# Coding Theory and Lattice Theory at the 1st NIST Post-Quantum Cryptography (PQC) Standardization Conference

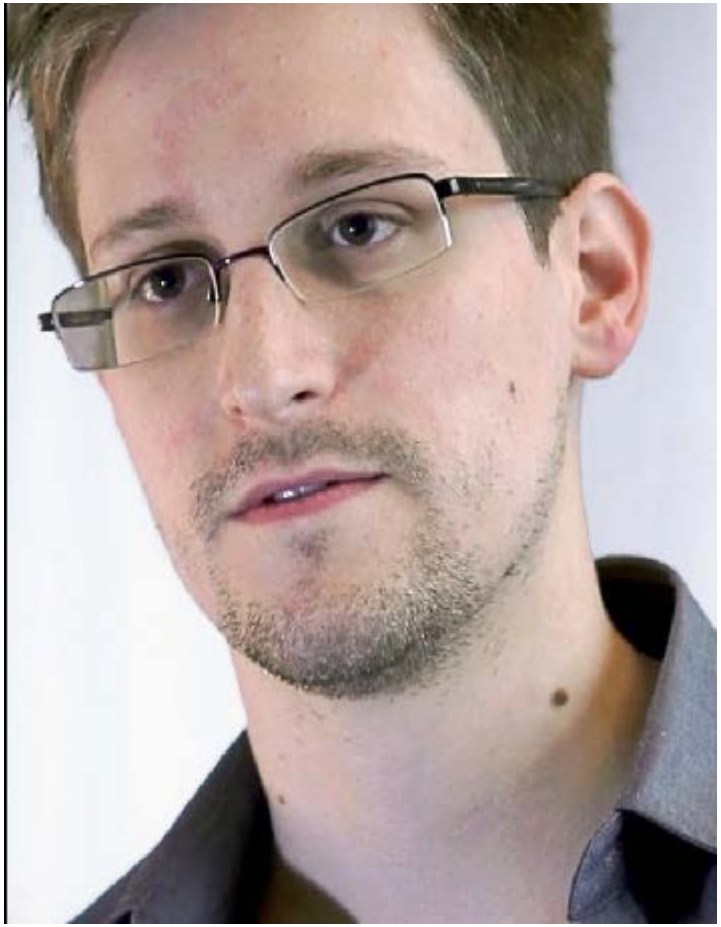
2018. 7.

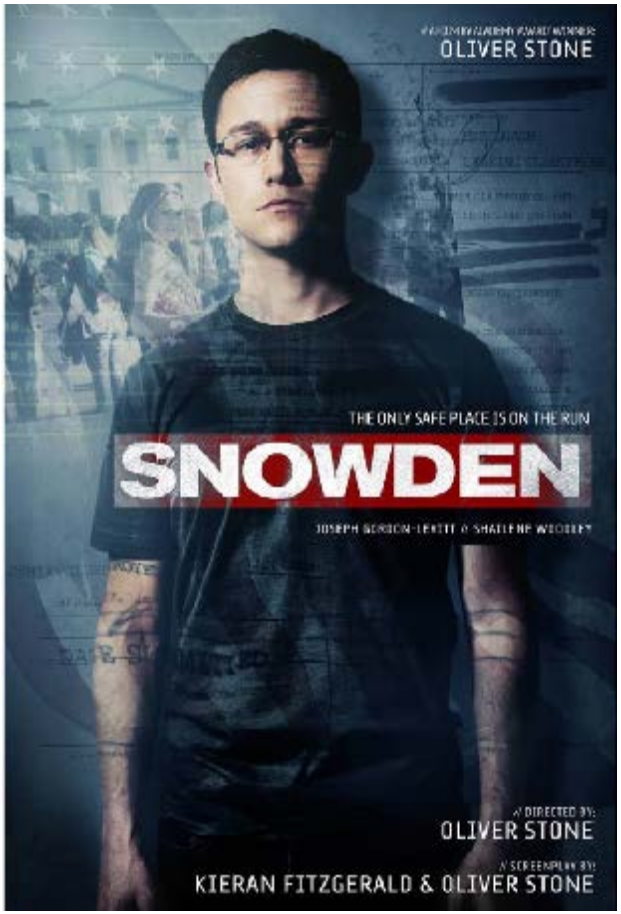
Han(KAIST) at Shanghai University

Niels Bohr

Anyone who is not shocked by
quantum theory has not understood it.

