LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

MNM TEAM

Quantum Secure Key Exchange for IEEE 802.1AE (MACSec)

Antrittsvortrag zur Masterarbeit

Robin Lösch

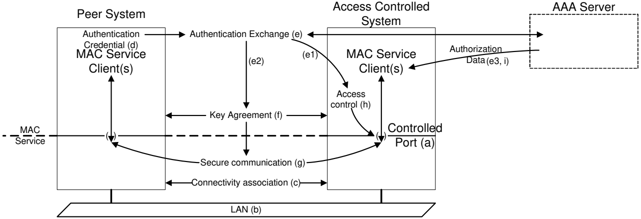
loesch@cip.ifi.lmu.de

Aufgabensteller:	Prof. Dr. Dieter Kranzlmüller
Betreuer:	Sophia Grundner-Culemann
	Dr. Tobias Guggemos

September 8, 2020

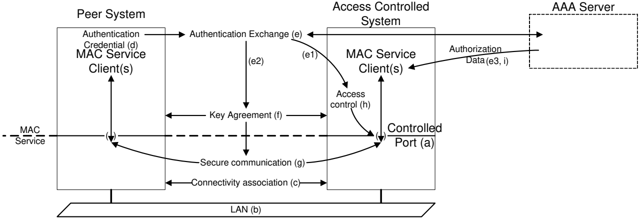
IEEE 802.1X

- Mutual authentication in LANs



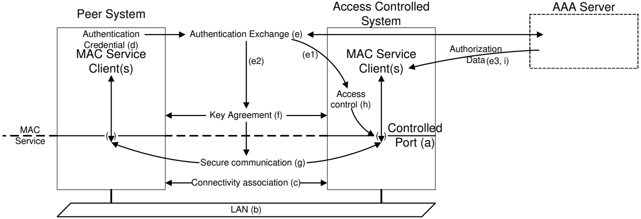
IEEE 802.1X

- Mutual authentication in LANs
  - Supplicant (Peer)



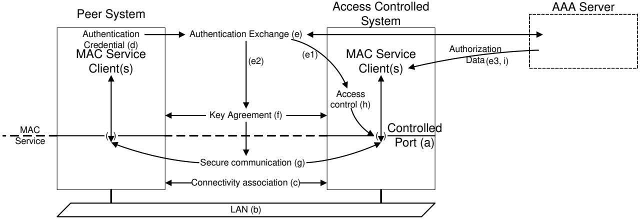
IEEE 802.1X

- Mutual authentication in LANs
  - Supplicant (Peer)
  - Authenticator (Switch)



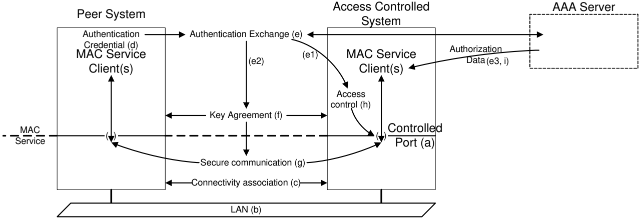
IEEE 802.1X

- Mutual authentication in LANs
  - Supplicant (Peer)
  - Authenticator (Switch)
  - Radius (AAA Server)



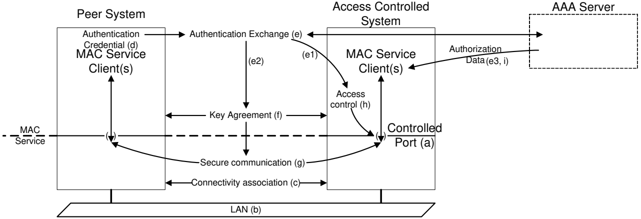
IEEE 802.1X

- Mutual authentication in LANs
  - Supplicant (Peer)
  - Authenticator (Switch)
  - Radius (AAA Server)
- Mutually trusted CAs (c)



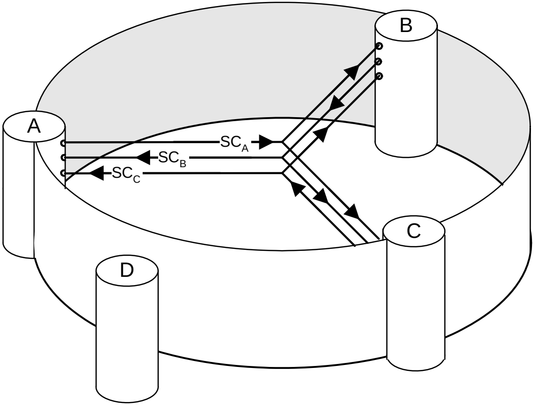
IEEE 802.1X

- Mutual authentication in LANs
  - Supplicant (Peer)
  - Authenticator (Switch)
  - Radius (AAA Server)
- Mutually trusted CAs (c)
- EAP framework (e,f)
  - Asymmetric key exchange



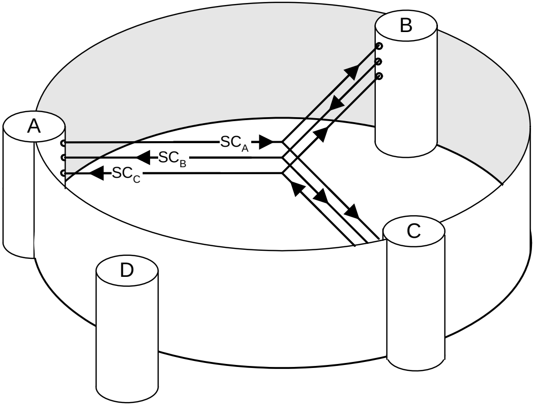
IEEE 802.1AE (MACSec)

