Quantum-Safe Cryptography

Ludovic Perret
ludovic.perret@lip6.fr

J.-C. Faugère
jean-charles.faugere@inria.fr

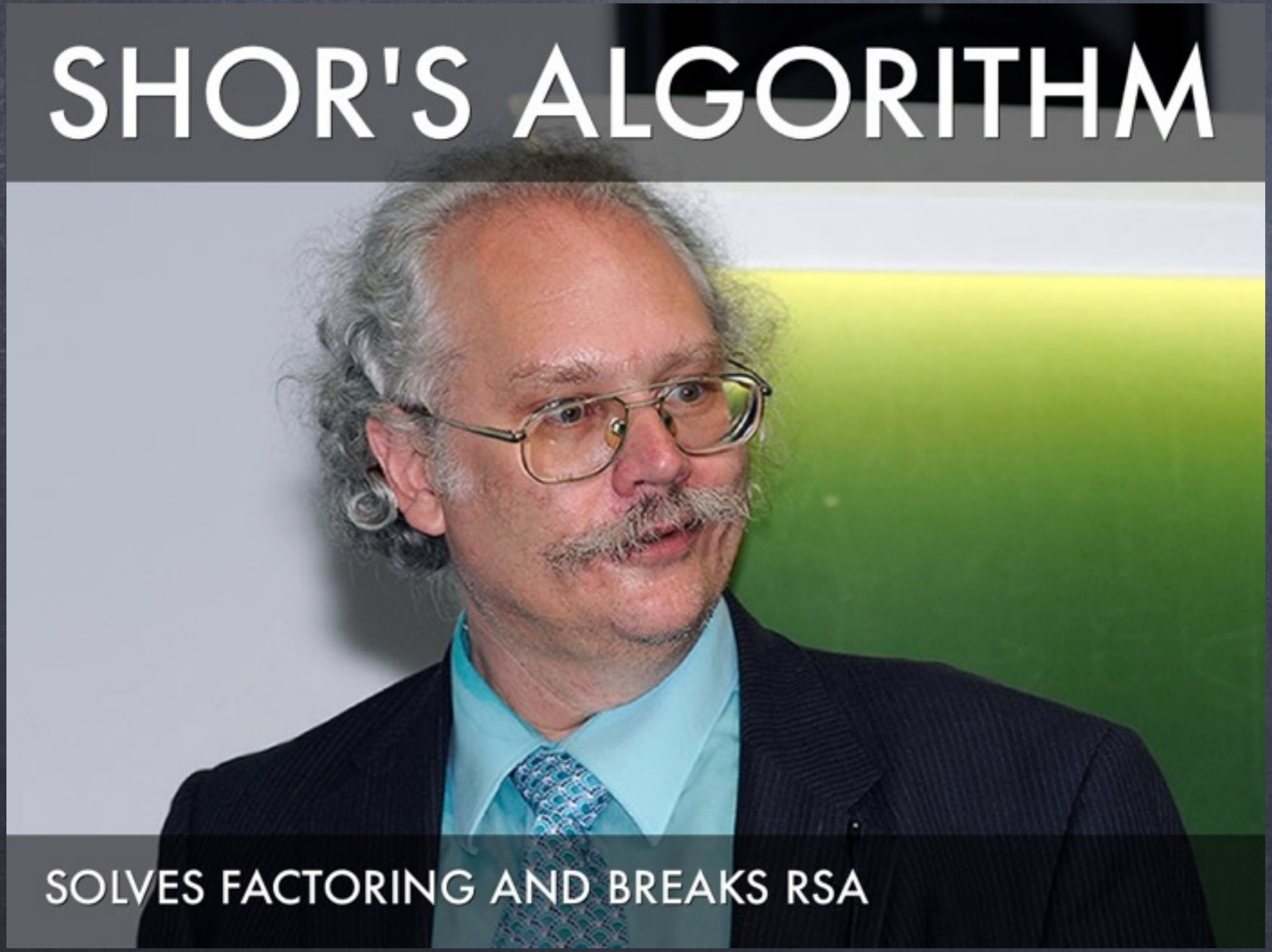
European Brokerage Event
Paris, September 2016

