Cryptographic Engineering

Peter Schwabe

Max Planck Institute for Security and Privacy

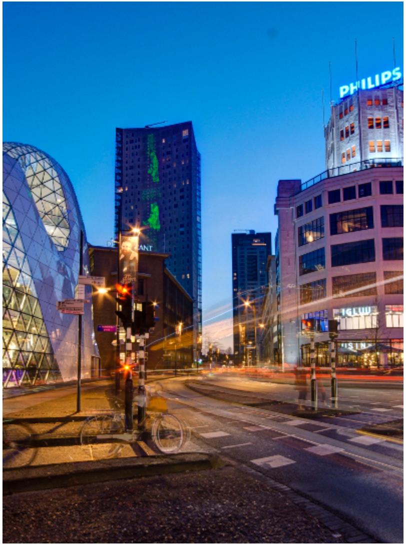
October 24, 2025

My way to MPI-SP

- 2001–2007: Aachen
  Studied Computer Science (Diplom)

My way to MPI-SP

- 2001–2007: Aachen
  Studied Computer Science (Diplom)
- 2008–2011: Eindhoven
  Ph.D. in Department of Mathematics



My way to MPI-SP

- 2001–2007: Aachen
  Studied Computer Science (Diplom)
- 2008–2011: Eindhoven
  Ph.D. in Department of Mathematics
- 2011–2012: Taipei
  Postdoc at Academia Sinica and NTU

My way to MPI-SP

- **2001–2007: Aachen**
  Studied Computer Science (Diplom)
- **2008–2011: Eindhoven**
  Ph.D. in Department of Mathematics
- **2011–2012: Taipei**
  Postdoc at Academia Sinica and NTU
- **Since 2013: Nijmegen**
  From Assistant to Full Professor

My way to MPI-SP

- **2001–2007: Aachen**
  Studied Computer Science (Diplom)
- **2008–2011: Eindhoven**
  Ph.D. in Department of Mathematics
- **2011–2012: Taipei**
  Postdoc at Academia Sinica and NTU
- **Since 2013: Nijmegen**
  From Assistant to Full Professor
- **Since 2020: Bochum**
  First MPRGL, since 2024 Director at MPI-SP

When I’m not doing research. . .

- I love travelling

When I’m not doing research. . .

- I love travelling
- if possible by motorcycle

When I’m not doing research. . .

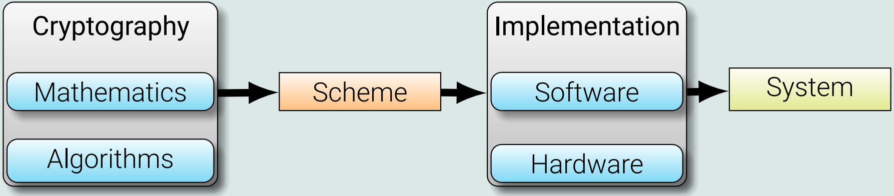
- I love travelling
- if possible by motorcycle
- and I’m a foodie

Cryptographic Engineering

> *“Cryptography* [. . .] *is the practice and study of techniques for secure communication in the presence of adversarial behavior.* [. . .] *Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, information security, electrical engineering, digital signal processing, physics, and others.”*
>
> —Wikipedia on *Cryptography*

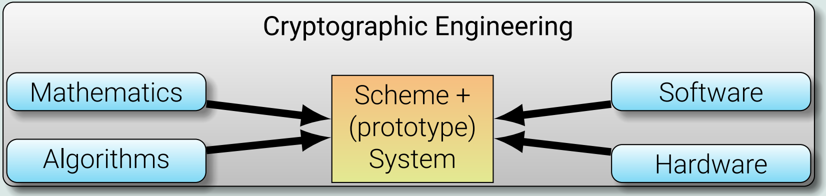
Cryptographic Engineering

The traditional approach



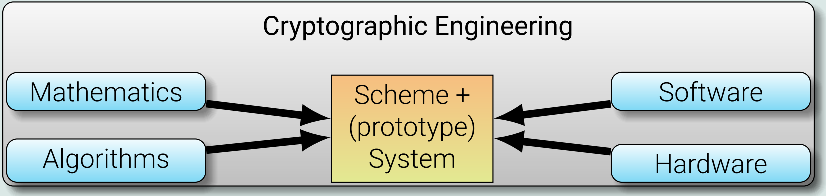
Cryptographic Engineering

A holistic approach



Cryptographic Engineering

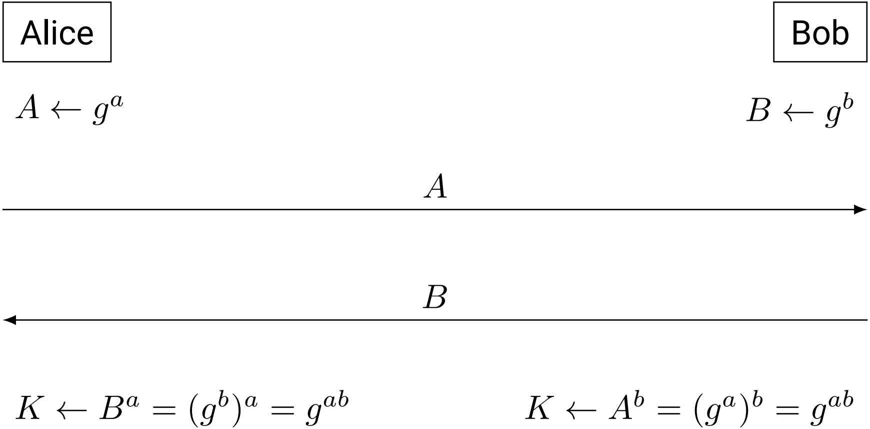
A holistic approach



Motivation from real-world problems – aim to make real-world impact

[A small demo]

