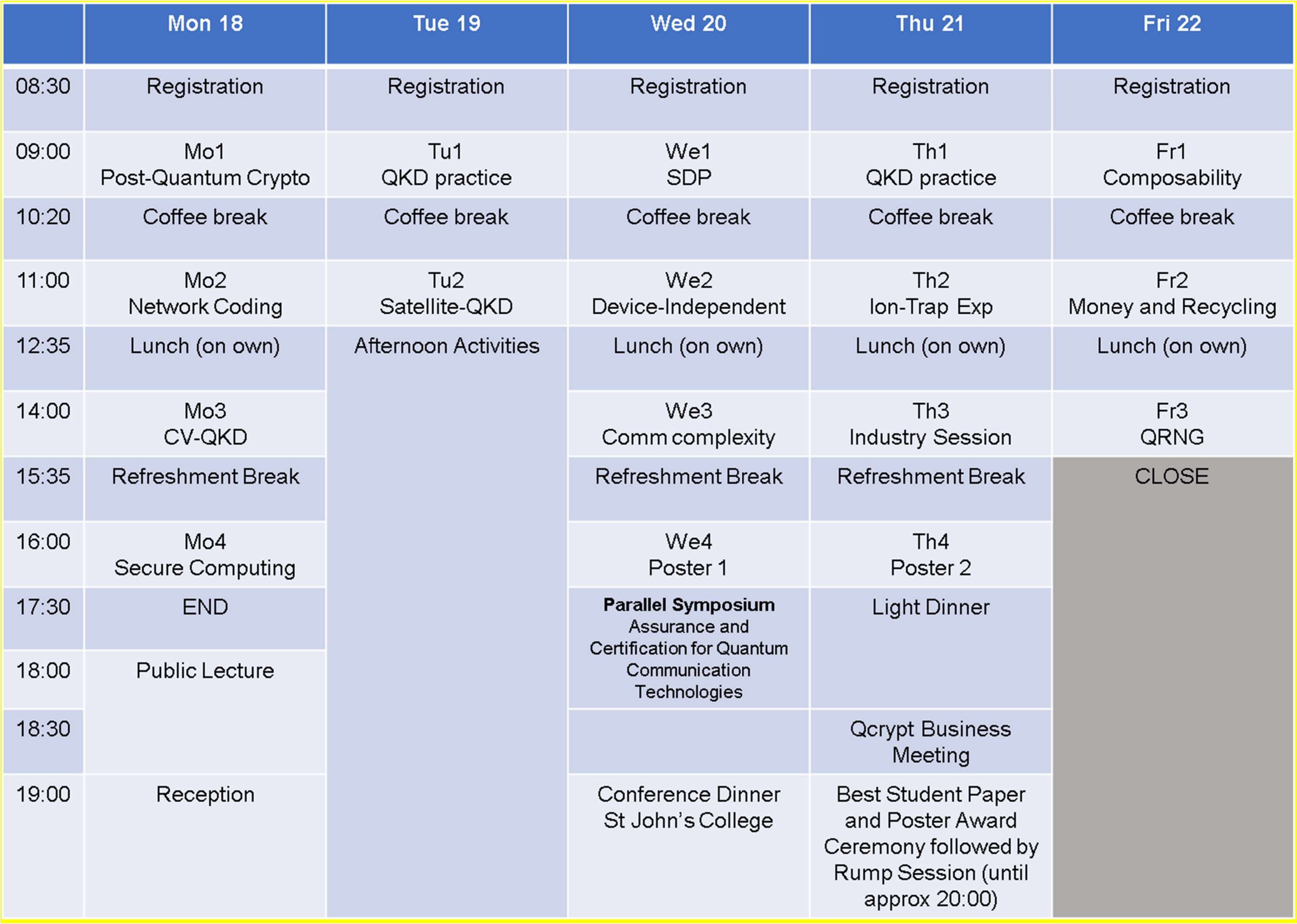
QCrypt 2017

Cambridge, UK

18-22 September 2017

UNIVERSITY OF CAMBRIDGE

QUANTUM COMMUNICATIONS HUB



	Mon 18	Tue 19	Wed 20	Thu 21	Fri 22
08:30	Registration	Registration	Registration	Registration	Registration
09:00	Mo1 Post-Quantum Crypto	Tu1 QKD practice	We1 SDP	Th1 QKD practice	Fr1 Composability
10:20	Coffee break	Coffee break	Coffee break	Coffee break	Coffee break
11:00	Mo2 Network Coding	Tu2 Satellite-QKD	We2 Device-Independent	Th2 Ion-Trap Exp	Fr2 Money and Recycling
12:35	Lunch (on own)	Afternoon Activities	Lunch (on own)	Lunch (on own)	Lunch (on own)
14:00	Mo3 CV-QKD		We3 Comm complexity	Th3 Industry Session	Fr3 QRNG
15:35	Refreshment Break		Refreshment Break	Refreshment Break	CLOSE
16:00	Mo4 Secure Computing		We4 Poster 1	Th4 Poster 2	
17:30	END		**Parallel Symposium** Assurance and Certification for Quantum Communication Technologies	Light Dinner	
18:00	Public Lecture				
18:30				Qcrypt Business Meeting	
19:00	Reception		Conference Dinner St John's College	Best Student Paper and Poster Award Ceremony followed by Rump Session (until approx 20:00)	

Dear QCrypt Attendee

Welcome to QCrypt 2017, the 7th International Conference on Quantum Cryptography. This is the first time that QCrypt is being held in the UK, though of course it has been held several times in Europe before. Autumn is one of the nicest times of the year in Cambridge (if it isn't raining) and we hope you enjoy your time in our beautiful and historic city.

The aim of the conference is to share the most important results in quantum cryptography and to act to help build the research community. It encourages the mixing of theoreticians and experimentalists, mathematicians, physicists and engineers. To help us achieve this aim in 2017, we have 4 tutorial papers, 8 invited papers, 31 oral papers and an amazing 160 posters. At the time of writing we also have over 300 registrants. So it would seem that the conference is doing its job.

Quantum technology is becoming an increasingly hot topic. For instance, the UK government is investing £270 million in the UK National Quantum Technologies Programme to bring quantum out of the lab into the market over a 20 year lifetime. It aims to create a coherent government, industry and academic quantum technology community to help develop and support the emerging new quantum technology markets. Other initiatives are taking place around Europe and the world. Hence it is exciting to see how the quantum cryptography research community is growing and maturing.

This conference is being organised by the University of Cambridge and the University of York, both of whom are members of the Quantum Communications Hub. The QComm hub aims to deliver quantum encryption systems that will in turn enable secure transactions and transmissions of data across a range of users in real-world applications: from government agencies and industrial set-ups to commercial establishments and the wider public. It is a partnership of eight UK universities as well as companies and public sector bodies.

Of course, additionally there has been a great deal of help from a wide variety of sources. I would very much like to thank the QCrypt steering and programme committees for their hard work, in particular Christian Schaffner who has proved such a dedicated link between these committees and the local organisers. I'd also like to thank the members of the student travel committee and Norbert Lütkenhaus for organising the industry session. Finally I would like to thank my colleagues at the Universities of Cambridge and York (particularly Adrian Wonfor for organising the venue, the ticketing and the IT, Victoria Barrett for the tours and other logistics and Klitos Andrea for the sponsorship), our student helpers, our colleagues in the Cavendish and Toshiba Research Europe for helping in the lab tour, as well as others who have provided facilities and services to the conference.

