

QCrypt 2021 business meeting

Agenda

- 2021 local committee report [Chris & Serge] (10 mins)
- 2021 program committee report [Carl & Tobias] (10 mins)
- 2022 presentation [2022 LC] (10 mins)
- 2023 solicitation of proposals [chair] (1 min)
- Questions/discussions [chair] (5-10 mins)
- ***2021 Best Student Paper Prize: Carl & Tobias (10 mins)***

QCrypt 2021 business meeting

Agenda

- 2021 local committee report [Chris & Serge] (10 mins)
- 2021 program committee report [Carl & Tobias] (10 mins)
- 2022 presentation [2022 LC] (10 mins)
- 2023 solicitation of proposals [chair] (1 min)
- Questions/discussions [chair] (5-10 mins)
- 2021 Best Student Paper Prize: Carl & Tobias (10 mins)



Christoph Marquardt
Max Planck Institute for the Science
of Light

SC chair



Gorjan Alagic
University of Maryland

SC co-chair



Akihisa Tomita
Hokkaido University

SC member



Serge Fehr
CWI Cryptology group, Leiden
University

SC member



Feihu Xu
University of Science and
Technology of China

SC member



Stacey Jeffery
CWI

SC member



Hugo Zbinden
University of Geneva

SC member



Marco Lucamarini
University of York

SC member

QCrypt 2021 business meeting

Agenda

- ***2021 local committee report [Chris & Serge] (10 mins)***
- 2021 program committee report [Carl & Tobias] (10 mins)
- 2022 presentation [2022 LC] (10 mins)
- 2023 solicitation of proposals [chair] (1 min)
- Questions/discussions [chair] (5-10 mins)
- 2021 Best Student Paper Prize: Carl & Tobias (10 mins)

QCrypt 2021 business meeting

Agenda

- 2021 local committee report [Chris & Serge] (10 mins)
- 2021 program committee report [Carl & Tobias] (10 mins)
- 2022 presentation [2022 LC] (10 mins)
- ***2023 solicitation of proposals [chair] (1 min)***
- Questions/discussions [chair] (5-10 mins)
- 2021 Best Student Paper Prize: Carl & Tobias (10 mins)

QCrypt 2021 business meeting

Hosting QCrypt 2023!

If you are interested, please send a letter of intent to
qcrypt-steer@googlegroups.com

by Nov. 1, 2021, with the following information:

1. Name and affiliation of main organizer
2. Possibilities of conference dates (preferably in late August 2023)
3. Location and size of intended conference venue
4. Contingency for fully or partially virtual event

The steering committee will ask the top contenders to work out a full proposal.

QCrypt 2021 business meeting

Agenda

- 2021 local committee report [Chris & Serge] (10 mins)
- 2021 program committee report [Carl & Tobias] (10 mins)
- 2022 presentation [2022 LC] (10 mins)
- 2023 solicitation of proposals [chair] (1 min)
- ***Questions/discussions [chair] (5-10 mins)***
- 2021 Best Student Paper Prize: Carl & Tobias (10 mins)

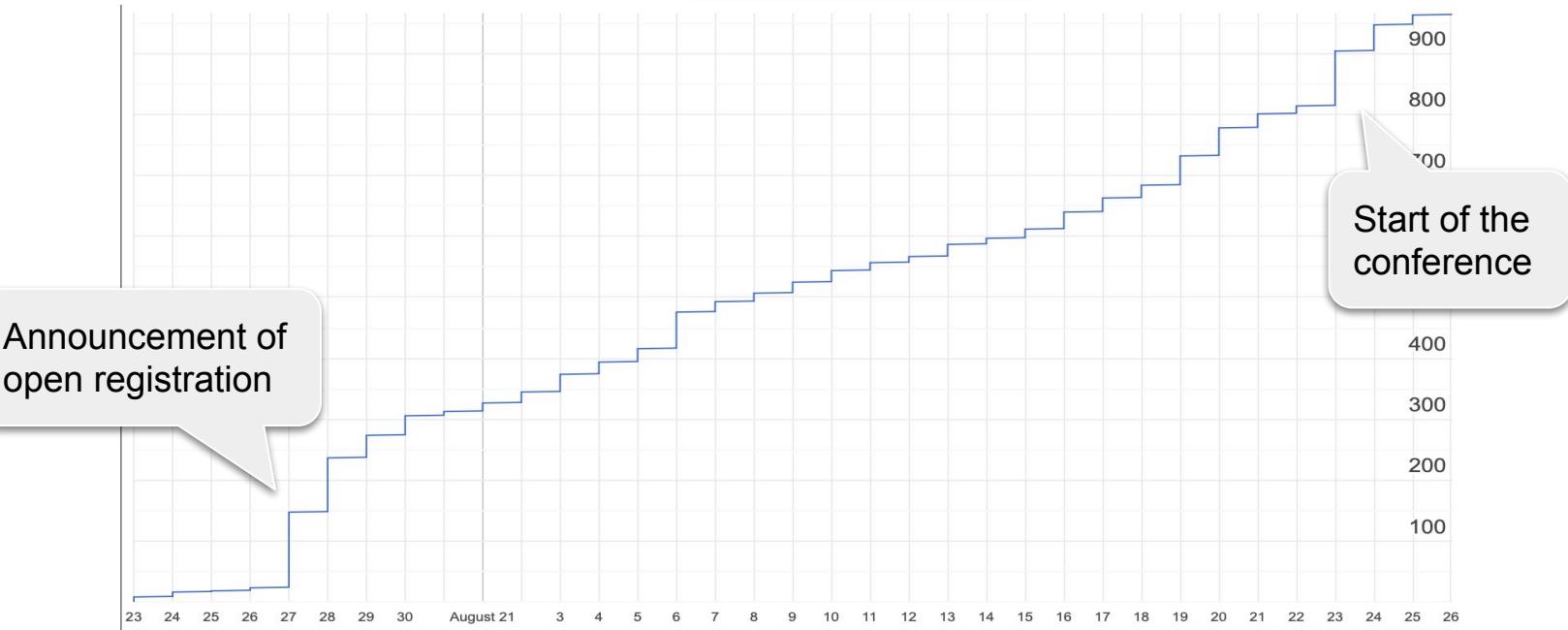
11th International Conference on Quantum Cryptography



