ETH Zurich
Schafmattstrasse
8093 Zurich
www.qcrypt.net

QCRYPT 2011

FIRST ANNUAL CONFERENCE ON QUANTUM CRYPTOGRAPHY
SEPTEMBER 12 – 16, 2011

PROGRAMME

Department of Physics

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Sponsors

PAULI CENTER
for Theoretical Studies

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

QSIT Quantum Science and Technology
National Centre of Competence in Research

nano-tera.ch

CQT Centre for Quantum Technologies

IQC Institute for Quantum Computing

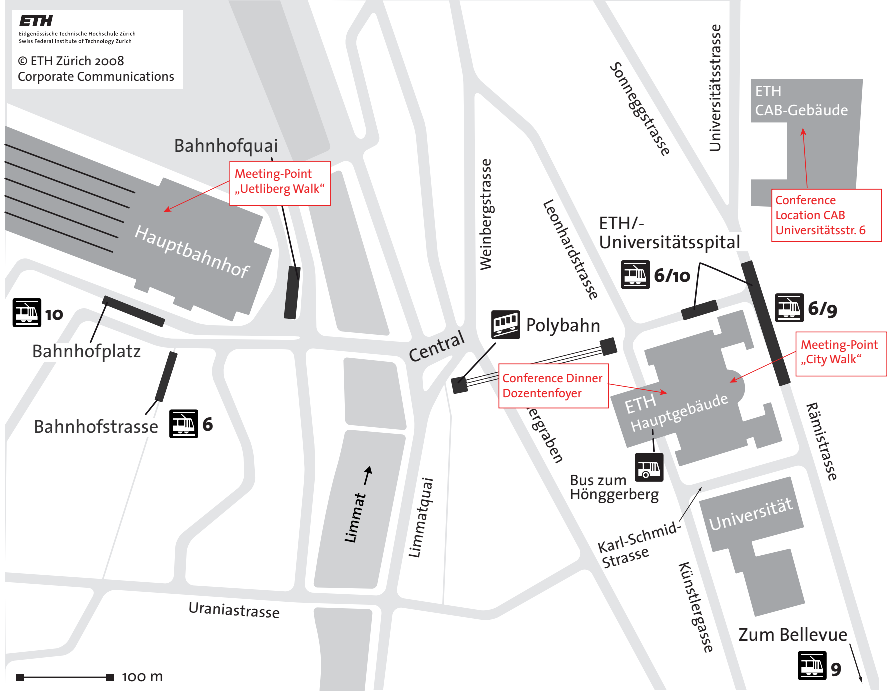
IDQ FROM VISION TO TECHNOLOGY

FNSNF
FONDS NATIONAL SUISSE
SCHWEIZERISCHER NATIONALFONDS
FONDO NAZIONALE SVIZZERO
SWISS NATIONAL SCIENCE FOUNDATION

DFG

Content

Information (Map and WLAN)



Venue

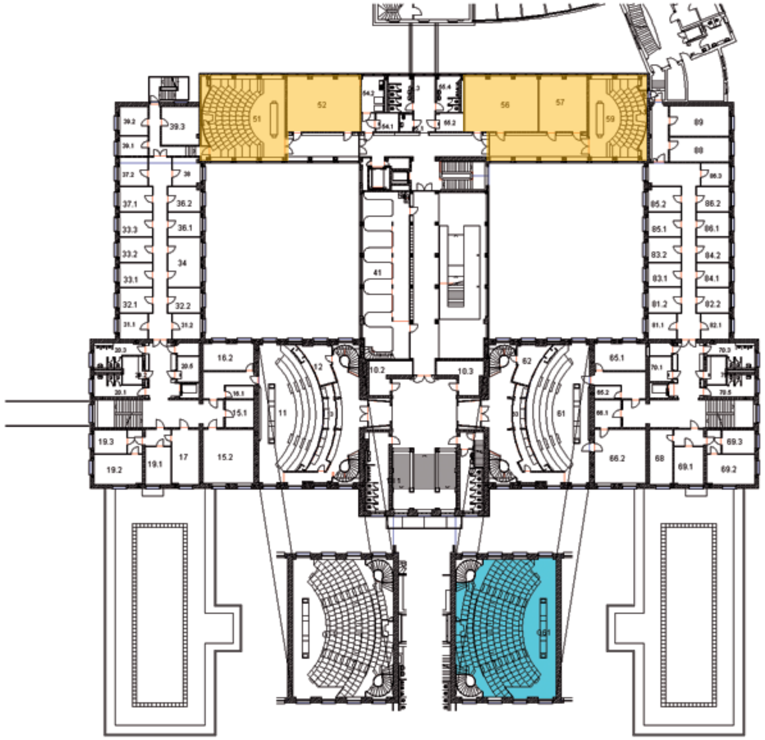
ETH Zürich
Building CAB
Conference room G 61
Universitätstrasse 6
8092 Zürich

