
Qrypt 2013
CONFERENCE ON QUANTUM CRYPTOGRAPHY
2013.qcrypt.net
Waterloo, Canada
August 5–9, 2013
IQC
WATERLOO



Welcome to the 3rd edition of QCrypt, the annual conference on quantum cryptography. We hope the conference will continue on the way to success!

We have about 170 registered participants. The program includes 4 tutorials, a mix of 9 invited and 22 contributed talks, and a long poster session with about 70 posters. The contributed talks were selected by an independent program committee chaired by Ivan Damgård from more than 60 submissions. The quality of submissions was high and we reluctantly had to delegate some excellent ones to the poster session.

The industrial exhibit features more than 10 booths from both academia and industry. We'll have 5 QKD systems there, and let's cross our fingers that every one of them distills some key.

New to this year's event is a hot topics session at the end of conference. Submissions to it are being reviewed and its content will be announced on Monday.

A best student paper prize and best poster prize will be announced at the conference dinner on Wednesday. The best poster prize is selected by you! Cast your vote at the end of poster session.

Finally, we hope you enjoy our social program. A trip to Elora village on Wednesday offers opportunities to splash and swim in our local river, as well as to enjoy small art galleries and shopping. The Saturday trip to Niagara Falls will get you soaked too, in a much bigger way :).

Vadim Makarov
Local organizing committee

Michele Mosca
Steering committee

QCrypt 2013 schedule

Sunday, August 4

18:00 - 21:00 Reception and registration

Monday, August 5

8:30 Registration

Session chair: Norbert Lütkenhaus

9:30 **Invited talk: The physics of cryptography**
Renato Renner

10:20 **Tutorial: What theorists should know when working with experimentalists (part 1)**
Marcos Curty

11:05 Coffee break

Session chair: Hoi-Kwong Lo

11:30 **Tutorial: What theorists should know when working with experimentalists (part 2)**
Marcos Curty

12:15 **Performing private database queries in a real-world environment using a quantum protocol**
Philip Chan, Itzel Lucio-Martinez, Xiaofan Mo, Christoph Simon, and Wolfgang Tittel

12:40 Lunch - provided in QNC

Session chair: Thomas Jennewein

13:40 **Invited talk: Satellite-based quantum communications**
Jane Nordholt

14:30 **Free-space quantum network with trusted relay**
Wei-Yue Liu, Hai-Lin Yong, Zhu Cao, Ji-Gang Ren, Xiongfeng Ma, Cheng-Zhi Peng, and Jian-Wei Pan

14:55 **A wideband balanced homodyne detector for high speed continuous variable quantum key distribution systems**
Duan Huang, Jian Fang, Chao Wang, Guangqiang He, Peng Huang, Ronghuan Yang, and Guihua Zeng

15:20 Coffee break

Session chair: Hugo Zbinden

15:50 **Experimental demonstration of the coexistence of continuous-variable quantum key distribution with an intense DWDM classical channel**
Paul Jouguet, Sébastien Kunz-Jacques, Rupesh Kumar, Hao Qin, Renaud Gabet, Eleni Diamanti, and Romain Alléaume

16:15 **Realization of finite-size continuous-variable quantum key distribution based on Einstein-Podolsky-Rosen entanglement**
Tobias Eberle, and Vitus Händchen, Fabian Furrer, Torsten Franz, Jörg Duhme, Reinhard F. Werner, and Roman Schnabel

16:40 **Saturation attack on continuous-variable quantum key distribution system**
Hao Qin, Rupesh Kumar, and Romain Alléaume

17:05 **Walk over to RAC building** (meet at registration desk; an organizer will guide the group; 15 min walk)

17:30 -18:30 **Tour of Institute for Quantum Computing's labs**
Venue: Research Advancement Centre (RAC) University of Waterloo
The tour includes:

Superconducting quantum devices lab (PI: Adrian Lupascu): superconducting systems and hybrid solid-state devices for quantum information processing, quantum optics and metrology.

Quantum photonics lab (PI: Thomas Jennewein): devices suitable for communication and computing with photons, ultra-long quantum communication links using terrestrial and satellite-based systems.

CoryLab (PI: David Cory): spin-based hybrid quantum sensors and other devices, from ultra-sensitive magnetometers to full-scale quantum information processors.