Registrations

Number of registrations:

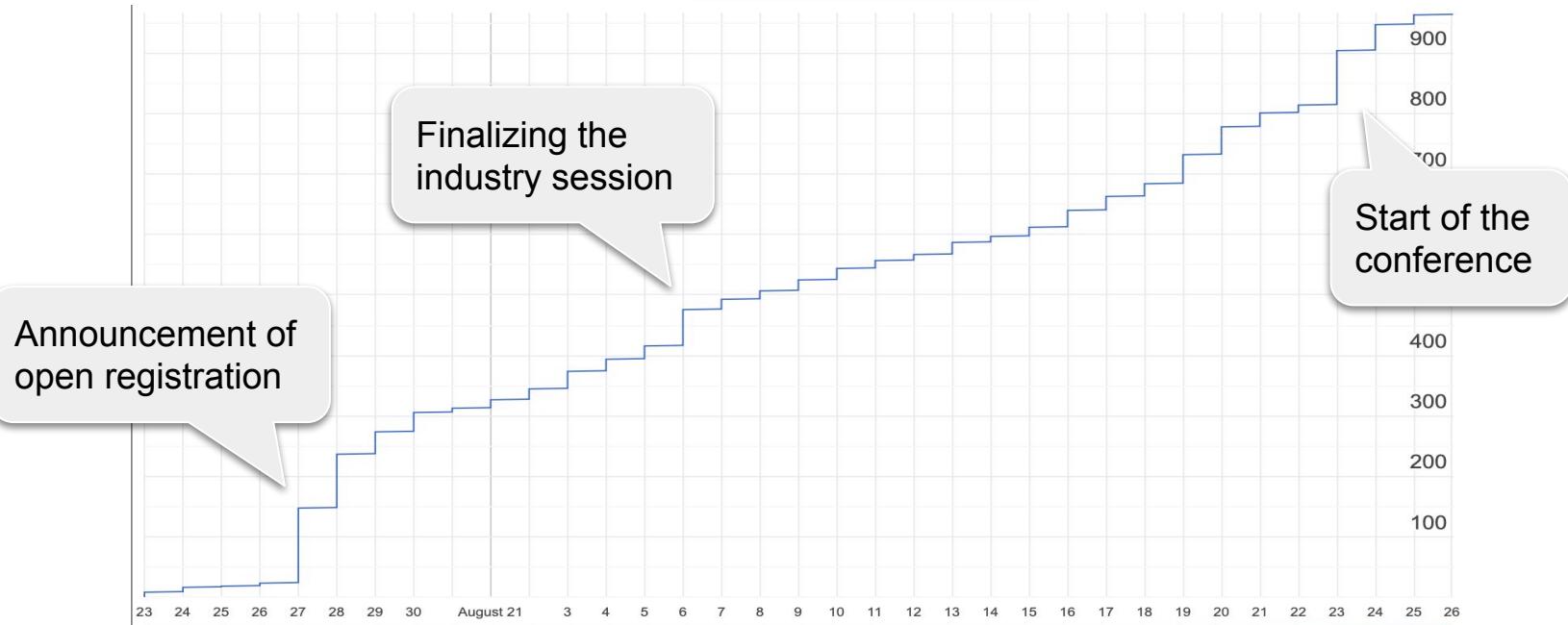
~1000



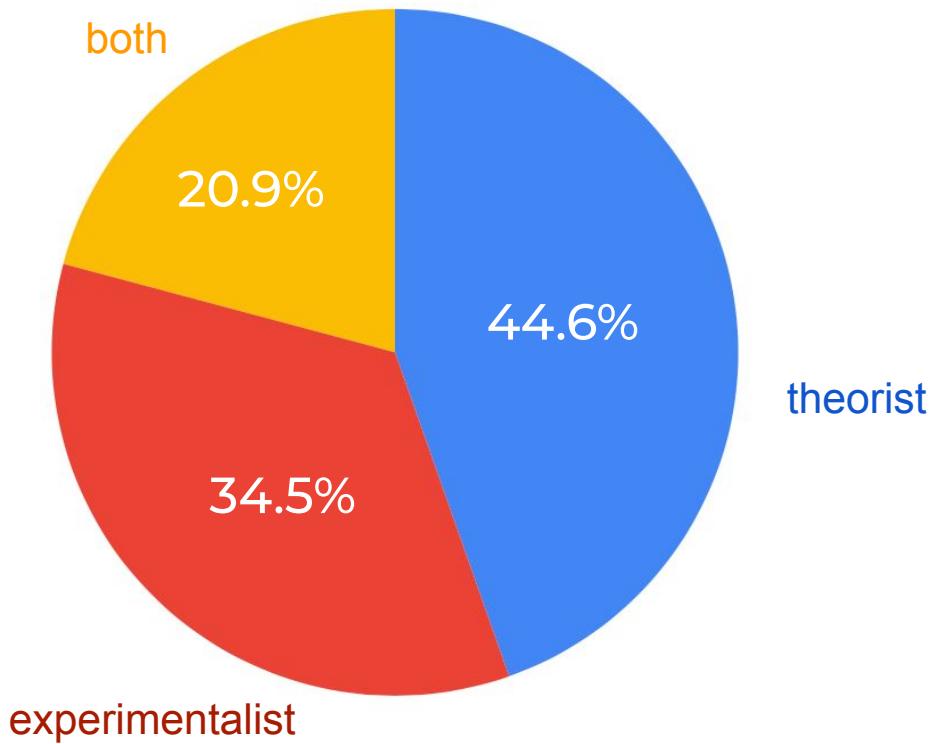
Registrations

Number of registrations:

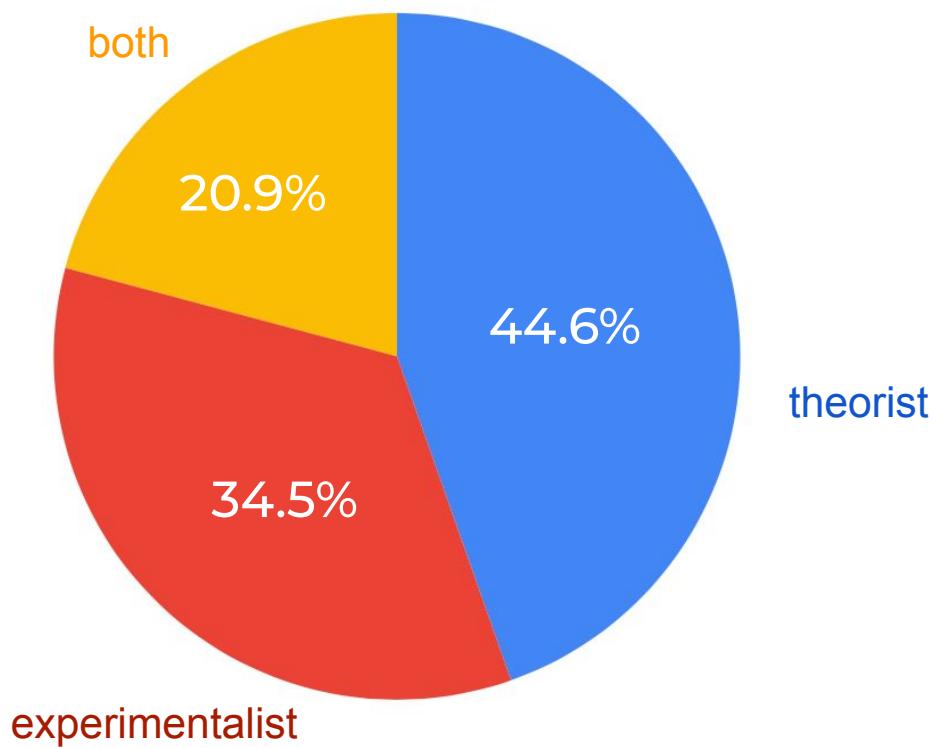
~1000



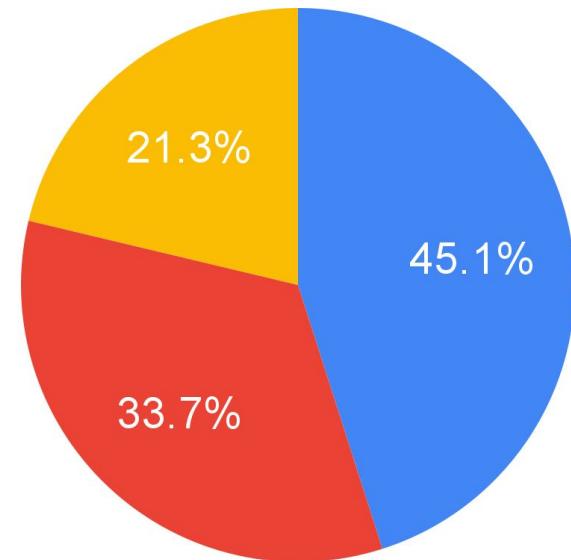
You consider yourself a ...



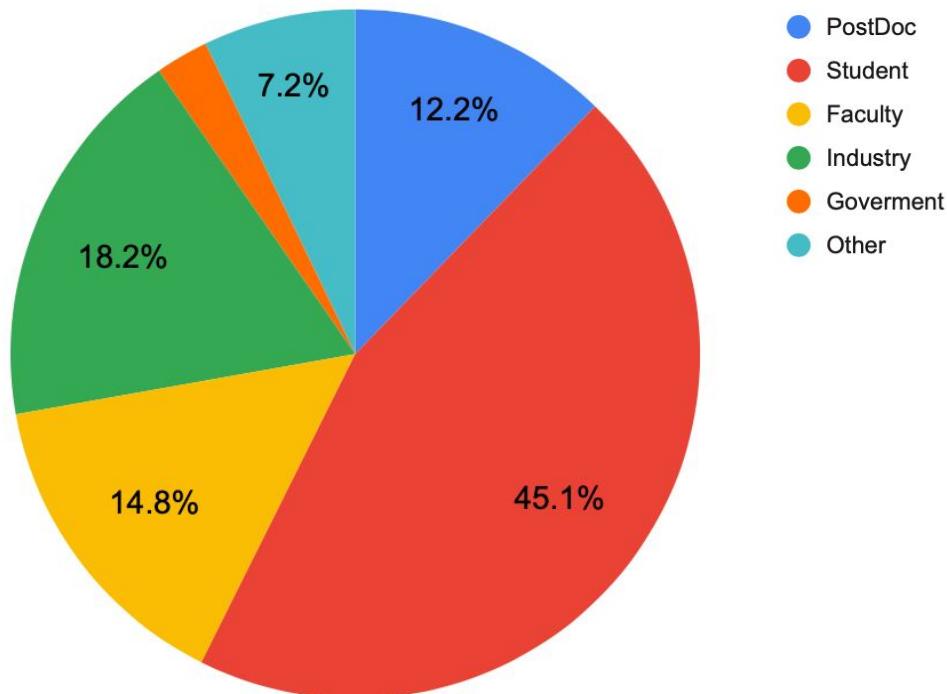
You consider yourself a ...



