quantum communication network might be costing, and some of the most promising quantum computation devices do not yet offer the possibility of “networked” function. One direction to solve the problems is to reduce the required communications by exploiting classical fully-homomorphic-encryption schemes. Another possible direction is to consider fully-classical client protocols with more restricted levels of security. Our work is also based on post-quantum computational security. We replace the quantum communication with a primitive that mimics a quantum channel keeping the client fully classical, and we give a concrete protocol and prove its security against a weak “quantum honest-but-curious” adversarial server. And our approach has a wide range of applications.

9:55-10:15

On basing one-way permutations on NP-hard problems under quantum reductions

Nai-Hui Chia, Sean Hallgren and Fang Song

Abstract: A fundamental pursuit in complexity theory concerns reducing worst-case problems to averagecase problems. There exist complexity classes such as PSPACE that admit worst-case to averagecase reductions. Many other classes such as NP, however, the evidence so far is typically negative, in the sense that existence of such reductions would cause collapses of the polynomial hierarchy. Basing cryptography, e.g., the average-case hardness of inverting one-way permutations, on NP-completeness is a particularly intriguing instance. We initiate a study of the quantum analogue of these questions and show that if NP-complete problems reduce to inverting one-waypermutations using certain types of quantum reductions, then coNP$\subseteq$QIP(2).

11:25-11:45

Quantum position-verification in the plane

Serge Fehr and Dominique Unruh

Abstract: Most positive results on position-based quantum cryptography (which require some restriction on the adversaries) are rigorously proven only in the 1-dimensional setting. For instance, in their original paper on the topic, Buhrman et al. gave a rigorous security analysis for a particular scheme that works in the 1-dimensional case, while offering only an informal argument for why the obvious extension of the scheme to higher dimensions should still be secure. As pointed out by Unruh, this informal argument for the higher dimensional case is actually incomplete and does not lead to a rigorous security proof. Aproof for higher dimensions was left as an open problem.
We make a first step in this direction by providing a rigorous security proof for the 2-dimensional version of the scheme by Buhrman et al. Our proof is by means of a careful decomposition of spacetime during the execution of the scheme into different regions, which are distinguished by the information that may be present there, and showing that the security of the scheme reduces to a monogamy-of-entanglement game.

11:45-12:05

Ultrafast waveguide-integrated single-photon detectors for on-chip QKD detection

Fabian Beutel, Julian Münzberg, Andreas Vetter, Wladick Hartmann, Simone Ferrari, Carsten Rockstuhl and Wolfram H.P. Pernice

Abstract: Efficient and fast single-photon detection is one of the key requirements for most quantum key distribution (QKD) schemes. At telecom wavelength around 1550 nm, existing detector technologies often exhibit shortcomings in at least one of the metrics that are crucial for high-performance QKD schemes, namely efficiency, dark-count rate (DCR) and recovery times. We present waveguide-integrated superconducting nanowire single-photon detectors (SNSPDs) showing detection efficiencies of 67 % with negligible DCR and ultra-fast recovery times of 480 ps, allowing for Gcps detection rates. The design also allows for direct integration with complex photonic circuits and therefore enables scalable and alignment-free QKD detection devices.

01 Superconducting nanowire single photon detection system for space quantum applications

Lixing You and Jingtao Liang.

03 True single-photon stimulated four wave mixing

Shuai Dong, Xin Yao, Sijing Chen, Weijun Zhang, Lixing You, Zhen Wang, Yidong Huang and Wei Zhang.

05 Optimal photon pairs for quantum communication

Mikolaj Lasota, Karolina Sedziak and Piotr Kolenderski.

07 Versatile relative entropy bounds for quantum networks

Luca Rigovacca, Go Kato, Stefan Baeuml, Myungshik Kim, William Munro and Koji Azuma.

09 Random private quantum states

Matthias Christandl, Roberto Ferrara and Cecilia Lancien Lancien.

11 Differential phase shift QKD security proof

Daan Leermakers and Boris Škorić. Round Robin.