Tuesday, August 6

Session chair: Yi-Kai Liu

9:00 **Invited talk: Research and development of the Tokyo QKD network project**
Kiyoshi Tamaki

9:50 **Tutorial: Extractors against classical and quantum adversaries (part 1)**
Amnon Ta-Shma

10:35 Coffee break

Session chair: Anne Broadbent

11:00 **Tutorial: Extractors against classical and quantum adversaries (part 2)**
Amnon Ta-Shma

11:45 **Building one-time memories from isolated qubits**
Yi-Kai Liu

12:10 **Achieving the limits of the noisy-storage model using entanglement sampling**
Frédéric Dupuis, Omar Fawzi, and Stephanie Wehner

12:35 Lunch - provided in QNC

Session chair: Wolfgang Tittel

13:40 **Invited talk: Unforgeable tokens: what we can do with imperfect qubit memories**
Fernando Pastawski

14:30 **An experimental implementation of oblivious transfer in the noisy storage model**
Chris Erven, Stephanie Wehner, Nick Gigov, Raymond Laflamme, and Gregor Weihs

14:55 **High bit rate quantum key distribution with quantified security**
Marco Lucamarini, Ketaki Patel, James F. Dynes, Bernd Fröhlich, Andrew W. Sharpe, Zhiliang L. Yuan, Richard V. Penty, and Andrew J. Shields

15:20 Coffee break

15:50 Poster session
Venue: Main atrium, Lazaridis Quantum-Nano Centre (QNC)
See list of posters later in the program.
Posters also stay on display for the duration of the conference.

19:00 **Public lecture:**
-20:00 Quantum computing and the entanglement frontier
John Preskill
NB! General public has priority. Conference participants please do not register. Conference participants can enter the hall after general public, if there are seats left.

Wednesday, August 7

Session chair: John Watrous

9:00 **Invited talk: Classical command of quantum systems**
Ben Reichardt

9:50 **Tutorial: Secure multiparty quantum computation (part 1)**
Michael Ben-Or

10:35 Coffee break

Session chair: Marco Piani

11:00 **Tutorial: Secure multiparty quantum computation (part 2)**
Michael Ben-Or

11:45 **One-sided device independence of BB84 via monogamy-of-entanglement game**
Marco Tomamichel, Serge Fehr, Jedrzej Kaniewski, and Stephanie Wehner

12:10 **Limits of privacy amplification against non-signalling memory attacks**
Rotem Arnon-Friedman and Amnon Ta-Shma

12:35 **Conference photo**

12:50 **Excursion to Elora** (with packed lunch)

For the Wednesday excursion we will be visiting the charming village of Elora. It is a short 40-minute drive away through the scenic countryside and we will have packed lunches that can be eaten on the bus. There will be 3 options for activities once we get there:

1. **Tubing in Elora Gorge:** River conditions permitting, you will be able to take a refreshing ride on a tube through the Elora Gorge. You should start here to make sure you have enough time on the river. All safety equipment will be provided, just bring your swimsuit!

2. **Elora Downtown:** This area boasts many shops and local art galleries for you to wander around in. With a downtown park, this is a great way to see the river and gorge without getting wet.

3. **Elora Quarry:** As the name implies, this was once an old limestone quarry and had since been filled with water and is now a popular swimming location. There is a sand beach and some cliffs for diving if you want an adrenaline rush.

Afternoon schedule:

12:50 Depart QNC (eat lunch on bus)
16:00 Early bus back to hotels and QNC
17:00 Buses leave Quarry for conference dinner
17:10 Buses leave Downtown for conference dinner
17:20 Buses leave Tubing for conference dinner







18:20 **Conference dinner**

Venue: Festival Room, South Campus Hall (SCH) University of Waterloo

Session chair: Nicolas Gisin

20:20 **After-dinner talk: Insecurity engineering**
Marc Weber Tobias
Venue: Festival Room, South Campus Hall (SCH) University of Waterloo

21:20 -22:20 **Open session: announces and other thoughts** (max 3 min each)
NB! Submit your title before 11:00 to qcrypt-open-session@vad1.com
Venue: Festival Room, South Campus Hall (SCH) University of Waterloo

Thursday, August 8

Session chair: Jane Nordholt

9:00 **Invited talk: Private-key quantum money**
Scott Aaronson

9:50 **Tutorial: Single-photon detectors (part 1)**
Krister Shalm

10:35 Coffee break

Session chair: Christian Schaffner

11:00 **Tutorial: Single-photon detectors (part 2)**
Krister Shalm

11:45 **Specious adversaries and quantum private information retrieval**
Ämin Baumeler and Anne Broadbent

12:10 **Reference frame agreement in quantum networks**
Tanvirul Islam, Loïck Magnin, Brandon Sorg and Stephanie Wehner

12:35 Lunch - provided in QNC

Session chair: Thomas Chapuran

13:40 **Invited talk: Spins and photons: toward quantum networks in diamond**
Lilian Childress

14:30 **Network-centric quantum communications with application to critical infrastructure protection**
Richard J. Hughes, Jane E. Nordholt, Kevin P. McCabe, Raymond T. Newell, Charles G. Peterson, and Rolando D. Somma