# Edward Snowden





Gauging the allure of designer drugs *p. 469*

Blown-up brains for a better inside view *pp. 474 & 543*

Single-crystal perovskite solar cells *pp. 519 & 522*

# Science

$10
30 JANUARY 2015
sciencemag.org

AAAS

SPECIAL ISSUE

## The End of PRIVACY

# European NextLeap

NEXT
generation
techno-social and
Legal
Encryption
Access and
Privacy

## In the wake of the Snowden revelations, public trust in the Internet has eroded.

NEXTLEAP aims to create, validate, and deploy communication and computation protocols that can serve as pillars for a secure, trust-worthy, annotable and privacy-respecting Internet that ensures citizens fundamental rights. For this purpose NEXTLEAP will develop an interdisciplinary internet science of decentralisation that provides the basis on which these protocols will be built.

# NIST (USA)

## The sky is falling?

- When will a quantum computer be built?
  - 15 years, $1 billion USD, nuclear power plant (PQCrypto 2014, Matteo Mariantoni)
- Impact:
  - Public key crypto:
    - ~~RSA~~
    - ~~Elliptic Curve Cryptography (ECDSA)~~
    - ~~Finite Field Cryptography (DSA)~~
    - ~~Diffie-Hellman key exchange~~
    - ~~Finite Field Cryptography (DSA)~~
    - ~~Diffie-Hellman key exchange~~

- April 9-11, PQCrypto 2018
- April 11-13, NIST PQC Standardization

- Pier 66 Hotel and Marina, Florida
- with 300-350 participants


Marriott

# First PQC Standardization Conference

*****Attendance has reached maximum capacity*****

**Registration is no longer available.**

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. The submission deadline of November 30, 2017 has passed. Please see the Round 1 Submissions for the listing of complete and proper submissions.

The conference will allow first round candidate's to publicly discuss and explain their accepted algorithm.

**Sponsorship Opportunity**

If your organization is interested in sponsoring the morning or afternoon breaks on Thursday or Friday, please contact Sara Kerman who will provide a Food and Beverage contact at the hotel for you to coordinate with. Sponsorship will include your organization's name on the sponsored break table, the event webpage and in the printed agenda, along with recognition at the opening and/or closing of that day's sessions.

This conference will be held at the **Pier 66 Hotel and Marina** and co-located with **PQCrypto 2018.**

## Registration Info

Attendance has reached the maximum capacity for the meeting room. **We can no longer accept late or onsite registrations.**

## EVENT DETAILS

**Starts:** April 11, 2018 - 03:00 PM EST
**Ends:** April 13, 2018 - 05:00 PM EST
**Please note that the conference will now begin Wednesday afternoon, April 11.**

***General Conference Inquires:*** *Sara Kerman*

**Format:** In-person **Type:** Conference

Agenda

**Attendance Type:** Open to public
**Audience Type:**
Industry,Government,Academia,Other
**Sponsors:**
***Microsoft Research***

# Invited talks at PQCrypto

- Jean-Pierre Tillich(INRIA)
- Attacks in code based cryptography

- Dave Wecker(Microsoft)
- Achieving Practical Quantum Computing

# Courtesy of PQCrypt 2018

- Dustin Moody(NIST) gave

- Let's Get Ready to Rumble :
  The NIST PQC "Competition"

- to discover the true facts about something secret
- We need more understandings about "quantum"

- "Not exactly a competition – it is and it isn't"

# Invited talks at standardization

- Rachel Player gave invited talk
- Estimate all the {NTRU, LWE} schemes

- Adi Shamir gave open discussion
- PQ-Crypto : A New Proposed Framework


# PQCrypto 2019

The Tenth International Conference on Post-Quantum Cryptography
Chongqing University, Chongqing, May 8-10, 2019

# Joint Meeting with 2019 Crypto

August 2019, Santa Barbara, California

- 2nd NIST PQC Workshop
- 2nd Round

- 2020/2021 3rd round ?
- 2022/2024 Draft standard ?

