MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

“My life in crypto”

Peter Schwabe

September 17, 2024

High-school until 2000

2001–2006: Studying in Aachen

- About 2h from my parents' place
- First time living on my own

2001–2006: Studying in Aachen

- About 2h from my parents' place
- First time living on my own
- Studied CS (with application subject medicine)
- 2nd year started working as student assistant

2001–2006: Studying in Aachen

- About 2h from my parents' place
- First time living on my own
- Studied CS (with application subject medicine)
- 2nd year started working as student assistant
- Met Michael Naehrig
- Thesis ("Diplomarbeit") on Implementation of elliptic and hyperelliptic curves

2001–2006: Studying in Aachen

- About 2h from my parents' place
- First time living on my own
- Studied CS (with application subject medicine)
- 2nd year started working as student assistant
- Met Michael Naehrig
- Thesis ("Diplomarbeit") on Implementation of elliptic and hyperelliptic curves
- Accepted offer for Ph.D. position

2001–2006: Studying in Aachen

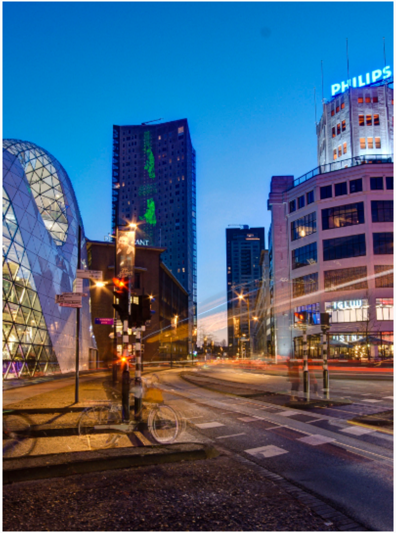
- About 2h from my parents' place
- First time living on my own
- Studied CS (with application subject medicine)
- 2nd year started working as student assistant
- Met Michael Naehrig
- Thesis ("Diplomarbeit") on Implementation of elliptic and hyperelliptic curves
- Accepted offer for Ph.D. position
- Quit after 16 months

Lesson 1: Make good decisions.

- Don’t take a certain path just because it’s easy
- Think about what you want
- Figure out what your options are
- Take time for your decision

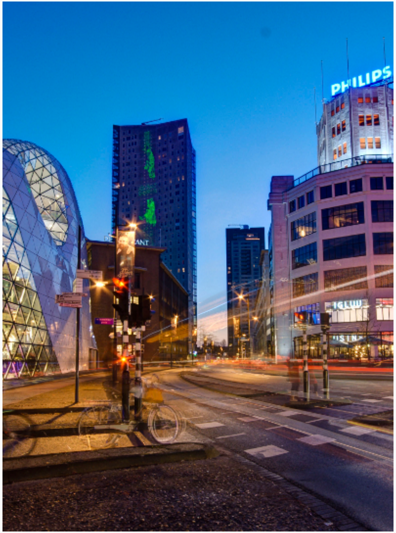
Ph.D. for real: Eindhoven

- Work on optimizing crypto software
- Very productive environment:
  - Great supervisors
  - Lots of colleagues in crypto
  - Collaborations with other groups
- Payed by EU project CACE



Ph.D. for real: Eindhoven

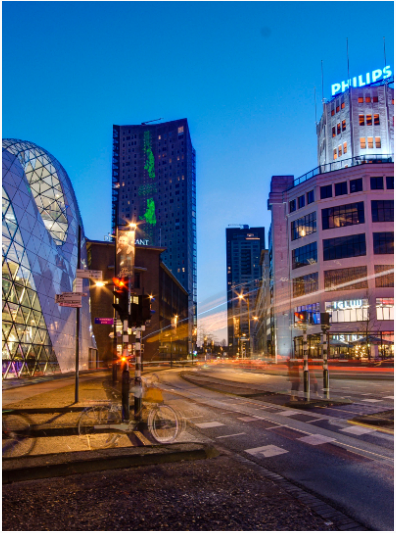
- Work on optimizing crypto software
- Very productive environment:
  - Great supervisors
  - Lots of colleagues in crypto
  - Collaborations with other groups
- Payed by EU project CACE
- Yes, Ph.D. students are payed in NL/DE!
- In DE, about 2500 EUR/month after tax



Ph.D. for real: Eindhoven

- Work on optimizing crypto software
- Very productive environment:
  - Great supervisors
  - Lots of colleagues in crypto
  - Collaborations with other groups
- Payed by EU project CACE
- Yes, Ph.D. students are payed in NL/DE!
- In DE, about 2500 EUR/month after tax
- Graduated in Jan 2011

  `https://cryptojedi.org/gallery/Defense-Peter/index.shtml`



Finding topics, part 1: as a student

Lesson 2: talk to people!

