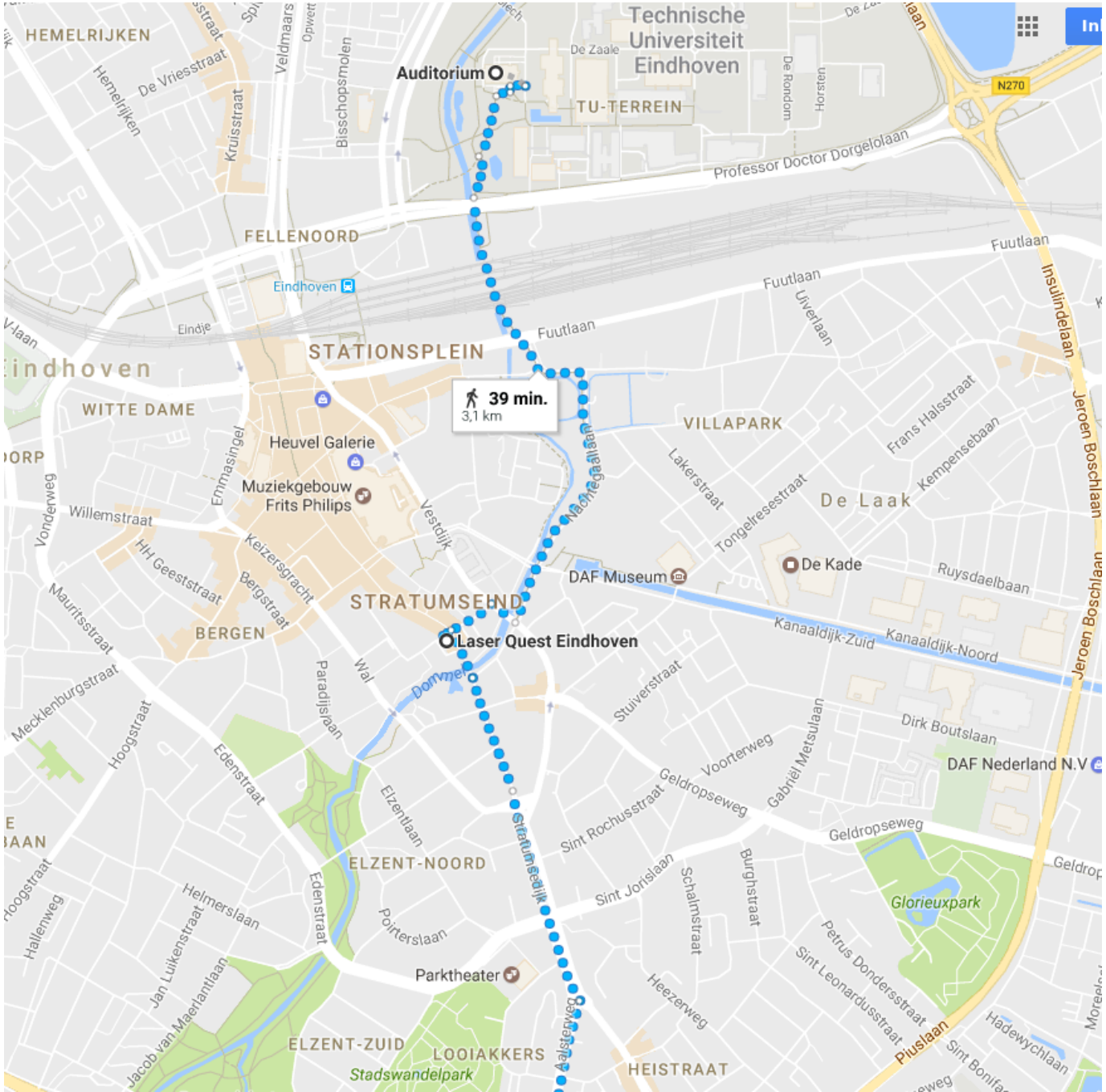
Summer school 2017

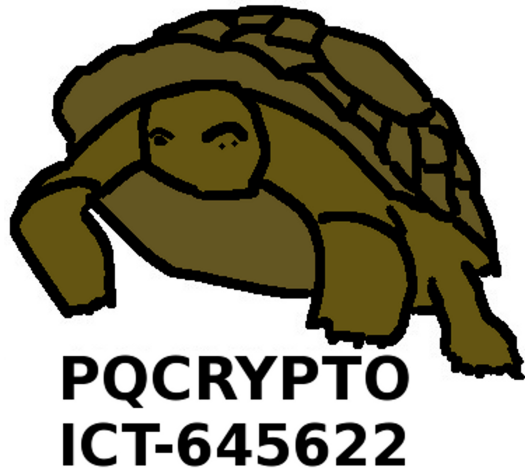
- 5 days of program – lots of talks + exercise sessions.
- We'll provide exercises for all lectures, pick some to solve in the exercise sessions. We'll be around to help (if you stay close to the Blauwe Zaal. It's best to work in small groups.
- Excursion starts Wed 15:00 at Laser Quest Eindhoven. We'll split into smaller groups for a scavanger hunt (with extra complications! ask a Dutch person about 'Who is the mole?') + other activities.
- Dinner starts at 19:30 at a Mongolian Grill


Auditorium
Technische Universiteit Eindhoven
TU-TERREIN
De Zaale
De Rondom
Horsten
N270
Professor Doctor Dorgelolaan
FELLENOORD
Eindhoven
Fuutlaan
Uiverlaan
Insulindelaan
Jeroen Boschlaan
STATIONSPLEIN
39 min.
3,1 km
WITTE DAME
Heuvel Galerie
Muziekgebouw Frits Philips
VILLAPARK
De Laak
Kempensebaan
Frans Halsstraat
Lakerstraat
Tongelresestraat
Nachtegaallaan
Vestdijk
Emmasingel
Willemstraat
Vonderweg
HH Geeststraat
Keizersgracht
Bergstraat
Mauritsstraat
BERGEN
STRATUMSEIND
DAF Museum
De Kade
Ruysdaelbaan
Kanaaldijk-Zuid
Kanaaldijk-Noord
Laser Quest Eindhoven
Dommel
Wal
Paradijslaan
Stuiverstraat
Dirk Boutslaan
DAF Nederland N.V
Voorterweg
Geldropseweg
Gabriël Metsulaan
Sint Rochusstraat
Mecklenburgstraat
Hoogstraat
Edenstraat
Elzentlaan
ELZENT-NOORD
Statumseweg
Sint Jorislaan
Schalmstraat
Burghstraat
Glorieuxpark
Helmerslaan
Hallenweg
Jan Luikenstraat
Jacob van Maerlantlaan
Pointerslaan
Parktheater
Heezerweg
Petrus Dondersstraat