13 Finite-key effects in multi-partite quantum key distribution protocols

Federico Grasselli, Hermann Kampermann and Dagmar Bruss.

15 Quantum controlled joint remote state preparation and quantum operation remote implementation

Ping Zhou, Shu-Xin Lv and Xian-Fang Jiao.

17 Entanglement-assisted private communication over quantum broadcast channels

Haoyu Qi, Kunal Sharma and Mark M. Wilde.

02 Progress in development of titanium transition-edge single-photon detectors

Jiaqiang Zhong, Wen Zhang, Yue Geng, Zheng Wang, Wei Miao, Qijun Yao and Sheng-Cai Shi.

04 Quantum secure communication based on ghost imaging

Xin Yao, Xu Liu and Wei Zhang.

06 Measurement of nonlocal variables

Lev Vaidman, Xiao-Ye Xu and Chuan-Feng Li.

08 Spectral measurement of breakdown flashes in InGaAs avalanche photodiodes

Yicheng Shi, Janet Lim Zheng Jie, Hou Shun Poh, Peng Kian Tan, Amelia Tan, Alexander Ling and Christian Kurtsiefer.

10 Intensity modulation as a preemptive measure against blinding of single-photon detectors based on self-differencing cancellation

Alexander Koehler-Sidki, James Dynes, Marco Lucamarini, George Roberts, Andrew Sharpe, Zhiliang Yuan and Andrew Shields.

12 Practical quantum appointment scheduling

Dave Touchette, Benjamin Lovitz and Norbert Lutkenhaus.

14 Simple security proof of twin-field type quantum key distribution protocol

Marcos Curty, Koji Azuma, Hoi-Kwong Lo.

16 Bounding the energy-constrained quantum and private capacities of phase-insensitive Gaussian channels

Kunal Sharma, Mark M. Wilde, Sushovit Adhikari and Masahiro Takeoka.

19 Atmospheric effects on continuous-variable quantum key distribution

Shiyu Wang, Peng Huang, Tao Wang, Hongxin Ma and Guihua Zeng.

21 A study about the error and disturbance in quantum measurements: theory and experiment

Yali Mao, Zhi-Hao Ma, Rui-Bo Jin, Qichao Sun, Qiang Zhang, Jingyun Fan and Jianwei Pan.

23 High-speed and high-performance polarization-based quantum key distribution system without side channels of multiple lasers

Heasin Ko, Byung-Seok Choi, Joong-Seon Choe, Kap-Joong Kim, Jong-Hoi Kim and Chun Ju Youn.

25 Near-term repeater experiment with NV centres: overcoming direct transmission limit

Filip Rozpedek, Kenneth Goodenough, Raja Yehia, Maximilian Ruf, Peter C. Humphreys, Ronald Hanson, Stephanie Wehner and David Elkouss.

27 Random number generation with cosmic photons

Cheng Wu and Qiang Zhang.

29 Eve strikes back in the era of measurement-device-independent quantum key distribution

Anqi Huang, Alvaro Navarrete, Ruoping Li, Vladimir Egorov, Shi-Hai Sun, Poompong Chaiwongkhot, Marcos Curty and Vadim Makarov.

31 Single photon entanglement distribution scheme applied to a purification protocol

Nicolo Lo Piparo, William Munro and Kae Nemoto.

33 Entanglement-assisted private communication over quantum broadcast channels

Haoyu Qi, Kunal Sharma and Mark M. Wilde.

35 Quantum key distribution network simulation module

Miralem Mehic, Marcin Niemiec and Miroslav Voznak.

18 Polarization variations in installed fibers and their influence on quantum key distribution systems

Yuyang Ding, Shuang Wang and Wei Chen.

20 Basis-encoding quantum key distribution using Gaussian-modulated coherent states

Peng Huang, Chao Wang and Guihua Zeng.

22 Precise quantification of quantum coherence with untrusted measurement devices

You-Qi Nie, Hongyi Zhou, Jian-Yu Guan, Qiang Zhang, Xiongfeng Ma, Jun Zhang and Jian-Wei Pan.