- Ethernet frame encryption



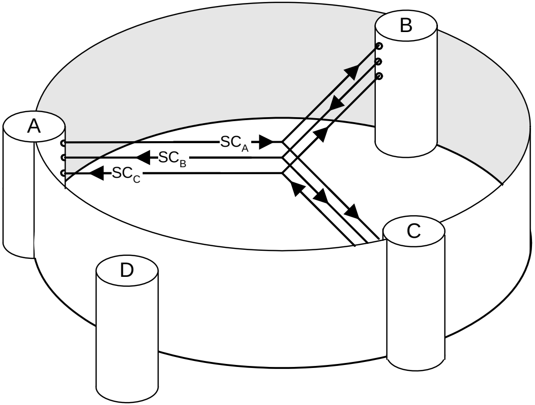
IEEE 802.1AE (MACSec)

- Ethernet frame encryption
  - Uses 802.1X CAs for authentication



IEEE 802.1AE (MACSec)

- Ethernet frame encryption
  - Uses 802.1X CAs for authentication
  - Uses MKA for symmetric key exchange



Motivation

- Quantum Computing is a “Hype Topic”

Motivation

- Quantum Computing is a “Hype Topic”
- Faster algorithms:
  - Search problems
  - Optimizations (Adiabatic QC)

Motivation

- Quantum Computing is a “Hype Topic”
- Faster algorithms:
  - Search problems
  - Optimizations (Adiabatic QC)
- New algorithms:
  - Quantum teleportation

Motivation

- Efficient solution for (some) computational problems

Motivation

- Efficient solution for (some) computational problems
- Modern crypto is based in such problems:

Motivation

- Efficient solution for (some) computational problems
- Modern crypto is based in such problems:
  - Grover's search algorithm

Motivation

- Efficient solution for (some) computational problems
- Modern crypto is based in such problems:
  - Grover's search algorithm
    Reduce symmetric crypto keyspace by $\mathcal{O}(\sqrt{n})$

Motivation

- Efficient solution for (some) computational problems
- Modern crypto is based in such problems:
  - Grover's search algorithm
    Reduce symmetric crypto keyspace by $\mathcal{O}(\sqrt{n})$
  - Shor's factorization algorithm

Motivation

- Efficient solution for (some) computational problems
- Modern crypto is based in such problems:
  - Grover's search algorithm
    Reduce symmetric crypto keyspace by $\mathcal{O}(\sqrt{n})$
  - Shor's factorization algorithm
    Breaks (EC)DH and RSA based crypto in polynomial time

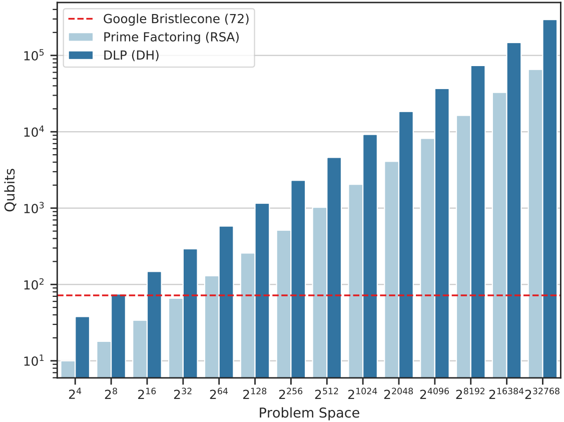
Practical Quantum Computer

When to panic?

Practical Quantum Computer

When to panic?

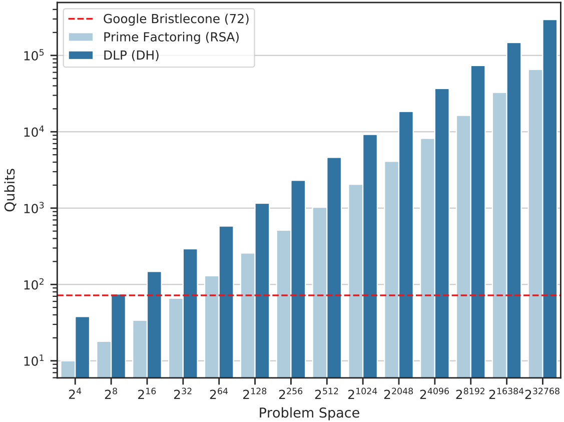
- #Qubits to break a n-bit key
    - RSA: $2n + 2$ [1]
    - DLP: $9n + 2\ln(n)$ [2]



Practical Quantum Computer

When to panic?

- #Qubits to break a n-bit key
  - RSA: $2n + 2$ [1]
  - DLP: $9n + 2\ln(n)$ [2]
- Coherency time
  - Keeping a state is tricky
  - Implementation dependent
  - Hard to predict



Practical Quantum Computer

- Even if we assume a Moore-like exp growth we still got plenty of time

Practical Quantum Computer

- Even if we assume a Moore-like exp growth we still got plenty of time
- We should use this time!