Sint Leonardusstraat
Piuslaan
Hadewychlaan
ELZENT-ZUID
LOOIAKKERS
Stadswandelpark
Aalsterweg
HEISTRAAT
HEMELRIJKEN
De Vriesstraat
Hemelrijken
Kruisstraat
Veldmaarschalk
Bisschopsmolen
Eindje

Introduction to post-quantum cryptography

Tanja Lange

Technische Universiteit Eindhoven



19 June 2017

PQCRYPTO Summer School

Cryptography

- Motivation #1: Communication channels are spying on our data.
- Motivation #2: Communication channels are modifying our data.

Sender
“Alice”

Untrustworthy network
“Eve”

Receiver
“Bob”

- Literal meaning of cryptography: “secret writing”.
- Achieves various security goals by secretly transforming messages.

iacrmemHEREATiacr.org

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

2013

1702 Members
(1580 in 2012)

1245 Regular+

457 Students


https://www.iacr.org/
https://www.iacr.org/docs/minutes/c2013mem-slides.pdf
IACR Mer
16 /
www.iacr.org
Your connection to this site is private.
Permissions
Connection
The identity of this website has been verified by RapidSSL SHA256 CA - G3.
No Certificate Transparency information was supplied by the server.
Certificate information
Your connection to www.iacr.org is encrypted using a modern cipher suite.
The connection uses TLS 1.2.
The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.
What do these mean?
iacrm

Secret-key encryption

- Prerequisite: Alice and Bob share a secret key  .
- Prerequisite: Eve doesn't know  .
- Alice and Bob exchange any number of messages.
- Security goal #1: **Confidentiality** despite Eve's espionage.