I hope you have a fascinating and enjoyable QCrypt 17.

Richard Penty
Local Organising Committee Chair

Tutorial Speakers

Christopher Portmann (ETH Zurich)
Composability in Quantum Cryptography

Andrew Shields (Toshiba Research Europe, Cambridge)
Core and access QKD networks

Jamie Sikora (CQT)
Semi-definite programming in quantum cryptography

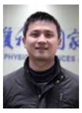
Douglas Stebila (McMaster University)
Practical post-quantum key exchange

Invited Speakers

Koji Azuma (NTT)
Quantum Network Coding

Anthony Leverrier (INRIA Paris)
Theoretical challenges of CV quantum cryptography

Morgan Mitchell (ICFO)
Integrated quantum random number generator chip



Chengzhi Peng (USTC)
Satellite-Based QKD

Valerio Scarani (CQT)
Self-testing

Wolfgang Tittel (University of Calgary)
Quantum teleportation across a metropolitan fibre network

Dave Touchette (University of Waterloo)
Quantum information complexity

Ian Walmsley (University of Oxford)
Advances in ion trap quantum computers and photonic links

Public Lecture

Simon Singh
The History of Secrecy
Simon Singh, author of The Code Book, looks at the history of codes and codebreaking over the last thousand years. The lecture will start with ancient codes, include a demonstration of a genuine Enigma cipher machine and end with a quick introduction to quantum cryptography.

After completing a PhD in particle physics at Cambridge, Simon Singh became a film-maker and science writer. His other books include Fermat's Last Theorem and Big Bang.

Committees

Program committee

- Gorjan Alagic (University of Copenhagen)
- Erika Andersson (Heriot-Watt University)
- Rotem Arnon-Friedman (ETH Zurich)
- Charles Ci Wen Lim (National University of Singapore)
- Roger Colbeck (University of York)
- Ivo Pietro Degiovanni (INRIM Turin)
- Dirk Englund (Massachusetts Institute of Technology)
- Ivette Fuentes (University of Vienna)
- Stacey Jeffery (CWI Amsterdam)
- Elham Kashefi (University of Edinburgh and UPMC CNRS)
- Hari Krovi (Raytheon BBN, Cambridge, Massachusetts)
- Nicola Laurenti (University of Padova)
- Anthony Leverrier (INRIA Paris)
- Marco Lucamarini (Toshiba Cambridge)
- Mohsen Razavi (University of Leeds)
- Hiroki Takesue (NTT)
- Marco Tomamichel (University of Technology Sydney)
- Dominique Unruh (University of Tartu)
- Thomas Vidick (California Institute of Technology) **(chair)**
- Paolo Villoresi (University of Padova) **(vice chair)**
- Christian Weedbrock (CipherQ)
- Feihu Xu (Massachusetts Institute of Technology)
- Hugo Zbinden (University of Geneva)

Steering committee

- Anne Broadbent (University of Ottawa)
- Marcos Curty (University of Vigo)
- Eleni Diamanti (CNRS, Univ Pierre et Marie Curie)
- Yi-Kai Liu (NIST / University of Maryland)
- Norbert Lütkenhaus (IQC, University of Waterloo)
- Masahide Sasaki (NICT)
- Christian Schaffner (University of Amsterdam, CWI, QuSoft) **(chair)**
- Qiang Zhang (University of Science and Technology of China)

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)

Industry Session organiser

- Norbert Lütkenhaus (IQC, University of Waterloo)

Rump Session chairs

- Charles H. Bennett (IBM Research)
- Gilles Brassard (Université de Montréal)

Local Organizing committee

- Richard Penty (University of Cambridge)
- Adrian Wonfor (University of Cambridge)
- Victoria Barrett (University of Cambridge)
- Klitos Andrea (York University
- Georgia Mortzou (York University)

Practical Information

Registration desk opening times

Monday	0830-1230	1330-1630
Tuesday	0830-1230	
Wednesday	0830-1230	1330-1630
Thursday	0830-1230	1330-1630
Friday	0830-1230	

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:	80 minutes plus 10 minutes questions

Poster Details

The available space for posters is 1160mm wide x 900mm high (A0 landscape).

Please put up your poster in poster room in the numbered location associated with your paper before your session begins. Please remove at the end of the session. Fixing materials will be provided.

Student Paper and Poster Prizes

The best student paper will be chosen by members of the Steering and Program Committee. However, all conference attendees can vote for the best poster in each of the two poster sessions. Please place your vote in the ballot box in the poster room by the end of each session. The three prizes will be presented at the beginning of the rump session on Thursday evening

Tuesday Afternoon Tours

Bletchley Park Tour	Meet in West Road park at 1pm for coach pick up. A packed sandwich lunch is provided – please exchange the lunch ticket for this.
Punting on the River Cam	Meet in West Road reception at 2pm to walk to punt station on river. The punt tour is guided but feel free to hire a punt afterwards if you want to give it a go yourself
Cambridge Bus Tour	Meet in West Road reception at 2pm to walk to Silver Street pick up point. This is a “hop on – hop off” tour and the tickets are valid all day.
Laboratory Tour, West Cambridge Site	Meet in West Road reception at 1.45pm to walk to West Cambridge Site. The tour will last approximately 2 hours.

Conference Dinner

Tickets for the dinner will be provided with your welcome pack at registration if you have paid for registration including the dinner. The dinner will take place in St John’s College (https://www.joh.cam.ac.uk/maps-directions). This is one of the earliest Colleges at Cambridge, founded in 1511 by the mother of King Henry VII, so it promises to be a very special location. Please go to the porters’ lodge and there should be signage to direct you. At 7pm there will be a drinks reception and dinner will commence at 7.30pm in the ancient college hall. The after dinner speaker will be Sir Peter Knight, who is Senior Fellow in Residence at the Kavli Royal Society International Centre at Chicheley Hall and Emeritus Professor of Quantum Optics at Imperial College, a member of the Quantum Technology Strategic Advisory Board and a continuing adviser to the UK government on science matters.

Monday 18th September

09:00 – 10:20 Session Mo1	**Post-Quantum Crypto (Chair Masahide Sasaki)**
09:00 – 10:20 Mo1	**Practical post-quantum key exchange (tutorial)** Douglas Stebila McMaster University

COFFEE BREAK

11:00 – 12:35 Session Mo2	**Network Coding (Chair Mohsen Razavi)**
	Quantum Network Coding (invited) Koji Azuma NTT
11:35 Mo22	**Multi-path multi-flow entanglement routing in a quantum network** Mihir Pant, Hari Krovi, Don Towsley, Leandros Tassiulas, Liang Jiang, Prithwish Basu, Dirk Englund and Saikat Guha.
11:55 Mo23	**Realistic parameter regimes for a single sequential quantum repeater** Filip Rozpedek, Kenneth Goodenough, Jeremy Ribeiro, Norbert Kalb, Valentina Caprara Vivoli, Andreas Reiserer, Ronald Hanson, Stephanie Wehner and David Elkous
12:15 Mo24	**Networked Quantum-Secured Communications with Hand-held and Integrated Devices: Bristol's Activities in the UK Quantum Communications Hub** Philip Sibson, David Lowndes, Stefan Frick, Alasdair Price, Henry Semenenko, Francesco Raffaelli, Dan Llewellyn, Jake Kennard, Yanni Ou, Fotini Ntavou, Emilio Hugues-Salas, Andy Hart, Richard Collins, Anthony Laing, Chris Erven, Reza Nejabati, Dimitra Simeonidou, Mark Thompson and John Rarity