14:55 **A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator**
Boris Korzh, Nino Walenta, Raphael Houlmann, and Hugo Zbinden

15:20 **Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution**
Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo

15:45 Coffee break

16:15 **Industry panel discussion**
-17:45 *(See handout)*

Friday, August 9

Session chair: Richard Hughes

9:00 **Invited talk: High performance single photon detectors using superconductors**
Sae Woo Nam

9:50 **Security analysis and experimental implementation of a relativistic bit commitment**
Tommaso Lunghi, Jedrzej Kaniewski, Felix Bussieres, Raphael Houlmann, Marco Tomamichel, Adrian Kent, Nicolas Gisin, Stephanie Wehner, Hugo Zbinden

10:15 **Relativistic quantum cryptography: experimental realization**
Igor V. Radchenko, Konstantin S. Kravtsov, Sergei P. Kulik, and Sergei N. Molotkov

10:40 Coffee break

Session chair: Gilles Brassard

11:10 **Invited talk: The structure of a world (which may be) described by quantum mechanics**
Anthony Leggett

12:00 **Universal uncertainty relations**
Gilad Gour, Shmuel Friedman, and Vlad Gheorghiu

12:25 **Continuous variable entropic uncertainty relations in the presence of quantum memory**
Mario Berta, Matthias Christandl, Fabian Furrer, Volkher Schultz, and Marco Tomamichel

12:50 Lunch - provided in QNC

Session chair: Michele Mosca

13:50 **Quantum one-time programs**
Anne Broadbent, Gus Gutoski, and Douglas Stebila

14:15 **Hot topics session**
Content will be announced on the first day of conference

15:15 **Concluding remarks**
-15:25

Saturday, August 10

8:20-16:15 Trip to Niagara Falls (Optional)

The trip costs $40. If you have not paid during online registration, please contact the registration desk for the availability of seats.

Trip schedule

8:00 Depart Waterloo Inn

8:10 Depart Ron Eydt Village

8:20 Depart Lazaridis Quantum-Nano Centre (QNC)

10:30 Arrive in Niagara Falls. We proceed by taking the silly boat called Maid of the Mist that sails close to the fall from the bottom. Afterwards there will be free time to walk around and see more attractions.

14:30 Depart Niagara Falls

One return bus will take participants directly to Toronto Pearson airport by 16:15, in time for late evening departures. The Waterloo bus will be back by 16:30.



Poster session

Tuesday, August 6
15:50–18:30

Posters also stay on display for the duration of the conference. For talks, see conference schedule.

Best poster prize will be selected by popular vote. Use the voting card included inside your badge, and cast your vote in the box at the registration desk before Wednesday at 12:35. The winner will be announced at the conference dinner.

Posters:

QKD in optical networks
Slavisa Aleksic, Dominic Winkler, Andreas Poppe, Gerald Franzl, Bernhard Schrenk, and Florian Hipp

Photon-pair states and violation of CHSH inequality
Álvaro J. Almeida, Luís P. Martins, Paulo S. André, and Armando N. Pinto

Post selection beyond quantum theory
Rotem Arnon-Friedman and Renato Renner

Experimental QKD with finite-key security analysis for noisy channels
Davide Bacco, Matteo Canale, Nicola Laurenti, Giuseppe Vallone, and Paolo Villoresi

Toward the generation of Bell certified randomness using photons
Jean-Daniel Bancal, Siddarth Koduru Josh, Chen Ming Chia, Alessandro Cere, Lana Sheridan, Valerio Scarani, and Christian Kurtsiefer

Quantum exams
Normand J. Beaudry, Omar Fawzi, and Renato Renner

Quantum repeaters and quantum key distribution: the role of quantum error correcting codes
Sylvia Bratzik, Hermann Kampermann, and Dagmar Bruß

Quantum communication in curved spacetimes
David Edward Bruschi, Ivette Fuentes, Tim Ralph, and Mohsen Razavi

Posters

Higher-dimensional quantum cryptography
Bradley Christensen, Kevin McCusker, Daniel Gauthier, Daniel Kumor, Venkat Chandar, and Paul Kwiat

A proposal for a wavelength multiplexed quantum metropolitan area network
Alex Ciurana, Jesus Martínez-Mateo, Nino Walenta, Hugo Zbinden, Momtchil Peev, Andreas Poppe, and Vicente Martín

Spatial multiplexing of integrated photonic crystal waveguide heralded single-photon sources
Matthew J. Collins, Chunle Xiong, Isabella H. Rey, Trung D. Vo, Jiakun He, Shayan Shahnia, Chris Reardon, Michael J. Steel, Thomas F. Krauss, Alex S. Clark, and Benjamin J. Eggleton