Practical Quantum Computer

- Even if we assume a Moore-like exp growth we still got plenty of time
- We should use this time!
    1. Design quantum safe algorithms

Practical Quantum Computer

- Even if we assume a Moore-like exp growth we still got plenty of time
- We should use this time!
  1. Design quantum safe algorithms
  2. **Implement quantum safe algorithms**

NIST PQ Project

- Start Dec 20, 2016
- 3. Round announced Jul 22, 2020

NIST PQ Project

- Start Dec 20, 2016
- 3. Round announced Jul 22, 2020
- Goal: Select quantum safe key exchange and signature algorithms

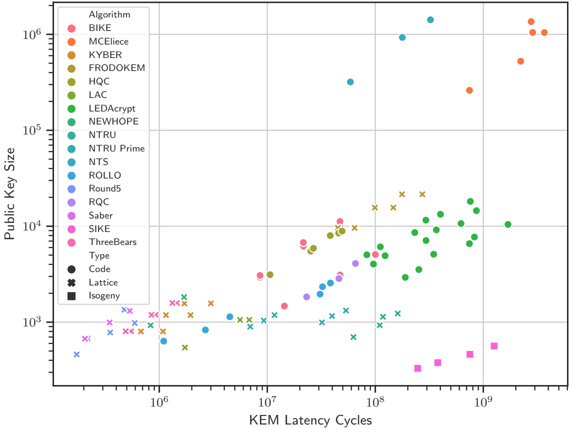
A clear winner?

A clear winner?

- Different Foundations
    - Lattice-based
    - Isogeny-based
    - Code-based

A clear winner?

- Different Foundations
  - Lattice-based
  - Isogeny-based
  - Code-based
- Different Trade-offs
  - Latency
  - Key size
  - Maturity



Requirements on Public Key Crypto

- Web-Server
  - Thousands of handshakes/s
  - Forward secrecy

Requirements on Public Key Crypto

- Web-Server
  - Thousands of handshakes/s
  - Forward secrecy
- IoT & WSN
  - Small traffic volume

Requirements on Public Key Crypto

- Web-Server
  - Thousands of handshakes/s
  - Forward secrecy
- IoT & WSN
  - Small traffic volume
- Long-term signatures
  - Maturity

Existing Applications

- Internet-Drafts for TLS 1.X[3][4][5][6][7]
- QuaSiModO: Quantum resistant IKEv2[8]
- “New Hope” in Google Chrome[9]

Why 802.1(X|AE)?

- Widely used in practice

Why 802.1(X|AE)?

- Widely used in practice
  - Enterprise LANs
  - WPA2-Enterprise

Why 802.1(X|AE)?

- Widely used in practice
    - Enterprise LANs
    - WPA2-Enterprise
- Heterogeneous environments

Why 802.1(X|AE)?

- Widely used in practice
  - Enterprise LANs
  - WPA2-Enterprise
- Heterogeneous environments
  - Data centers ⇔ IoT networks
  - Helps understanding algorithms

Why 802.1(X|AE)?

- Widely used in practice
  - Enterprise LANs
  - WPA2-Enterprise
- Heterogeneous environments
  - Data centers ⇔ IoT networks
  - Helps understanding algorithms
- Industry relevance

Why 802.1(X|AE)?

- Widely used in practice
    - Enterprise LANs
    - WPA2-Enterprise
- Heterogeneous environments
    - Data centers ⇔ IoT networks
    - Helps understanding algorithms
- Industry relevance
    - Part of QuaSiModO/ADVA cooperation

Outline

Goals

Outline

Goals

- Evaluation of IEEE 802.1(X|AE)

Goals

- Evaluation of IEEE 802.1(X|AE)
  - Identify vulnerable components
  - Extract requirements for quantum safe design

Goals

- Evaluation of IEEE 802.1(X|AE)
  - Identify vulnerable components
  - Extract requirements for quantum safe design
- Evaluation of quantum safe algorithms

Goals

- Evaluation of IEEE 802.1(X|AE)
  - Identify vulnerable components
  - Extract requirements for quantum safe design
- Evaluation of quantum safe algorithms
- Design of a quantum safe alternative

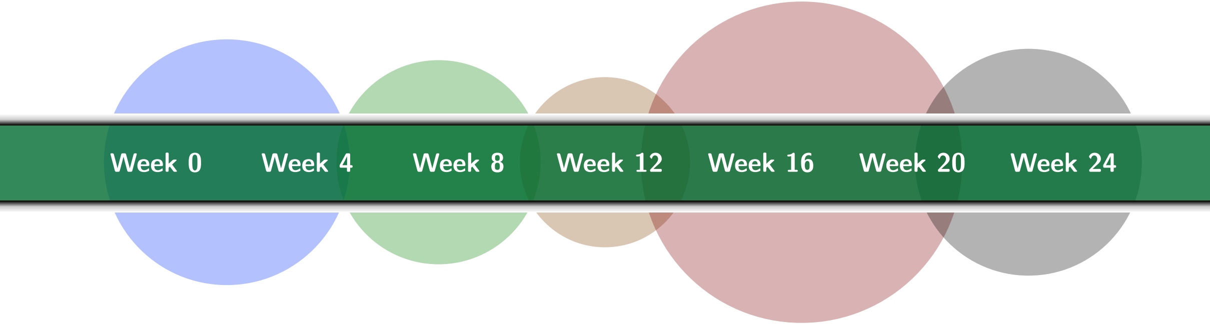
Goals

- Evaluation of IEEE 802.1(X|AE)
  - Identify vulnerable components
  - Extract requirements for quantum safe design
- Evaluation of quantum safe algorithms
- Design of a quantum safe alternative
- Implementation in a real-world test-case

