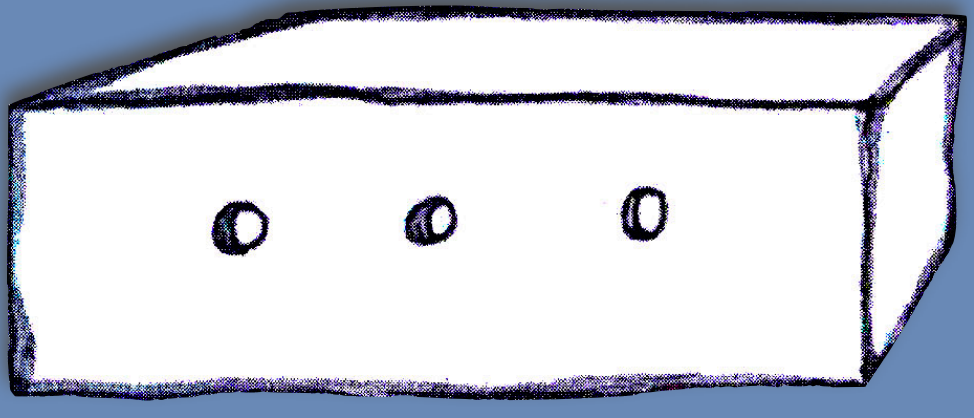
QCRYPT 2019

26-30 AUGUST 2019



TOURISME / MONTRÉAL

$|\uparrow\downarrow\rangle$

Gold Sponsors

Silver Sponsors

INSTITUT TRANSDISCIPLINAIRE
D'INFORMATION QUANTIQUE

Bronze Sponsors

Welcome to QCrypt2019

QCrypt 2019, the 9th International Conference on Quantum Cryptography, is the place where the most important new results in quantum cryptography are presented and discussed. The conference aims at helping build our research community by encouraging computer scientists, mathematicians, physicists and engineers to interact on different aspects of quantum cryptography. To fulfil this mission, 4 tutorials, 8 invited speakers, 28 contributed papers (of which two were asked to merge), 8 industry session panelists and nearly 150 posters have been selected to form an exciting program. In addition, Michele Mosca has agreed to deliver a public lecture on *Building a more secure quantum future*. This event is open to everyone free of charge.

This 2019 edition is organized jointly by the Université de Montréal (Gilles Brassard and Louis Salvail), McGill University (Claude Crépeau), and the Université du Québec à Montréal (Sébastien Gambs), with substantial logistic and financial help from Tourisme Montréal. The conference is taking place at the Cœur des sciences, on the campus of Université du Québec à Montréal. This is located near many attractions that Montreal has to offer. The conference banquet takes place in the beautiful Belvédère of the Centre des sciences de Montréal.

Many people have provided us with invaluable help. In particular, we are grateful to the program committee, chaired by Anthony Leverrier, for having selected the contributed talks among 98 submissions, and to the steering committee, chaired by Marcos Curty, for having planed the tutorials and the invited talks. Many thanks to Christoph Marquardt and Hugo Zbinden for the organization of the industry session. A special thank you to Simon Désaulniers for his help in many practical aspects of the conference planning and in designing this booklet. We also thank all the personnel of the departments of Computer Science both at the University of Montréal and at the Université du Québec à Montréal, as well as from the Cœur des Sciences, who were involved in many aspects of the organization of this event. Last but not least, we are very grateful to our sponsors, without whom the organization of such a conference would be nearly impossible.

We wish you all an enjoyable and productive conference.

Gilles, Claude, Sébastien and Louis, 19 August 2019.

WiFi on the campus

If you need to connect to the Internet, feel free to use our private WiFi access.

Network	`Visiteurs UQAM`
Username	`coeurdessciences1`
Password	`b372RKu2`

Schedule

All talks will take place in the Amphithéâtre of Cœur des sciences, except for the rump session, which will take place in the Agora.

In the following pages, the type of an event is T for Tutorial, I for Invited and C for Contributed.