Compact single-photon detectors for high bit-rate quantum key distribution
Lucian Comandar, Bernd Fröhlich, Ketaki A. Patel, Marco Lucamarini, James F. Dynes, Andrew W. Sharpe, Zhiliang L. Yuan, Richard V. Penty, and Andrew J. Shields

Long-distance distribution of genuine energy-time entanglement
Alvaro Cuevas, Gonzalo Carvacho, Gabriel Saavedra, Jaime Cariñe, Wallon A. T. Nogueira, Miguel Figueroa, Adan Cabello, Paolo Mataloni, Gustavo Lima, and Guilherme B. Xavier

High speed implementation of LDPC based error correction for quantum key distribution
Alexander R. Dixon

CV-QKD on Hannover campus: key generation and error correction
Jörg Duhme, Kais Abdelkhalek, Rene Schwonnek, Fabian Furrer, and Reinhard F. Werner

Composable security of delegated quantum computation
Vedran Dunjko, Joseph F. Fitzsimons, Christopher Portmann, and Renato Renner

Networks based on QKD and weakly trusted repeaters
David Elkouss, Jesus Martinez-Mateo, Alex Ciurana, and Vicente Martin

Posters

Quantum computing on encrypted data: theory and experiment
Kent A. G. Fisher, Anne Broadbent, Lynden K. Shalm, Zhizhong Yan, Jonathan Lavoie, Robert Prevedel, Thomas Jennewein, and Kevin J. Resch

A practical approach to true quantum randomness generation
Daniela Frauchiger and Renato Renner

Free randomness amplification using bipartite chain correlations
Andrzej Grudka, Karol Horodecki, Michal Horodecki, Pawel Horodecki, Marcin Pawlowski, and Ravishankar Ramanathan

The QKD trusted node
Don Hayford, Gregoire Ribordy, Rick Wolterman, and Alex Morrow

Pushing quantum optical receiver technology towards satellite-mediated global quantum key distribution
Brendon Higgins, Jean-Philippe Bourgoin, Nikolay Gigov, Evan Meyer-Scott, Zhizhong Yan, and Thomas Jennewein

Quantum hacking on continuous-variable quantum key distribution system by using a wavelength attack
Jing-Zheng Huang, Christian Weedbrook, Zhen-Qiang Yin, Mo Li, and Zheng-Fu Han

Wroclaw quantum network – QKD deployment in a metropolitan network
Monika Jacak, Tadeusz Martynkien, Andrzej Janutka, Janusz Jacak, Damian Melniczuk, Wojciech Donderowicz, Jacek Gruber, and Ireneusz Józwiak

Testing of influence of polarization perturbation on dark channel in the system of entangled photons QKD (EPR Quelle, AIT)
Monika Jacak, Damian Melniczuk, Lucjan Jacak, Ireneusz Józwiak, and Jacek Gruber

Quantum hacking: demonstrating feasibility of a Trojan-horse attack on a commercial QKD system
Nitin Jain, Imran Khan, Elena Anisimova, Christoffer Wittmann, Vadim Makarov, Christoph Marquardt, and Gerd Leuchs

Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states
Mu-Sheng Jiang, Shi-Hai Sun, Chun-Yan Li, Lin-Mei Liang

Posters

Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution
Paul Jouguet, S ebastien Kunz-Jacques, and Eleni Diamanti

Security of CV-QKD with transmitted local oscillator
Go Kato, Kiyoshi Tamaki, Koji Azuma, and Masaki Owari

Optimal working points for continuous-variable quantum channels
Imran Khan, Christoffer Wittmann, Nitin Jain, Nathan Killoran, Norbert Lütkenhaus, Christoph Marquardt, and Gerd Leuchs

Searching for optimal generalized Winnow protocol
Donny Kok-Ann Teo and Khoongming Khoo

Criteria for realistic single photon sources in quantum repeater applications
Mikolaj Lasota, Czes law Radzewicz, and Konrad Banaszek

Development of integrated quantum key distribution system over 25 km
Min-Soo Lee, Min Ki Woo, Byung Kwon Park, Il Young Kim, Os-ung Kwon, Sang-Wook Han, and Sung Moon

Fault-tolerate quantum key distribution over a collective-noise channel
Chunyan Li

O-band photon-pair source on silicon chip
Mao Tong Liu, Ying Huang, and Han Chuen Lim

Quantum flows for secret key distribution
Luis A. Lizama-Perez, J. Mauricio Lopez, and Eduardo De Carlos Lopez

Long-distance measurement-device-independent QKD
Nicoló Lo Piparo and Mohsen Razavi

Efficient Bell state measurement with time-bin qubits
Itzel Lucio-Martinez, Philip Chan, Raju Valivarthi, Joshua A. Slater, Francesco Marsili, Varun B. Verma, Jeffrey A. Stern, Matthew D. Shaw, Daniel Oblak, Sae Woo Nam, and Wolfgang Tittel