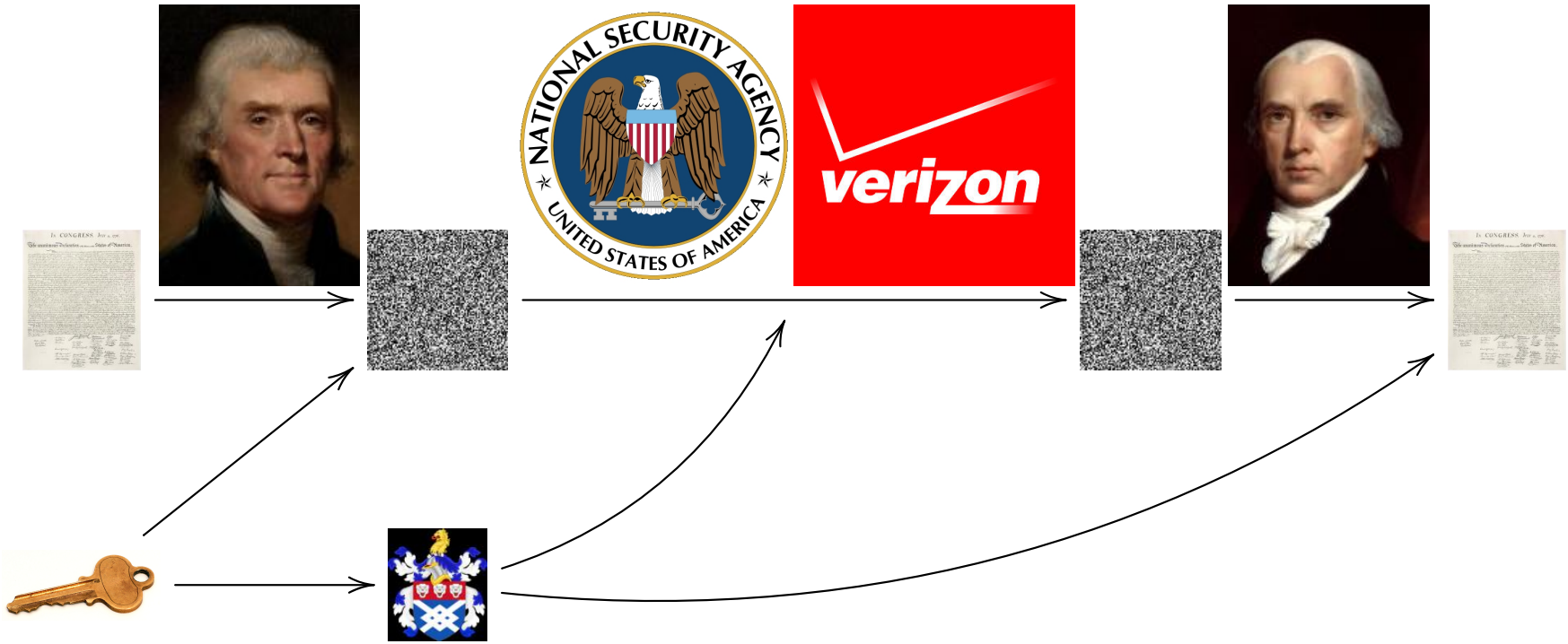
Secret-key authenticated encryption

- Prerequisite: Alice and Bob share a secret key  .
- Prerequisite: Eve doesn't know  .
- Alice and Bob exchange any number of messages.
- Security goal #1: **Confidentiality** despite Eve's espionage.
- Security goal #2: **Integrity**, i.e., recognizing Eve's sabotage.