Sunday, 25 August 2019

18:00 to 21:00: Opening Reception, (Salle polyvalente)

Monday, 26 August 2019

Time	Type	Author(s)	Title
9:00	T	Norbert Lütkenhaus	Implementation security of QKD
10:15	**Break (Salle polyvalente)**		
10:45	I	Ronald Hanson	Quantum networks of diamond spins

11:20	C	Gayane Vardoyan, Saikat Guha, Philippe Nain and Don Towsley	On the capacity region of bipartite and tripartite entanglement switching and key distribution
11:40	C	Daniel Llewellyn, Caterina Vigliar, Benjamin Slater, Beatrice Da Lio, Stefano Paesani, Jorge Barreto, Dondu Sahin, Massimo Borghi, John G. Rarity, Leif K. Oxenløwe, Karsten Rottwitt, Jianwei Wang, Yunhong Ding, Mark G. Thompson and Davide Bacco	High-dimensional chip-to-chip entanglement distribution through multicore fibre
12:00	**Lunch (on your own)**		
13:30	I	Jigang Ren	QKD based on satellite-ground entanglement distribution
14:05	C	Marco Avesani, Luca Calderaro, Matteo Schiavon, Costantino Agnesi, Alberto Santamato, Andrea Stanco, Mujtaba Zahidy, Alessia Scriminich, Giulio Foletto, Giampiero Contestabile, Marco Chiesa, Alessandro Nottola, Davide Rotta, Stefano Tirelli, Massimo Artiglia, Alberto Montanaro, Marco Romagnoli, Vito Sorianello, Daniele Dequal, Giuseppe Bianco, Claudia Facchinetti, Alberto Tuozzi, Francesco Vedovato, Giuseppe Vallone and Paolo Villoresi	QCoSOne: A chip-based prototype for daylight free-space QKD at telecom wavelength for future satellite optical payloads
14:25	C	Henry Semenenko, Philip Sibson, Andy Hart, Mark Thompson and Chris Erven	Chip-based measurement-device-independent quantum key distribution

14:45	C	Tobias Eriksson, Takuya Hirano, Benjamin Puttnam, Georg Rademacher, Ruben Luís, Mikio Fujiwara, Ryo Namiki, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada and Masahide Sasaki	Continuous variable quantum key distribution multiplexed with high throughput coherent channels
15:05	**Break (Salle polyvalente)**		
15:35	C	Ignatius William Primaatmaja, Emilien Lavie, Koon Tong Goh, Chao Wang and Charles Ci Wen Lim	Almost-tight and versatile security analysis of measurement-device-independent quantum key distribution
15:55	C	Niraj Kumar, Iordanis Kerenidis and Eleni Diamanti	Experimental demonstration of quantum advantage for one-way communication complexity with application in construction of robust quantum money
16:15-16:35	C	Norbert Lütkenhaus, Ashutosh Marwah and Dave Touchette	Erasable bit commitment from temporary quantum trust
16:45-18:45	**Poster Session (mostly odd-numbered posters)**		
19:00-20:15	**Building a more secure quantum future** A Public Lecture by Michele Mosca		

T: Tutorial, I: Invited, C: Contributed

Tuesday, 27 August 2019

Time	Type	Author(s)	Title
9:00	T	Rotem Arnon-Friedman	DI-QKD and DI-QRNG, discussing security proofs and practical challenges
10:15	**Break (Salle polyvalente)**		
10:45	I	Eneet Kaur	Fundamental limits on key rates in DI-QKD

11:20	C	René Schwonnek, Ernest Y.-Z. Tan, Ramona Wolf, Koon Tong Goh and Charles C.-W. Lim	A numerical method for computing reliable secret key rates for device-independent quantum key distribution
11:40	C	Alex Bredariol Grilo	A simple protocol for verifiable delegation of quantum computation in one round
12:00-12:20	C	Rotem Arnon-Friedman and Jean-Daniel Bancal	Device-independent certification of one-shot distillable entanglement
12:30	**Group Photo**		
After-noon	**Free time**		

T: Tutorial, I: Invited, C: Contributed

Wednesday, 28 August 2019

Time	Type	Author(s)	Title
9:00	T	Fang Song	Zero-knowledge proofs meet quantum computing
10:15	**Break (Salle polyvalente)**		
10:45	I	Zvika Brakerski	Quantum fully homomorphic encryption
11:20	C	Thomas Vidick and Tina Zhang	Classical zero-knowledge arguments for quantum computations
11:40	C	Alex Bredariol Grilo, William Slofstra and Henry Yuen	Perfect zero knowledge for quantum multiprover interactive proofs
12:00	**Lunch (on your own)**		
13:30	I	Stefanie Barz	Secure computing with classical and quantum resources