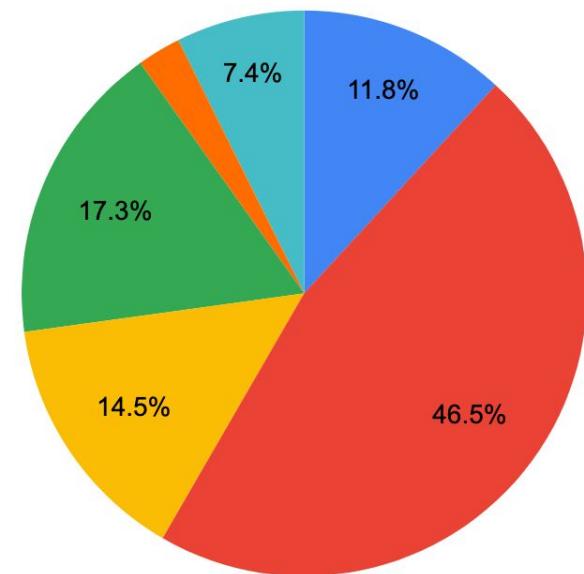
Status on Monday



Current Position



Status on Monday



Finances, 2020 and 2021



Income:

- Sponsors: circa 50k EUR, mix of 2020 and 2021
- Surplus QCrypt 2019: 30k EUR

Expenses:

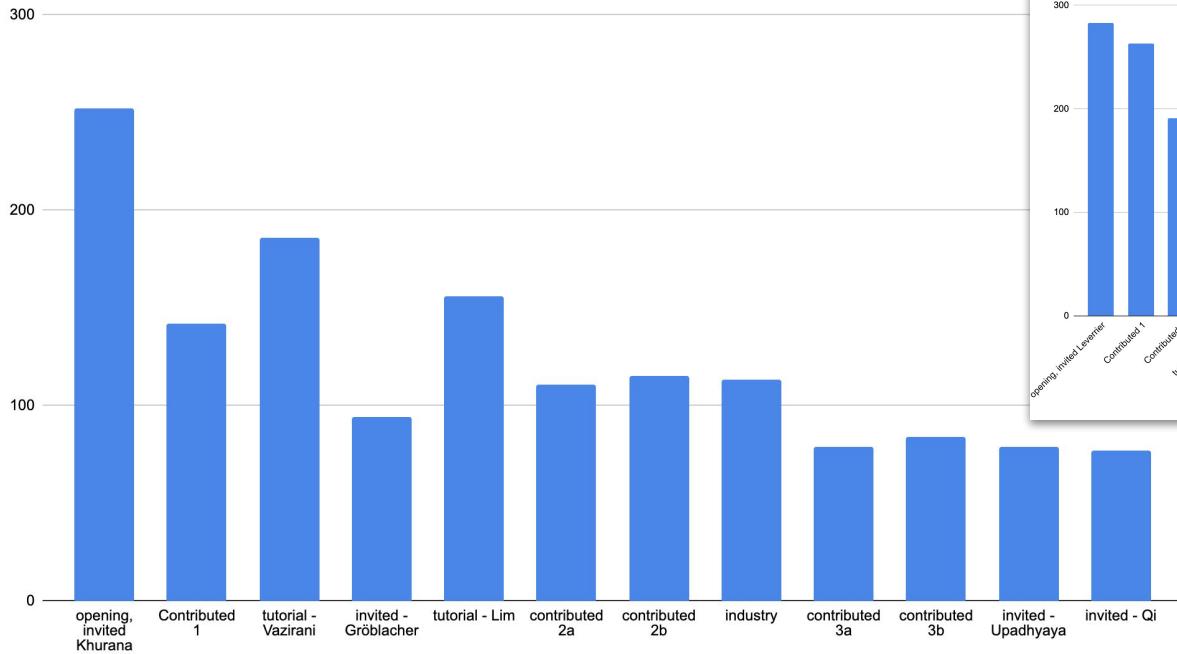
- UvA congress office: combined with last year
- Remo.co (2020): 850 EUR
- Meetanyway.com (2021): ~25k EUR



Zoom participants per session



Zoom Participants per session





Zoom attendee reports

For every session of the webinar, zoom records

- First name
- Last name
- Email
- Registration Time
- Join Time
- Leave Time
- Time in Session
- Country/Region Name

Connecting from China

Difficult to access:

- YouTube
- GoogleForms
- Meetanyway.com

Talks, posters and slides can be downloaded from:

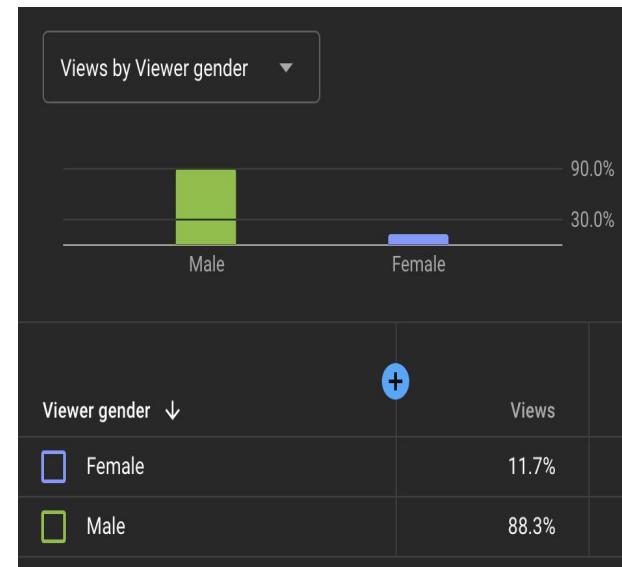
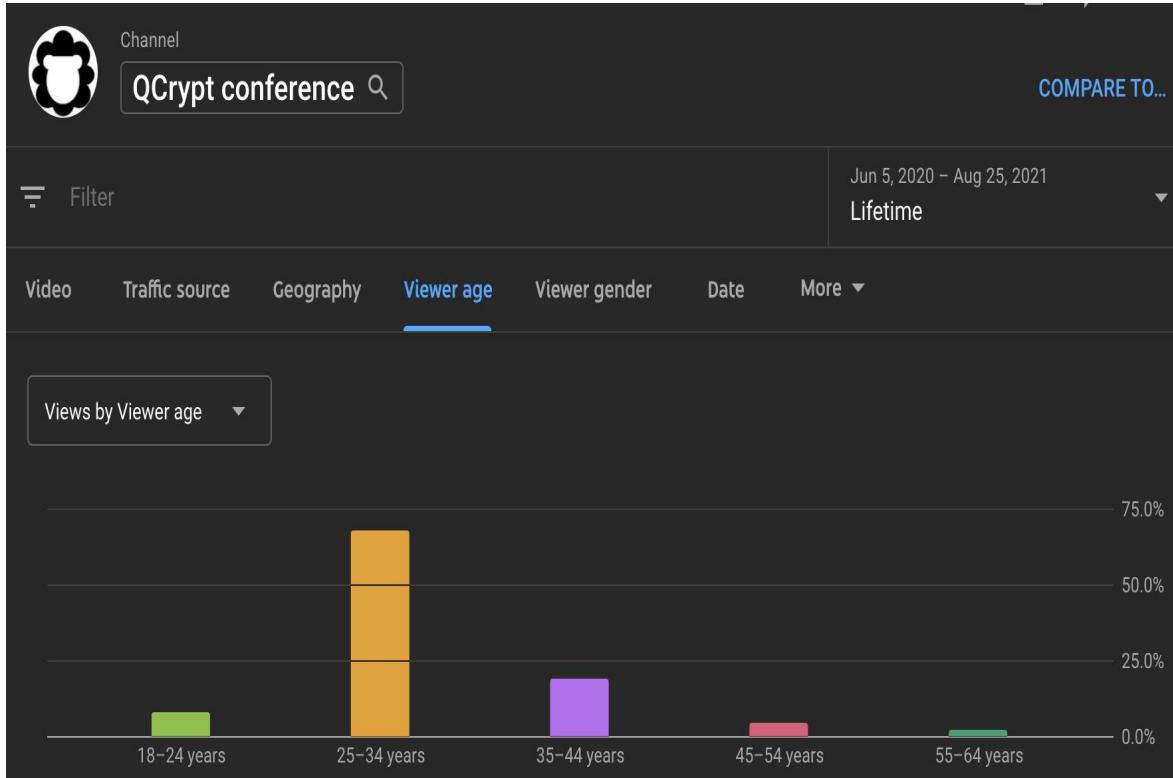
- SurfDrive:

<https://surfdrive.surf.nl/files/index.php/s/GVXUIIThzcWkd9W>





YouTube stats



<https://2021.qcrypt.net>

- JAM stack: JavaScript, API, Markup
- Hugo: static-website generator
- Netlify: Serverless hosting on open-source plan
- templates from the Kubernetes Community
- <https://github.com/QCrypt/website-2021>
- Old QCrypt websites: <https://qcrypt.github.io/>