Secret-key authenticated encryption

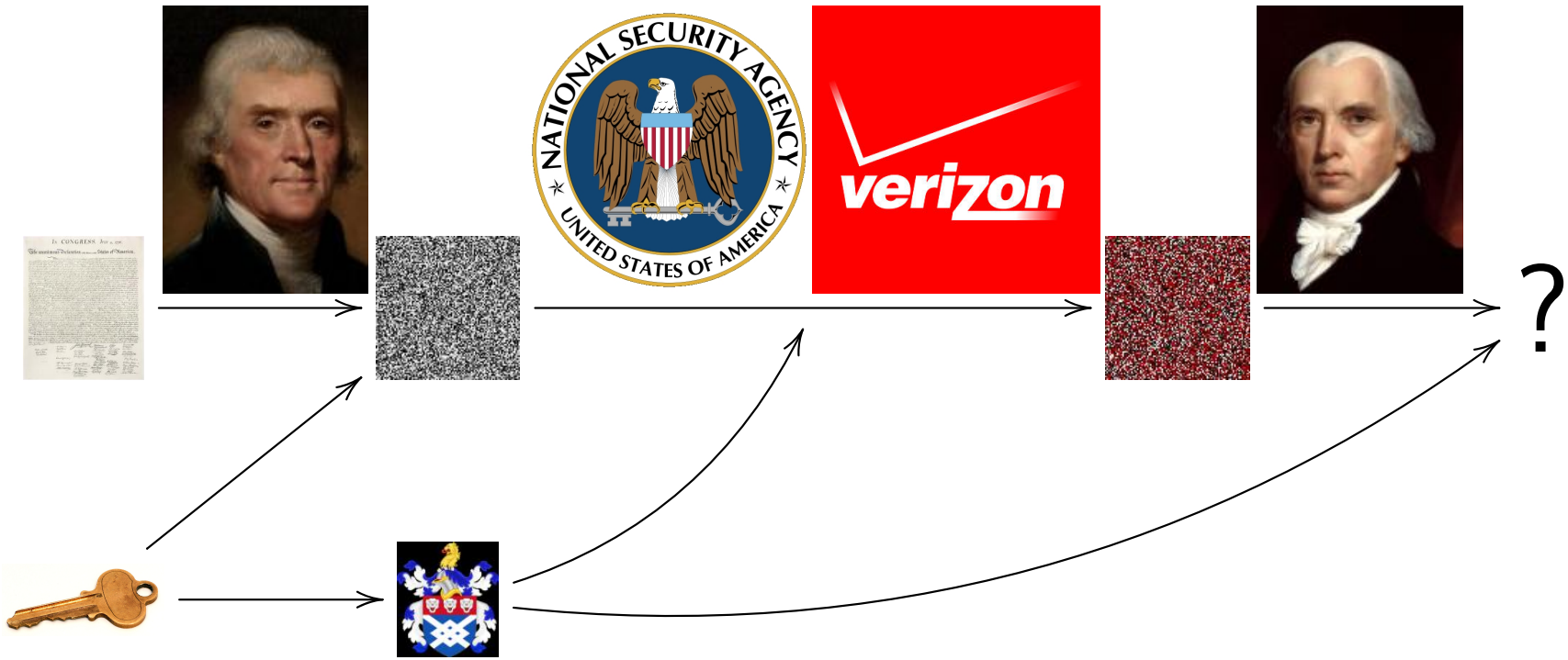
- Prerequisite: Alice and Bob share a secret key  .
- Prerequisite: Eve doesn't know  .
- Alice and Bob exchange any number of messages.
- Security goal #1: **Confidentiality** despite Eve's espionage.
- Security goal #2: **Integrity**, i.e., recognizing Eve's sabotage.