- First topics were chosen/suggested by my supervisors
- Present your work, discuss
- Most fun collaborations came out of “hallway sessions”

Finding topics, part 1: as a student

Lesson 2: talk to people!

- First topics were chosen/suggested by my supervisors
- Present your work, discuss
- Most fun collaborations came out of “hallway sessions”
- Multiple possible motivations to work on a topic:
    - Your supervisor asks you to do it
    - Natural followup/extension to work you’ve done
    - You want to learn about a particular topic
    - You want to work with some specific person

Lesson 2: talk to people!

- First topics were chosen/suggested by my supervisors
- Present your work, discuss
- Most fun collaborations came out of “hallway sessions”
- Multiple possible motivations to work on a topic:
  - Your supervisor asks you to do it
  - Natural followup/extension to work you’ve done
  - You want to learn about a particular topic
  - You want to work with some specific person
- Interesting “switching point” during Ph.D.:
  - At first, you need *some* topic
  - At some point, you need to *choose* from *many* topics

Finding a Postdoc position

- Ask.

Finding a Postdoc position

- Ask.
- Ask early.

Finding a Postdoc position

- Ask.
- Ask early.
- Finding a Postdoc position is easy
- Postdocs are “cheap”
- Good Postdocs are simply great!

2011–2012: Postdoc in Taiwan

- Continued work on crypto software
- Continued working with my Ph.D. supervisors
  - Great collaboration
  - **Not the idea of a postdoc!**

2011–2012: Postdoc in Taiwan

- Continued work on crypto software
- Continued working with my Ph.D. supervisors
  - Great collaboration
  - **Not the idea of a postdoc!**
- Always felt welcome, Taiwan is extremely friendly

2011–2012: Postdoc in Taiwan

- Continued work on crypto software
- Continued working with my Ph.D. supervisors
  - Great collaboration
  - **Not the idea of a postdoc!**
- Always felt welcome, Taiwan is extremely friendly
- (Most) things function very well, just differently

2011–2012: Postdoc in Taiwan

- Continued work on crypto software
- Continued working with my Ph.D. supervisors
  - Great collaboration
  - **Not the idea of a postdoc!**
- Always felt welcome, Taiwan is extremely friendly
- (Most) things function very well, just differently
- Could ignore e-mails from my employer

Lesson 3: Move outside your comfort zone!

- Academic research is highly international
- Experience life in a (very) different country
  - What does it mean to not speak the language?
  - What does it mean to be in a different culture?
  - What does it mean to have your friends/family in a different timezone?

Lesson 3: Move outside your comfort zone!

- Academic research is highly international
- Experience life in a (very) different country
  - What does it mean to not speak the language?
  - What does it mean to be in a different culture?
  - What does it mean to have your friends/family in a different timezone?
- Important life lesson, helps you understand others
- For me: amazing experience!
- Worth much more than writing another two or three papers

From Taipei to Nijmegen

- Applied for Assistant Professor position
- Interview after 30h trip, Friday at midnight

From Taipei to Nijmegen

- Applied for Assistant Professor position
- Interview after 30h trip, Friday at midnight
- E-mail Monday morning: “you got the job!”

From Taipei to Nijmegen

- Applied for Assistant Professor position
- Interview after 30h trip, Friday at midnight
- E-mail Monday morning: “you got the job!”
- Started January 2013

From Taipei to Nijmegen

- Applied for Assistant Professor position
- Interview after 30h trip, Friday at midnight
- E-mail Monday morning: “you got the job!”
- Started January 2013
- NWO Veni grant in 2013

From Taipei to Nijmegen

- Applied for Assistant Professor position
- Interview after 30h trip, Friday at midnight
- E-mail Monday morning: “you got the job!”
- Started January 2013
- NWO Veni grant in 2013
- ~~NWO Vidi grant~~ and ERC StG in 2018