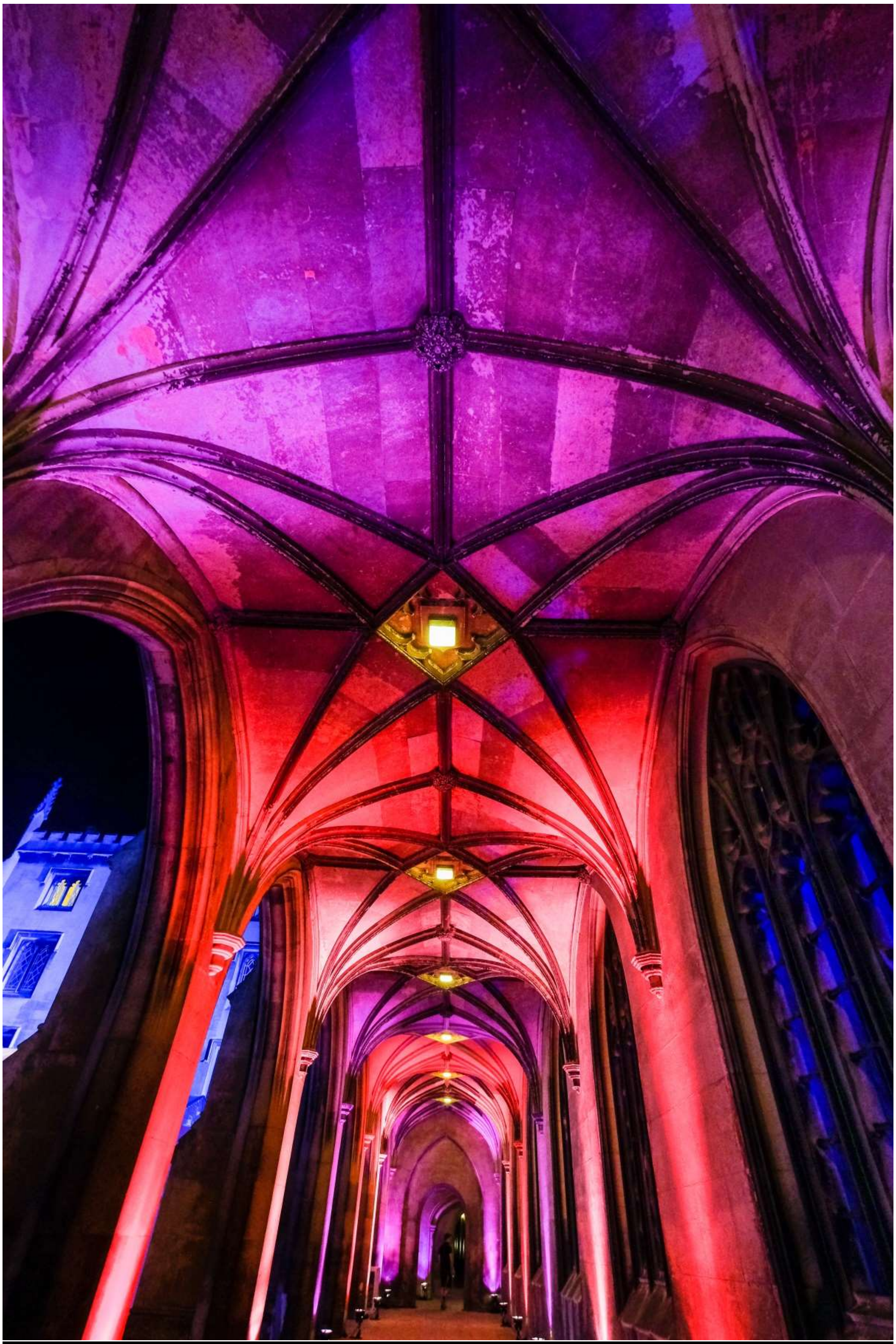
LUNCH BREAK (ON YOUR OWN)

14:00 – 15:35 Session Mo3	**CV-QKD (Chair Hari Krovi)**
14:00 Mo31	**Theoretical challenges of CV quantum cryptography (invited)** Anthony Leverrier INRIA Paris
14:35 Mo32	**Reliable numerical key rates for quantum key distribution** Patrick Coles, Adam Winick and Norbert Lutkenhaus.
14:55 Mo33	**Pilot-Disciplined CV-QKD with True Local Oscillator** Fabian Laudenbach, Bernhard Schrenk, Christoph Pacher, Roland Lieger, Edwin Querasser, Gerhard Humer, Michael Hentschel, Hannes Hübel, Chi-Hang Fred Fung, Andreas Poppe and Momtchil Peev
15:15 Mo34	**Experimental demonstration of the differential quadrature phase shift protocol** George Roberts, Marco Lucamarini, James Dynes, Seb Savory, Zhiliang Yuan and Andrew Shields

COFFEE BREAK

16:00 – 17:40 Session Mo4	**Secure Computing (Chair Thomas Vidick)**
16:00 Mo41	**Limitations on Transversal Computation through Quantum Homomorphic Encryption** Michael Newman and Yaoyun Shi
16:20 Mo42	**Quantum Fully Homomorphic Encryption With Verification** Gorjan Alagic, Yfke Dulek, Christian Schaffner and Florian Speelman
16:40 Mo43	**On the implausibility of classical client blind quantum computing** Scott Aaronson, Alexandru Cojocaru, Alexandru Gheorghiu and Elham Kashefi.
17:00 Mo44	**Quantum Tokens for Digital Signatures** Shalev Ben-David and Or Sattath

17:20 Mo45	**Reconfigurable network for quantum digital signatures mediated by measurement-device-independent quantum key distribution** George L. Roberts, Marco Lucamarini, Zhiliang Yuan, James Dynes, Lucian Comandar, Andrew W. Sharpe, Andrew Shields, Marcos Curty, Ittoop V. Puthoor and Erika Andersson



Tuesday 19th September

09:00 – 10:20 Session Tu1	QKD Practice (Chair Marcos Curty)
09:00 – 10:20 Tu1	**Core and access QKD networks (tutorial)** Andrew Shields Toshiba Research Europe, Cambridge

COFFEE BREAK

11:00 – 12:35 Session Tu2	Satellite QKD (Chair Qiang Zhang)
11:00 Tu21	**Satellite-Based QKD (invited)** Chengzhi Peng USTC
11:35 Tu22	**Drone-based Quantum Key Distribution** Alexander Hill, Joseph Chapman, Kyle Herndon, Christopher Chopp, Daniel Gauthier and Paul Kwiat
11:55 Tu23	**Handheld Quantum Key Distribution** Peter Freiwang, Gwenaelle Mélen, Jannik Luhn, Tobias Vogl, Markus Rau, Clemens Sonnleitner, Wenjamin Rosenfeld and Harald Weinfurter
12:15 Tu24	**Measurement-device-independent quantum key distribution in practical scenarios** Chao Wang, Wei Chen, Fang-Xiang Wang, Yu-Yang Ding, Yong-Jun Qian, Shuang Wang, Zhen-Qiang Yin, Guang-Can Guo, and Zheng-Fu Han

LUNCH BREAK (ON YOUR OWN)

Free Afternoon	Activities
1pm	**Bletchley Park Tour.** Meet in West Road park at 1pm for coach pick up.
1.45pm	**Laboratory Tour, West Cambridge Site.** Meet in West Road reception at 1.45pm to walk to West Cambridge Site.
2pm	**Punting on the River Cam.** Meet in West Road reception at 2pm to walk to punt station on river.
2pm	**Cambridge Bus Tour.** Meet in West Road reception at 2pm to walk to Silver Street pick up point.