Public-key signatures



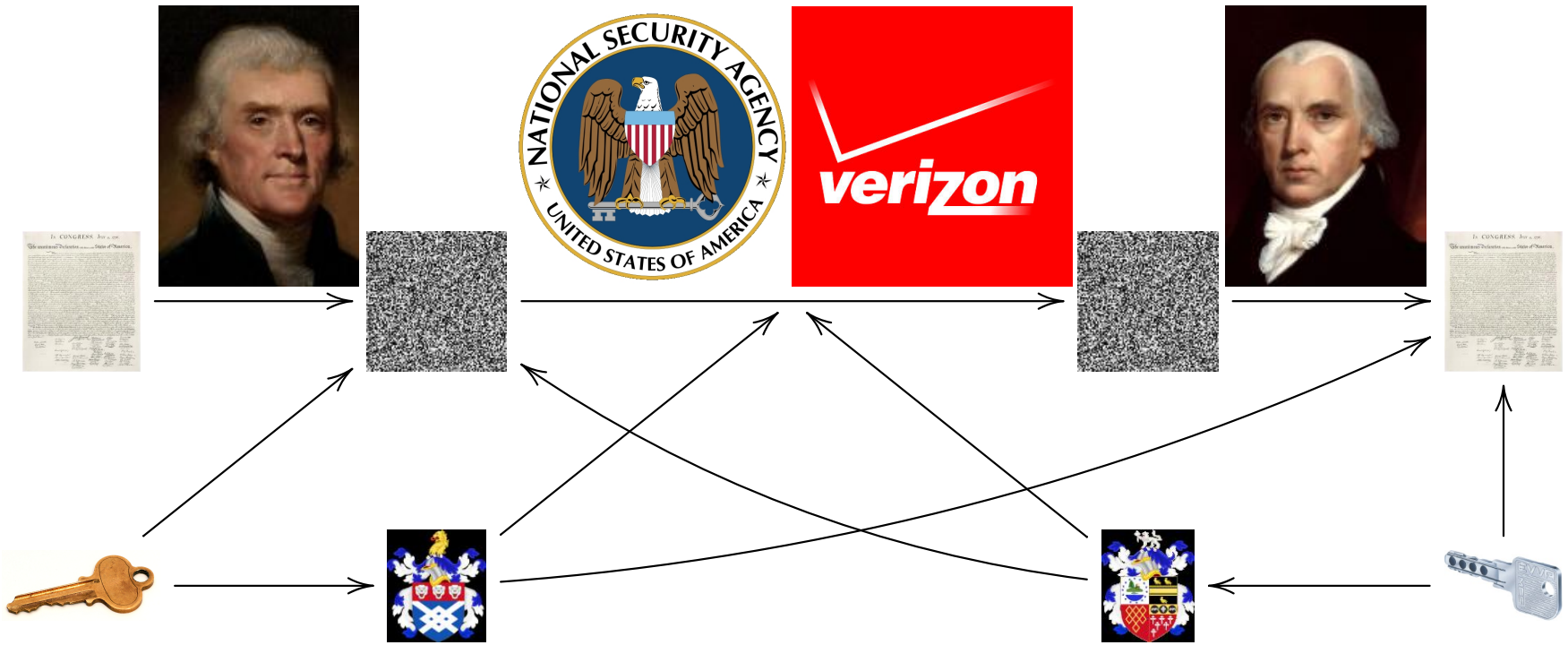
- Prerequisite: Alice has a secret key  and public key  .
- Prerequisite: Eve doesn't know  . Everyone knows  .
- Alice publishes any number of messages.
- Security goal: Integrity.

Public-key signatures



- Prerequisite: Alice has a secret key  and public key  .
- Prerequisite: Eve doesn't know  . Everyone knows  .
- Alice publishes any number of messages.
- Security goal: Integrity.

Public-key authenticated encryption ("DH" data flow)



- Prerequisite: Alice has a secret key  and public key  .
- Prerequisite: Bob has a secret key  and public key  .
- Alice and Bob exchange any number of messages.
- Security goal #1: Confidentiality.
- Security goal #2: Integrity.

Many more security goals studied in cryptography

- Protecting against denial of service.
- Stopping traffic analysis.
- Securely tallying votes.
- Searching encrypted data.
- Much more.

Attackers exploit physical reality

- 1996 Kocher: Typical crypto is broken by **side channels**.
- Response: Hundreds of papers on side-channel defenses.

Attackers exploit physical reality

- 1996 Kocher: Typical crypto is broken by **side channels**.
- Response: Hundreds of papers on side-channel defenses.
- Today's focus: Large universal **quantum computers**.
- Massive research effort. Tons of progress summarized in, e.g., https://en.wikipedia.org/wiki/Timeline_of_quantum_computing.
- Mark Ketchen, IBM Research, 2012, on quantum computing: "We're actually doing things that are making us think like, 'hey this isn't 50 years off, this is maybe just 10 years off, or 15 years off.' It's within reach."
- Fast-forward to 2022, or 2027. Universal quantum computers exist.
- Shor's algorithm solves in polynomial time:
  - Integer factorization. RSA is dead.
  - The discrete-logarithm problem in finite fields. DSA is dead.
  - The discrete-logarithm problem on elliptic curves. ECDHE is dead.
- This breaks all current public-key cryptography on the Internet!

Attackers exploit physical reality

- 1996 Kocher: Typical crypto is broken by **side channels**.
- Response: Hundreds of papers on side-channel defenses.
- Today's focus: Large universal **quantum computers**.
- Massive research effort. Tons of progress summarized in, e.g., https://en.wikipedia.org/wiki/Timeline_of_quantum_computing.
- Mark Ketchen, IBM Research, 2012, on quantum computing: "We're actually doing things that are making us think like, 'hey this isn't 50 years off, this is maybe just 10 years off, or 15 years off.' It's within reach."
- Fast-forward to 2022, or 2027. Universal quantum computers exist.
- Shor's algorithm solves in polynomial time:
  - Integer factorization. RSA is dead.
  - The discrete-logarithm problem in finite fields. DSA is dead.
  - The discrete-logarithm problem on elliptic curves. ECDHE is dead.
- This breaks all current public-key cryptography on the Internet!
- Also, Grover's algorithm speeds up brute-force searches.
- Example: Only 2^{64} quantum operations to break AES-128; 2^{128} quantum operations to break AES-256.