THE FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION
HORIZON 2020

UPMC Sorbonne Universités
INRIA Paris CNRS

Motivation

- public-key cryptography = hard mathematical problems
  - Dlog, Factorisation

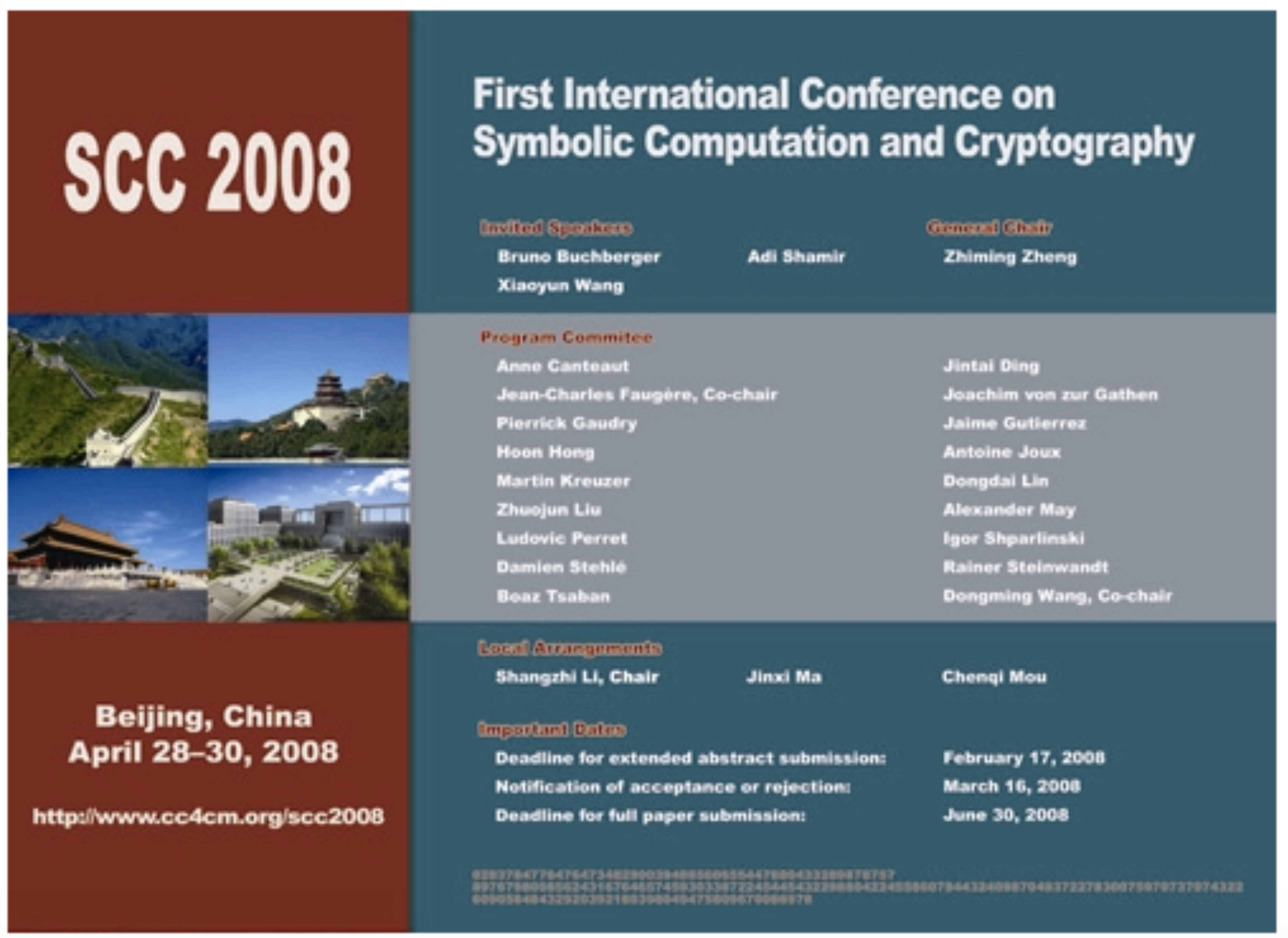


Quantum-Safe (aka post-quantum) Cryptography
Established Academic Topic

THE FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION

HORIZON 2020

- Cryptographic primitives secure against classical and quantum computers.



SCC 2008

First International Conference on Symbolic Computation and Cryptography

Invited Speakers

Bruno Buchberger
Adi Shamir
Xiaoyun Wang

General Chair

Zhiming Zheng

Program Commitee

Anne Canteaut
Jean-Charles Faugère, Co-chair
Pierrick Gaudry
Hoon Hong
Martin Kreuzer
Zhuojun Liu
Ludovic Perret
Damien Stehlé
Boaz Tsaban
Jintai Ding
Joachim von zur Gathen
Jaime Gutierrez
Antoine Joux
Dongdai Lin
Alexander May
Igor Shparlinski
Rainer Steinwandt
Dongming Wang, Co-chair