14:05	C	Kento Maeda, Toshihiko Sasaki and Masato Koashi	Operator dominance method: a simple monitoring scheme of a TF-type QKD in finite-size regime
14:25	C	Yang Liu, Zong-Wen Yu, Weijun Zhang, Jian-Yu Guan, Jiu-Peng Chen, Chi Zhang, Xiao-Long Hu, Hao Li, Teng-Yun Chen, Lixing You, Zhen Wang, Xiang-Bin Wang, Qiang Zhang and Jian-Wei Pan	Experimental Twin-field quantum key distribution through sending-or-not-sending
14:40	C	Mariella Minder, Mirko Pittaluga, George L. Roberts, Marco Lucamarini, James F. Dynes, Zhiliang Yuan and Andrew J. Shields	Experimental twin field quantum key distribution beyond the repeaterless secret key capacity bound
14:55	C	Xiaoqing Zhong, Jianyong Hu, Marcos Curty, Li Qian and Hoi-Kwong Lo	Proof-of-principle experimental demonstration of twin-field type quantum key distribution
15:10	**Break (Salle polyvalente)**		
15:40	C	Anne Broadbent and Sébastien Lord	Uncloneable quantum encryption via oracles
16:00	C	Myrto Arapinis, Mahshid Delavar, Mina Doosti and Elham Kashefi	Security analysis of quantum physical unclonable functions
16:20-16:40	C	Marie-Christine Roehsner, Joshua Kettlewell, Tiago Batalhao, Joseph Fitzsimons and Philip Walther	Quantum advantage for probabilistic one-time programs
16:45-18:45	**Poster Session (mostly even-numbered posters)**		
19:15-23:00	**Banquet** **With the special participation of illusionist Luc Langevin** Salle belvédère du Centre des sciences de Montréal		

T: Tutorial, I: Invited, C: Contributed

Thursday, 29 August 2019

Time	Type	Author(s)	Title
9:00	T	Manfred Lochter	Practical Quantum Security: A user perspective
10:15	**Break (Salle polyvalente)**		
10:45	I	Mark L. Zhandry	Quantum techniques in post-quantum crypto
11:20	C	Yanbao Zhang, Honghao Fu, Krister Shalm, Joshua Bienfang, Martin Stevens, Michael Mazurek, Sae Woo Nam, Carlos Abellan, Waldimar Amaya, Morgan Mitchell, Carl Miller, Alan Mink and Emanuel Knill	Efficient randomness certification by quantum probability estimation
11:40	C	Davide Rusca, Thomas van Himbeeck, Anthony Martin, Jonatan Bohr Brask, Hamid Tebyanian, Stefano Pironio, Nicolas Brunner and Hugo Zbinden ↑ merged with ↓ Thomas Van Himbeeck and Stefano Pironio	Fast and practical implementation of self-testing QRNG based on an energy bound. ↑ merged with ↓ Correlations and randomness generation based on an energy constraint
12:00	**Lunch (on your own)**		
13:30	I	Zhiliang Yuan	10 Mb/s quantum key distribution
14:05	**Industry Session**†		
16:45	Business Meeting and Prize Ceremony		
19:00	**Rump Session** **Organized by Charles Bennett in Agora of Coeur des sciences** (cold food and drinks will be available during the session)		

T: Tutorial, I: Invited, C: Contributed

Industry session†

Organized by Christoph Marquardt (Max Planck Institute) and Hugo Zbinden (University of Geneva) with the participation of eight panelists:

- Juan Miguel Arrazola (Xanadu)
- Rachid El Bansarkhani (QuantiCor Security)
- Cordell Grant (QEYnet)
- Imran Khan (Infiniquant)
- Michele Mosca (evolution Q)
- Stefan Röhrich (Rohde & Schwarz Cybersecurity)
- Gene Savchuk (QuantumXC)
- Patrick Scully (Ciena)

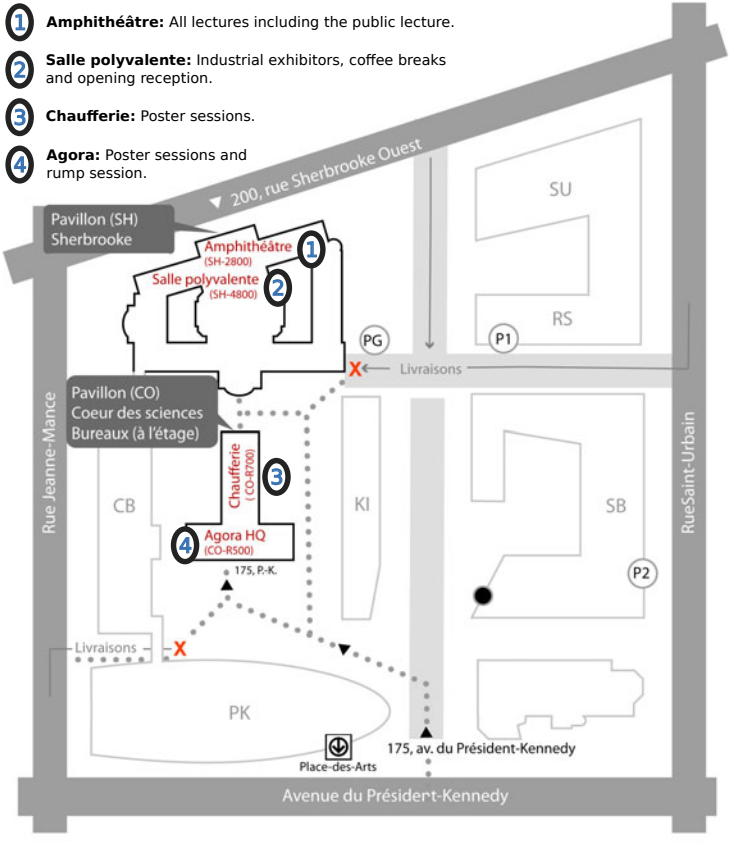
There will be a 30 minute break in the middle of the session.