Goals

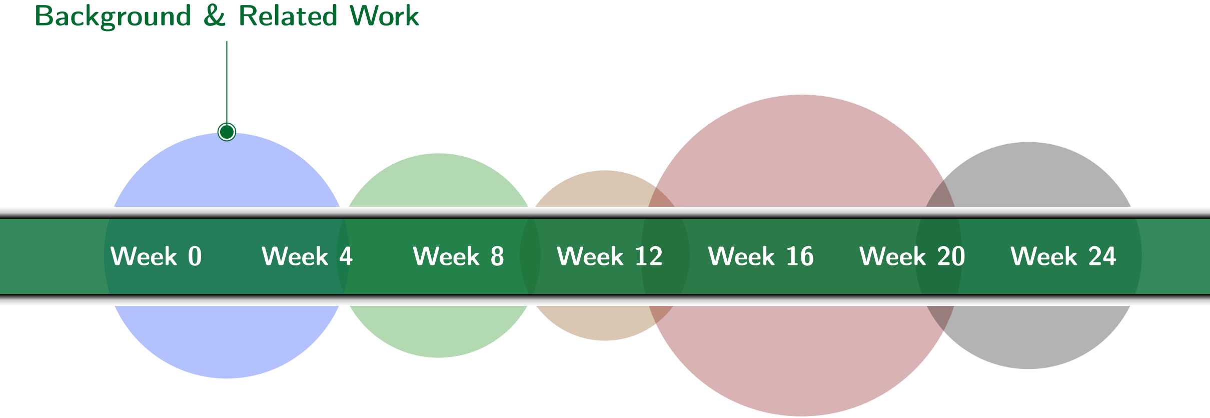
- Evaluation of IEEE 802.1(X|AE)
  - Identify vulnerable components
  - Extract requirements for quantum safe design
- Evaluation of quantum safe algorithms
- Design of a quantum safe alternative
- Implementation in a real-world test-case
- Extensive experimental evaluation