Local Arrangements

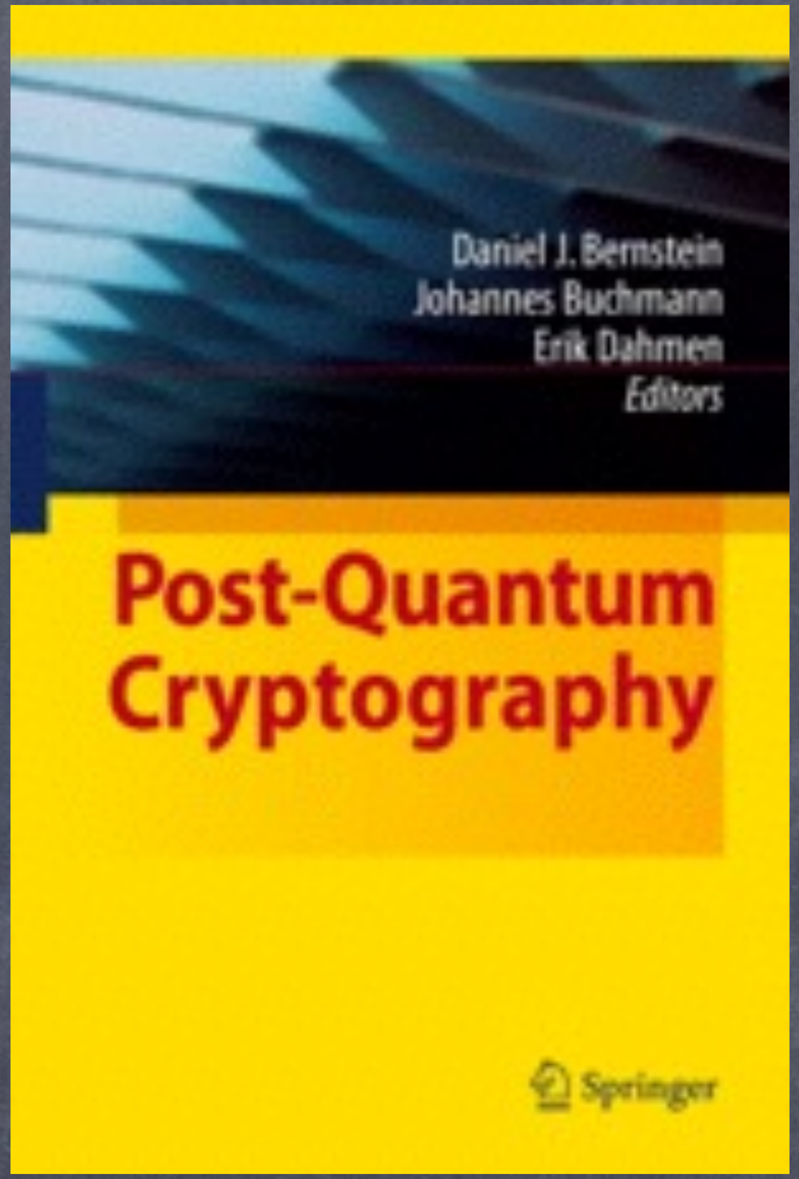
Shangzhi Li, Chair
Jinxi Ma
Chenqi Mou

Important Dates

Deadline for extended abstract submission:	February 17, 2008
Notification of acceptance or rejection:	March 16, 2008
Deadline for full paper submission:	June 30, 2008

Beijing, China
April 28–30, 2008

http://www.cc4cm.org/scc2008



Daniel J. Bernstein
Johannes Buchmann
Erik Dahmen
Editors

Post-Quantum Cryptography

Springer

PQCrypto 2016

Quantum-Safe Cryptography
Established EU Topic

NESSIE New European Schemes for Signature, Integrity and Encryption

- Cryptographic primitives secure against classical and quantum computers.