# Submissions

- Among 82 submissions
- 69 complete submissions
- But 5 withdrawals (69 – 5 = 64)

- And 59 presentations (64 = 59 + 5)
- (5 did not give presentation)

- On average, given 15 minutes

# Among 64 = 59 + 5

- Lattice based total 26
- signature 5
- key exchange/encryption 21

- Code based total 19
- signature 2
- key exchange/encryption 17

278[212, 30, 22, 7, 2, 1, 4, 1]

- 212 person in 1 proposal each
- 7 persons in 4 proposals each
- 1 person submitted 8 proposals


Greenland
Iceland
Finland
Sweden
Norway
Russia
Canada
United States
Mexico
Poland
Ukraine
Kazakhstan
Mongolia
France
Spain
Italy
Turkey
China
South Korea
Iraq
Iran
Afghanistan
Pakistan
Algeria
Libya
Egypt
Saudi Arabia
India
Thailand
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Kenya
DR Congo
Tanzania
Angola
Namibia
Botswana
Madagascar
South Africa
Indonesia
Papua New Guinea
Australia
New Zealand
Venezuela
Colombia
Peru
Bolivia
Chile
Argentina
North Pacific Ocean
North Atlantic Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean

# Lepton : LPN-based KEMs with Post-Quantum Security

**Yu Yu** and Jiang Zhang

Shanghai Jiao Tong University

# The Design of LAC

Xianhui Lu, Yamin Liu, Dingding Jia
Haiyang Xue, Jingnan He, Zhenfei Zhang

Chinese Acedemy of Science

# KCL(Key Consensus from Lattice)

Yunlei Zhao

Fudan University (on behalf of the KCL team)

# Dustin Moody (NIST)

- Let's Get Ready to Rumble :
  The NIST PQC "Competition"

- We see our role as managing a process of achieving community consensus in a transparent and timely manner.

# Dustin Moody (NIST)

- More clear criteria ?
- Please help us.
- Merge similar proposals ?
- Please help us.

# Adi Shamir (Weizmann)

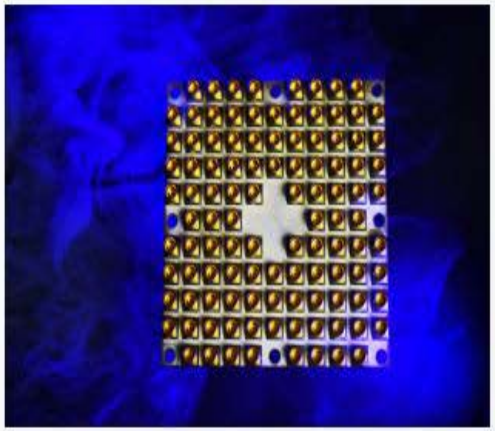
- There is no immediate need.

- RDP framework

- R = research level
- D = development level  Lattice, McElice, NTRU
- P = production level  empty

- Not isogeny, Mersenne

# The Rise of Quantum Computing



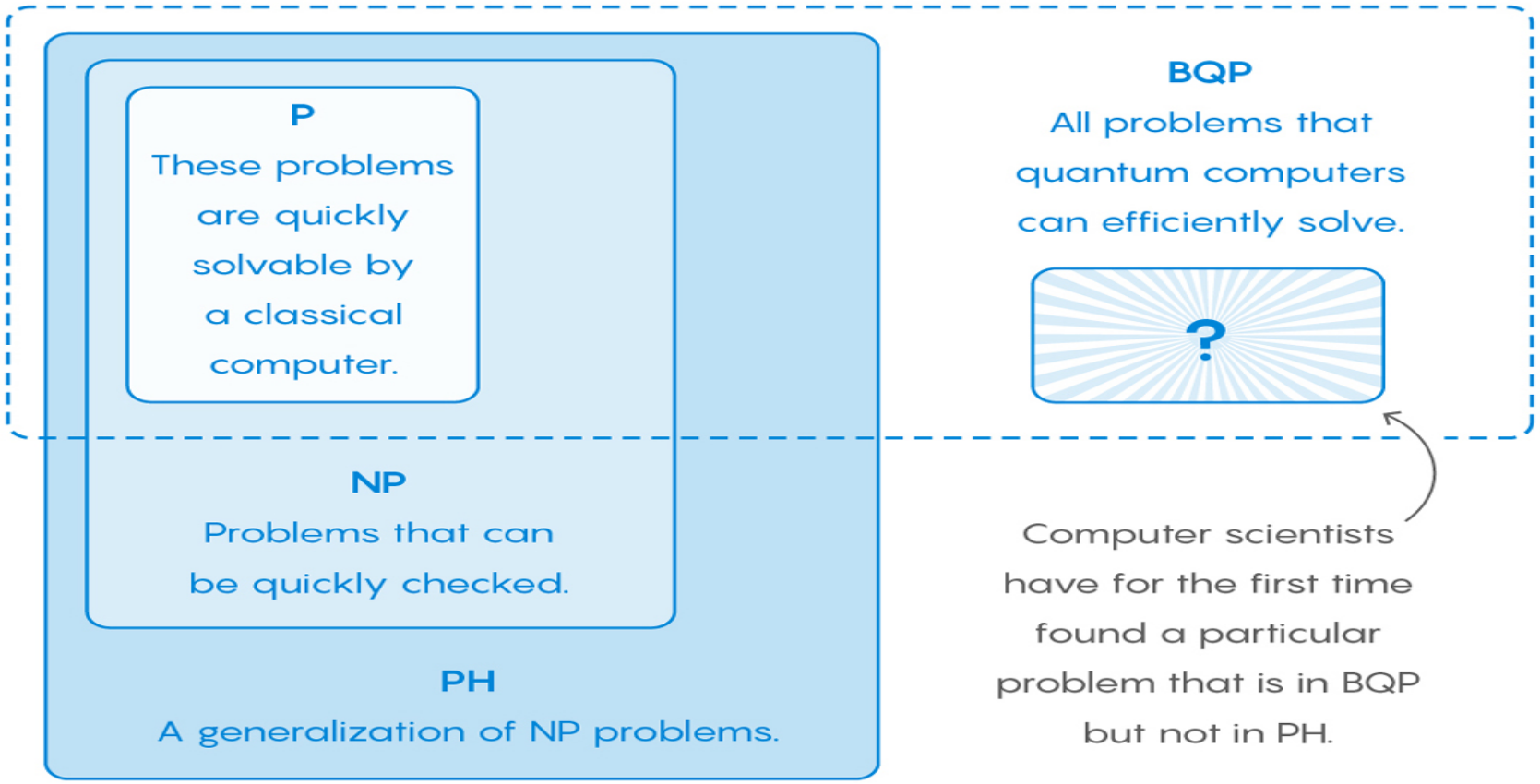
Intel's 49-qubit chip
"Tangle-Lake"
January 2018