Posters

Recent battle between quantum cryptographer and hacker
Xiongfeng Ma, Yang Liu, Yan-Lin Tang, Teng-Yun Chen, Hua-Lei Yin, Chi-Hang Fred Fung, Hai-Lin Yong, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Li Li, Nai-Le Liu, Cheng-Zhi Peng, Zeng-Bing Chen, Qiang Zhang, and Jian-Wei Pan

Insider-proof encryption with applications for quantum key distribution
Matthew McKague and Lana Sheridan

New release of an open source QKD software: design and implementation of new algorithms, modularization and integration with IPSec
Oliver Maurhart, Christoph Pacher, Andreas Happe, Thomas Lorünser, Cristina Tamas, Andreas Poppe, and Momtchil Peev

Super-polynomial complex quantum states
Huy Nguyen Le, Yu Cai, Xingyao Wu, and Valerio Scarani

Methods to increase coupling efficiency of entangled photon pairs from periodically poled lithium niobate waveguides into optical fibers
Lee Oesterling, David Nippa, Sean Krupa, and Eric Stinaff

Quantum bit error estimation based on the syndrome of a linear code
Christoph Pacher and Gottfried Lechner

High-performance sum-product decoding of quasi-cyclic LDPC codes
Christoph Pacher and Bernhard Ömer

Memory-assisted measurement-device-independent quantum key distribution
Christiana Panayi, Mohsen Razavi, Xiongfeng Ma, and Norbert Lütkenhaus

Experimental plug'n'play quantum coin flipping
Anna Pappa, Paul Jouguet, Thomas Lawson, Matthieu Legré, Patrick Trinkler, Iordanis Kerenidis, Eleni Diamanti

Posters

An algorithmically defined QRNG
Raphael C. Pooser, Travis S. Humble, Philip G. Evans, Warren P. Grice and Brian W. Williams

Cryptographic security of quantum key distribution
Christopher Portmann and Renato Renner

Generation and application of time-shifted single photons in parametric down conversion for quantum communication
Igor E. Protsenko, Sergey A. Magnitsky, and Mikhail Y. Saygin

Sequential Quantum Secret Sharing and a 'Quantum Bank'
Maharshi Ray

Architectural considerations in multiple-access quantum key distribution networks
Mohsen Razavi, Nicoló Lo Piparo, and Christiana Panayi

Exact computation of tail probability of hypergeometric distribution and its application to quantum key distribution
Kenta Sakakibara, Ryutaroh Matsumoto, and Tomohiko Uyematsu

Modelling of probabilistic dynamics in quantum repeater processes
René Schwonnek, Kais Abdelkhalek, and Jörg Duhme

An accurate analysis of the BINARY information reconciliation protocol by generating functions
Sean Seet, Ruth Ng Ii-Yung, and Khoongming Khoo

Reference frame independent QKD
Philip Sibson, Kanin Aungskunsiri, Enrique Martin Lopez, Anthony Laing, Jeremy O'Brien, and Mark Thompson

Long-distance quantum communications using quantum memories having on-demand recall in the frequency domain
Neil Sinclair, Erhan Saglamyurek, Hassan Mallazadeh, Joshua A. Slater, Mathew George, Raimund Ricken, Morgan Hedges, Daniel Oblak, Wolfgang Sohler, and Wolfgang Tittel

Polarization shift keying for free space QKD: effect of noise on reliability of the QKD protocols
Ram Soorat and Ashok Vudayagiri

Posters

A high-speed QRNG for security applications
Mathilde Soucarros, Samuel Burri, Edoardo Charbon, Christopher Chunnilall, Daniela Frauchiger, Alessio Meneghetti, Jean-Benoît Page, Francesco Regazzoni, Renato Renner, and Damien Stucki

Decoy state quantum key distribution with a simplified trusted node
William Stacey, Razeih Annabestani, Xiongfeng Ma, and Norbert Lütkenhaus

Practical decoy state measurement-device-independent quantum key distribution with weak coherent state
Shi-Hai Sun, Ming Gao, Chun-Yan Li, Zhi Ma, and Lin-Mei Liang

Fast real time secure quantum random number generator based on quantum vacuum fluctuations
Thomas Symul, Syed Assad, Jing Yan Haw, and Ping Koy Lam

Fundamental finite block length limits for one-way information reconciliation in quantum key distribution
Marco Tomamichel

Performance of rate-adaptive reconciliation with the maximum-likelihood estimator of error rate
Patcharapong Treeviriyanupab, Paramin Sangwongngam, and Keattisak Sripimanwat