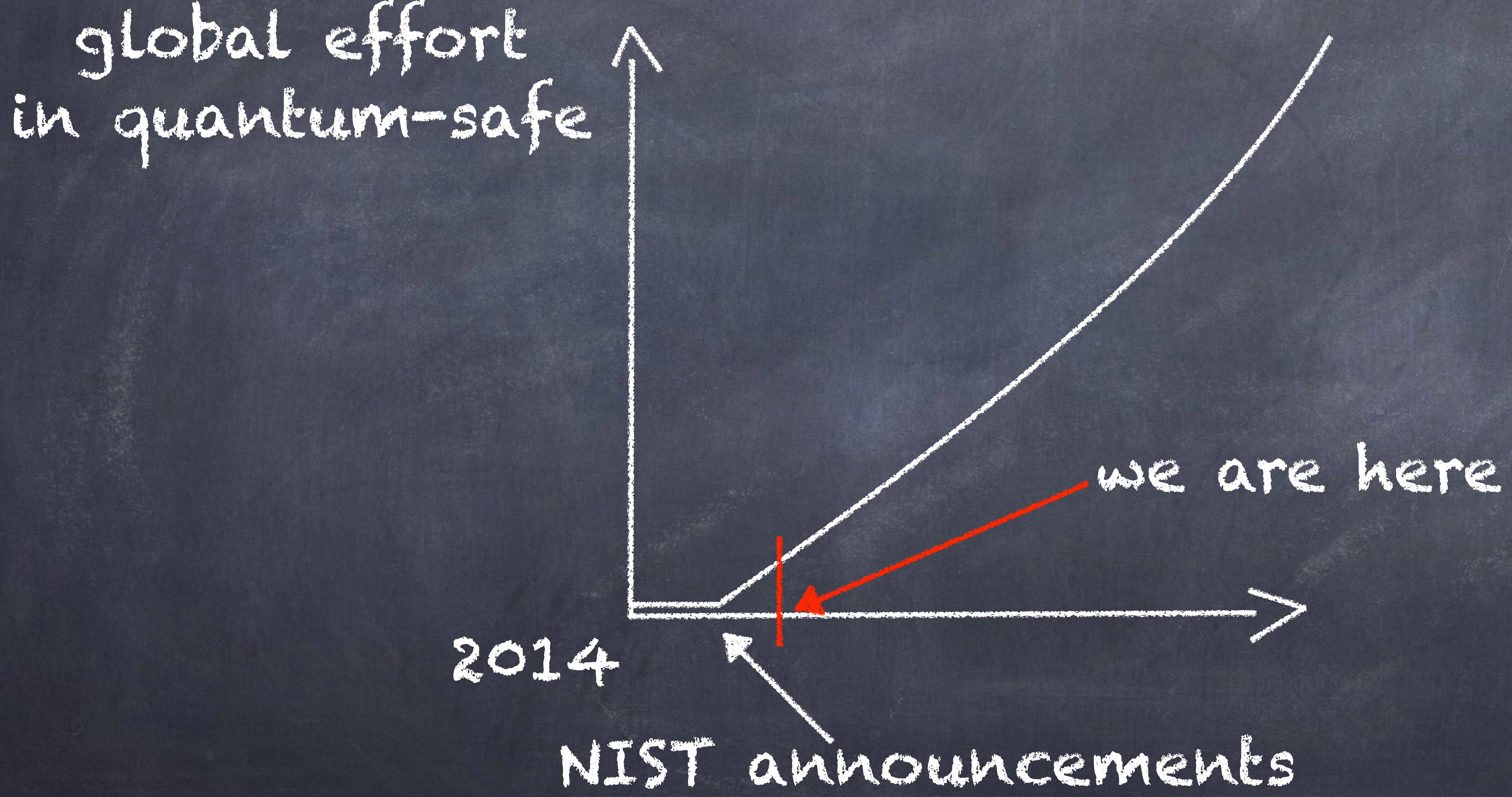
ECRYPT

ECRYPT II

SAFEcrypto

PQCRYPTO
ICT-645622

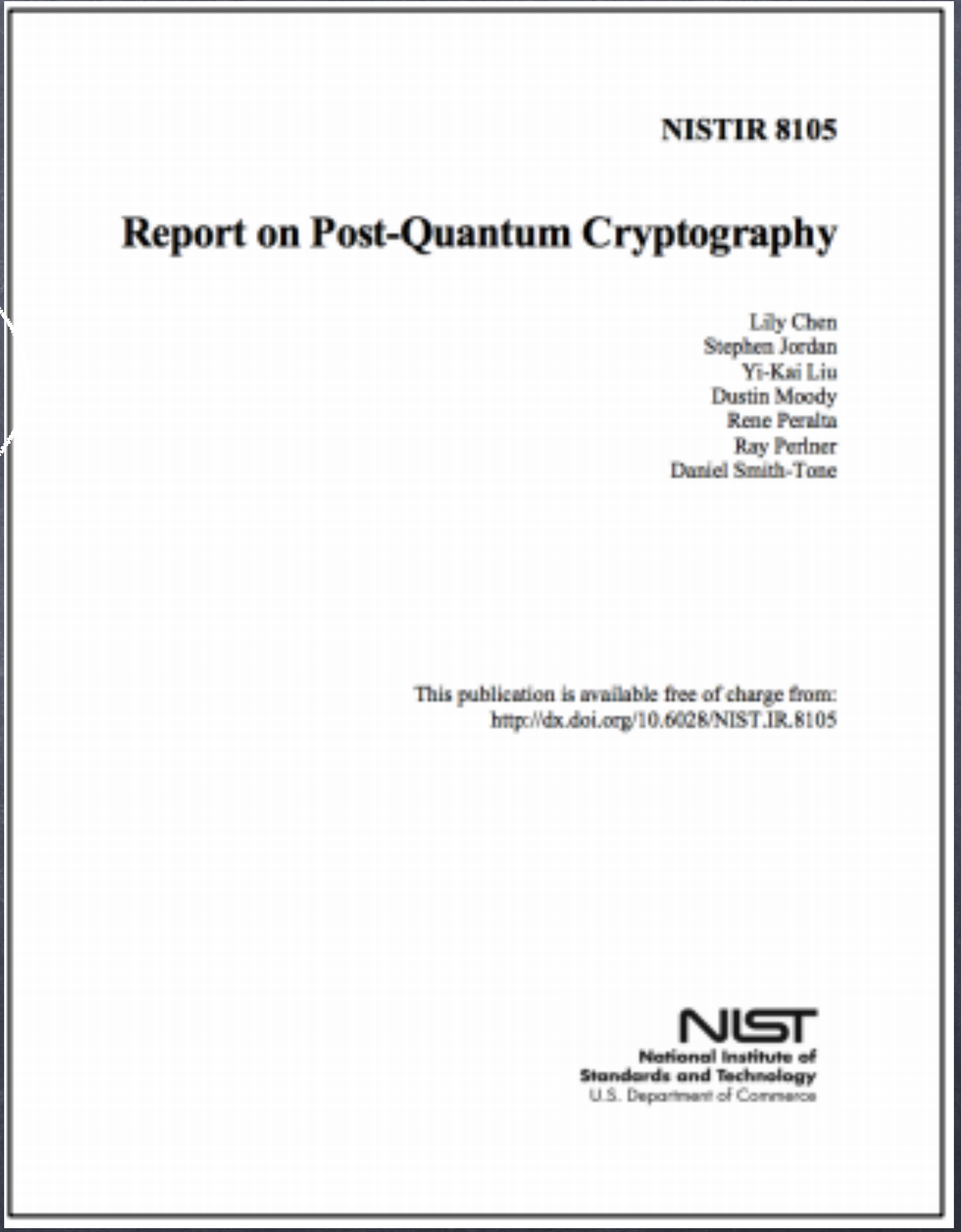
Quantum-Safe Blow-Up



NIST Standardization Process Timeline

September 16, 2016	Feedback on call for proposals
Fall 2016	Formal Call for Proposals
Nov. 2017	Deadline for submissions
Early 2018	Workshop - Submitter's Presentations
3-5 years	Analysis Phase + 1-2 workshops
2 years later	Draft standards ready

Key-exchange, signature, pk encryption



NISTIR 8105

Report on Post-Quantum Cryptography

Lily Chen
Stephen Jordan
Yi-Kai Liu
Dustin Moody
Rene Peralta
Ray Perlner
Daniel Smith-Tone

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8105

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

http://www.nist.gov/pqcrypto

Quantum-Safe Cryptography Industry Specification Group
ETSI

- Chairman. Mark Pecen (ISARA Corporation, Waterloo, Canada)