Physical cryptography: a return to the dark ages

- Imagine a lockable-briefcase salesman proposing a "locked-briefcase Internet" using "provably secure locked-briefcase cryptography":
  - Alice puts secret information into a lockable briefcase.
  - Alice locks the briefcase.
  - A courier transports the briefcase from Alice to Bob.
  - Bob unlocks the briefcase and retrieves the information.
  - There is a mathematical proof that the information is hidden!
  - Throw away algorithmic cryptography!

Physical cryptography: a return to the dark ages

- Imagine a lockable-briefcase salesman proposing a "locked-briefcase Internet" using "provably secure locked-briefcase cryptography":
  - Alice puts secret information into a lockable briefcase.
  - Alice locks the briefcase.
  - A courier transports the briefcase from Alice to Bob.
  - Bob unlocks the briefcase and retrieves the information.
  - There is a mathematical proof that the information is hidden!
  - Throw away algorithmic cryptography!
- Most common reactions from security experts:
  - This would make security much worse.

Physical cryptography: a return to the dark ages

- Imagine a lockable-briefcase salesman proposing a "locked-briefcase Internet" using "provably secure locked-briefcase cryptography":
  - Alice puts secret information into a lockable briefcase.
  - Alice locks the briefcase.
  - A courier transports the briefcase from Alice to Bob.
  - Bob unlocks the briefcase and retrieves the information.
  - There is a mathematical proof that the information is hidden!
  - Throw away algorithmic cryptography!
- Most common reactions from security experts:
  - This would make security much worse.
  - You can't do signatures.

Physical cryptography: a return to the dark ages

- Imagine a lockable-briefcase salesman proposing a "locked-briefcase Internet" using "provably secure locked-briefcase cryptography":
  - Alice puts secret information into a lockable briefcase.
  - Alice locks the briefcase.
  - A courier transports the briefcase from Alice to Bob.
  - Bob unlocks the briefcase and retrieves the information.
  - There is a mathematical proof that the information is hidden!
  - Throw away algorithmic cryptography!
- Most common reactions from security experts:
  - This would make security much worse.
  - You can't do signatures.
  - This would be insanely expensive.

Physical cryptography: a return to the dark ages

- Imagine a lockable-briefcase salesman proposing a "locked-briefcase Internet" using "provably secure locked-briefcase cryptography":
  - Alice puts secret information into a lockable briefcase.
  - Alice locks the briefcase.
  - A courier transports the briefcase from Alice to Bob.
  - Bob unlocks the briefcase and retrieves the information.
  - There is a mathematical proof that the information is hidden!
  - Throw away algorithmic cryptography!
- Most common reactions from security experts:
  - This would make security much worse.
  - You can't do signatures.
  - This would be insanely expensive.
  - We should not dignify this proposal with a response.

Security advantages of algorithmic cryptography

- Keep secrets heavily shielded inside authorized computers.
- Reduce trust in third parties:
  - Reduce reliance on closed-source software and hardware.
  - Increase comprehensiveness of audits.
  - Increase comprehensiveness of formal verification.
  - Design systems to be secure even if **algorithm and public keys are public**.
    Critical example: **signed** software updates.
- Understand security as thoroughly as possible:
  - Publish comprehensive specifications.
  - Build large research community with clear security goals.
  - Publicly document attack efforts.
  - Require systems to convincingly survive many years of analysis.