Wednesday 20th September

09:00 – 10:20 Session We1	**SDPs (Chair TBC)**
09:00 We11	**Semi-definite programming in quantum cryptography (tutorial)** Jamie Sikora CQT

COFFEE BREAK

11:00 – 12:35 Session We2	**Device-Independent (Chair Marco Lucamarini)**
11:00 We21	**Self-testing (invited)** Valerio Scarani
11:35 We22	**A semi-device-independent framework based on natural physical assumptions and its application to random number generation** Thomas Van Himbeeck, Erik Woodhead, Nicolas Cerf, Raul Garcia-Patron Sanchez and Stefano Pironio
11:55 We23	**Post-Quantum Security of Fiat-Shamir** Dominique Unruh.
12:15 We24	**Post-quantum security of the sponge construction** Jan Czajkowski, Leon Groot Bruinderink, Andreas Hülsing, Christian Schaffner and Dominique Unruh

LUNCH BREAK (ON YOUR OWN)

14:00 – 15:35 We3	**Comm complexity (Chair TBC)**
14:00 We31	**Quantum information complexity (invited)** David Touchette University of Waterloo
14:35 We32	**Provably secure key establishment against quantum adversaries** Aleksandrs Belovs, Gilles Brassard, Peter Høyer, Marc Kaplan, Sophie Laplante and Louis Salvail.
14:55 We33	**One-Shot Private Classical Capacity of Quantum Wiretap Channel: Based on one-shot quantum covering lemma** Jaikumar Radhakrishnan, Pranab Sen and Naqueeb Warsi
15:15 We34	**Computational Notions of Quantum Min-Entropy** Yi-Hsiu Chen, Kai-Min Chung, Ching-Yi Lai, Salil Vadhan and Xiaodi Wu

COFFEE BREAK

16:00 – 17:30 Session We4	**Poster Session 1**
We401	**Wireless Access to Quantum Networks** Osama Elmabrok, Masoud Ghalaii and Mohsen Razavi
We402	**Light Source Monitoring in Quantum Key Distribution with Photon Number Resolving Detector at Room Temperature** Gan Wang, Zhengyu Li, Ziyang Chen, Yucheng Qiao and Hong Guo
We403	**Double-port pumped time-bin entangled photon pair generation using Si ring resonator** Mikio Fujiwara, Ryota Wakabayashi, Masahide Sasaki and Masahiro Takeoka
We404	**Continuous-variable quantum key distribution using coherent polarization state discretely modulated by an intrinsically stable polarization-modulated unit** Linxi Hu, Yuanjia Wang, Jindong Wang and Guangqiang He
We405	**Environmental symmetries and channel classification for secure quantum communication** Davide Nuzzi, Gabriele Baldi, Paola Verrucchi and Alessandro Cuccoli
We406	**Entropy source evaluation of a vacuum fluctuation based quantum random number generator** Arne Kordts, Dino Solar Nikolic, Tobias Gehring, Ulrik Lund Andersen, Cosmo Lupo and Thomas Brochmann Pedersen
We407	**Experimental detection of steerability for Bell-local states with two measurement settings** Adeline Orieux, Marc Kaplan, Vivien Venuti, Tanumoy Pramanik, Isabelle Zaquine and Eleni Diamanti
We408	**On the problem of non-zero word error rates for fixed-rate error correction codes in continuous variable quantum key distribution** Sarah Johnson, Andrew Lance, Lawrence Ong, Mahyar Shirvanimoghaddam, Timothy Ralph and Thomas Symul
We409	**Effect of atmospheric turbulence on spatial-mode detector efficiency mismatch** Poompong Chaiwongkhot, Katanya Kuntz, Anqi Huang, Jean-Philippe Bourgoin, Shihan Sajeed, Norbert Lutkenhaus, Thomas Jennewein and Vadim Makarov
We410	**Quantum coin hedging, and a counter measure** Maor Ganz and Or Sattath
We411	**Investigating feasibility of broadband continuous variable quantum key distribution in telecom fibers with local local oscillator** Nitin Jain, Christian Jacobsen, Dino Solar Nikolic, Arne Kordts, Cosmo Lupo, Ruben Grigoryan, Tobias Gehring, Ulrik Andersen, Thomas Pedersen and Stefano Pirandola
We412	**Hybrid quantum cryptography: everlasting security with performances beyond QKD** Romain Alleaume
We413	**Experimental Continuous-Variable Oblivious Transfer** Tobias Gehring, Fabian Furrer, Christian Schaffner, Christoph Pacher, Roman Schnabel and Stephanie Wehner
We414	**Classical-Noise-Suppressed Quantum Random Number Generator Based On Phase Noise** Ziyang Chen, Zhengyu Li, Yulong Feng, Gan Wang and Hong Guo
We415	**Continuous-variable measurement-device-independent multipartite quantum communication** Guangqiang He and Ya-Dong Wu
We416	**High speed time-domain balanced homodyne detector** Yongmin Li, Shanna Du, Zongyang Li, Wenyuan Liu and Xuyang Wang
We417	**Reference pulse attack on continuous variable quantum key distribution with local local oscillator** Shengjun Ren, Rupesh Kumar, Adrian Wonfor, Xinke Tang, Richard Penty and Ian White