Thanks to the Team



Caitlin Boonstra
ILLC, University of Amsterdam
 registration updates



Jelle Don
CWI Cryptology Group
 support



Yfke Dulek
CWI, QuSoft
 support / website



Alex Grilo
CNRS/Sorbonne Université
 social media



Melanie Haije
University of Amsterdam
 Congress Office



Esteban Landerreche
 design



Mehrdad Tahmasbi
CWI, QuSoft
 support



Peter van Ormondt
ILLC, University of Amsterdam
 registration form



Wessel van Woerden
CWI Cryptology Group
 support

Thanks to Serge



CWI
Cryptology Group

&

Leiden University



University of Amsterdam
ILLC

&

QuSoft

Thanks to Serge ... and Chris



CWI
Cryptology Group

&

Leiden University

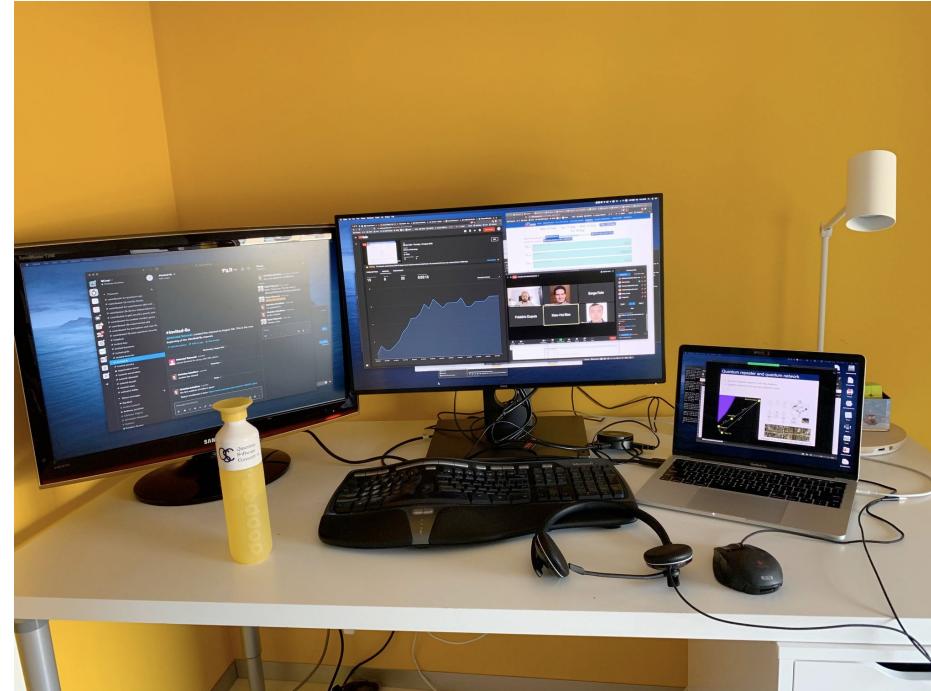
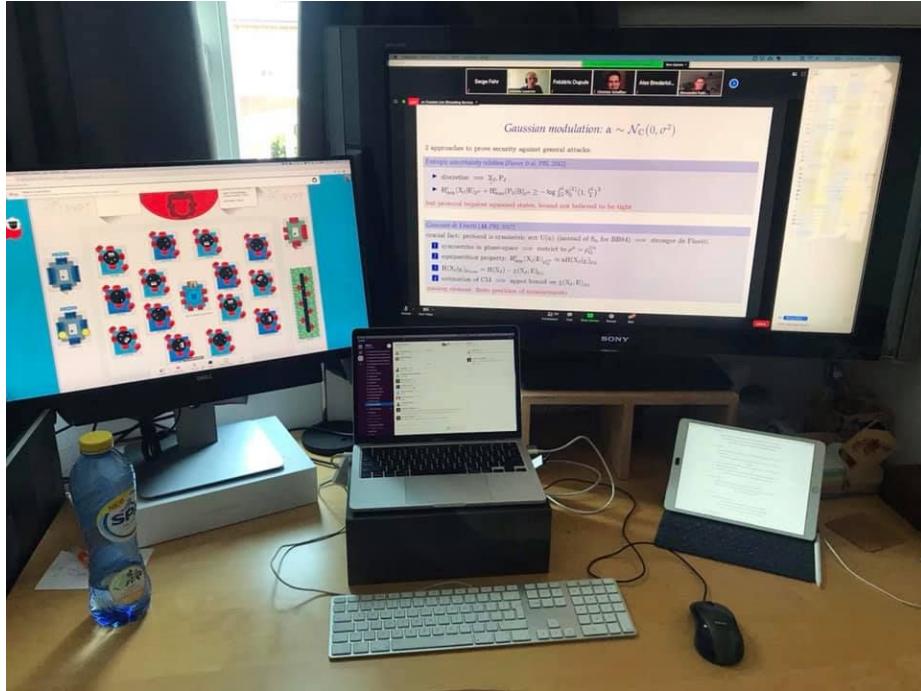


University of Amsterdam
ILLC

&

QuSoft

Home office impressions



QCrypt 2021 central command



Report from the Program Committee

Carl A. Miller (QuICS, NIST), chair
Tobias Gehring (DTU), co-chair

QCRYPT 2021

Early Decisions

- Extra-large committee.
- Software: HotCRP instead of EasyChair.
(<https://qcrypt2021.quics.umd.edu>)
- Call For Papers said: “Research on classical post-quantum cryptography is considered to be within scope if it makes innovative use of quantum information concepts.”

Program Committee Members

Andrea Coladangelo (University of California, Berkeley)

Andreas Hulsing (Eindhoven University of Technology)

Andreas Poppe (Austrian Institute of Technology)

Anne Broadbent (University of Ottawa)

Antonio Acin (ICFO)

Carl Miller (NIST and University of Maryland)

Charles Ci-Wen Lim (National University of Singapore)

Daniel J. Gauthier (Ohio State University)

Davide Bacco (Technical University of Denmark)

Elham Kashefi (University of Edinburgh and CNRS LIP6
Sorbonne Universite)

Erika Andersson (Heriot-Watt University)

Florian Speelman (QuSoft and University of Amsterdam)

George Kanellos (University of Bristol)

Giuseppe Vallone (University of Padova)

Ivo Pietro Degiovanni (INRIM Istituto Nazionale di Ricerca
Metrologica)

Jamie Sikora (Virginia Tech)

Marco Tomamichel (National University of Singapore)

Nino Walenta (Fraunhofer Heinrich Hertz Institute Berlin)

Paolo Villoresi (University of Padova)

Roger Colbeck (University of York)

Romain Alleaume (Telecom Paris)

Rotem Arnon-Friedman (Weizmann Institute of Science)

Rupesh Kumar (University of York)

Sean Hallgren (Penn State University)

Thomas Jennewein (University of Waterloo)

Tobias Gehring (Technical University of Denmark)

Veronica Fernandez (Spanish National Research Council (CSIC))

Virginia D'Auria (Institut de Physique de Nice)

Vladyslav Usenko (Palacky University, Olomouc)

Xiongfeng Ma (Tsinghua University)

Yanbao Zhang (NTT Basic Research Lab)

Yfke Dulek (QuSoft and CWI Amsterdam)

Yuan Cao (University of Science and Technology of China)

Yury Kurochkin (Russian Quantum Center)

Zhiliang Yuan (Beijing Academy of Quant. Info. Sci.)