- Assess and make recommendations for quantum-safe cryptographic primitives
- Quantum-Safe-Crypto Workshops (4th , Toronto, September)

QUANTUM THREATS
CRYPTOGRAPHIC RESEARCH
INDUSTRY
GOVERNMENT
INTERNATIONAL STANDARDS
PROTECTING EXISTING INFRASTRUCTURE
EMERGING SOLUTIONS

JOIN THE QUANTUM-SAFE CYBERSECURITY COMMUNITY IN TORONTO THIS SEPTEMBER.

BUILD YOUR STRATEGY TO PROTECT YOUR SYSTEMS IN THE QUANTUM ERA.

4TH ETSI/IQC WORKSHOP ON QUANTUM-SAFE CRYPTOGRAPHY

SEPTEMBER 19-21 2016
HILTON HOTEL
145 RICHMOND STREET W TORONTO, ONTARIO

ISARA
ETSI World Class Standards
UNIVERSITY OF WATERLOO
IQC Institute for Quantum Computing
CryptoWorks21

Quantum-safe Security Working Group
Cloud Security Alliance

- Chairs. Bruno Huttner (ID Quantique) and Jane Melia (QuintessenceLabs)
  - « What is Post- Quantum Cryptography », « What is Quantum-Safe Security ? », « What is Quantum-Key Distribution ? »