We418	**CubeSat detector assembly for investigating in-orbit mitigation of radiation damage** Nigar Sultana, Jin Gyu Lim, Jean-Philippe Bourgoin, Vadim Makarov and Thomas Jennewein
We419	**Security of counterfactual communication** Lev Vaidman
We420	**State comparison amplification of optical quantum coherent states** Ross Donaldson, Luca Mazzarella, Robert Collins, John Jeffers and Gerald Buller
We421	**Experimental DPTS protocol over 170 km fiber-based link** Davide Bacco, Beatrice Da Lio, Daniele Cozzolino, Yunhong Ding, Kjeld Dalgaard, Karsten Rottwitt and Leif Oxenløwe
We422	**Maintaining quantum-secured blockchain with urban fiber quantum key distribution network** Evgenii Kiktenko, Nikolay Pozhar, Maxim Anufriev, Anton Trushechkin, Ruslan Yunusov, Yuriy Kurochkin, Alexander Lvovsky and Aleksey Fedorov
We423	**Decentralized Routing and Diameter Bounds in Entangled Quantum Networks** Laszlo Gyongyosi
We424	**Quantum Communications Network Based on Polarization Entanglement at Telecom Wavelength** Soeren Wengerowsky, Siddarth Koduru Joshi, Fabian Steinlechner, Hannes Huebel, Anton Zeilinger and Rupert Ursin
We425	**Practical noise models for CV-QKD implementations** Fabian Laudenbach, Christoph Pacher, Fred Fung, Momtchil Peev, Andreas Poppe and Hannes Hübel
We426	**Quantum Anonymous Veto Protocol** Ramij Rahaman and Guruprasad Kar
We427	**A hierarchical modulation coherent communication scheme for simultaneous four-state continuous-variable quantum key distribution and classical communication** Can Yang, Cheng Ma, Linxi Hu and Guangqiang He
We428	**Hyperentangled Time-bin and Polarization QKD for Space Applications** Joseph Chapman, Charles Ci Wen Lim, Christopher Zeitler and Paul Kwiat
We429	**The Quantum Cut-and-Choose Technique and Quantum Two-Party Computation** Elham Kashefi, Luka Music and Petros Wallden
We430	**Decoy state quantum key distribution with imperfect sourceEnhancing performance and security of practical quantum communication using quantum frequency conversion** Anqi Huang, Shi-Hai Sun, Zhihong Liu and Vadim Makarov
We431	**Enhancing performance and security of practical quantum communication using quantum frequency conversion** Nitin Jain, Paritosh Manurkar, Prem Kumar and Gregory Kanter
We432	**Quantum key distribution with an efficient countermeasure against intensity fluctuations in optical pulses** Ken-Ichiro Yoshino, Mikio Fujiwara, Kensuke Nakata, Tatsuya Sumiya, Toshihiko Sasaki, Masahiro Takeoka, Masahide Sasaki, Akio Tajima, Masato Koashi and Akihisa Tomita
We433	**Secure decoy-state quantum key distribution with calibration of unknown light sources** Masahiro Kumazawa, Toshihiko Sasaki and Masato Koashi
We434	**Towards high-dimensional entanglement-based quantum communication in free space** Sebastian Ecker, Fabian Steinlechner, Matthias Fink, Bo Liu, Jessica Bavaresco, Marcus Huber, Thomas Scheidl and Rupert Ursin
We435	**Ultrafast and passive source-device-independent Quantum Random Number Generator**Marco Avesani, Davide Marangon, Giuseppe Vallone and Paolo Villoresi
We436	**Can we have a secure Quantum network?** Mohammad Al-Amri, Zhenghong Li, Xihua Yang and M. Suhail Zubairy

We437	**The development of accurate measurements to provide assurance for QKD technologies**Christopher Chunnilall, Robert Kirkwood, Pravin Patel and Alastair Sinclair
We438	**Quantum Cryptography with Weak Measurements** James Troupe and Jacob Farinholt
We439	**Teleportation Simulation of non-Pauli Channels** Thomas Cope, Leon Hetzel, Leonardo Banchi and Stefano Pirandola
We440	**Information-theoretic security proof of differential-phase-shift quantum key distribution protocol based on complementarity** Akihiro Mizutani, Toshihiko Sasaki, Go Kato, Yuki Takeuchi and Kiyoshi Tamaki
We441	**Quantum-Enhanced Physical Layer Cryptography: A new paradigm for free-space key distribution**
We442	**Quantum-Classical Transmission on Single Wavelength** Bruno Huttner and Matthieu Legre
We443	**The Engineering of a Scalable Multi-Site Communications System Utilizing QKD** Piotr K. Tysowski, Xinhua Ling, Norbert Lutkenhaus and Michele Mosca
We444	**Optimal attacks on Quantum Key Recycling with qubits** Daan Leermakers and Boris Skoric
We445	**Multicarrier Continuous-Variable Quantum Key Distribution** Laszlo Gyongyosi
We446	**Short pulse attack on continuous-variable quantum key distribution system** Hao Qin, Anqi Huang and Vadim Makarov
We447	**Low-Cost Single-Laser Differential Phase Shift Transmitter Towards SFP-based QKD Tail-End Optics** Michael Hentschel, Bernhard Schrenk, Roland Lieger, Edwin Querasser and Hannes Hübel
We448	**Path Entangled Quantum Networks** Rob Thew
We449	**High-precision phase compensation for continuous-variable quantum key distribution with feedback optimization technique** Yingming Zhou, Weiqi Liu, Tao Wang, Peng Huang and Guihua Zeng
We450	**Correlations with on-chip detection and modulation for CVQKD** Mauro Persechino, Luis Trigo Vidarte, Melissa Ziebell and Paul Crozat
We451	**Long term test of a fast and compact Quantum Random Number Generator** Davide G. Marangon, Alan Plews, Marco Lucamarini, James Dynes, Andrew Sharpe, Zhiliang Yuan and Andrew Shields
We452	**Post-Quantum Elliptic Curve Cryptography** Vladimir Soukharev
We453	**QKD network on mixed encoding schemes** Evgeny Kiktenko, Nikolay Pozhar, Maxim Anufriev, Alexander Duplinsky, Alan Kanapin, Alexander Miller, Vadim Rodimin, Alexander Sokolov, Vasily Ustimchik, Sergey Vorobey, Anton Losev, Anton Trushechkin, Aleksey Fedorov, Vladimir Kurochkin and Yury Kurochkin
We454	**Security proof of quantum key distribution with detection-efficiency mismatch** Yanbao Zhang, Patrick Coles, Adam Winick and Norbert Lutkenhaus
We455	**Almost tight lower bounds for 1-out-of-2 quantum oblivious transfer** Ryan Amiri, Petros Wallden and Erika Andersson
We456	**Finite-key Security Analysis of Quantum Key Distribution with Information Leakage** Weilong Wang and Marcos Curty
We457	**Challenges for a DIQKD implementation** Gláucia Murta, Suzanne van Dam, Jérémy Ribeiro, Ronald Hanson and Stephanie Wehner
We458	**MDI-DPS-QKD utilizing QSS setup** Muataz Alhussein and Kyo Inoue

We459	**Quantum Digital Signatures Transmitted Over a Channel Loss Equivalent to 134 km** Robert Collins, Ryan Amiri, Mikio Fujiwara, Toshimori Honjo, Kaoru Shimizu, Kiyoshi Tamaki, Masahiro Takeoka, Ross Donaldson, Masahide Sasaki, Erika Andersson and Gerald Buller
We460	**Amorphous MoSi SNSPDs with a low time jitter and a high detection efficiency** Misael Caloz, Boris Korzh, Claire Autebert, Nuala Timoney, Matthieu Perrenoud, Markus Weiss, Christian Schönenberger, Richard Warburton, Hugo Zbinden and Félix Bussières
We461	**Fibre characterisation for quantum key distribution field trials** Zhihao Liu and Hanwu Chen
We462	**Improvement of Controlled Bidirectional Quantum Secure Direct Communication Network Using Classical XOR Operation and Quantum Entanglement** Zhihao Liu and Hanwu Chen
We463	**Practical Security of Continuous-Variable Quantum Key Distribution with Imperfect Random Basis-Choice Operations** Weiqi Liu, Yingming Zhou, Jinye Peng, Peng Huang and Guihua Zeng
We464	**Numerical evidence for bound secrecy from two-way postprocessing in quantum key distribution** Sumeet Khatri and Norbert Lutkenhaus
We465	**Asynchronous continuous-variable quantum key distribution against practical attacks** Peng Huang, Tao Wang and Guihua Zeng
We466	**Continuous variable quantum key distribution protocol with photon subtraction at receiver** Kyongchun Lim, Changho Suh and June-Koo Kevin Rhee
We467	**An On-chip Homodyne Detector for Generating Quantum Random Numbers and Measuring Coherent States** Francesco Raffaelli, Giacomo Ferranti, Dylan Mahler, Philip Sibson, Jake Kennard, Alberto Santamato, Gary Sinclair, Damien Bonneau, Mark Thompson and Jonathan Matthews
We468	**Low-noise, low-complexity CV-QKD architecture** Hans H. Brunner, Lucian C. Comandar, Fotini Karinou, Stefano Bettelli, David Hillerkuss, Fred Fung, Dawei Wang, Spiros Mikroulis, Maxim Kuschnerov, Andreas Poppe, Changsong Xie and Momtchil Peev
We469	**Gigahertz quantum signatures compatible with telecommunication technologies** Matthew Thornton, Callum Croal, Imran Khan, Christoph Marqurdt, Gerd Leuchs and Natalia Korolkova
We470	**A novel long-distance continuous-variable quantum key distribution scheme with state-discrimination receiver and non-Gaussian operation** Qin Liao, Ying Guo, Duan Huang, Peng Huang and Guihua Zeng
We471	**Coherence lifetime of chalcogenide glasses for quantum memory applications** Stuart Gray, Jun Yang, Bruce Aitken and Daniel Nolan
We472	**Three-observer Bell inequality violation on a two-qubit entangled state** Matteo Schiavon, Luca Calderaro, Mirko Pittaluga, Giuseppe Vallone and Paolo Villoresi
We473	**Practical security for subcarrier wave quantum key distribution against collective beam-splitting attack.** Anton Kozubov, Andrei Gaidash, George Miroshnichenko, Dmitri Horoshko and Arthur Gleim
We474	**High-Rate Quantum Key Distribution with Time-Bin Qudits** Daniel Gauthier, Nurul Islam, Charles Lim, Jungsang Kim and Clinton Cahall
We475	**Randomness amplification using independent devices arbitrarily correlated with the Santha-Vasirani source** Maciej Stankiewicz
We476	**Quantum Key Distribution as a Service** Joo Yeon Cho, Thomas Szyrkowiec and Helmut Griesser
We477	**Exploiting no-Signalling Extremal Distributions to find Bell Inequalities** Thomas Cope and Roger Colbeck