Zvika Brakerski (Weizmann Institute of Science)

The Process

- We received 137 talk submissions (versus ~100 in a typical year). 80 were marked as “Theory” and 44 as “Experiment.” (Some were both or neither.)
- After that we had:
 1. Review period (4 weeks)
 2. Discussion period (2 weeks)
 3. Vote (1 week)(About two-thirds of acceptances were at stage 2; the rest were at stage 3.)

The Process

- We accepted 29 talks, including 2 merges. Acceptance rate 23%.
 - 15 experimental talks (loosely defined)
 - 14 theoretical talks
- We accepted 141 posters. Acceptance rate 100%.
- Student Paper Prize:
 - The PC selected 5 finalists.
 - The SC and the PC chairs then chose 2 winners.

(Coming up ...)

Thanks to our subreviewers!

Alex Bredariol Grilo
Alexander Duplinsky
Alexander Poremba
Anand Natarajan
André Chailloux
Andreas Winter
Andrey Tayduganov
Andru Gheorghiu
Anran Jin
Anthony Leverrier
Anurag Anshu
Arthur Mehta
Bo Li
Christian Majenz
Dakshita Khurana
David Elkouss
Dmitry Kronberg
Elie Wolfe
Eric Culf
Ernest Tan
Evgeny Kiktenko

Fang Song
Felix Leditzky
Fermi Ma
Frédéric Dupuis
Frederic Grosshans
Gabriel Molina-Terriza
Gabriel Senno
George Nikolopoulos
Giacomo De Palma
Giulio Malavolta
Gláucia Murta
Guoding Liu
Harold Ollivier
Honghao Fu
James Bartusek
Jana Sotáková
Janis Nötzel
Jian-Yu Guan
Josep Lumbreras
Joseph Renes
Kai-Min Chung

Kaushik Chakraborty
Kiyoshi Tamaki
Koon Tong Goh
Marc-Olivier Renou
Mario Berta
Masahito Hayashi
Máté Farkas
Matthew McKague
Matty Hoban
Navneeth Ramakrishnan
Nir Bitansky
Obada Alia
Omri Shmueli
Pei Zeng
Peter Brown
Peter Yuen
Prabhanjan Ananth
Qipeng Liu
Quoc Huy Vu
Rabib Islam
Renato Renner

Roberto Rubboli
Rui Wang
Sébastien Lord
Srijita Kundu
Stacey Jeffery
Stefan Baeuml
Supartha Podder
Theodoros Kapourniotis
Thomas Vidick
Tom Van Himbeeck
Vadim Rodimin
Valerio Scarani
Víctor Zapatero
Xingjian Zhang
Yingkai Ouyang
Yizhi Huang
Yu-Huai Li
Zhenhuan Liu

QCRIPT 2022 (8/29-9/2)

BO-YIN YANG / KAI-MIN CHUNG

at Academia Sinica, Taipei, Taiwan



TAIWAN IS A NICE PLACE



*Tall mountains, green fields, hot springs,
lovely beaches. Great food, nice people.*

Not much COVID-19. (Oh yes, Taiwan Beer!)

Pix: 101, Alishan, Taroko Gorge, Ching-Sui cliffs

VENUE: OUR HUMANITIES AND SOCIAL SCIENCES BUILDING



GETTING INTO TAIWAN ... AND STAYING IN TAIPEI

- > Visa-free entry 15+days available (if without COVID-19) to many countries:
Academia Sinica handles invitations and visas well for those remaining;
Visa assistance details as the time gets closer -- we are experienced;
- > Flights are numerous and convenient and TPE easily accessible by train
- > Negotiating for reserved rooms in Academia Sinica Academic Activities Center and nearby hotels:
Shuttles from/to off-campus hotels in the morning/evening;
Average price is likely ~ US\$100 (including breakfast and wifi!);
- > You are free to try AirBnB etc. they have many rooms in Taipei
- > Mass Transport cheap and plentiful

WHEN THINGS GO WRONG -- A HYBRID OR VIRTUAL QCrypt

A Virtual Event is today's new Norm

Our venue cost us \$0 to cancel

We plan to set up a local meetings server anyway (Jitsi/BigBlueButton)

We won't have much income but a lot of expenses are invited speakers and that goes away as well

A Hybrid Event is really a virtual event with some local attendees

HSSB (Our Venue) is well decked out in terms of sound+video equipment and connectivity

Main Conference Room at $\frac{1}{4}$ capacity (social distancing) holds 100

We plan constant monitoring of the virtual meeting room for questions



LOOKING FORWARD TO WELCOMING YOU IN TAIWAN FOR QCRYPT 2022

Hope to see you all then and there!
Bo-Yin & Kai-Min



Student Paper Prizes

Carl A. Miller (QuICS, NIST), chair
Tobias Gehring (DTU), co-chair

QCRYPT 2021



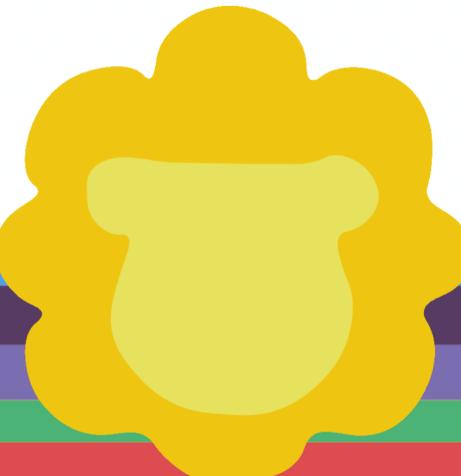
High-rate quantum key distribution with silicon photonics