Confidence-inspiring crypto takes time to build

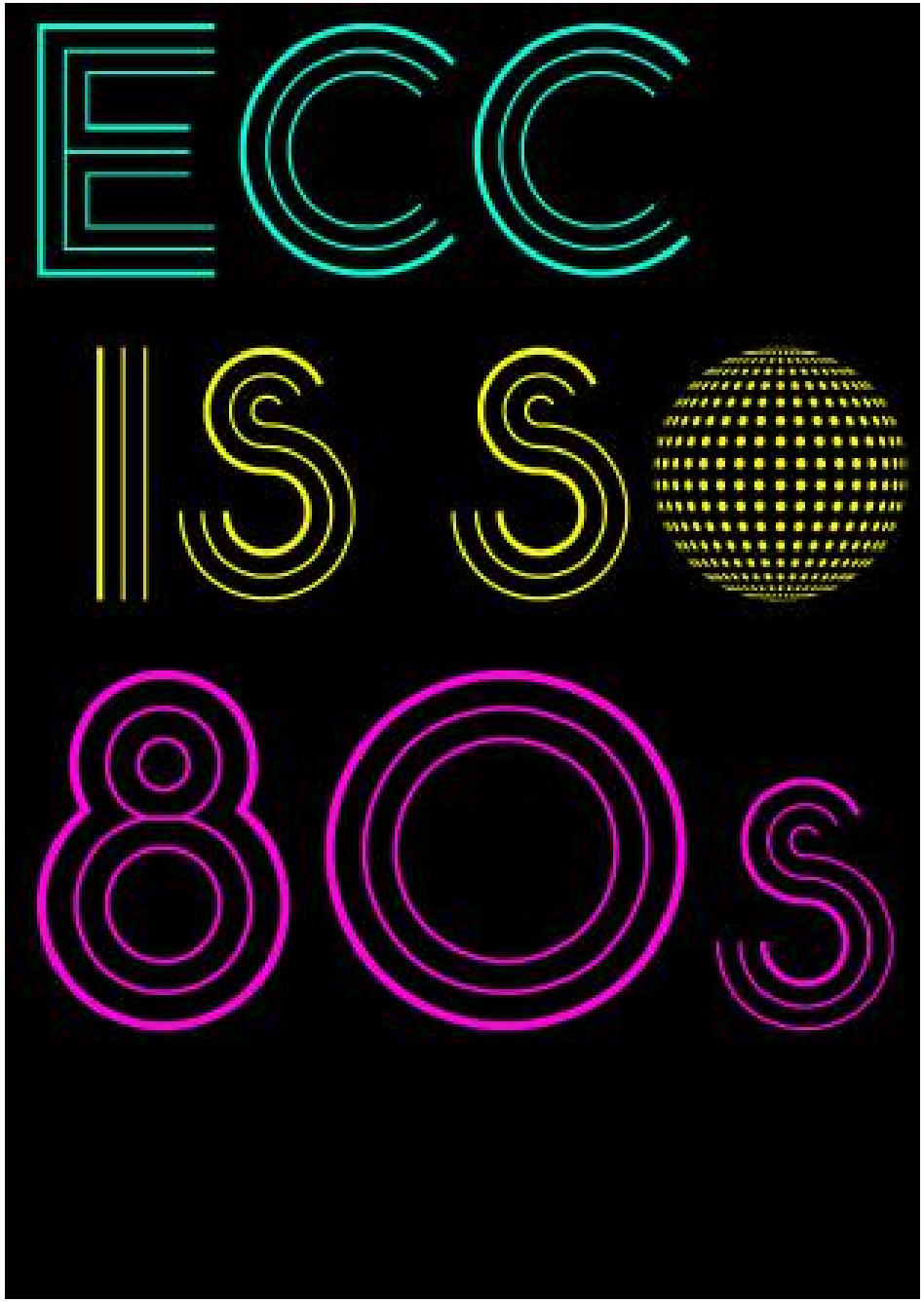
- Many stages of research from cryptographic design to deployment:
  - Explore space of cryptosystems.
  - Study algorithms for the attackers.
  - Focus on secure cryptosystems.

Confidence-inspiring crypto takes time to build

- Many stages of research from cryptographic design to deployment:
  - Explore space of cryptosystems.
  - Study algorithms for the attackers.
  - Focus on secure cryptosystems.
  - Study algorithms for the users.
  - Study implementations on real hardware.
  - Study side-channel attacks, fault attacks, etc.
  - Focus on secure, reliable implementations.
  - Focus on implementations meeting performance requirements.
  - Integrate securely into real-world applications.

Confidence-inspiring crypto takes time to build

- Many stages of research from cryptographic design to deployment:
  - Explore space of cryptosystems.
  - Study algorithms for the attackers.
  - Focus on secure cryptosystems.
  - Study algorithms for the users.
  - Study implementations on real hardware.
  - Study side-channel attacks, fault attacks, etc.
  - Focus on secure, reliable implementations.
  - Focus on implementations meeting performance requirements.
  - Integrate securely into real-world applications.
- Example: ECC introduced **1985**; big advantages over RSA. Robust ECC started to take over the Internet in **2015**.
- Can't wait for quantum computers before finding a solution!