Outline

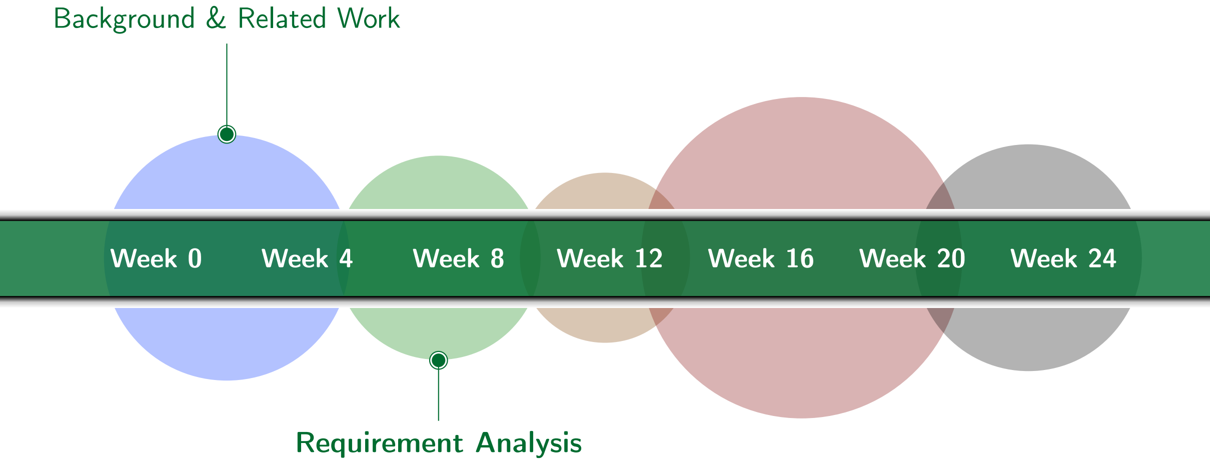


Week 0 Week 4 Week 8 Week 12 Week 16 Week 20 Week 24

Outline


Background & Related Work
Week 0
Week 4
Week 8
Week 12
Week 16
Week 20
Week 24

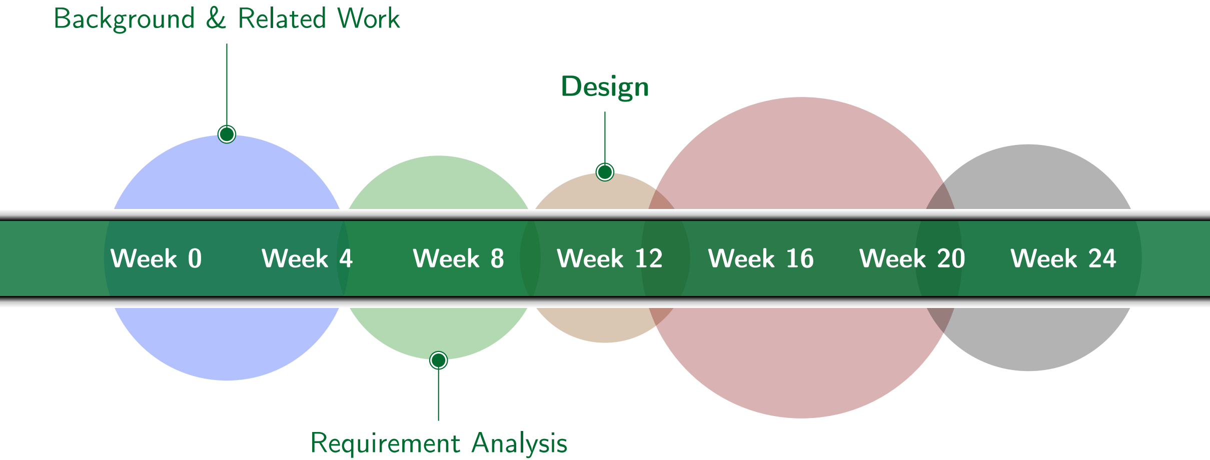
Outline



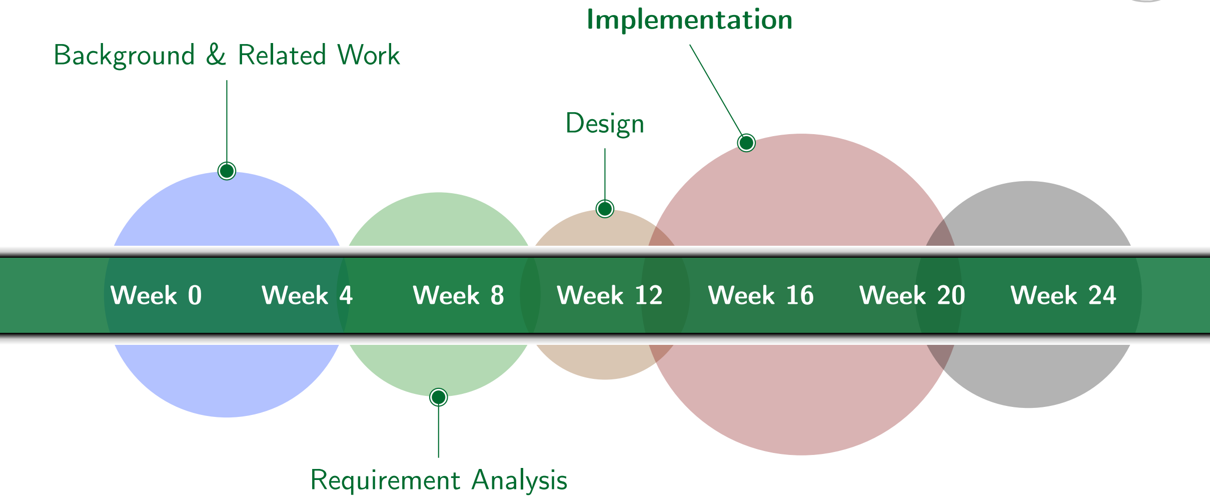
Background & Related Work

Requirement Analysis

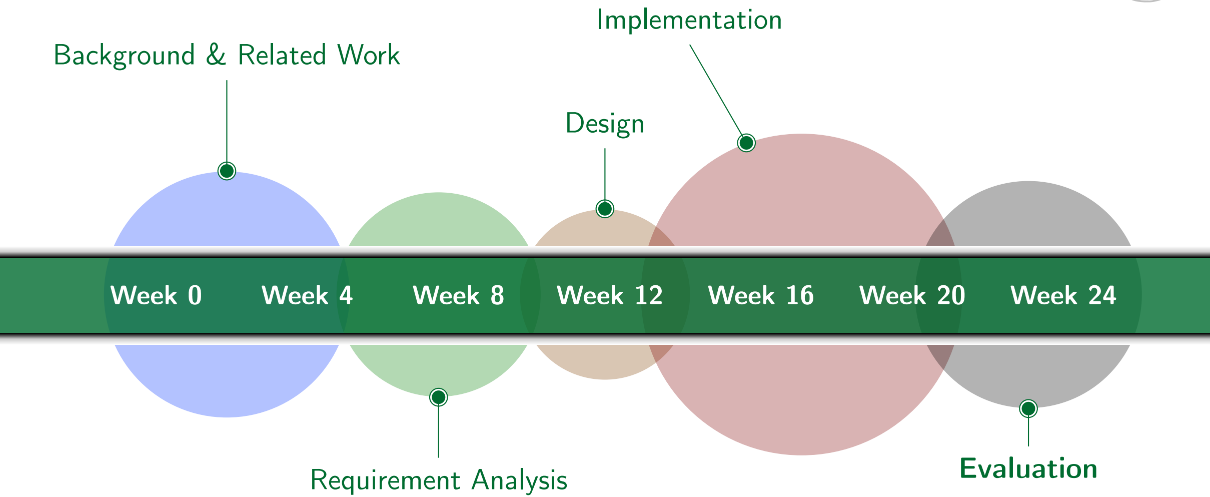
Outline


Background & Related Work
Design
Week 0
Week 4
Week 8
Week 12
Week 16
Week 20
Week 24
Requirement Analysis