W-LAN

1. Check available WLAN
2. Connect to WLAN "public"
3. Open browser
4. Login at welcome page with

Login: qcrypt11
Password: september

Rooms (floor G, building CAB)



🟨 Meeting and working rooms

G 51
G 52
G 56
G 57
G 59

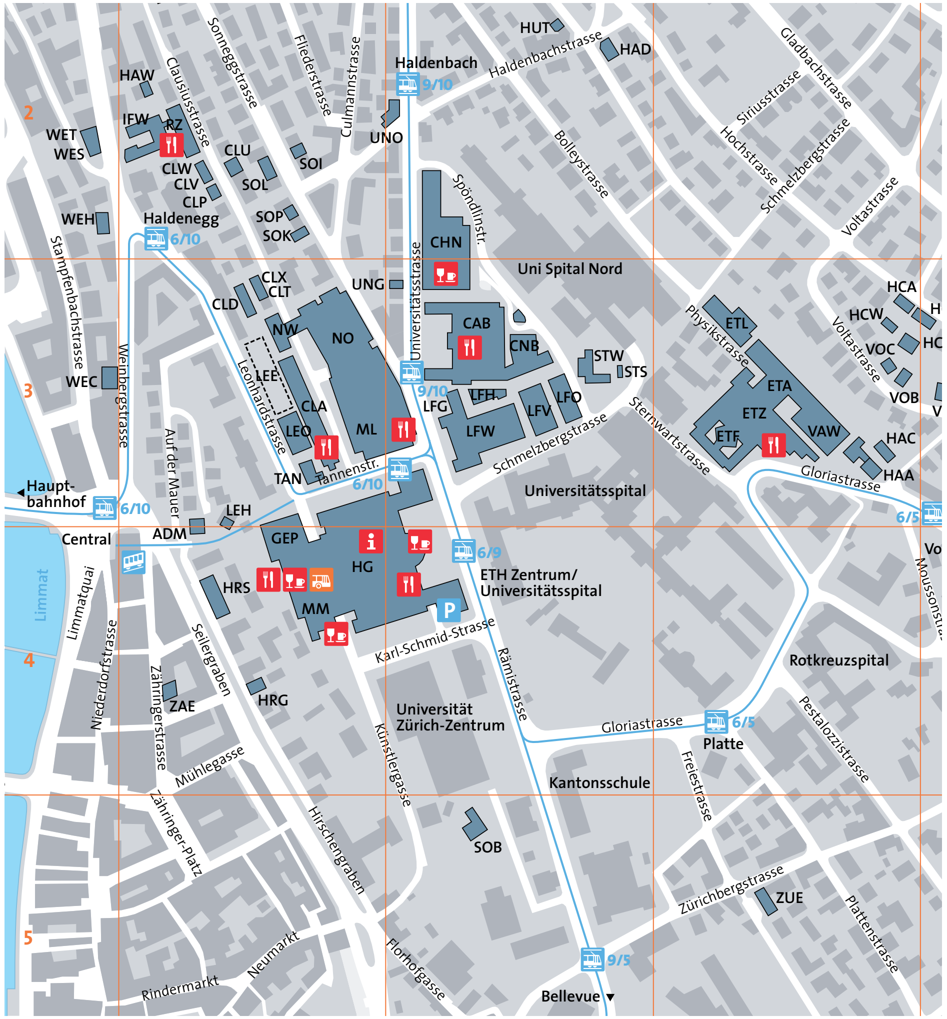
🟦 Conference room

G 61

Opening hours of ETH canteens

Monday, September 12 – Friday, September 16, 2011

Location	Opening hours
CHN Bistro Universitätsstrasse 22 Building CHN	09.00 – 16.30 (closed on Monday, Sept. 12)
foodLAB Universitätsstrasse 6 Building CAB	08.30 – 15.30 (recommended on Monday, Sept. 12)
Tannenbar Corner Universitäts-/Tannenstrasse Building ML	07.00 – 17.00
Clausiusbar Tannenstrasse 3 Building CLA	07.30 – 16.00
Mensa Polyterrasse Leonhardstrasse 34 Building MM B	11.15 – 13.30 17.30 – 19.30
Cafeteria Polyterrasse Leonhardstrasse 34 Building MM C	06.45 – 19.45
bQM Leonhardstrasse 34 Building MM C	11.30 – 22.00
Polysnack Rämistrasse 101 Building HG F32	07.30 – 17.00
CafeBar Rämistrasse 101 Building HG main entrance	07.00– 19.00



Tramhaltestelle

Polybahn

ETH-Pendelbus «Science City Link»

Mensa

Cafeteria

Info-Loge Hauptgebäude (Telefon +41 44 632 25 50)

Social programmes

Wednesday, September 14, 2011

(The list of the registered participants for the Guided City Walk and for the walk to Uetliberg will be announced at the conference).

1. Guided City Walk (2 hours)