Diffie-Hellman key exchange



Alice

Bob

$A \leftarrow g^a$

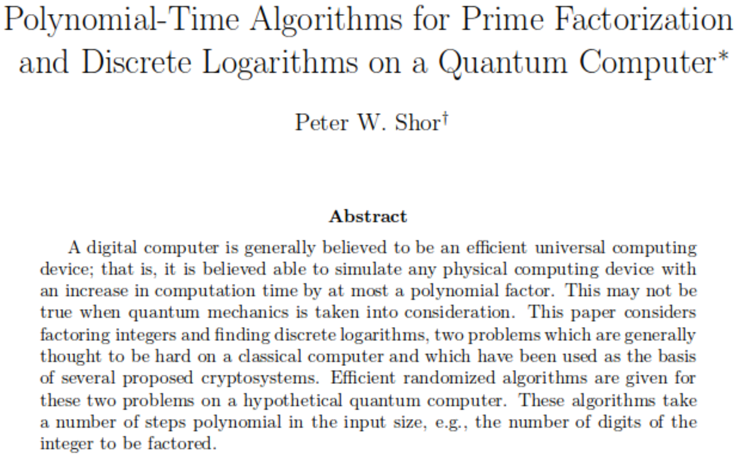
$B \leftarrow g^b$

A

B

$K \leftarrow B^a = (g^b)^a = g^{ab}$

$K \leftarrow A^b = (g^a)^b = g^{ab}$



Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

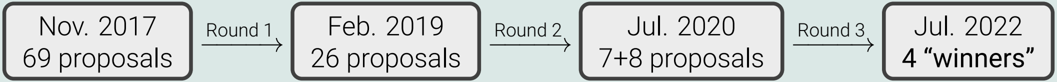
NIST PQC

- National Institute of Standards and Technology (USA)
- *Everybody* could submit proposals for post-quantum crypto (PQC)
- Open process in close collaboration with research community

NIST PQC

- National Institute of Standards and Technology (USA)
- *Everybody* could submit proposals for post-quantum crypto (PQC)
- Open process in close collaboration with research community

NIST PQC



Nov. 2017
69 proposals

Round 1 →

Feb. 2019
26 proposals

Round 2 →

Jul. 2020
7+8 proposals

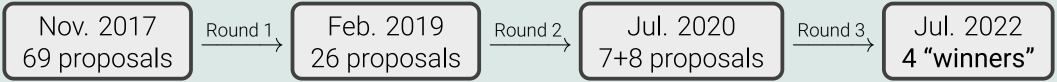
Round 3 →

Jul. 2022
4 "winners"

NIST PQC

- National Institute of Standards and Technology (USA)
- *Everybody* could submit proposals for post-quantum crypto (PQC)
- Open process in close collaboration with research community

NIST PQC



Nov. 2017
69 proposals

Round 1 →

Feb. 2019
26 proposals

Round 2 →

Jul. 2020
7+8 proposals

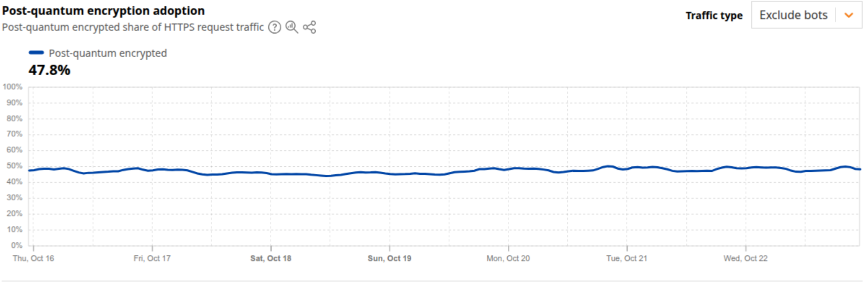
Round 3 →

Jul. 2022
4 “winners”

> *“The public-key encryption and key-establishment algorithm that will be standardized is **CRYSTALS-KYBER**. The digital signatures that will be standardized are **CRYSTALS-Dilithium**, FALCON, and **SPHINCS**$^+$.*
>
> —NIST IR 8413-upd1

[Back to our demo]

PQC deployment



Post-quantum encryption adoption

Post-quantum encrypted share of HTTPS request traffic

Traffic type: Exclude bots

Post-quantum encrypted

47.8%

https://radar.cloudflare.com/adoption-and-usage#post-quantum-encryption-adoption

- Hundreds of billions of connections per day at Cloudflare alone
- Also used in secure messaging (Signal, iMessage)
- Also in cloud infrastructure (AWS)
- Signatures deployed in automotive SW updates and for secure boot