Likang Zhang

Co-authors Wei Li; Hao Tan, Yan-Lin Tang, Kejin Wei, Sheng-Kai Liao, Cheng-Zhi Peng, Feihu Xu & Jian-Wei Pan

Issued By
Christoph Marquardt
Steering Committee Chair

Issued By
Carl Miller
Program Committee Chair





LOOKING FORWARD TO WELCOMING YOU IN TAIWAN FOR QCRYPT 2022

Hope to see you all then and there!
Bo-Yin & Kai-Min





Device-independent protocols from computational assumptions

Tony Metger

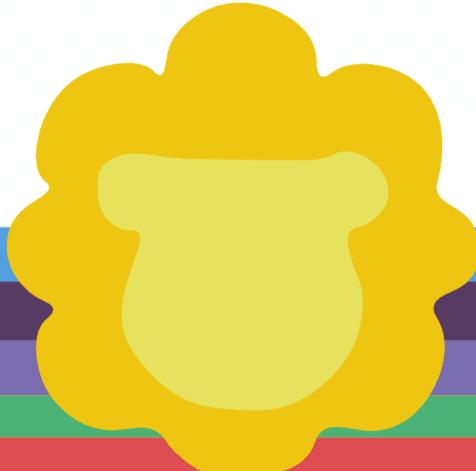
Co-authors Yfke Dulek, Andrea Coladangelo, Rotem Arnon-Friedman & Thomas Vidick

Issued By

Christoph Marquardt
Steering Committee Chair

Issued By

Carl Miller
Program Committee Chair



Finalists

#106: Finite-size DIQKD with noisy preprocessing and random key measurements

Ernest Y.-Z. Tan, Xavier Valcarce, Pavel Sekatski, Jean-Daniel Bancal, Rene Schwonnek, Renato Renner, Nicolas Sangouard, Charles C.-W. Lim

#109: Drone-Based Quantum Key Distribution (QKD)

Andrew Conrad, Samantha Isaac, Roderick Cochran, Daniel Sanchez-Rosales, Akash Gutha, Tahereh Rezaei, Brian Wilens, Daniel J. Gauthier, Paul Kwiat

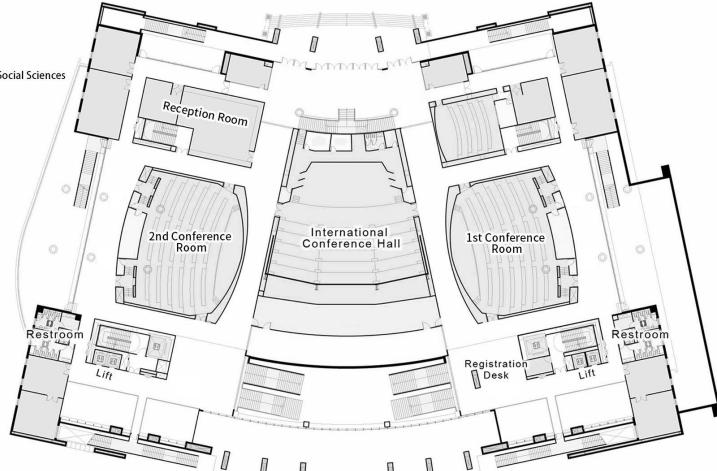
#134: Quantum Private Broadcasting

Anne Broadbent, Carlos E. Gonzalez-Guillen, Christine Schuknecht

VENUE: PLENTY OF SPACE FOR EVERYTHING

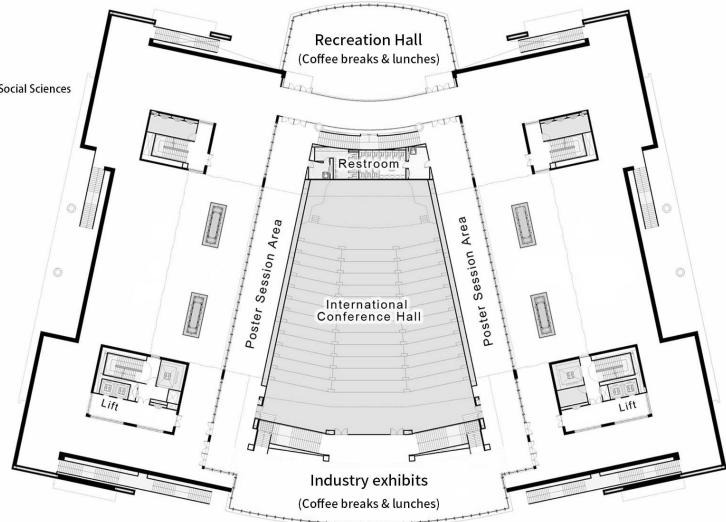
3F

Building for Humanities and Social Sciences



4F

Building for Humanities and Social Sciences



> Includes a modern conference hall and subsidiary meeting rooms

> Foyers are available for posters

CALL FOR CONTRIBUTIONS

- > We expect:
 - exciting technical program;
- > We need you:
 - to work hard;
 - produce new exciting results;
 - submit them to QCrypt 2022;
- > We will also be looking for:
 - sponsors;
 - industry exhibitors;
- > Let us know if you are interested (2022@qcrypt.net)

+-----+
| QCrypt |
+-----+
| 2022 |
+=====+
| 12th |
+-----+
| International |
+-----+
| Conference |
+-----+
| On |
+-----+
| Quantum |
+-----+
| Cryptography |
+-----+



LOOKING FORWARD TO WELCOMING YOU IN TAIWAN FOR QCRYPT 2022

Hope to see you all then and there!
Bo-Yin & Kai-Min