From Taipei to Nijmegen

- Applied for Assistant Professor position
- Interview after 30h trip, Friday at midnight
- E-mail Monday morning: “you got the job!”
- Started January 2013
- NWO Veni grant in 2013
- ~~NWO Vidi grant~~ and ERC StG in 2018
- Associate Professor in 2018
- Head of Digital Security Group from 2019
- Full Professor in 2020

Teaching

- A good teacher needs to be a “good entertainer”

Teaching

- A good teacher needs to be a “good entertainer”
- Think about a coherent story for a course

Teaching

- A good teacher needs to be a “good entertainer”
- Think about a coherent story for a course
- Very tricky to make sure that
  - weak students learn something and can pass
  - strong students are still challenged
- Tough mandatory homework + much easier exam

Teaching

- A good teacher needs to be a “good entertainer”
- Think about a coherent story for a course
- Very tricky to make sure that
    - weak students learn something and can pass
    - strong students are still challenged
- Tough mandatory homework + much easier exam
- Teaching (preparation) takes a lot of time!
- Well-prepared exams take less time to grade

Leading a group

- Start small, grow slowly!

Leading a group

- Start small, grow slowly!
- Most important: **A good atmosphere and happy people**
  - Understand and support individual needs and wishes
  - Respect different cultures, priorities, working hours, etc.
  - Clearly communicate what is important to you

Leading a group

- Start small, grow slowly!
- Most important: **A good atmosphere and happy people**
  - Understand and support individual needs and wishes
  - Respect different cultures, priorities, working hours, etc.
  - Clearly communicate what is important to you
- Best thing: See other people succeed and grow

Leading a group

- Start small, grow slowly!
- Most important: **A good atmosphere and happy people**
    - Understand and support individual needs and wishes
    - Respect different cultures, priorities, working hours, etc.
    - Clearly communicate what is important to you
- Best thing: See other people succeed and grow
- Worst thing: Having to “kick people in the butt”

Lesson 4: Everything takes time!

- Most(?) academics are notoriously over-committed.
- Job description: 40% teaching, 40% research, 20% service
- More realistic: 50% teaching, 50% research, 50% service
- You cannot be excellent at everything

Lesson 4: Everything takes time!

- Most(?) academics are notoriously over-committed.
- Job description: 40% teaching, 40% research, 20% service
- More realistic: 50% teaching, 50% research, 50% service
- **You cannot be excellent at everything**
- Learn to prioritize
- Learn to say **no**

Getting funding

Two approaches

1. Figure out what people will pay you for and do that
2. **Figure out what you want to do and get people to pay you for it**

Getting funding

Two approaches

1. Figure out what people will pay you for and do that
2. **Figure out what you want to do and get people to pay you for it**

- We are lucky, there is money in CS
- Don't be afraid to ask (e.g., for conference stipends)
- Grant proposals have their own rules. . .

Getting funding

Two approaches

1. Figure out what people will pay you for and do that
2. **Figure out what you want to do and get people to pay you for it**

- We are lucky, there is money in CS
- Don't be afraid to ask (e.g., for conference stipends)
- Grant proposals have their own rules. . .

"Money makes money"

Getting funding

Two approaches

1. Figure out what people will pay you for and do that
2. **Figure out what you want to do and get people to pay you for it**

- We are lucky, there is money in CS
- Don't be afraid to ask (e.g., for conference stipends)
- Grant proposals have their own rules. . .

"Der Teufel scheißt immer auf den größten Haufen"

Finding topics, part 2: as faculty

Lesson 5: Travel. And talk to people!

- With more overview comes larger need to filter
- As a “group leader” you don’t choose for yourself alone!
- Still multiple reasons to pick a certain topic:

Lesson 5: Travel. And talk to people!

- With more overview comes larger need to filter
- As a “group leader” you don’t choose for yourself alone!
- Still multiple reasons to pick a certain topic:
  - Scientific interest or curiosity

Finding topics, part 2: as faculty

Lesson 5: Travel. And talk to people!

- With more overview comes larger need to filter
- As a “group leader” you don’t choose for yourself alone!
- Still multiple reasons to pick a certain topic:
    - Scientific interest or curiosity
    - Money

Finding topics, part 2: as faculty

Lesson 5: Travel. And talk to people!