The walk starts at exactly 14.30 and we will meet at the main entrance of the main building ETH Zentrum (HG).
Guides: Renata Keller and Annamària Pàl-Müller

2. Walk to a local hill (Uetliberg)
13:50 Meet under the blue angel in the mainhall of the
railway station Zurich (Hauptbahnhof),
lunch packs and tickets will be distributed on the train.
14:05 Take the train to Uitikon Waldegg (S10, Gleis 2)
14:18 Walk up
16:00 Arrive at the top
17:36 Take the train back to the Hauptbahnhof
(also at 17:06, 18:06, takes approx. 25 min)

3. Conference Dinner
The conference dinner starts at 19:00.
Take elevator in the main building (HG) to floor J and walk up the stairs to:

Restaurant "Dozentenfoyer"
Main Building (HG), Floor J
Rämistrasse 101, 8092 Zürich

1

2

Committees

Steering Committee

Matthias Christandl (chair)
Roger Colbeck
Michele Mosca
Renato Renner
Louis Salvail
Wolfgang Tittel
Stephanie Wehner

Programme Committee

Romain Alléaume
Aram Harrow
Hoi-Kwong Lo
Norbert Lütkenhaus
Valerio Scarani
Christian Schaffner
Barbara Terhal (chair)
Gregor Weihs
Jürg Wullschleger

Advisory Committee

Charles H. Bennett
Gilles Brassard
Ivan Damgaard
Artur Ekert
Nicolas Gisin
Richard Hughes
Masahide Sasaki

Local Organizing Committee

Matthias Christandl (Coordination)
Beatrix Hottiger (Administration)
Lidia del Rio (Poster)
Michael Walter (Website)