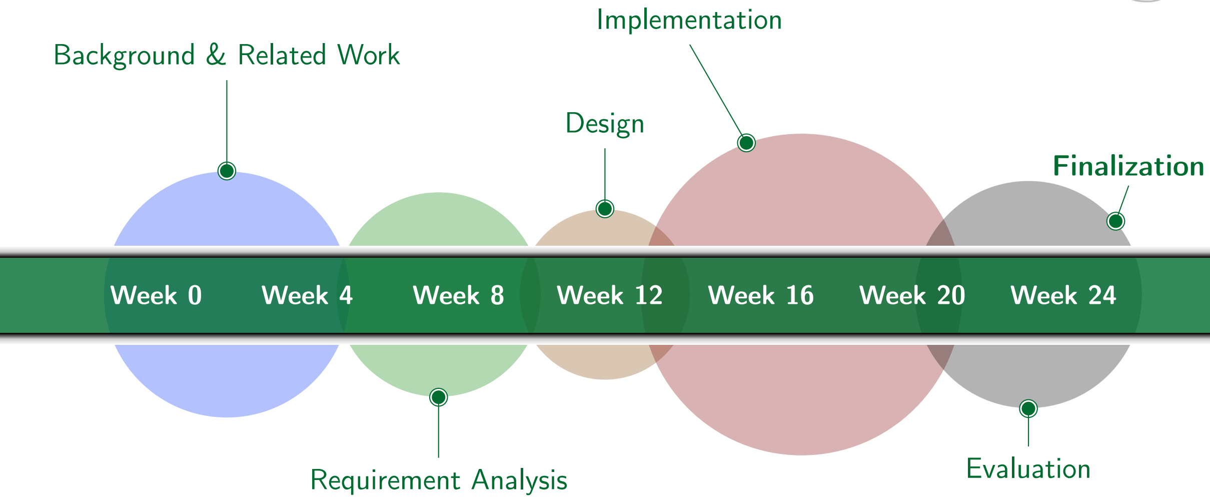
Outline


Implementation
Background & Related Work
Design
Week 0
Week 4
Week 8
Week 12
Week 16
Week 20
Week 24
Requirement Analysis

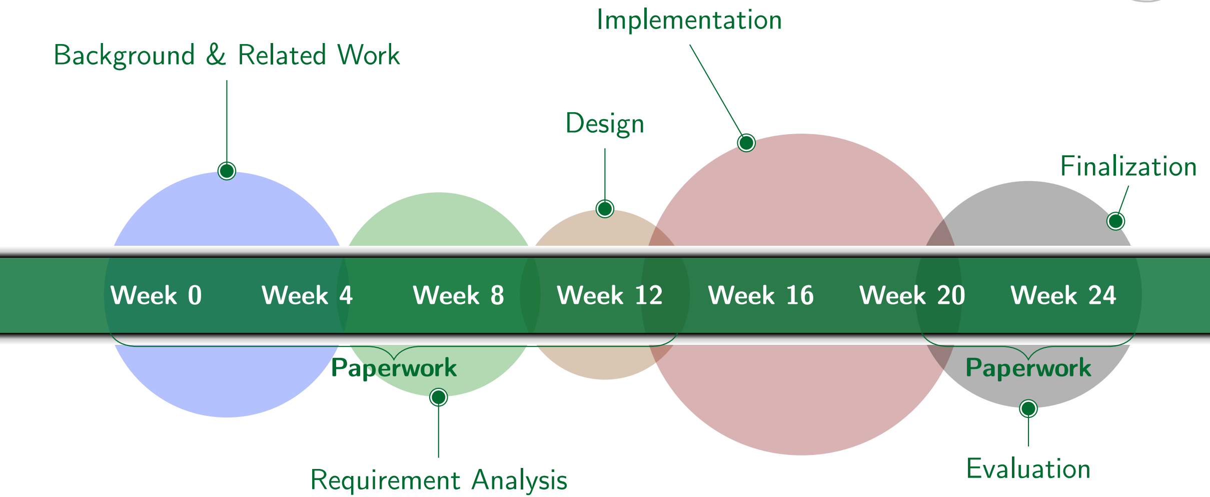
Outline


Implementation
Background & Related Work
Design
Week 0
Week 4
Week 8
Week 12
Week 16
Week 20
Week 24
Requirement Analysis
Evaluation

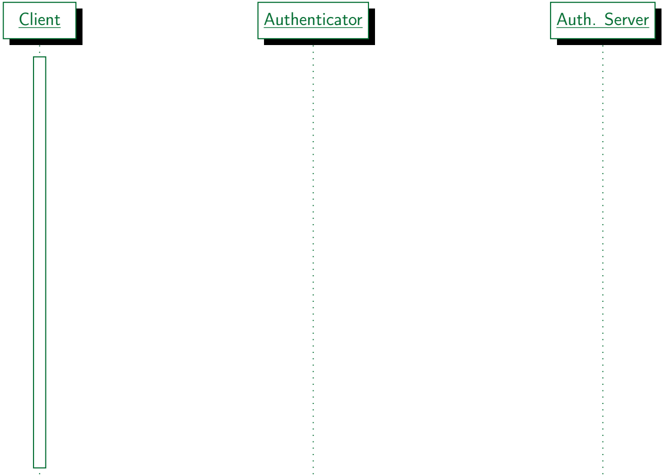
Outline


Background & Related Work
Implementation
Design
Finalization
Week 0
Week 4
Week 8
Week 12
Week 16
Week 20
Week 24
Requirement Analysis
Evaluation

Outline


Implementation
Background & Related Work
Design
Finalization
Week 0
Week 4
Week 8
Week 12
Week 16
Week 20
Week 24
Paperwork
Paperwork
Requirement Analysis
Evaluation