Friday, 30 August 2019

Time	Type	Author(s)	Title
9:00	I	Gorjan Alagic	Can you sign a quantum state?
9:35	C	Jelle Don, Serge Fehr, Christian Majenz and Christian Schaffner	Security of the Fiat-Shamir transformation in the quantum random-oracle model
9:55	C	Fabio Banfi, Ueli Maurer, Christopher Portmann and Jiamin Zhu	Composable and finite computational security of quantum message transmission
10:15	**Break (Salle polyvalente)**		
10:45	C	Jan Czajkowski, Christian Majenz, Christian Schaffner and Sebastian Zur	Quantum lazy sampling and game-playing proofs for quantum indifferentiability
11:05	C	Alexandru Gheorghiu and Thomas Vidick	Computationally-secure and composable remote state preparation
11:25	C	Christian Majenz, Christian Schaffner and Jeroen van Wier	Non-malleability for quantum public-key encryption
11:45	**End of Conference**		

T: Tutorial, I: Invited, C: Contributed

Map of Conference Venue



Building a more secure quantum future

A Public Lecture by Michele Mosca

Abstract

While quantum computers will bring immense computing capability that cannot be achieved with any feasible amount of regular computing power, they also break some of the mostly widely used codes that we depend on to protect our digital systems. For the advent of a quantum computer to be a positive milestone in human history, we must first fix these fundamental building blocks of cyber security.

Come hear how this threat is actually a great opportunity to make our digital infrastructures more secure than they otherwise would be. And learn about the exciting science that underpins new tools for making our world more safe and secure, including quantum satellite communications.

Michele Mosca is co-founder of the Institute for Quantum Computing at the University of Waterloo, a Professor in the Department of Combinatorics & Optimization of the Faculty of Mathematics, and a founding member of Waterloo's Perimeter Institute for Theoretical Physics. He was the founding Director of CryptoWorks21, a training program in quantum-safe cryptography. He is a founder of the ETSI-IQC workshop series in Quantum-Safe Cryptography, and the not-for-profit Quantum-Safe Canada. He co-founded evolutionQ Inc. to support organizations as they evolve their quantum-vulnerable systems to quantum-safe ones and softwareQ Inc. to provide quantum software tools and services.

He obtained his doctorate in Mathematics in 1999 from Oxford on the topic of Quantum Computer Algorithms. His research interests include quantum computation and cryptographic tools designed to be safe against quantum technologies. He is globally recognized for his drive to help academia, industry and government prepare our cyber systems to be safe in an era with quantum computers.

Dr. Mosca's awards and honours include 2010 Canada's Top 40 Under 40, Queen Elizabeth II Diamond Jubilee Medal (2013), SJU Fr. Norm Choate Lifetime Achievement Award (2017), and a Knighthood (Cavaliere) in the Order of Merit of the Italian Republic (2018).

How to Reach the Banquet

The address to the banquet is the following:

```
Salle Belvédère
2 rue de la Commune
Quai King Edward
Centre des sciences de Montréal
Vieux-Port (Old Harbour)
```

To get there, one can take the subway up to station Place d'Armes. Once out of the subway, it is a 9 minute walk to Salle Belvédère. Alternatively, you can walk from the conference venue to the banquet in less than a half hour by going down Saint-Urbain Street.

Industrial Exhibitors

Exhibitor booths will be displayed in the coffee break room. The room is called Salle polyvalente (SH-4800) and is located just above the Amphithéâtre (SH-2800) in which lectures will take place.