ECC
IS
80s

History of post-quantum cryptography

- 2003 Daniel J. Bernstein introduces term Post- quantum cryptography.
- PQCrypto 2006: International Workshop on Post-Quantum Cryptography.

History of post-quantum cryptography

- 2003 Daniel J. Bernstein introduces term Post- quantum cryptography.
- PQCrypto 2006: International Workshop on Post-Quantum Cryptography.
- PQCrypto 2008, PQCrypto 2010, PQCrypto 2011, PQCrypto 2013.
- 2014 EU publishes H2020 call including post-quantum crypto as topic.
- ETSI working group on "Quantum-safe" crypto.
- PQCrypto 2014.
- April 2015 NIST hosts first workshop on post-quantum cryptography
- August 2015 NSA wakes up

NSA announcements

August 11, 2015

IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.

NSA announcements

August 11, 2015

> *IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.*

August 19, 2015

> *IAD will initiate a transition to quantum resistant algorithms in the not too distant future.*

NSA comes late to the party and botches its grand entrance.

NSA announcements

August 11, 2015

> *IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.*

August 19, 2015

> *IAD will initiate a transition to quantum resistant algorithms in the not too distant future.*

NSA comes late to the party and botches its grand entrance.

Worse, now we get people saying "Don't use post-quantum crypto, the NSA wants you to use it!".

NSA announcements

August 11, 2015

> *IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.*

August 19, 2015

> *IAD will initiate a transition to quantum resistant algorithms in the not too distant future.*

NSA comes late to the party and botches its grand entrance.

Worse, now we get people saying "Don't use post-quantum crypto, the NSA wants you to use it!". Or "NSA says NIST P-384 is post-quantum secure".

NSA announcements

August 11, 2015

> *IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.*

August 19, 2015

> *IAD will initiate a transition to quantum resistant algorithms in the not too distant future.*

NSA comes late to the party and botches its grand entrance.

Worse, now we get people saying "Don't use post-quantum crypto, the NSA wants you to use it!". Or "NSA says NIST P-384 is post-quantum secure". Or "NSA has abandoned ECC."

Post-quantum becoming mainstream

- PQCrypto 2016: 22–26 Feb in Fukuoka, Japan, $>$ 200 people

- NIST is calling for post-quantum proposals; submissions due Nov 2017.

Post-Quantum Cryptography for Long-term Security

- Project funded by EU in Horizon 2020, running 2015 – 2018.
- 11 partners from academia and industry, TU/e is coordinator

Work packages

PQCRYPTO is designing a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, adapting to the different performance challenges of mobile devices, the cloud, and the Internet.

Technical work packages

- WP1: Post-quantum cryptography for small devices
  Leader: Tim Güneysu, co-leader: Peter Schwabe
- WP2: Post-quantum cryptography for the Internet
  Leader: Daniel J. Bernstein, co-leader: Frederik Vercauteren
- WP3: Post-quantum cryptography for the cloud
  Leader: Nicolas Sendrier, co-leader: Christian Rechberger

Non-technical work packages

- WP4: Management and dissemination
  Leader: Tanja Lange
- WP5: Standardization
  Leader: Walter Fumy

Initial recommendations of long-term secure post-quantum systems

Daniel Augot, Lejla Batina, Daniel J. Bernstein, Joppe Bos, Johannes Buchmann, Wouter Castryck, Orr Dunkelman, Tim Güneysu, Shay Gueron, Andreas Hülsing, Tanja Lange, Mohamed Saied Emam Mohamed, Christian Rechberger, Peter Schwabe, Nicolas Sendrier, Frederik Vercauteren, Bo-Yin Yang

Initial recommendations

- **Symmetric encryption** Thoroughly analyzed, 256-bit keys:
  - AES-256
  - Salsa20 with a 256-bit key

  Evaluating: Serpent-256, ...
- **Symmetric authentication** Information-theoretic MACs:
  - GCM using a 96-bit nonce and a 128-bit authenticator
  - Poly1305
- **Public-key encryption** McEliece with binary Goppa codes:
  - length $n = 6960$, dimension $k = 5413$, $t = 119$ errors

  Evaluating: QC-MDPC, Stehlé-Steinfeld NTRU, ...
- **Public-key signatures** Hash-based (minimal assumptions):
  - XMSS with any of the parameters specified in CFRG draft
  - SPHINCS-256

  Evaluating: HFEv-, ...