Google's 72-qubit chip
"Bristlecone"
March 2018

IBM's 50-qubit
quantum computer
November 2017

# A New Island on the Complexity Map

What can a quantum computer do that any possible classical computer cannot? Computer scientists have finally found a way to separate two fundamental computational complexity classes.



- NewHope used by Google - lattice
- Picnic supported by Microsoft – block
- Crystals-Dilithium by IBM – lattice
- Classic McElice – Tanja Lange(Eindhoven)

# Classic McEliece : conservative code-based cryptography

Tanja Lange (Eindhoven) and others

Highlights : 40 years of cryptanalysis

# Jean-Pierre Tillich (INRIA)

- Attacks in code-based cryptography : a survey, new results and open problems

- In Hamming metric : BIKE, HQC, LEDAkem, LEDApkc, Lepton, QC-MDPC, RaCoSS

- In rank metric : Edon-K, LAKE, LOCKER, McNie, Ourobouros-R, RankSign, RQC

# Rachel Player (Sorbonne)

- Estimate all the {NTRU, LWE} schemes

- Disagreement in the literature about estimating lattice reduction
- Our goal is to show the discrepancies in the concrete security estimation space.
- There are many examples where under one cost model , scheme A appears to be harder than scheme B, while under another cost model, scheme B appears harder.

# Discussions

- NIST PQC forum

- https://groups.google.com/a/list.nist.gov/forum/#!forum/pqc-forum

# Personal thoughts

- For about 60% of submissions, there is no attacks reported in PQC forum.

- After merging, modifications etc., there will be about 25 algorithms at the 2nd round next year.

# continued

- Code-based cryptography : design and security by Carlos Cid

- Between code-based and lattice-based crypto

- Lattice-based : try to hide a secret vector in a high-di mensional lattice **over q** by introducing small errors to **all coordinates**
- Code-based : try to hide a secret vector in a **very** high -dimensional lattice **over 2** by introducing errors to **some coordinates**

# continued

- Crystals-Dilithium by IBM
- Based on module LWE not ring LWE. So dimension increases as 256n
- $M \oplus M \oplus M \oplus \cdots$

# continued

- Mersenne-756839 by Antoine Joux
- Modulo operation with modulus $2^n - 1$
- Very similar with NTRU.

- Interesting, not meaning interesting because it is secure.
- Will be presented at Crypto in August




# PQCrypto 2019

The Tenth International Conference
Chongqing University, Chongqing,
May 8-10, 2019

谢谢谢谢谢谢谢谢
谢谢谢谢