High-assurance cryptography

FORMOSA
CRYPTO

- Effort to **formally verify** crypto
- Founded in 2021
- Now 17 partner institutions

High-assurance cryptography

FORMOSA
CRYPTO

- Effort to **formally verify** crypto
- Founded in 2021
- Now 17 partner institutions

High-assurance ML-KEM

- End-to-end computer verified
  - High-speed assembly-level code
  - Machine-readable specification
  - Indistinguishability security notion

High-assurance cryptography

FORMOSA CRYPTO

- Effort to **formally verify** crypto
- Founded in 2021
- Now 17 partner institutions

High-assurance ML-KEM

- End-to-end computer verified
  - High-speed assembly-level code
  - Machine-readable specification
  - Indistinguishability security notion
- Implementation security
  - No secret branches
  - No secret memory indices
  - No variable-time arithmetic

High-assurance cryptography

FORMOSA
CRYPTO

- Effort to **formally verify** crypto
- Founded in 2021
- Now 17 partner institutions

High-assurance ML-KEM

- End-to-end computer verified
  - High-speed assembly-level code
  - Machine-readable specification
  - Indistinguishability security notion
- Implementation security
  - No secret branches
  - No secret memory indices
  - No variable-time arithmetic
  - **Also during speculative execution**

High-assurance cryptography

FORMOSA CRYPTO

- Effort to **formally verify** crypto
- Founded in 2021
- Now 17 partner institutions

High-assurance ML-KEM

- End-to-end computer verified
  - High-speed assembly-level code
  - Machine-readable specification
  - Indistinguishability security notion
- Implementation security
  - No secret branches
  - No secret memory indices
  - No variable-time arithmetic
  - **Also during speculative execution**
- Real-world deployment is WIP

Post-Quantum HW Root of Trust

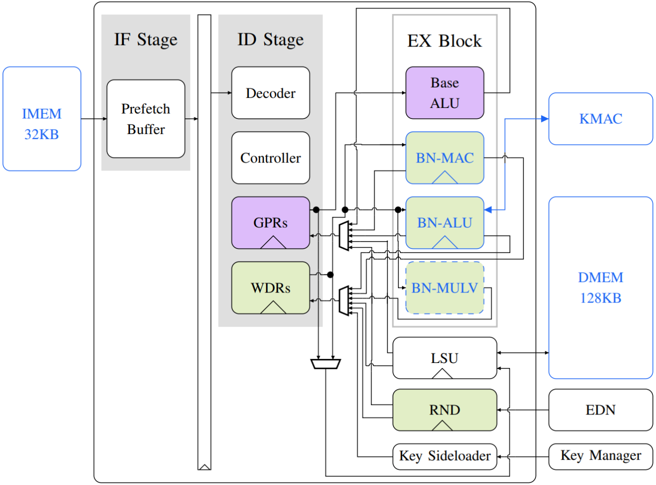
opentitan

- Open-source HW root of trust
- HW/SW co-design to support PQC
- Hopefully in silicon soon
- Enables new research directions

Industry Partners

zeroRISC

Rivos



Thank you!

Amin Abdulrahman, Andreas Hülsing, Andreas Zankl, Andrew ’bunnie’ Huang, Antoine Séré, Augustine Tang, Basavesh Ammanaghatta Shivakumar, Bas Westerbaan, Benjamin Grégoire, Cameron Low, Chitchanok Chuengsatiansup, Christian Rechberger, Christoph Dobraunig, Damien Stehlé, Daniel J. Bernstein, Dominic Rizzo, Eike Kiltz, Evan Apinis, Felix Oberhansl, Florian Mendel, Francisca Barros, François Dupressoir, Gilles Barthe, Gregor Seiler, Gustavo Xavier Delerue Marinho Alves, Hoang Nguyen Hien Pham, Hugo Pacheco, Ignacio Cuevas, Jade Philipoom, Jan Jancar, Jean-Christophe Léchenet, Jean-Philippe Aumasson, Jieyu Zheng, Jintai Ding, John M. Schanck, Joost Rijneveld, Joppe Bos, José Bacelar Almeida, Léo Ducas, Lionel Blatter, Lucas Tabary-Maujean, Luís Esquível, Manuel Barbosa, Maria Eichlseder, Martin M Lauridsen, Matthias J. Kannwischer, Miguel Quaresma, Panos Kampanakis, Pierre-Yves Strub, Roberto Avanzi, Robert Schilling, Rolfe Schmidt, Ruben Gonzalez, Ruben Niederhagen, Ruben Niederhagen, Santiago Arranz-Olmos, Scott Fluhrer, Shi Bai, Stefan Kölbl, Stefan-Lukas Gazdag, Swarn Priya, Tancrede Lepoint, Tanja Lange, Tiago Oliveira, Ting-han Lim, Tobias Stelzer, Vadim Lyubashevsky, Vincent Hwang, Vincent Laporte, Ward Beullens, Yuval Yarom, Zhiyuan Zhang

Thank you!

https://cryptojedi.org