24 Achieving security of quantum group communication

Zheng-Hong Li, M. Suhail Zubairy and M. Al-Amri.

26 QKD for global navigation satellite systems: experimental feasibility study with a link of 20000 km

Luca Calderaro, Costantino Agnesi, Daniele Dequal, Francesco Vedovato, Matteo Schiavon, Alberto Santamato, Vincenza Luceri, Giuseppe Bianco, Giuseppe Vallone and Paolo Villoresi.

28 1.3-μm-band up-conversion single-photon detector based on integrated PPLN waveguides

Fei Ma, Ming-Yang Zheng, Xiu-Ping Xie, Qiang Zhang and Jian-Wei Pan.

30 Dual-wavelength up-conversion single-photon detectors based on integrated PPLN waveguides

Mingyang Zheng, Fei Ma, Xiuping Xie, Qiang Zhang and Jianwei Pan.

32 State tomographic characterization of BB84 states generated by a dual-parallel modulator

Weiyang Zhang, Akihisa Tomita, Yu Kadosawa, Kuzihisa Ogawa and Atsushi Okamoto.

37 Scalable QKD networks based on subcarrier wave architecture and software-defined paradigm: ITMO University initiative in Russian quantum networking

Artur Gleim, Vladimir Egorov, Vladimir Chistiakov, Artur Vasiliev, Andrei Gaidash, Anton Kozubov, Semen Smirnov, Sergei Kynev, Nikita Buldakov, Oleg Sadov, Andrey Shevel, Sergei Khoruzhnikov, Oleg Bannik, Lenar Gilyazov, Konstantin Melnik, Narkis Arslanov, Ilnur Latypov, Sergei Moiseev, Xi-Cheng Zhang and Sergei Kozlov.

39 Long distance continuous-variable measurement-device-independent quantum key distribution with photon subtraction

Hong-Xin Ma, Peng Huang, Dong-Yun Bai, Hai-Lun Yan, Shi-Yu Wang, Wan-Su Bao and Gui-Hua Zeng.

41 Quantum-safe internet based on service-oriented quantum key distribution network

Zhangchao Ma, Lei Sun and Jianquan Wang.

43 Generating secrecy from the act of secrecy

Anne Ghesquiere and Ben Varcoe

45 Implementing hybrid quantum-postquantum security in a prototype network

Alasdair Price, John Rarity and Chris Erven.

47 Necessary criteria for quantum secure direct communication and how to achieve them

Shihan Sajeed and Hoi-Kwong Lo.

49 Highly flexible continuous-variable quantum cryptographic transmitter using pilot tones and integrated quantum random number generator

Nitin Jain, Hou-Man Chin, Dino Solar Nikolic, Arne Kordts, Darko Zibar, Tobias Gehring and Ulrik Andersen.

51 Quantum key distribution with small satellites

Peter Freiwang, Qube-Consortium – Zft, Qube-Consortium – Dlr Ikn, Qube-Consortium – Mpl, Qube-Consortium – Ohb, Wenjamin Rosenfeld and Harald Weinfurter.

34 The 1-decoy state protocol: the best choice for practical QKD

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

36 On quantum indifferentiability

Ehsan Ebrahimi, Tore Vincent Carstens, Dominique Unruh and Gelo Noel Tabia.

38 Industrial QKD with polarization states

Alexander Duplinsky, Evgeny Kiktenko, Nikolay Pozhar, Vladimir Kurochkin, Aleksey Fedorov and Yury Kurochkin.

40 Quantum ciphertext authentication and key recycling with the trap code

Yfke Dulek and Florian Speelman.

42 Authenticated teleportation under different trust settings

Anu Unnikrishnan and Damian Markham.

44 High-dimensional quantum communication

T.B.H. Tentrup, L.V. Amitonova, I.M. Vellekoop and P.W.H. Pinkse.