We478	**Position-Based Quantum Cryptography for Multi-located Prover and Single Verifier** Sarah Noles and Abhishek Parakh
We479	**A 5.4 Gbps real time quantum random number generator with simple implementation** Jie Yang, Jinlu Liu, Qi Su, Fan Fan and Bingjie Xu
We480	**Continuous-Variable Quantum Key Distribution Enhanced by Quantum Scissors** Masoud Ghalaii, Rupesh Kumar, Carlo Ottaviani, Stefano Pirandola and Mohsen Razavi

Thursday 21st September

09:00 – 10:20 Session Th1	QKD practice (Chair Eleni Diamanti)
09:00 Th11	**Quantum teleportation across a metropolitan fibre network (invited)** Wolfgang Tittel University of Calgary
09:35 Th12	**10Mb/s quantum key distribution** Zhiliang Yuan, Alan Plews, Ririka Takahashi, Kazuaki Doi, Winci Tam, Andrew Sharpe, Alexander Dixon, Evan Lavelle, James Dynes, Akira Murakami, Marco Lucamarini, Yoshimichi Tanizawa, Hideaki Sato and Andrew Shields Toshiba
09:55 Th13	**An efficient countermeasure against correlated intensity fluctuations in optical pulses on high-speed decoy BB84 QKD systems** Akihisa Tomita, Ken-Ichiro Yoshino, Mikio Fujiwara, Tatsuya Sumiya, Toshihiko Sasaki, Kensuke Nakata, Akio Tajima, Masato Koashi, Masahiro Takeoka and Masahide Sasaki

COFFEE BREAK

11:00 – 12:35 Session Th2	Ion-Trap Experiments (Chair Paolo Villoresi)
11:00 Th21	**Advances in ion trap quantum computers and photonic links (invited)** Ian Walmsley University of Oxford
11:35 Th22	**Entanglement distillation between solid-state quantum network nodes** Norbert Kalb, Andreas Reiserer, Peter Humphreys, Jacob Bakermans, Sten Kamerling, Naomi Nickerson, Simon Benjamin, Daniel Twitchen, Matthew Markham and Ronald Hanson
11:55 Th23	**Quantum key distribution over multicore fiber based on silicon photonics** Yunhong Ding, Davide Bacco, Kjeld Dalgaard, Xinlun Cai, Xiaoqi Zhou, Karsten Rottwitt and Leif Oxenløwe
12:15 Th24	**The European Coordinated Effort to develop the Metrology for Quantum-Cryptography** Ivo Pietro Degiovanni, Stefan Kueck, Geiland Porrovecchio, Ivano Ruo-Berchera, Christopher J. Chunnilall, Marco Gramegna, Toomas Kubarsepp, Andrei Pokatilov, Farshid Manoocheri and Aigar Vaigu

LUNCH BREAK (ON YOUR OWN)

14:00 – 15:30 Session Th3	Industry Session (Chair Norbert Lutkenhaus)
14:00 Th31	**What is BT doing with QKD?** Andrew Lord BT Labs
14:15 Th32	**Standards for Quantum Random Number Generators** Bruno Huttner IDQuantique
14:30 Th33	**Panel Discussion**

COFFEE BREAK

16:00 – 17:30 Session Th4	Poster Session 2
Th401	**Thermal quantum cryptography: Solutions at the microwave regime** Carlo Ottaviani, Cosmo Lupo and Stefano Pirandola
Th402	**Backflash as a security threat for quantum key distribution: quantification and protection** Ivo Pietro Degiovanni, Alice Meda, Giorgio Brida, Marco Genovese, Alberto Tosi and Zhiliang L Yuan
Th403	**Analysis of modulation parameters inequality in subcarrier wave quantum communication and its application to countering unambiguous state discrimination attack** Andrei Gaidash, Anton Kozubov, Vladimir Egorov, Artur Gleim and George Miroshnichenko
Th404	**Polarization-multiplexing self-coherent phase reference in continuous-variable quantum key distribution** Tao Wang, Peng Huang and Guihua Zeng
Th405	**Invisible Trojan-horse attack** Shihan Sajeed, Carter Minshull, Nitin Jain and Vadim Makarov
Th406	**Dominant Noise Source in DWDM Scheme of 1550nm Continuous-variable Quantum Key Distribution** Yijia Zhao, Yichen Zhang, Song Yu and Hong Guo
Th407	**Novel CV QKD Protocol: Guess How You Got It** Ilhwan Park, Junsang Oh, Yongseen Kim and Junekoo Rhee
Th408	**Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction** Ying Guo, Qin Liao, Yijun Wang, Duan Huang, Peng Huang and Guihua Zeng
Th409	**Multipartite measurement-device independent quantum cryptography: Conferencing and secret sharing** Carlo Ottaviani, Cosmo Lupo, Riccardo Laurenza and Stefano Pirandola
Th410	**Recent development status of compact 2K GM cryocoolers** Mingyao Xu and Qian Bao
Th411	**Experimental Demonstration of Passive-Decoy-State Quantum-Key-Distribution with Two Independent Lasers** Shi-Hai Sun, Guangzhao Tang, Chun-Yan Li and Linmei Liang
Th412	**Demonstration of quantum cipher communication using quadrature amplitude modulation technologies over 100 km optical fiber** Takuya Hirano, Ryo Namiki, Motoharu Ono, Tsubasa Ichikawa, Masato Yoshida, Toshihiko Hirooka, Keisuke Kasai and Masataka Nakazawa
Th413	**Multinode subcarrier wave quantum communication network** Oleg Bannik, Vladimir Chistyakov, Lenar Gilyazov, Konstantin Melnik, Artur Vasiliev, Narkis Arslanov, Andrei Gaidash, Anton Kozubov, Vladimir Egorov, Sergei Kozlov, Artur Gleim and Sergei Moiseev
Th414	**The Quantum Trojan Horse Attack** Scott Vinay, Mark Pearce and Pieter Kok
Th415	**Quantum secret sharing and Mermin operator** Minjin Choi, Yonghae Lee and Soojoon Lee
Th416	**Lower Dimensional Sections of Qutrit State Space using 3-Dimensional Vectors** Vinod Mishra
Th417	**Flow ambiguity: A path towards classically driven blind quantum computation** Atul Mantri, Tommaso Demarie, Nicolas Menicucci and Joseph Fitzsimons
Th418	**Quantum Key Distribution Without Sifting** Alasdair Price, John Rarity and Chris Erven
Th419	**Improving performance of decoy-state free-space QKD using information on fluctuating transmittance in turbulent channel** Wenyuan Wang, Feihu Xu and Hoi-Kwong Lo
Th420	**A complete linear optic Bell measurement for long distance quantum communication** Seung-Woo Lee, Timothy C. Ralph and Hyunseok Jeong
Th421	**New Approaches to Increase Efficiency of Cascade Information Reconciliation Protocol** Metin Toyran, Mustafa Toyran and Sıtkı Öztürk