Scientific programme

Monday, September 12, ETH, Building CAB, Universitätstrasse 6, 8092 Zürich

08.00	Registration at ETH Zurich, CAB building, floor G, in front of the lecture hall 61
09.00	Opening of QCRYPT 2011 Introduction by Professor Dr Olaf Kübler, former president of ETH Zurich
09.05	**Artur Ekert** • Quo vadis, quantum cryptography
10.00	Marcin Pawlowski and **Nicolas Brunner** • Semi-device-independent security of one-way quantum key distribution
10.30	Break
11.00	**Eugene Polzik** • Quantum memories for light: status and perspectives
12.00	**Andreas Poppe**, Isabelle Herbauts, Bibiane Blauensteiner, Thomas Jennewein and Hannes Huebel • On-demand Entanglement Distribution Network
12.30	Lunch (recommended for Monday: restaurant foodLAB in the CAB building)
14.00	**Robert König** • Simplified instantaneous non-local quantum computation with applications to position-based cryptography
15.00	Harry Buhrman, Serge Fehr, Christian Schaffner and **Florian Speelman** • The Garden-Hose Game and Application to Position-Based Quantum Cryptography
15.30	Break
16.00	**Anne Broadbent** • Quantum Computing on Encrypted Data
16.30	Gilles Brassard, Peter Hoyer, **Kassem Kalach**, Marc Kaplan, Sophie Laplante and Louis Salvail • Merkle Puzzles in a Quantum World
17.00	Welcome Apéro

Scientific programme

Tuesday, September 13, ETH, Building CAB, Universitätstrasse 6, 8092 Zürich

09.00	**Philippe Grangier** • Quantum Cryptography with Continuous Variables
10.00	Guido Berlin, Gilles Brassard, **Félix Bussières**, Nicolas Godbout, Joshua A. Slater and Wolfgang Tittel • Experimental quantum coin flipping in the presence of loss
10.30	Break
11.00	**Dominique Unruh** • Composition in Quantum Cryptography
12.00	**Severin Winkler**, Marco Tomamichel, Stefan Hengl and Renato Renner • Impossibility of Growing Commitments
12.30	Lunch
14.00	**Masahide Sasaki** • Wavelength Division Multiplexing Quantum Key Distribution with High Throughput Key Distillation Engine
15.00	**Nino Walenta**, Charles Ci Wen Lim, Olivier Guinnard, Raphael Houlmann and Hugo Zbinden • Fast coherent-one way quantum key distribution and high-speed encryption
15.30	**Paul G. Kwiat**, Kevin T. McCusker and Bradley Christensen • Higher-Dimensional Quantum Cryptography
16.00- 18.00	Break and Poster Session

Scientific programme

Wednesday, September 14, ETH, Building CAB, Universitätstrasse 6, 8092 Zürich

09.00	**Nicolas Gisin** • Quantum Memories for Quantum Networks and Device-Independent QKD
10.00	**Stephanie Wehner** • Security in the noisy-storage model
10.30	Break
11.00	**Thomas Vidick** • Randomness extraction against quantum adversaries
12.00	**Toyohiro Tsurumaru** and Masahito Hayashi • Dual universality of hash functions and its applications to classical and quantum cryptography
12.30	**Feihu Xu**, Bing Qi, Xiongfeng Ma, He Xu, Haoxuan Zheng and Hoi-Kwong Lo • A high speed quantum random number generator with quantum phase noise
13.00	Lunch and Excursions
19.00- 23.00	Conference Dinner (Dozentenfoyer at ETH Zurich, main building, floor J) After Dinner Speech by Charles Bennett and Gilles Brassard

Scientific programme

Thursday, September 15, ETH, Building CAB, Universitätstrasse 6, 8092 Zürich

09.00	**Vadim Makarov** • Loopholes in implementations of quantum cryptography
10.00	Lluis Masanes, Stefano Pironio and **Antonio Acin** • Secure device-independent quantum key distribution with causally independent measurement devices
10.30	Break
11.00	**Richard J. Hughes** • Satellite-based quantum communications
12.00	**Jean-Philippe Bourgoin**, Evan Meyer-Scott, Bassam Helou and Thomas Jennewein • Detailed link analysis of satellite quantum communication
12.30	Lunch
14.00	**Marco Tomamichel** and Renato Renner • The Uncertainty Relation and its Applications in Cryptography
14.30	**Niek J. Bouman**, Serge Fehr, Carlos Gonzalez-Guillen and Christian Schaffner • An All-But-One Entropic Uncertainty Relation, and Application to Password-based Identification
15.00	Break
15.30	**Industry Venture Session**
17.00-19.00	Apéro and Industry Showcase