Experimental distillation of continuous variable entanglement by measurement-based noiseless linear amplification
Nathan Walk, Helen M. Chrzanowski, Syed M. Assad, Jiri Janousek, Jing-Yan Haw, S. Hosseini, Timothy C. Ralph, Ping Koy Lam, and Thomas Symul

Easily implemented rate compatible reconciliation protocol for quantum key distribution
Zhengchao Wei, and Zhi Ma

A quantum cloning bound and application to quantum key distribution
Erik Woodhead

Posters

Practical measurement device independent quantum key distribution
Feihu Xu, Marcos Curty, Bing Qi, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo

Continuous QKD and data encryption at up to 100 Gbit/s
Hugo Zbinden, Nino Walenta, Boris Korzh, Charles Lim Ci Wen, Nicolas Gisin, Norbert Felber, and Patrick Trinkler

Experimental feasibility test of measurement-device-independent quantum key distribution on free-space channel
Hai-Lin Yong, Chang Liu, Dong-Dong Li, Wen-Jie Zou, Ji-Gang Ren, Cheng-Zhi Peng, and Jian-Wei Pan

Efficient decoy-state quantum key distribution
Zhen Zhang, Zhengchao Wei, Weilong Wang, and Xiongfeng Ma

Experimental demonstration of secure communication based on quantum illumination
Zheshen Zhang, Maria Tengner, Tian Zhong, Franco N. C. Wong, and Jeffrey H. Shapiro

Thank you to all QCrypt 2013 conference sponsors.

Main sponsor & conference host:



The Institute for Quantum Computing is a scientific research institute at the University of Waterloo harnessing the quantum laws of nature to develop powerful new technologies that will transform information technology and drive the 21st century economy. We focus on three main applications: computing, communications and sensing. Research at IQC is fundamentally interdisciplinary, spanning theory and experiment to pursue every avenue of quantum information science including quantum information theory, quantum algorithms, quantum complexity, quantum error correction and fault tolerance, spin-based quantum information processing, nanoelectronics-based quantum information, optical uantum information processing, quantum cryptography. IQC fosters collaborations across the sciences, mathematics and engineering as well as across borders.

Conference sponsors:



The Centre for Quantum Technologies (CQT) was established as Singapore's inaugural Research Centre of Excellence in December 2007. It brings together quantum physicists and computer scientists to explore the quantum nature of reality and quantum possibilities in technology. CQT receives core funding from Singapore's National Research Foundation and Ministry of Education and is hosted by the National University of Singapore (NUS).



Perimeter Institute is a leading centre for scientific research, training and educational outreach in foundational theoretical physics. Founded in 1999 in Waterloo, Ontario, Canada, its mission is to advance our understanding of the universe at the most fundamental level, stimulating the breakthroughs that could transform our future. Perimeter also trains the next generation of physicists through innovative programs, and shares the excitement and wonder of science with students, teachers and the general public.

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

ETH Zurich is one of the leading international universities for technology and the natural sciences. It is well-known for its excellent education, ground-breaking fundamental research and for putting its new findings directly into practice. It offers researchers an inspiring working environment and its students a comprehensive education. The focal points of its research include energy supply, risk management, developing the cities of the future, global food security and human health.

CryptoWorks21

The NSERC CREATE Training Program in Building a Workforce for the Cryptographic Infrastructure of the 21st Century (CryptoWorks21) is a supplementary program for graduate students and postdoctoral fellows who would like to develop next-generation cryptographic tools.



Telecom ParisTech is one of the "Grandes Ecoles" (French higher education establishments) in the field of information and communication technology (ICT). It belongs to the Institut Mines-Telecom and is under the authority of the French Ministry of Industry. Its mission is to provide education programs for engineers and managers, and to conduct research in ICT.



Quantum Communication Technology, together with Shandong Institute of Quantum Science and Technology Co., Ltd. (SIQST), is the first and biggest provider of multi-protocol network security products and services based on quantum technology, in China. The companies produce state-of-the-art quantum communication systems and series of innovative opt-electronic units with the commercial applications for the financial industry, government organizations and other enterprises, as well as the research applications for the scientific societies. Initially founded by the Chinese leading quantum physics research group from Hefei National Laboratory for Physical Science at Micro-scale (HFNL), University of Science and Technology of China (USTC), the companies are continually transferring cutting-edge scientific and technical achievements into mature commercial products, making great efforts to promote wide-range applications of quantum technology and forming the Chinese quantum industry.



The Austrian Institute of Technology (AIT) takes a leading position in the Austrian innovation system and a key role in Europe as the RTO focusing on the key infrastructure topics of the future. AIT provides research and technological development to realize basic innovations for the next generation of infrastructure related technologies in the fields of health & environment, energy, mobility and safety & security. These technological research areas are supplemented by the competence in foresight & policy development. As a national and international network node at the interface of science and industry AIT enables innovation through its scientific-technological expertise, market experience, tight customer relationships and high quality research infrastructure.