- With more overview comes larger need to filter
- As a “group leader” you don’t choose for yourself alone!
- Still multiple reasons to pick a certain topic:
  - Scientific interest or curiosity
  - Money
  - Easy topic to get top-venue publications

Finding topics, part 2: as faculty

Lesson 5: Travel. And talk to people!

- With more overview comes larger need to filter
- As a “group leader” you don’t choose for yourself alone!
- Still multiple reasons to pick a certain topic:
  - Scientific interest or curiosity
  - Money
  - Easy topic to get top-venue publications
  - Big potential real-world impact

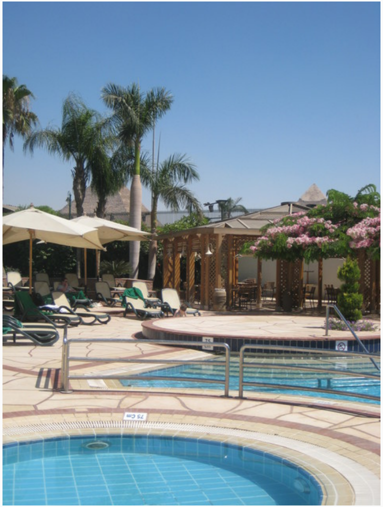
Finding topics, part 2: as faculty

Lesson 5: Travel. And talk to people!

- With more overview comes larger need to filter
- As a “group leader” you don’t choose for yourself alone!
- Still multiple reasons to pick a certain topic:
  - Scientific interest or curiosity
  - Money
  - Easy topic to get top-venue publications
  - Big potential real-world impact
  - Fun collaboration

Great collaborations and how/where they started

Great collaborations and how/where they started



Great collaborations and how/where they started

4630 Bochum

Lesson 6: Be nice.

Lesson 6: Be nice.

- . . . to your readers

Lesson 6: Be nice.

- . . . to your readers
- . . . to collaborators

Lesson 6: Be nice.

- . . . to your readers
- . . . to collaborators
- . . . to competing groups

Lesson 6: Be nice.

- . . . to your readers
- . . . to collaborators
- . . . to competing groups
- . . . to students

Lesson 6: Be nice.

- . . . to your readers
- . . . to collaborators
- . . . to competing groups
- . . . to students
- . . . to random people sending you e-mail

Lesson 6: Be nice.

- . . . to your readers
- . . . to collaborators
- . . . to competing groups
- . . . to students
- . . . to random people sending you e-mail

However:

- Don't be a yes-person
- Say what you want
- Don't let others exploit you

Cryptography – the very basics

Alice

- Alice encrypts a message M using a key K obtains ciphertext C
- Sends C to Bob

Bob

- Bob decrypts C using K and obtains M

Let me introduce Eve

- Eve does not know the key K, tries to obtain the message M

Let me introduce Eve

- Eve does not know the key K, tries to obtain the message M
- What can Eve do?
  - Listen on the transmission channel

Let me introduce Eve

- Eve does not know the key K, tries to obtain the message M
- What can Eve do?
  - Listen on the transmission channel
  - Modify messages going over the channel
  - Send messages herself

Let me introduce Eve

- Eve does not know the key K, tries to obtain the message M
- What can Eve do?
  - Listen on the transmission channel
  - Modify messages going over the channel
  - Send messages herself
  - Obtain message-ciphertext pairs encrypted under K

Let me introduce Eve

- Eve does not know the key K, tries to obtain the message M
- What can Eve do?
  - Listen on the transmission channel
  - Modify messages going over the channel
  - Send messages herself
  - Obtain message-ciphertext pairs encrypted under K
  - Massive computations (for example to compute K)

Let me introduce Eve

- Eve does not know the key K, tries to obtain the message M
- What can Eve do?
  - Listen on the transmission channel
  - Modify messages going over the channel
  - Send messages herself
  - Obtain message-ciphertext pairs encrypted under K
  - Massive computations (for example to compute K)
  - More later . . .