Not Only an Academic Topic

IBM

id Quantique

Microsoft

Security Innovation

AtoS

Quintessence labs

CISCO

intel

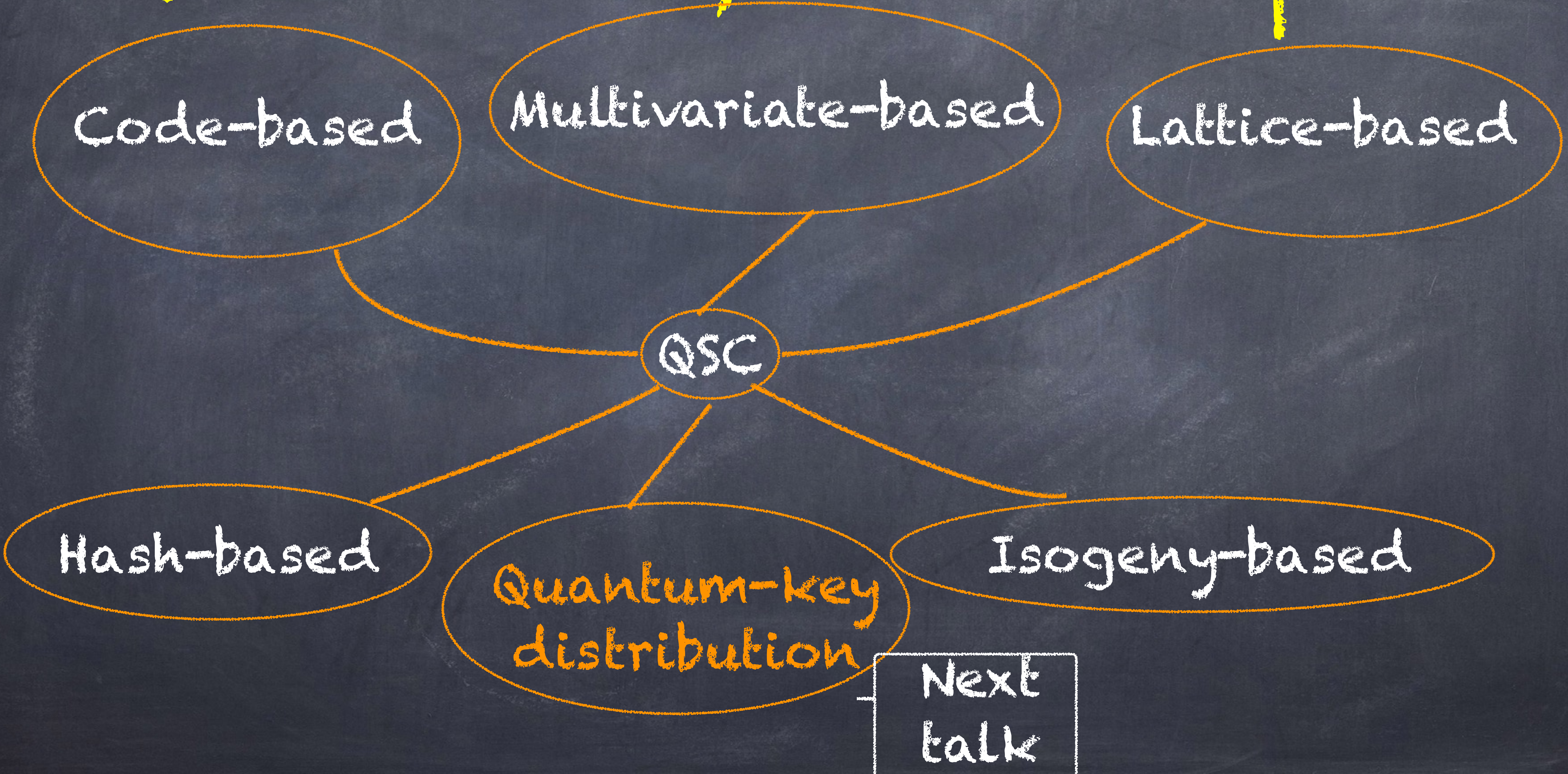
Post-Quantum

Alibaba.com

ISARA

TOSHIBA
Leading Innovation

Quantum-Safe Landscape



Code-based

Multivariate-based

Lattice-based

QSC

Hash-based

Quantum-key distribution

Isogeny-based

Next talk

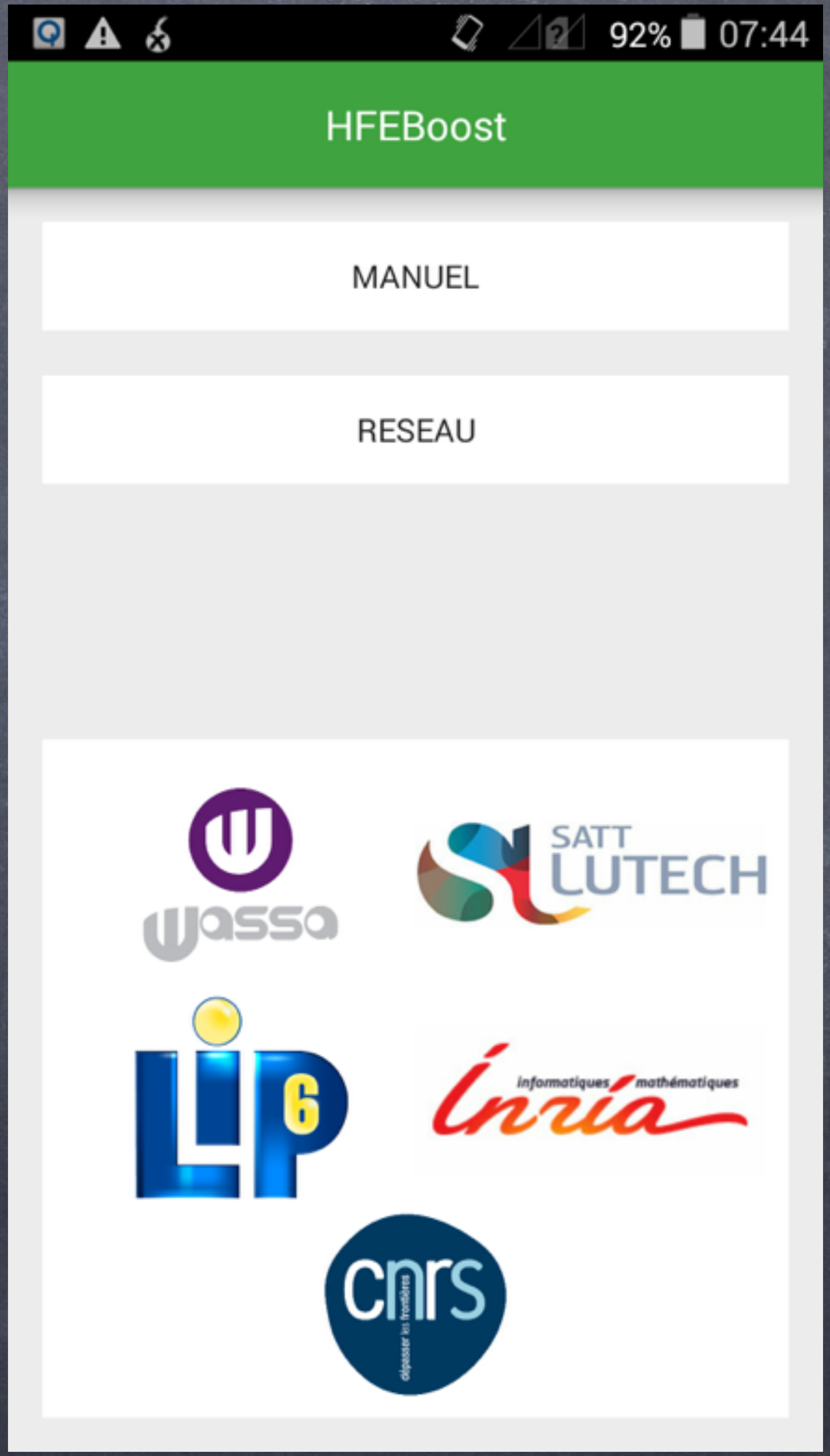
Multivariate Public-Cryptography

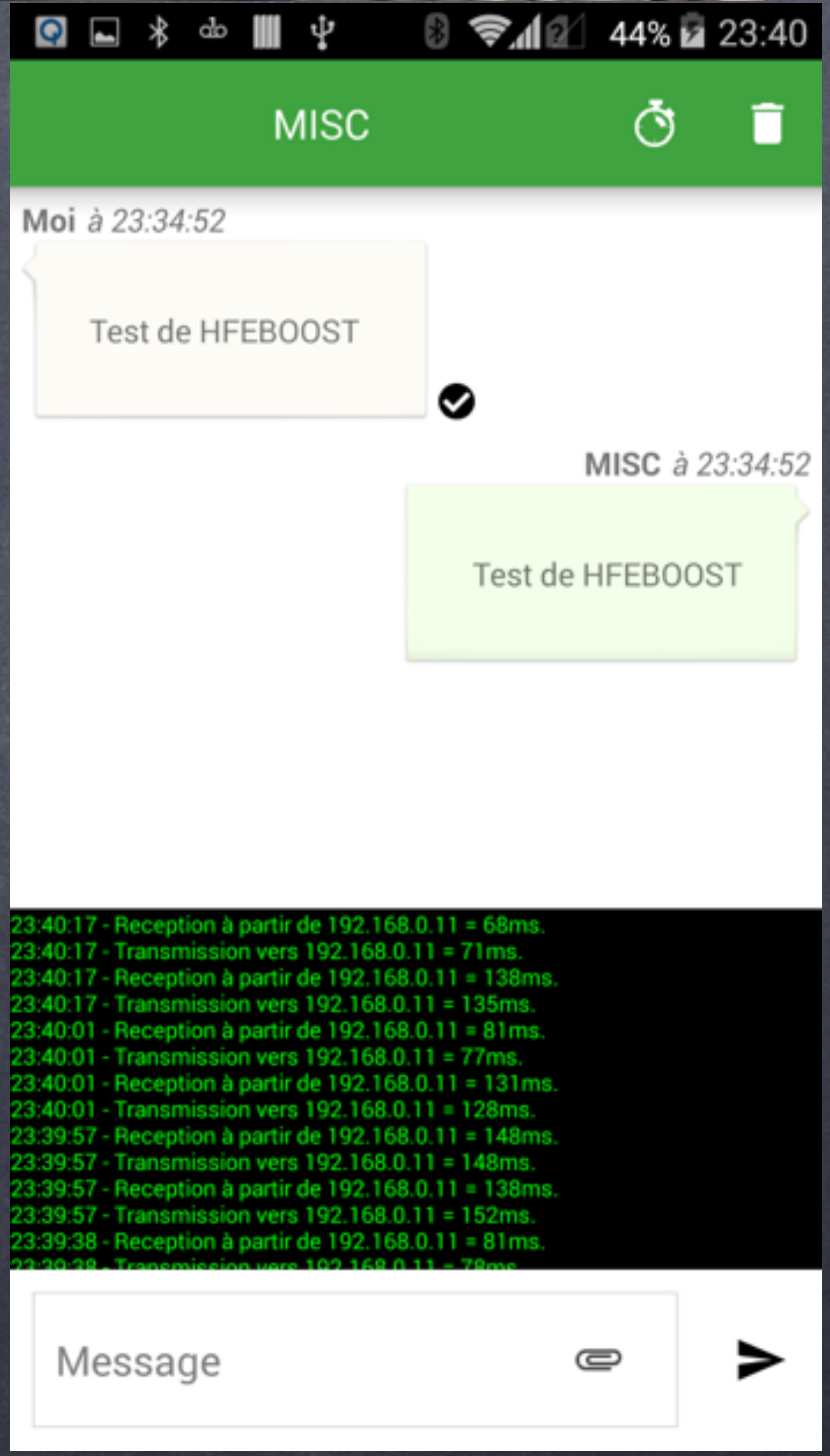
Input. Non linear polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$

Question. Find – if any – $(z_1, \ldots, z_n) \in \mathbb{F}_q^n$