Th422	**A phase-randomized coherent state by cross-Kerr nonlinearity for quantum key distribution** Seung-Woo Lee and Jaewan Kim
Th423	**Time-Frequency QKD over Free-Space and Fiber Channels** Jasper Rödiger, Nicolas Perlot, Ronald Freund and Oliver Benson
Th424	**Multiplexed entanglement generation over quantum networks using multi-qubit nodes** Suzanne B. van Dam, Peter C. Humphreys, Filip Rozpedek, Stephanie Wehner and Ronald Hanson
Th425	**Composable Security of Measurement-Device-Independent Continuous-Variable Quantum Key Distribution against Coherent Attacks** Cosmo Lupo, Carlo Ottaviani, Panagiotis Papanastasiou and Stefano Pirandola
Th426	**Genome analysis data transmission using quantum cryptography** Akira Murakami, Ririka Takahashi, Yoshimichi Tanizawa, Hideaki Sato, Tomoaki Chiba and Masao Nagasaki
Th427	**Characterising linear optical networks with decoy-state techniques** Álvaro Navarrete, Wenyuan Wang, Feihu Xu and Marcos Curty
Th428	**Experimental covert communication over metropolitan distances** Yang Liu, Juan Miguel Arrazola, Wen-Zhao Liu, Ignatius William Primaatmaja, Qiang Zhang, Valerio Scarani and Jian-Wei Pan
Th429	**Feasibility of satellite QKD with continuous variable** Daniele Dequal, Luis Trigo Vidarte, Eleni Diamanti, Giuseppe Vallone and Paolo Villoresi
Th430	**Multiparty Delegated Quantum Computing** Anna Pappa and Elham Kashefi
Th431	**Hybrid Photonic Loss Resilient Entanglement Swapping** Ryan Parker, Jaewoo Joo, Mohsen Razavi and Timothy Spiller
Th432	**Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits** Ding Yuyang, Chen Wei, Chen Hua, Wang Chao, Li Yaping, Wang Shuang, Yin Zhenqiang, Guo Guangcan and Han Zhengfu
Th433	**High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers** Gustavo Lima
Th434	**Composable Security in Relativistic Quantum Cryptography** V. Vilasini, Christopher Portmann and Lídia Del Rio
Th435	**Quantum hashing is maximally secure against classical leakage** Cupjin Huang and Yaoyun Shi
Th436	**A Discrete Fourier Transform on Lattices with Quantum Applications** Lior Eldar and Peter Shor
Th437	**Constructing optimal quantum error correcting codes from absolute maximally entangled states** Zahra Raissi, Christian Gogolin, Arnau Riera and Antonio Acín
Th438	**Transmission and distillation of quantum states on a turbulent atmospheric channel** Kevin Günthner, Ömer Bayraktar, Andreas Thurn, Christian Peuntinger, Dominique Elser, Christoph Marquardt and Gerd Leuchs
Th439	**Efficient quantum communications with coherent state fingerprints** Niraj Kumar, Adeline Orieux, Eleni Diamanti and Iordanis Kerenidis
Th440	**Versatile Random Numbers Extraction by Single Photon Detection** Andrea Stanco, Davide Giacomo Marangon, Giuseppe Vallone and Paolo Villoresi
Th441	**Quantum hacking of free-space QKD system by wavelength control** Min Soo Lee, Minki Woo, Jisung Jung, Il Young Kim, Yong-Su Kim, Sang-Wook Han and Sung Moon
Th442	**Continuous-variable quantum network coding for coherent states** Tao Shang, Ke Li and Jianwei Liu
Th443	**Quantum Randomness from Probability Estimation with Classical Side Information** Yanbao Zhang, Emanuel Knill, Peter Bierhorst and Scott Glancy

Th444	**Software-defined subcarrier wave quantum networking operated by OpenFlow protocol** Vladimir Egorov, Vladimir Chistyakov, Oleg Sadov, Artur Vasiliev, Peter Fedchenkov, Vladimir Grudinin, Oleg Lazo, Andrey Shevel, Nikita Buldakov, Sergey Kynev, Artur Gleim, Sergei Khoruzhnikov and Sergei Kozlov
Th445	**Quantum key distribution system with 2.5 GHz clock rate** Alberto Boaron, Boris Korzh, Gianluca Boso, Raphael Houlmann, Charles Ci Wen Lim, Ming-Jun Li, Daniel Nolan and Hugo Zbinden
Th446	**Ongoing efforts on development of quantum technology by SK Telecom** Sean Kwak
Th447	**Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution** Xuyang Wang, Wenyuan Liu, Pu Wang and Yongmin Li
Th448	**Security of decoy-state QKD with alternate key distillation** Tatsuya Sumiya, Toshihiko Sasaki, Masato Koashi, Ken-Ichiro Yoshino, Mikio Fujiwara, Kensuke Nakata, Masahiro Takeoka, Masahide Sasaki, Akio Tajima and Akihisa Tomita
Th449	**Reconciliation with polar codes by Gaussian approximation for continuous-variable quantum key distribution** Yongseen Kim, Changho Suh and June-Koo Kevin Rhee
Th450	**Fully device independent protocols beyond QKD** Jérémy Ribeiro, Gláucia Murta and Stephanie Wehner
Th451	**Experimental asymmetric Plug-and-Play Measurement-device-independent quantum key distribution** Guang-Zhao Tang, Shi-Hai Sun, Fei-Hu Xu, Huan Chen, Chun-Yan Li and Lin-Mei Liang
Th452	**Experimental Validation of an End-to-End QKD Encryption Service in MPLS environments** Alejandro Aguado, Jesús Martinez-Mateo, Victor Lopez, Diego Lopez, Momtchil Peev and Vicente Martin
Th453	**Unconstrained capacities of quantum key distribution and entanglement distillation for pure-loss bosonic broadcast channels** Masahiro Takeoka, Kaushik Seshadreesan and Mark Wilde
Th454	**Linear-optical frequency beamsplitter for fiber-optic quantum networks** Hsuan-Hao Lu, Joseph Lukens, Nicholas Peters, Ogaga Odele, Andrew Weiner and Pavel Lougovski
Th455	**Performance improvement of NbTiN superconducting nanowire single photon detectors by avalanche switching architecture** Shigehito Miki, Taro Yamashita, Masahiro Yabuno and Hirotaka Terai
Th456	**General bounds for sender-receiver capacities in multipoint quantum communications** Riccardo Laurenza and Stefano Pirandola
Th457	**Satellite Realization of Wheeler's Delayed-Choice Thought Experiment** Costantino Agnesi and Francesco Vedovato
Th458	**Learning with errors is easy with quantum samples** Alex Bredariol Grilo and Iordanis Kerenidis
Th459	**Entanglement Verification in Quantum Recursive Networks with Tampered Nodes** Michele Amoretti and Stefano Carretta
Th460	**Passive round-robin differential-quadrature-phase-shift quantum key distribution with untrusted detectors** Hongwei Liu, Haiqiang Ma, Wenxiu Qu, Tianqi Dou, Yitian Chen, Jipeng Wang and Yuemei Li
Th461	**Quantum State Comparison Amplifier with Feedforward State Correction** Luca Mazzarella, Ross Donaldson, Robert Collins, Ugo Zanforlin, Gerald Buller and John Jeffers
Th462	**Quantum cryptography using thermal states** Anne Ghesquiere, Freya Wilson, Elizabeth Newton, Matthew Everitt and Benjamin Varcoe
Th463	**Quantum-dot-based quantum relay operating at telecom wavelength** Jan Huwer, Martin Felle, Mark Stevenson, Joanna Skiba-Szymanska, Martin Ward, Ian Farrer, Richard Penty, David Ritchie and Andrew Shields