Scientific programme

Friday, September 16, ETH, Building CAB, Universitätstrasse 6, 8092 Zürich

09.00	**Andrew Shields** • High bit rate QKD
10.00	**Fabian Steinlechner**, Pavel Trojek, Marc Jofre, Arnaud Gardelein, Harald Weinfurter and Valerio Pruneri • A high brightness source of polarization entangled photons
10.30	Break
11.00	**Jonathan Oppenheim** • Public Quantum Communication
12.00	**Debbie Leung**, Patrick Hayden and Dominic Mayers • Universal composable security of quantum message authentication with key recycling
12.30	Closing Remarks

Affiliated Meeting: Space-QUEST Topical Team Meeting

The Space-QUEST project will hold its Topical Team Meeting on Friday, September 16, 2011 in the afternoon.
Participants of QCRYPT are welcome to attend this event.

Friday, September 16, ETH, Building CAB, Universitätstrasse 6, 8092 Zürich

14.00	Space-QUEST Topical Team Meeting
15.30	Break
15.45-17.00	Space-QUEST Topical Team Meeting

Poster session

There will be a poster session on Tuesday, September 13 between 16:00 – 18:00. The following posters have been accepted.

1	Aysajan Abidin and Jan-Åke Larsson • Security of Authentication with a Fixed Key in Quantum Key Distribution
2	Razieh Annabestani and Norbert Lutkenhaus • Efficient QKD on Trusted Repeater Networks
3	M. Bawaj, M. Lucamarini, G. Di Giuseppe, D. Vitali and P. Tombesi • Decoy-detector technique implementation based on Field Programmable Gate Array (FPGA)
4	Aurélien Bocquet, Anthony Leverrier and Romain Alléaume • Optimal eavesdropping on BB84 without quantum memory
5	Jan Bouda, Matej Pivoluska and Martin Plesch • Encryption with weakly random keys using quantum cyphertext
6	Abdessattar Bouzid, Jun-Bum Park, Sean Kwak and Sung Moon • Reduced after-pulsing of InGaS/InP single photon avalanche diodes for quantum cryptography
7	Cyril Branciard • One-side Device Independent Quantum Key Distribution: Security and feasibility
8	S. Bratzik, S. Abruzzo, M. Mertz, H. Kampermann and D. Bruß • Quantum key distribution with finite resources: Min-entropy vs. von Neumann-entropy
9	Matteo Canale, Davide Bacco, Simon Calimani, Francesco Renna, Nicola Laurenti, Giuseppe Vallone and Paolo Villoresi • Performance analysis of a low-cost, low-complexity, free-space QKD scheme based on the B92 protocol
10	Marcos Curty and Tobias Moroder • Heralded qubit amplifiers for device-independent quantum key distribution
11	Jörg Duhme • Quantum key distribution on Hannover Campus: Theory
12	T. Eberle, V. Händchen, J. Duhme, T. Franz, R. F. Werner and R. Schnabel • Quantum Key Distribution on Hanover Campus: Experiment
13	T. Ferreira da Silva, G. B. Xavier, J. P. von der Weid and G. P. Temporão • Monitoring single-photon detectors against eavesdropping in quantum cryptography systems
14	Torsten Franz, Fabian Furrer and Reinhard F. Werner • Extremal Quantum Correlations and Cryptographic Security
15	Mario Berta, Fabian Furrer and Volkher B. Scholz • The Smooth Entropy Formalism on von Neumann Algebras
16	N. Daniel Kumar • Key generation across an untrusted entanglement-free QKD network
17	Rupesh Kumar • Experimental one-way quantum key distribution with Trines
18	Charles Ci Wen Lim, Nino Walenta and Hugo Zbinden • A new Coherent One-Way protocol that is highly immune against unambiguous state discrimination attacks
19	M. Lucamarini, M. Bawaj, G. Di Giuseppe, D. Vitali and P. Tombesi • Recent advancements in the Bennett 1992 protocol
20	Mhlambululi Mafu, Adriana Marais and Francesco Petruccione • Towards the security of coherent-one-way quantum key distribution protocol
21	Anne Marin and Damian Markham • Reed Solomon Codes for Quantum Secret Sharing Protocols
22	Kevin T. McCusker and Paul G. Kwiat • Engineering and Applications of High-Efficiency Heralding of Single Photons
23	Markus Mertz • QKD with finite resources: The role of quantum noise
24	C. Pacher, A. Abidin, T. Lorünser, M. Peev, R. Ursin, A. Zeilinger and J.-A. Larsson • Hacking QKD protocols that employ non-ITS authentication
25	Stefano Bettelli, Momtchil Peev and Christoph Pacher • Symmetries and attack parametrisation in discrete-variable quantum cryptographic protocols