46 A simple protocol for certifying graph states and applications in quantum networks

Damian Markham and Alexandra Krause.

48 POVM description of single photon ON/OFF detectors including timing-jitter effects

Élie Gouzien, Bruno Fedrici, Alessandro Zavatta, Sébastien Tanzilli and Virginia D'Auria.

50 Anonymous transmission in a quantum network using the W state

Victoria Lipinska, Gláucia Murta and Stephanie Wehner.

52 Reference pulse attack on a trusted phase noise CV-QKD system using a local local oscillator

Shengjun Ren, Rupesh Kumar, Adrian Wonfor, Xinke Tang, Richard Penty and Ian White.

53 Fast quantum algorithms for solving multivariate quadratic equations over finite fields

Jean-Charles Faugère, Kelsey Horan, Delaram Kahrobaei, Marc Kaplan, Elham Kashefi and Ludovic Perret.

55 Quantum alarm: a novel approach to monitor the physical security of optical transport networks

Yupeng Gong, Rupesh Kumar, Adrian Wonfor, Richard Penty and Ian White.

57 Photon-pair characterization using a single SPD by detector time-multiplexing

Yulin Zheng, Jiakun He, Wei Geng and Yunchuan Kong.

59 Experimental quantum key distribution at 1.3 Gbit/s secret-key rate over a 10-dB-loss channel

Zheshen Zhang, Changchen Chen, Quntao Zhuang, Jane Heyes, Franco Wong and Jeffrey Shapiro.

61 Feedforward attack in decoy-state quantum key distribution

Toshihiko Sasaki, Tatsuya Sumiya and Masato Koashi.

63 Entanglement of macroscopic light states via delocalized single photon addition

Nicola Biagi, Luca Costanzo, Marco Bellini and Alessandro Zavatta.

65 Post-processing optimization for continuous-variable quantum key distribution

Laszlo Gyongyosi.

67 Spaceborne low-noise Si APD single photon detectors

Yang Meng

69 Hybrid manager for QKD network

Xiao Duan, Tim Edwards, Rupesh Kumar, Helmut Griesser, Andrew Straw, Adrian Wonfor, Catherine White, Andrew Lord and Timothy Spiller.

54 Small form factor, low cost electronics for chip scale and handheld quantum key distribution systems

Andy Hart, Henry Semenenko, Stefan Frick, Chris Erven, David Lowndes, Philip Sibson, Mark Thompson and John Rarity.

56 Post-selection technique against phase and polarization dependent loss in quantum communication

Chenyang Li, Marcos Curty, Feihu Xu, Olinka Bedroya and Hoi-Kwong Lo.

58 Security vulnerabilities of trusted noise detector model in continuous-variable quantum key distribution

Hao Qin, Jan Gulla, Anqi Huang and Vadim Makarov.

60 Randomness certification by quantum contextuality in a trappedion

Mark Um, Qi Zhao, Pengfei Wang, Ye Wang and Kihwan Kim.

62 Enhanced free-space continuous-variable quantum key distribution

Vladyslav Usenko, Ivan Derkach, Laszlo Ruppert and Radim Filip.

64 Integrating quantum key distribution with classical communications in backbone fiber network

Yingqiu Mao, Bi-Xiao Wang, Chunxu Zhao, Guangquan Wang, Ruichun Wang, Honghai Wang, Fei Zhou, Jimin Nie, Qing Chen, Yong Zhao, Qiang Zhang, Jun Zhang, Teng-Yun Chen and Jian-Wei Pan.

66 Finite-size analysis of continuous-variable quantum key distribution using a nondeterministic noiseless linear amplifier under realistic conditions

Dongyun Bai, Peng Huang, Hongxin Ma, Tao Wang, Tailong Xiao and Guihua Zeng.

68 Focus on the calibration of practical QKD systems —quantum man-in-the-middle attack and the corresponding security analysis

Yangyang Fei, Xiangdong Meng, Ming Gao, Hong Wang and Zhi Ma.