Outline

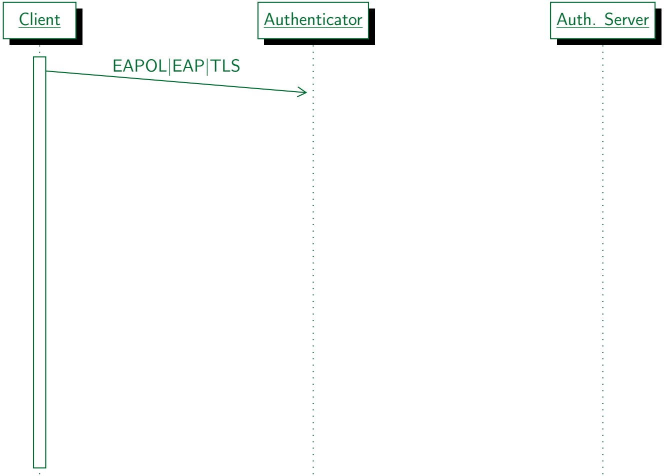


Client

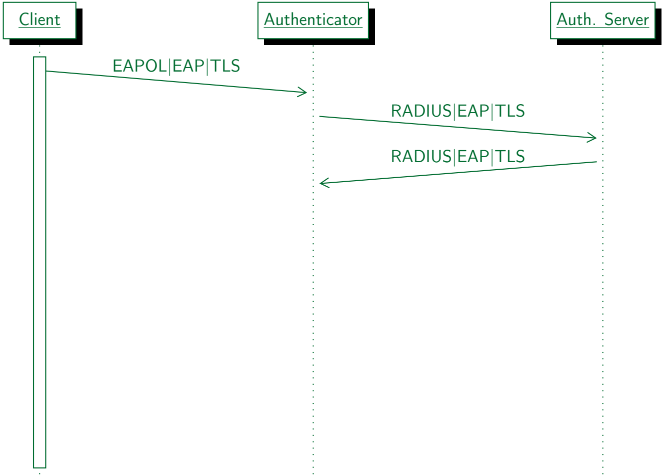
Authenticator

Auth. Server

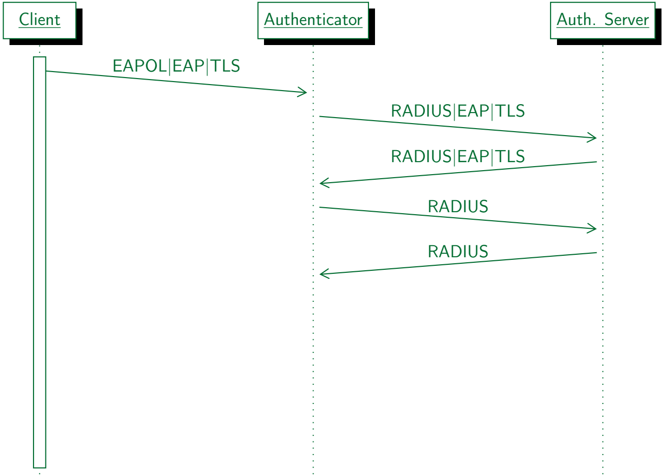
Outline



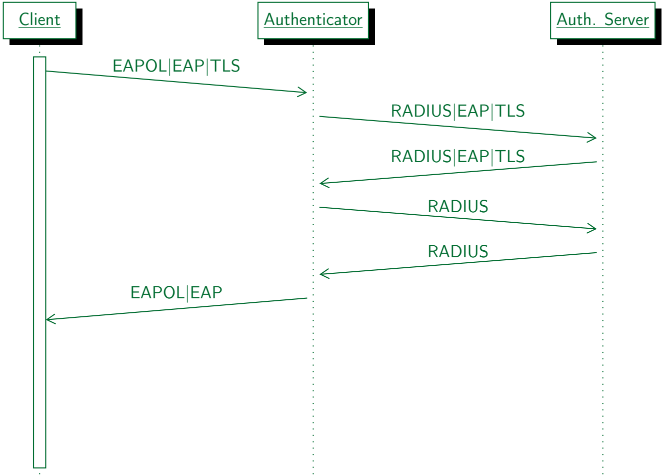
Outline


Client
Authenticator
Auth. Server
EAPOL|EAP|TLS
RADIUS|EAP|TLS
RADIUS|EAP|TLS

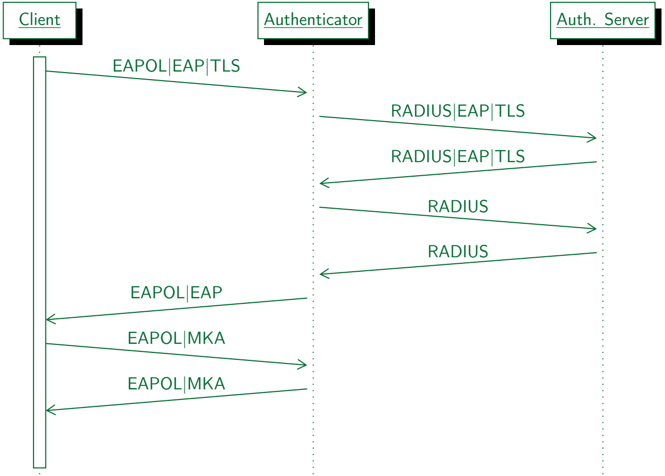
Outline


Client
Authenticator
Auth. Server
EAPOL|EAP|TLS
RADIUS|EAP|TLS
RADIUS|EAP|TLS
RADIUS
RADIUS