$$\begin{cases} p_1(z_1, \ldots, z_n) = 0 \\ \vdots \\ p_m(z_1, \ldots, z_n) = 0 \end{cases}$$

- PoSSo is NP-Hard [Garey-Johnson]
- « Random instances » of PoSSo are hard to solve in practice
- No (known) exponential quantum speedup





Moi à 23:34:52

Test de HFEBOOST

MISC à 23:34:52

Test de HFEBOOST

```
23:40:17 - Reception à partir de 192.168.0.11 = 68ms.
23:40:17 - Transmission vers 192.168.0.11 = 71ms.
23:40:17 - Reception à partir de 192.168.0.11 = 138ms.
23:40:17 - Transmission vers 192.168.0.11 = 135ms.
23:40:01 - Reception à partir de 192.168.0.11 = 81ms.
23:40:01 - Transmission vers 192.168.0.11 = 77ms.
23:40:01 - Reception à partir de 192.168.0.11 = 131ms.
23:40:01 - Transmission vers 192.168.0.11 = 128ms.
23:39:57 - Reception à partir de 192.168.0.11 = 148ms.
23:39:57 - Transmission vers 192.168.0.11 = 148ms.
23:39:57 - Reception à partir de 192.168.0.11 = 138ms.
23:39:57 - Transmission vers 192.168.0.11 = 152ms.
23:39:38 - Reception à partir de 192.168.0.11 = 81ms.
23:39:38 - Transmission vers 192.168.0.11 = 78ms.
```

Many Challenges in Quantum-Safe

Quantum-Safe standards will be released

Classical and quantum cryptanalysis

Combining physical techniques and algorithmic techniques

Finding good parameters

Efficient and secure implementations

Is secret-key cryptography really quantum-safe