Th464	**On the use of pseudorandom quantum states in quantum cryptography** Anton Trushechkin, Pavel Tregubov, Eugenii Kiktenko, Yuriy Kurochkin and Aleksey Fedorov
Th465	**Experimental Demonstration of Practical Unforgeable Quantum Money** Mathieu Bozzio, Eleni Diamanti and Iordanis Kerenidis
Th466	**Quantum random oracle model for quantum digital signature** Tao Shang, Qi Lei and Jianwei Liu
Th467	**High performance field trials of QKD over a metropolitan network** Adrian Wonfor, James Dynes, Rupesh Kumar, Han Qin, Richard Penty, Ian White and Andrew Shields
Th468	**Noisy entanglement-assisted classical capacity as a security framework for two-way quantum key distribution protocols** Quntao Zhuang, Zheshen Zhang and Jeffrey Shapiro
Th469	**Temporal and intensity fluctuation of photon pulses in a high- speed polarization based quantum key distribution system** Heasin Ko, Byeong-Seok Choi and Chun Ju Youn
Th470	**On using intensity fluctuations for eavesdropping on coherent states quantum cryptography** Dmitry Kronberg and Yury Kurochkin
Th471	**Practical discrete-state QKD with lossy channels: avoiding unambiguous state discrimination attack** Konstantin Kravtsov, Igor Radchenko, Sergei Kulik and Sergei Molotkov
Th472	**Crosstalk Limitations on Reconfigurable QKD Networks** Xinke Tang, Adrian Wonfor, Rupesh Kumar, Shengjun Ren, Richard Penty and Ian White
Th473	**Finite-resource teleportation stretching for continuous-variable systems** Riccardo Laurenza, Samuel Braunstein and Stefano Pirandola
Th474	**Quantum Key Distribution with Coherent States** Jie Lin, Patrick Coles, Adam Winick and Norbert Lütkenhaus
Th475	**Quantum description of timing jitter for single photon ON/OFF detectors** Élie Gouzien, Bruno Fedrici, Alessandro Zavatta, Sébastien Tanzilli and Virginia D'Auria
Th476	**Fast semi-device-independent quantum random number generator based on unambiguous state discrimination** Jonatan Bohr Brask, Anthony Martin, William Esposito, Raphael Houlman, Joseph Bowles, Hugo Zbinden and Nicolas Brunner
Th477	**Knowledge Concealing Evidencing of Knowledge of a Quantum State** Emily Adlam and Adrian Kent
Th478	**Optimization and CV-QKD Post-Processing in the Open Source AIT QKD Software R10** Oliver Maurhart, Christoph Pacher, Chi-Hang Fred Fung and Momtchil Peev
Th479	**A Realizable Quantum Simulator of the Integer Factorization Problem** Jose Luis Rosales and Vicente Martin-Ayuso
Th480	**Finite-size analysis of thermal and continuous-variables measurement-device-independent quantum cryptography** Panagiotis Papanastasiou, Carlo Ottaviani and Stefano Pirandola

LIGHT DINNER

18:00 – 20:00 Session Th5	**Rump Session**
18:30 Th31	**QCrypt Business Meeting (Chair Christian Schaffner)** Review of QCrypt17; preview of QCrypt 2018; bids for 2019; open discussion;
19:30 Th32	**Presentation of student and poster prizes** **Rump Session (Chairs Charlie Bennett and Gilles Brassard)**

Friday 22nd September

09:00 – 10:20 Session Fr1	**Composability (Chair Christian Schaffner)**
09:00 Fr11	**Composability in Quantum Cryptography (tutorial)** Christopher Portman ETH Zurich

COFFEE BREAK

11:00 – 12:35 Session Fr2	**Money and Recycling (Chair Dominique Unruh)**
11:00 Fr21	**Experimental Quantum Money** Jian-Yu Guan, Juan Miguel Arrazola, Ryan Amiri, Qiang Zhang, Norbert Lutkenhaus and Jian-Wei Pan
Merged with Fr22	**Experimental demonstration of practical unforgeable quantum money** Mathieu Bozzio, Adeline Orieux, Luis Trigo Vidarte, Isabelle Zaquine, Iordanis Kerenidis and Eleni Diamanti
11:35 Fr23	**Quantum Authentication and Encryption with Key Recycling** Serge Fehr and Louis Salvail
11:55 Fr24	**Quantum non-malleability and authentication** Gorjan Alagic and Christian Majenz
12:15 Fr24	**Quantum authentication with key recycling** Christopher Portmann

LUNCH BREAK (ON YOUR OWN)

14:00 – 15:35 Session Fr3	**QRNG (Chair Roger Colbeck)**
14:00 Fr31	**Integrated quantum random number generator chip (invited)** Morgan Mitchell ICFO
14:35 Fr32	**Device-independent Randomness Amplification and Privatization** Max Kessler and Rotem Arnon-Friedman
14:55 Fr33	**Randomness in nonlocal games between mistrustful players** Honghao Fu, Carl Miller and Yaoyun Shi Honghao Fu, Carl Miller and Yaoyun Shi

CONFERENCE ENDS

Exhibitors

MPD
MICRO PHOTON DEVICES

PicoQuant
Unternehmen für optoelektronische Forschung und Entwicklung

Quantum Opus

OEC
OptoElectronic Components

IDQ

⟨InfiniQuant⟩
secure · quantum · telecom

IOP Publishing

pacer
advancing technology

Quintessence labs

Tektronix®

WHITEWOOD

Quantum union

TOSHIBA

GOLD sponsors

Alibaba Cloud

量子网络
CAS QUANTUMNET

IDQ

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

国盾量子
QuantumCTek

SK telecom

BRONZE Sponsors

CQT Centre for Quantum Technologies
National University of Singapore

CryptoWorks21

NPL