71 Unidimensional continuous-variable quantum key distribution

Xuyang Wang, Wenyuan Liu, Shenshen Yang, Pu Wang and Yongmin Li.

73 Satellite-based quantum links for QKD: beam effects and weather dependence

Carlo Liorni, Hermann Kampermann and Dagmar Bruß.

75 Reference-frame-independent measurement-device-independent quantum key distribution based on polarization multiplexing

Hongwei Liu, Jipeng Wang, Shi-Hai Sun and Haiqiang Ma.

77 Experimental analysis of reference-frame-independent QKD between moving parties via free-space quantum channel

Juhwan Yoon Yoon, Tanumoy Pramanik, Byung Kwon Park, Min-Sung Kang, Sang Wook Han, Sangin Kim, Yong-Su Kim and Sung Moon.

79 A new-comer in quantum random world

Jeong Woon Choi.

81 Field trial of a high-secure-key-rate QKD system

Akira Murakami, Mamiko Kujiraoka, Doi Kazuaki, Ririka Takahashi, Alexander R. Dixon, Yoshimichi Tanizawa, Hideaki Sato, Zhiliang Yuan, Alan Plews, Winci Tam, Andrew Sharpe, Evan Lavelle, James Dynes, Marco Lucamarini, Andrew Shields, Tomoaki Chiba, Takako Takai-Igarashi, Fuji Nagami and Masao Nagasaki.

83 Performance evaluation of practical device-independent quantum key distribution

Víctor Castrillo and Marcos Curty.

85 Bounds on device-independent advantage distillation in the IID scenario

Ernest Y.-Z. Tan and Renato Renner.

87 Loss-tolerant quantum cryptography with leaky sources

Margarida Pereira, Marcos Curty and Kiyoshi Tamaki.

70 Finite-key security analysis of measurement-device-independent quantum key distribution with leaky sources

Weilong Wang and Marcos Curty.

72 A denial-of-service attack on fiber-based continuous-variable quantum key distribution

Yuan Li, Peng Huang and Guihua Zeng.

74 A memory-saving scheme of privacy amplification algorithm for continuous-variable quantum key distribution

Dengwen Li, Peng Huang and Guihua Zeng.

76 Synthesis of Er3+ doped Y2O3 transparent ceramics for quantum optical memory studies

Haitao Zhang, Jun Yang, Jason Allen Brown, Thomas D. Ketcham, Stuart Gray and Daniel A. Nolan.

78 Quantum repeaters with optimal encoding from absolutely maximally entangled states

Daniel Alsina Leal and Mohsen Razavi.

80 Continuous variable quantum key distribution multiplexed with classical channels

Tobias Eriksson, Takuya Hirano, Georg Rademacher, Benjamin Puttnam, Ruben Luís, Mikio Fujiwara, Ryo Namiki, Ken-Ichiro Yoshino, Akio Tajima, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada and Masahide Sasaki.

82 Restricted memory attacks in continuous-variable quantum key distribution

Nedasadat Hosseinidehaj, Nathan Walk and Timothy Ralph.

84 Fiber quantum random number generator, based on quantum nature of vacuum fluctuations

Alena Ivanova, Sergey Chivilikhin and Artur Gleim.

89 **Quantum lattice enumeration**

Yixin Shen, Phong Q. Nguyen and Yoshinori Aono.

91 **CV-MDI QKD with squeezed states based on uncertainty principle**

Ziyang Chen, Yichen Zhang, Gan Wang, Zhengyu Li and Hong Guo.

93 **Field trial of transmitting polarisation entangled photons from a quantum dot**

Zi-Heng Xiang, Jan Huwer, R. Mark Stevenson, Joanna Skiba-Szymanska, Martin Ward, Ian Farrer, David Ritchie and Andrew Shields.

95 **A REST API for QKD key delivery: performance, integration, and phase-in approach**

Yoshimichi Tanizawa, Ririka Takahashi, Alexander Dixon, Hideaki Sato, James Dynes, Joo Cho and Andrew Shields.