26	Anna Pappa, Andre Chailloux, Eleni Diamanti and Iordanis Kerenidis • Practical Quantum Coin Flipping
27	Christian Peuntinger, Bettina Heim, Christopher Wittmann, Christoph Marquardt and Gerd Leuchs • Daylight Free-Space Quantum Communication using Continuous Polarization Variables
28	Michael A. Popov • Quantum Immune One-Way Function
29	Lorenzo Procopio • Spatial correlations of photon pairs generated by spontaneous parametric down conversion
30	Daniel Barbosa de Brito, Fábio Alencar Mendonça and Rubens Viana Ramos • Theory and Applications of the Spectral Analysis of the Photocurrent produced by Single-Photon Detectors
31	Sebastian Nauerth, Markus Rau, Martin Fürst, Henning Weier, Christian Kurtsiefer and Harald Weinfurter • High speed quantum random number generation
32	Markus Rau, Sebastian Nauerth, Martin Fürst, Harald Weinfurter, Tobias Heindel, Christian Schneider, Stephan Reitzenstein, Sven Höfling, Martin Kamp and Alfred Forchel • Freespace QKD using a Quantum Dot-Micropillar Single Photon Source
33	Mohsen Razavi • Synchronous versus Asynchronous Secret Key Exchange over Star Networks
34	Adriana Marais and Lana Sheridan • Security in the Differential Phase Shift Protocol
35	Lana Sheridan, Thinh Phuc Le and Valerio Scarani • The Reference Frame Independent Protocol: Finite-key security and Generalizations
36	Constantin V. Usenko • One more series of protocols for quantum cryptography
37	Shuang Wang, Wei Chen, Zheng-Qiang Yin, Guang-Can Guo and Zheng-Fu Han • Field test of the wavelength-saving quantum key distribution network
38	Shun Watanabe • Finite Analysis of QKD Protocol with Hashed Two-Way Classical Communication
39	Christian Weedbrook • Continuous-Variable Quantum Key Distribution using Thermal States
40	W. Donderowicz, A. Janutka, M. Jacak, J. Gruber, P. Tomczak, G. Kayyali, I. Jóźwiak and W. Jacak • Wrocław University of Technology Quantum Cryptography Laboratory Research Programme
41	G. B. Xavier, G. P. Temporão and J. P. von der Weid • Quantum cryptography in long optical fibers employing orthogonal states
42	Nelly Ng Huei Ying and Stephanie Wehner • Implementation of Bit Commitment protocol in the Noisy Storage Model
43	Matteo Canale, Francesco Renna, Nicola Laurenti • QKD secrecy for privacy amplification matrices with selective individual attacks