More cryptography

- How does Bob know that the message comes form Alice?
  Answer: authentication (of users) using a key K_a

More cryptography

- How does Bob know that the message comes form Alice?
  Answer: authentication (of users) using a key K_a
- How does Bob know that the message hasn't been modified?
  Answer: authentication (of the message) using a key K_a

More cryptography

- How does Bob know that the message comes form Alice?
  Answer: authentication (of users) using a key K_a
- How does Bob know that the message hasn't been modified?
  Answer: authentication (of the message) using a key K_a
- How do Alice and Bob get K in the first place?
  Answer: Key-exchange protocols

More cryptography

- How does Bob know that the message comes form Alice?
  Answer: authentication (of users) using a key K_a
- How does Bob know that the message hasn't been modified?
  Answer: authentication (of the message) using a key K_a
- How do Alice and Bob get K in the first place?
  Answer: Key-exchange protocols
- How can Alice send a message such that everybody can be sure that she sent that message?
  Answer: Cryptographic signatures

More cryptography

- How does Bob know that the message comes form Alice?
  Answer: authentication (of users) using a key K_a
- How does Bob know that the message hasn't been modified?
  Answer: authentication (of the message) using a key K_a
- How do Alice and Bob get K in the first place?
  Answer: Key-exchange protocols
- How can Alice send a message such that everybody can be sure that she sent that message?
  Answer: Cryptographic signatures

Eve's goals

- In short: Everything forbidden

More cryptography

- How does Bob know that the message comes form Alice?
  Answer: authentication (of users) using a key K_a
- How does Bob know that the message hasn't been modified?
  Answer: authentication (of the message) using a key K_a
- How do Alice and Bob get K in the first place?
  Answer: Key-exchange protocols
- How can Alice send a message such that everybody can be sure that she sent that message?
  Answer: Cryptographic signatures

Eve's goals

- In short: Everything forbidden
- Impersonate Alice or Bob, forge messages, obtain keys (most powerful attack!)

The NSA (Eve)

National Security Agency

- US American secret service
- Largest employer for mathematicians in the world
  - Estimated $40000 - 75000$ employees
  - “Black budget” of US$$52.6$ billion / year
  - Power-bill for Utah data center (estimated): US$$40$ million / year

Pictures from the Wikimedia Commons

How secure is cryptography?

Kerckhoffs' principle

An encryption algorithm takes as input a message and a key. The security of the system must rely only on the secrecy of the key, not on the secrecy of the algorithm.

How secure is cryptography?

Kerckhoffs’ principle

An encryption algorithm takes as input a message and a key. The security of the system must rely only on the secrecy of the key, not on the secrecy of the algorithm.

- Strongest attack: find the key

How secure is cryptography?

Kerckhoffs' principle

An encryption algorithm takes as input a message and a key. The security of the system must rely only on the secrecy of the key, not on the secrecy of the algorithm.

- Strongest attack: find the key
- Security of the system (simplified): Hardness to find the key
- If the best known algorithm takes 2^n "operations" to find the key, we say that a system is assumed to have *n* bits of security

How secure is cryptography?

Kerckhoffs' principle

An encryption algorithm takes as input a message and a key. The security of the system must rely only on the secrecy of the key, not on the secrecy of the algorithm.

- Strongest attack: find the key
- Security of the system (simplified): Hardness to find the key
- If the best known algorithm takes 2^n "operations" to find the key, we say that a system is assumed to have *n* bits of security
- Generic attack against *n*-bit key: try all possibilities. Cost: 2^n

How secure is cryptography?

Kerckhoffs' principle

An encryption algorithm takes as input a message and a key. The security of the system must rely only on the secrecy of the key, not on the secrecy of the algorithm.

- Strongest attack: find the key
- Security of the system (simplified): Hardness to find the key
- If the best known algorithm takes 2^n "operations" to find the key, we say that a system is assumed to have *n* bits of security
- Generic attack against *n*-bit key: try all possibilities. Cost: 2^n
- If a system is believed to have *n* bits of security, an attacker can break it
  - if he can carry out 2^n operations, or
  - if he knows a better attack

How many bits of security has X?

keylength.com

- Various institutions give recommendations based on best known attacks
- NIST (every year)
- ECRYPT (until 2012)
- BSI, ANSSI

How many bits of security has X?

keylength.com

- Various institutions give recommendations based on best known attacks
- NIST (every year)
- ECRYPT (until 2012)
- BSI, ANSSI

How many bits of security has X?

keylength.com

- Various institutions give recommendations based on best known attacks
- NIST (every year)
- ECRYPT (until 2012)
- BSI, ANSSI

Some examples of popular schemes (NIST, 2012)

- **AES-128:** 128 bits
- **RSA-1024:** 80 bits
- **RSA-2048:** 112 bits
- **256-bit elliptic curve:** 128 bits

Can Eve break AES-128?