96 **Quantum secure direct communication: different versions lead to practical applications**

Chitra Shukla and Gui Lu Long

99 **A simple security proof of twin-field quantum key distribution**

Jie Lin and Norbert Lütkenhaus.

101 **Momtchil Peev and Christoph Pacher.**

Michael Hentschel, Ian Glendinning, Bernhard Ömer, Chi-Hang Fred Fung,

103 **Eavesdropping strategy for coherent one-way protocol based on soft filtering operation**

Dmitry Kronberg, Anastasia Nikolaeva, Yury Kurochkin and Alexey Fedorov.

105 **Equalization technique of multiple input multiple output (MIMO) methods in quantum coherent communications**

Nina Tadza, Rupesh Kumar, Adrian Wonfor, Richard Penty and Ian White.

86 **Development of practical post-processing board connecting random number generators and QKD system**

Ken-Ichiro Yoshino and Akio Tajima.

88 **A theoretical framework for QR-PUFS**

Giulio Gianfelici, Hermann Kampermann and Dagmar Bruß.

90 **Quantum computational hybrid cryptography**

Nilesh Vyas and Romain Alléaume.

92 **Miniaturised hand-held quantum key distribution system with tracking capability**

Hyunchae Chun, David Lowndes and Iris Choi.

94 **Patterning-effect-free intensity modulator for decoy-state quantum key distribution**

George Roberts, Mirko Pittaluga, Mariella Minder, James F. Dynes, Zhiliang Yuan, Marco Lucamarini and Andrew J. Shields.

96 **Experimental demonstration of simultaneous quantum and classical coherent communication using a single wavelength channel**

Rupesh Kumar, Adrian Wonfor, Richard Penty and Ian White.

98 **Beating direct transmission bounds for quantum key distribution with a multiple quantum memory station**

Róbert Trényi and Norbert Lütkenhaus.

100 **Secure key delivery for QKD-integrated optical communication**

Joo Cho and Yoshimichi Tanizawa.

102 **Securing the control channel of a moving robot with quantum key distribution**

Nikolai Dema, Kirill Artemov, Artur Vasiliev, Vladimir Chistyakov, Artur Gleim, Sergei Kolyubin and Vladimir Egorov.

107 An adaptive framework for quantum-secure device-independent randomness expansion

Peter Brown, Sammy Ragy and Roger Colbeck.

109 Obtaining better performance in the measurement-device-independent quantum key distribution with heralded single-photon sources

Xingyu Zhou, Chunhui Zhang, Chunmei Zhang and Qin Wang.

111 Optimal conditions for Bell test using a spontaneous parametric down-conversion source

Yoshiaki Tsujimoto, Kentaro Wakui, Mikio Fujiwara, Kazuhiro Hayasaka, Shigehito Miki, Hirotaka Terai, Masahide Sasaki and Masahiro Takeoka.

113 Quantum research CubeSat (QUARC)

Luca Mazzarella, Christopher Lowe, David Lowndes, Steve Greenland, Steven Owens, Hina Khan, Malcolm Macdonald, John Rarity and Daniel Oi.

115 Modulation index decoy states protocol for subcarrier wave quantum key distribution system

Andrei Gaidash, Vladimir Chistyakov, Anton Kozubov, Artur Gleim and George Miroshnichenko.

117 312.5 MHz sine-wave gated single photon detector with active quenching circuits: the investigation of dependence of the afterpulsing probability from the circuit design

Anton Losev, Vladimir Zavodilenko and Yuri Kurochkin.

119 Precise overestimation of quantum bit error rate to minimize failure probability of low density parity check error correction

Vladimir Chistiakov, Andrei Gaidash, Anton Kozubov, Vladimir Egorov, Artur Gleim and George Miroshnichenko.

104 Adaptive forward error correcting design for faster post-processing in practical CV-QKD systems

Nina Tadza, Rupesh Kumar, Adrian Wonfor, Richard Penty and Ian White.