Industrial exhibit

The exhibit runs for the duration of the conference and includes companies and research groups showcasing their products and experimental prototypes.

Conference sponsors participating in the industrial exhibit:

ID Quantique's focus is to provide innovative and cost-effective solutions that leverage the tremendous capabilities offered by quantum photonics, associated with cutting edge analog and digital electronics. The company is organized in three business units: Network Encryption, Scientific Instrumentation and Random Number Generators. *On display: commercial plug-and-play QKD system Clavis2, entangled photon source, single-photon detectors.*

OptoElectronic Components is a supplier of single photon counting detector modules with ultra-fast timing resolution from Micro Photon Devices, TCSPC electronics and software from PicoQuant, and infrared photon counting detector modules based on superconducting nanowires.

The Institute for Quantum Science and Technology is a multidisciplinary group of researchers from the areas of Computer Science, Mathematics, Chemistry, and Physics. *On display: research prototype of measurement-device-independent QKD system (from Wolfgang Tittel's group).*

Anhui Asky Quantum Technology was established in July 2009, a spin-off from the University of Science and Technology of China. It is the first domestic quantum information company, with an existing staff of more than 80 people. Anhui Asky Quantum Technology aims to provide high-tech quantum information products. *On display: single-photon detector, laser source.*



Single Quantum offers complete single photon detection systems based on superconducting nanowire single photon detectors. In the near infrared, including telecom wavelengths, our detectors reach detection efficiencies up to 35%. Our closed cycle cooling system does not consume liquid helium.



SeQureNet is a start-up company and a spin-off from the quantum information team of Telecom ParisTech. The domains of expertise of SeQureNet are continuous variable quantum key distribution, cryptography and network security. *On display: commercial continuous-variable QKD system.*



Scontel develops, manufactures and supplies superconducting single photon detectors and ultra-low noise one-, two- or multi-channel single photon detection systems (SSPD) for the visible and near infrared range which operate in continuous mode. We also produce high-speed detectors and receivers for the THz and mid-infrared range. Cryogen-free SSPD systems and THz receivers are available.



Tektronix is a leading supplier of test and measurement equipment. Whenever you view a web site, click a mouse, make a cell phone call, or turn on a TV you touch our work. As a world leader in test, measurement and monitoring technology, we enable our customers to do more than they ever have. We help them measure, analyze and test next generation devices to ensure accurate performance, reliability, and compatibility.



Teledyne LeCroy is a leading provider of oscilloscopes, protocol analyzers and related test and measurement solutions that enable companies across a wide range of industries to design and test electronic devices of all types. Since our founding in 1964, we have focused on creating products that improve productivity by helping engineers resolve design issues faster and more effectively.

COMMUNITECH

COM DEV International Ltd. is a global designer and manufacturer of space hardware. We are world leaders in the production of space-qualified passive microwave equipment, specialized electronics and optical subsystems. We have over 1,100 employees at facilities in Canada, the United Kingdom and the United States. COM DEV manufactures advanced products and subsystems that are sold to major satellite builders for use in communications, space science, and remote sensing. Our technology is used on more than 700 spacecraft, including 80 percent of all commercial communications satellites ever launched. Our core capability is space engineering. We understand the unique challenges inherent in producing equipment for use in space. We regularly apply the expertise acquired through more than three decades in this industry to the development of new and innovative space technologies. Our disciplined manufacturing and quality control processes ensure we can meet the high standards of quality, reliability, timeliness and cost efficiency that our customers demand.

Other participants in the industrial exhibit:

GAP-Optique from the University of Geneva
On display: research prototype of coherent-one-way QKD system

Korea Institute of Science and Technology
On display: research prototype of plug-and-play QKD system

Hoi-Kwong Lo's group from the University of Toronto
On display: fast random number generator

Thomas Jennewein's group from the Institute for Quantum Computing, University of Waterloo
On display: random number generator, time-stamp unit, 3D print model of Canadian quantum satellite

Cambridge University Press

Conference venue



QCrypt 2013 is hosted by the Institute for Quantum Computing, University of Waterloo. It will take place in the Mike & Ophelia Lazaridis Quantum-Nano Centre (QNC) on the campus of the University of Waterloo, 200 University Avenue West, Waterloo.

Travel tips

Flights

The closest international airport to Waterloo is Toronto's Pearson International Airport (airport code YYZ). Toronto is approximately 1.5-hour drive from Waterloo. You can take a taxi there with Waterloo Taxi (519-888-7777) for a cost of $90.

The closest regional airport to Waterloo is Region of Waterloo Airport (airport code YKF). The University is a 25-minute drive from the airport. You can take a taxi there with Waterloo Taxi for a cost of about $50.