- Analysis by Bernstein (slightly modified):
  - How much energy does it take to break AES-128?
  - How much energy do we get?

Can Eve break AES-128?

- Analysis by Bernstein (slightly modified):
  - How much energy does it take to break AES-128?
  - How much energy do we get?
- Second question first:
  - Sun is radiating $\approx 2^{58}$ watts onto the earth
  - Geothermal energy: $\approx 2^{46}$ watts
  - Gravitation of moon and sun: $\approx 2^{43}$ watts

Can Eve break AES-128?

- Analysis by Bernstein (slightly modified):
  - How much energy does it take to break AES-128?
  - How much energy do we get?
- Second question first:
  - Sun is radiating $\approx 2^{58}$ watts onto the earth
  - Geothermal energy: $\approx 2^{46}$ watts
  - Gravitation of moon and sun: $\approx 2^{43}$ watts
- First question:
  - Best mass-market chips: $\approx 2^{68}$ bit ops / watt / year
  - Perfect power usage: 2^{126} bit ops / year
  - AES key guess takes 2^{13} bit ops
  - Break key with probability 1: > 30000 years

So, why do we need research in crypto?

Assumptions, assumptions, assumptions. . .

Side channels

Image by Natasha Martin/Timaru Herald

Side channels

Image by Natasha Martin/Timaru Herald

- So far: attacker could see inputs and outputs
- Attackers can see more:
  - power consumption,
  - electromagnetic radiation
  - timing **(even remotely!)**

Side channels

Image by Natasha Martin/Timaru Herald

- So far: attacker could see inputs and outputs
- Attackers can see more:
  - power consumption,
  - electromagnetic radiation
  - timing **(even remotely!)**
- Side-channel attacks: Use this data to break cryptographic protection

Side channels

Image by Natasha Martin/Timaru Herald

- So far: attacker could see inputs and outputs
- Attackers can see more:
  - power consumption,
  - electromagnetic radiation
  - timing **(even remotely!)**
- Side-channel attacks: Use this data to break cryptographic protection
- Side-channel attacks target specific implementations

It gets much worse than that. . .

MELTDOWN

Hertzbleed

CACHE OUT

[A small demo]

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.

[Back to our demo]

Ongoing research in my group

Post-Quantum Cryptography

- Signatures and KEMs in NIST-PQC
- Beyond NIST-PQC, e.g., NIKE
- Protocol migration (KEMTLS, PQ-Wireguard)
- Embedded implementations (e.g., pqm4)

Ongoing research in my group

Post-Quantum Cryptography

- Signatures and KEMs in NIST-PQC
- Beyond NIST-PQC, e.g., NIKE
- Protocol migration (KEMTLS, PQ-Wireguard)
- Embedded implementations (e.g., pqm4)

Formosa Crypto

- **High-assurance** crypto
- Intersection of crypto and formal methods
- Collaboration with many groups across Europe
- `https://formosa-crypto.org`

Ongoing research in my group

Post-Quantum Cryptography

- Signatures and KEMs in NIST-PQC
- Beyond NIST-PQC, e.g., NIKE
- Protocol migration (KEMTLS, PQ-Wireguard)
- Embedded implementations (e.g., pqm4)

Formosa Crypto

- **High-assurance** crypto
- Intersection of crypto and formal methods
- Collaboration with many groups across Europe
- `https://formosa-crypto.org`

OpenTitan collaboration

- Open Source HW root of trust
- See `https://opentitan.org`
- (High-assurance) PQC on OpenTitan
- Side-channel security for OpenTitan

Ongoing research in my group

Post-Quantum Cryptography

- Signatures and KEMs in NIST-PQC
- Beyond NIST-PQC, e.g., NIKE
- Protocol migration (KEMTLS, PQ-Wireguard)
- Embedded implementations (e.g., pqm4)

OpenTitan collaboration

- Open Source HW root of trust
- See `https://opentitan.org`
- (High-assurance) PQC on OpenTitan
- Side-channel security for OpenTitan

Formosa Crypto

- **High-assurance** crypto
- Intersection of crypto and formal methods
- Collaboration with many groups across Europe
- `https://formosa-crypto.org`

Microarchitectural security

- Protection against SW side channels
- HW SCA and countermeasures
- Spectre countermeasures
- Integration with Formosa Crypto