106 Carrier phase estimation for simultaneous quantum and classical communication without any phase reference

Tao Wang, Peng Huang, Shiyu Wang, Hongxin Ma, Dongyun Bai and Guihua Zeng.

108 Secret-key rates for device-independent QKD beyond CHSH violation

Timo Holz, Hermann Kampermann and Dagmar Bruss.

110 A simple scheme for realizing the passive decoy-state quantum key distribution

Chun-Hui Zhang, Dong Wang, Chun-Mei Zhang and Qin Wang.

112 Second-harmonic generation of 671 nm laser with high efficiency in an external ring cavity

Xing-Yang Cui, Qi Shen, Mei-Chen Yan, Tao Yuan, Chao Zeng, Wen-Zhuo Zhang, Xing-Can Yao, Cheng-Zhi Peng, Xiao Jiang, Yu-Ao Chen and Jian-Wei Pan.

114 A learning scheme with coherent state Amplification

Luca Mazzarella and John Jeffers.

116 Finite-key analysis for subcarrier wave quantum key distribution

Anton Kozubov, Andrei Gaidash, Artur Gleim and George Miroshnichenko.

118 Resource analysis of future quantum repeater networks

Yumang Jing and Mohsen Razavi.

121 Entity authentication scheme for one-to-many quantum key distribution system based on BB84 protocol

Haeun Kim, Hojoong Park, Ju-Sung Kang, Yongjin Yeom, Byung Kwon Park, Min-Sung Kang, Sang-Wook Han and Sung Moon.

123 1×4 Quantum key distribution access network in metropolitan area

Byung Kwon Park, Min-Sung Kang, Min Ki Woo, Min Soo Lee, Sang-Wook Han and Sung Moon.

125 Efficient quantum fingerprinting with wavelength division multiplexing

Xiaoqing Zhong, Li Qian and Hoi-Kwong Lo.

127 Plug-and-play unidimensional continuous-variable quantum key distribution

Xinchao Ruan, Hang Zhang, Ying Guo, Ling Zhang and Duan Huang.

129 Differential-phase-shift continuous-variable quantum key distribution

Minglu Cai, Zihang Zhou, Jian Zhou, Ying Guo, Ling Zhang and Duan Huang.

131 Continuous-variable quantum key distribution based on optical frequency comb

Yiyu Mao, Yijun Wang, Ying Guo, Ling Zhang and Duan Huang.

133 Blind modulation format identification based on machine learning for continuous variable quantum key distribution

Peng Liu, Hang Zhang, Ying Guo, Ling Zhang and Duan Huang.

135 Integrated photonic devices for measurement-device-independent quantum key distribution

Henry Semenenko, Philip Sibson, Chris Erven and Mark Thompson.

137 Filling schemes for quantum key pools in optical networks secured by quantum key distribution under single failure

Hua Wang, Yongli Zhao, Xiaosong Yu and Jie Zhang.

120 Quantum network entity authentication with a blind third party

Min-Sung Kang, Chang-Ho Hong, Yong-Su Kim, Sang-Wook Han and Sung Moon.

122 Selection of unitary operations in quantum secret sharing protocols without entanglement

Juan Xu, Jiabin Yuan, Jihao Fan and Dan Li.

124 Quantum byzantine agreement with continuous variable GHZ-like states

Yanyan Feng, Ronghua Shi and Ying Guo.

126 Phase noise estimation and suppression for continuous-variable quantum key distribution

Wei Zhao, Ying Guo, Hai Zhong, Ling Zhang and Duan Huang.

128 Continuous-variable quantum key distribution using orbital angular momenta

Di Jin, Ying Guo, Ling Zhang and Duan Huang.

130 Noise effects on entanglement distribution by separable Gaussian states

Fei Li, Jian Zhou, Yanyan Feng, Ronghua Shi and Ying Guo.

132 First continuous quadrature modulation for continuous-variable quantum key distribution

Fabian Laudenbach, Bernhard Schrenk, Christoph Pacher, Philip Walther and Hannes Hübel.