Train/bus

The closest bus and train stations are in Kitchener. The Kitchener bus station is located at 15 Charles Street. The University is a 15-minute drive from the bus station. You can book a taxi in advance with Waterloo Taxi (519-888-7777).

The Kitchener train station is located at 126 Weber Street West. University is a 15-minute drive from the bus station. You can book a taxi in advance with Waterloo Taxi.

QCrypt 2013 program committee

- Harry Buhrman (CWI Amsterdam and Amsterdam University)
- Matthias Christandl (ETH Zürich)
- Ivan Damgård (Aarhus University) ivan@cs.au.dk - *chair*
- Frédéric Dupuis (Aarhus University)
- Artur Ekert (CQT Singapore and Oxford University)
- Nicolas Gisin (Université de Genève)
- Norbert Lütkenhaus (IQC Waterloo)
- Renato Renner (ETH Zürich)
- Louis Salvail (Université de Montréal)
- Christian Schaffner (University of Amsterdam)
- Akihisa Tomita (Hokkaido University)
- Gregor Weihs (University of Innsbruck)
- Stefan Wolf (USI Lugano)

Steering committee

- Matthias Christandl (ETH Zürich)
- Roger Colbeck (ETH Zürich)
- Michele Mosca (IQC Waterloo) - *chair*
  michele.mosca@uwaterloo.ca
- Louis Salvail (Université de Montréal)
- Masahide Sasaki (NICT Tokyo)
- Wolfgang Tittel (University of Calgary)
- Stephanie Wehner (CQT Singapore)

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 (Los Alamos)
- Masahide Sasaki (NICT Tokyo)

Local organizing committee

- Elena Anisimova - welcome package
- Jean-Philippe Bourgoin - website design and poster session
- Kathryn Fedy - program and assistance
- Catherine Holloway - assistance at excursion
- Stacey Jeffery - open session, assistance at excursion
- Sarah Kaiser - excursion planning
- Peter Kovacs - photography and video
- Norbert Lütkenhaus
- Xian Ma - assistance at excursion
- Vadim Makarov makarov@vad1.com - chair
- Marco Piani - social networks (Facebook, Google+) and various administration
- Ryan Robinson-Hatton - program and assistance
- Shihan Sajeed - publication of talk materials after the conference
- Kimberly Simmermaker ksimmermaker@uwaterloo.ca - registration, support and general magic
- William Stacey wstacey@ualberta.ca - industrial exhibit



We thank other people not listed who offered helping hands when needs arose.

Special thanks to Anne Broadbent (IQC Waterloo) for raising the sheep Loulou and other fluffy critters.

QCrypt charter

Goal of the conference

The Annual conference on quantum cryptography (QCrypt) is a conference for students and researchers working on all aspects of quantum cryptography. This includes theoretical and experimental research on the possibilities and limitations of secure communication and computation with quantum mechanical devices or in the presence of quantum mechanical devices. (The conference includes but is not limited to research on quantum key distribution.)

It is the goal of the conference to represent the previous year's best results on quantum cryptography and to support the building of a research community in quantum cryptography. In order to achieve this goal, the conference will feature both invited and contributed talks, selected by the steering committee and programme committee, respectively. In line with this goal, the conference has no published proceedings. QCrypt welcomes the submission of any interesting and important result, while allowing researchers from a wide range of disciplines to pursue publication in any appropriate venue.

Steering committee

The steering committee (SC) is responsible for shaping the medium- and long-term course of the conference series and for making sure that the conferences maintain a high scientific and organisational standard. In particular, the SC has the responsibility to select the main organiser, venue and programme chair for the next conference. The SC has approximately 7 members and is chaired by the next conference's main organiser. The SC chair is responsible for the external relations of the conference.

The first two conferences will take place at the ETH Zurich and CQT Singapore, and the organisers are prepared to continue organizing the conference alternately. This cycle may be expanded if proposals of high quality are received to host the conference. The conference takes place over one week (Monday to Friday) in August or September, although some flexibility may be permitted depending on local circumstances.

The SC selects the invited speakers. At most half of the talk time of the conference can be given to invited speakers. The remaining talk time is reserved for contributed talks. SC members cannot be invited speakers, but are allowed to submit and present contributed papers.

Program committee

The role of the program committee (PC) is to select the best submissions. The PC chair (selected by the SC), helped by advice from the SC, recruits the PC members, typically 10 or more people representing the broad range of subfields specified above. PC members are allowed to submit papers and to present contributed papers. PC members must declare a conflict of interest on submissions to which they contributed so that they are not involved in discussing these papers in the PC.

Advisory committee

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

2013.qcrypt.net

Next QCrypt conference will take place September 1-5, 2014 in Paris.

University of Waterloo north campus

University of Waterloo south campus