134 Feasibility of device-independent randomness expansion

Sammy Ragy, Peter Brown and Roger Colbeck.

136 QKD post processing in OpenCL built on top of the open source AIT QKD Software R10

Oliver Maurhart, Michael Hentschel, Ian Glendinning and Christoph Pacher.

139 A 42 GHz clock-rate source for entangled telecom photons

Fabian Laudenbach, Sophie Zeiger, Bernhard Schrenk, Christoph Pacher and Hannes Hübel.

141 Employing quantum cryptography for providing Byzantine fault tolerance

Evgeniy Kiktenko, Andrey Koziy and Aleksey Fedorov

143 Quantum money with verification by untrusted measurement devices

Karol Horodecki and Maciej Stankiewicz.

145 The madrid SDN-QKD network

Vicente Martin-Ayuso, Alejandro Aguado, Diego Lopez, Momtchil Peev, Victor Lopez, Antonio Pastor, Andreas Poppe, Hans Brunner, Stefano Bettelli, Fred Fung, David Hillerkuss, Lucian Comandar and Dawei Wang.

147 Secure critical infrastructures via QKD: the madrid QKD network

Vicente Martin-Ayuso, Alejandro Aguado, Diego Lopez, Victor Lopez-Alvarez, Antonio Pastor, Momtchil Peev, Andreas Poppe, Hans H. Brunner, Stefano Bettelli and Fred Fung.

149 Generalized spatial-mode detection efficiency mismatch in a free-space QKD system with Zernike polynomials

Poompong Chaiwongkhot, Katanya B. Kuntz, Jean-Philippe Bourgoin, Norbert Lutkenhaus, Vadim Makarov and Thomas Jennewein.

151 Laser damage attack against optical attenuators in quantum key distribution

Anqi Huang, Ruoping Li, Serguei Tchouragoulov, Vladimir Egorov and Vadim Makarov.

153 Performance analysis of satellite-based quantum key distribution

Hao Qin, Haoze Chen and Jimin Nie.

138 Quantum state redistribution with local coherence

Anurag Anshu, Rahul Jain and Alexander Streltsov.

140 Compressive sensing based channel parameter estimation for continuous-variable quantum key distribution

Zhe He, Yu Su, Ling Zhang, Ying Guo, Guihua Zeng and Duan Huang.

142 Finite-key analysis for memory-assisted decoy-state quantum key distribution

Guillermo Curras Lorenzo and Mohsen Razavi.

144 An approximation method for analysis and design of multi-edge type LDPC codes

Hossein Mani, Tobias Gehring, Christoph Pacher and Ulrik Lund Andersen.

146 Correlations with on-chip detection for continuous-variable QKD

Luis Trigo Vidarte, Mauro Persechino, Eleni Diamanti and Philippe Grangier.

148 Feasibility study of satellite continuous-variable QKD

Daniele Dequal, Eleni Diamanti and Luis Trigo Vidarte.

150 States preparation and calibration for polarization encoding QKD scheme

Alexander Duplinskiy, Vasiliy Ustimchik, Alan Kanapin, Vladimir Kurochkin and Yury Kurochkin.

152 Finite-Key Analysis for Quantum-Classical Access Networks with Hybrid Links

Osama Elmabrok, Sima Bahrani, Guillermo Curras Lorenzo and Mohsen Razavi.

Gold Sponsors

量子网络
CAS QUANTUMNET

国盾量子
QuantumCTek

Silver Sponsors

Baidu 百度

赋同科技
PHOTEC

Alibaba Group
阿里巴巴集团

Tencent 腾讯

Quantum union

JIQT

UNIVERSITY OF
CAMBRIDGE

Bronze Sponsors

IDQ

IOP Publishing

SPARK
您身边的仪器顾问

etsc 东隆科技
ETSC Technologies Co., Ltd

KEYSIGHT
TECHNOLOGIES

国耀量子雷达
GLORY CHINA QUANTUM LIDAR

RMY
润铭宇

Optowide 腾景科技