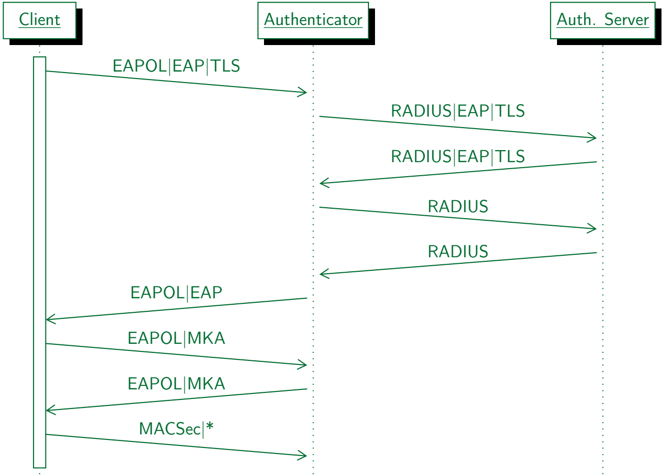
Outline


Client
Authenticator
Auth. Server
EAPOL|EAP|TLS
RADIUS|EAP|TLS
RADIUS|EAP|TLS
RADIUS
RADIUS
EAPOL|EAP

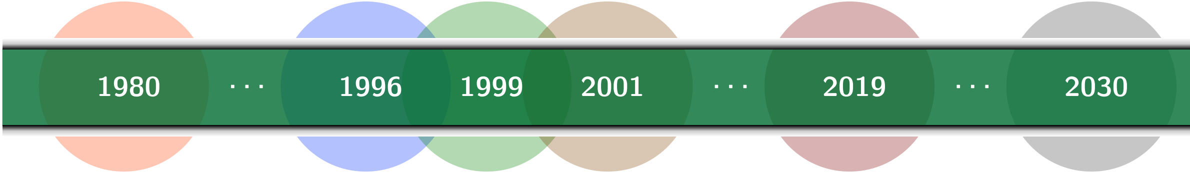
Outline


Client
Authenticator
Auth. Server
EAPOL|EAP|TLS
RADIUS|EAP|TLS
RADIUS|EAP|TLS
RADIUS
RADIUS
EAPOL|EAP
EAPOL|MKA
EAPOL|MKA

Outline


Client
Authenticator
Auth. Server
EAPOL|EAP|TLS
RADIUS|EAP|TLS
RADIUS|EAP|TLS
RADIUS
RADIUS
EAPOL|EAP
EAPOL|MKA
EAPOL|MKA
MACSec|*

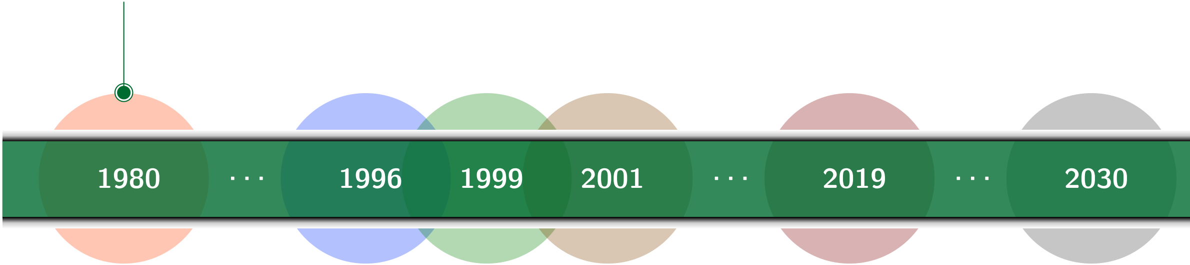
A short history of quantum computing



1980 · · · 1996 1999 2001 · · · 2019 · · · 2030

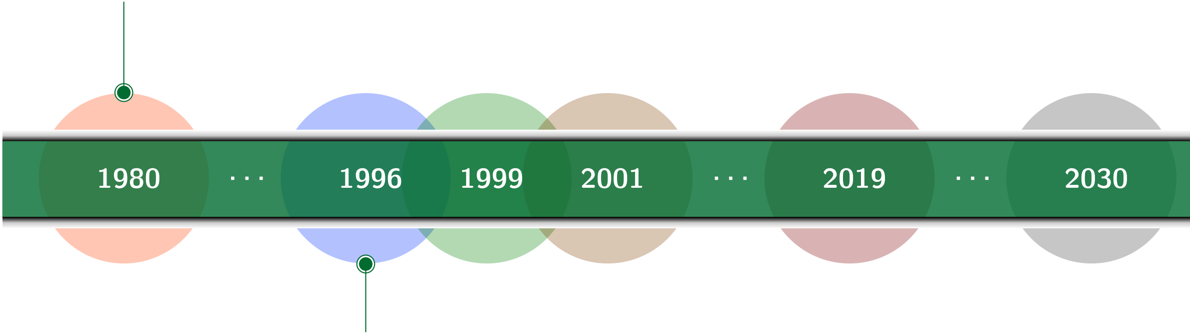
A short history of quantum computing

Benioff's Quantum TM[10]



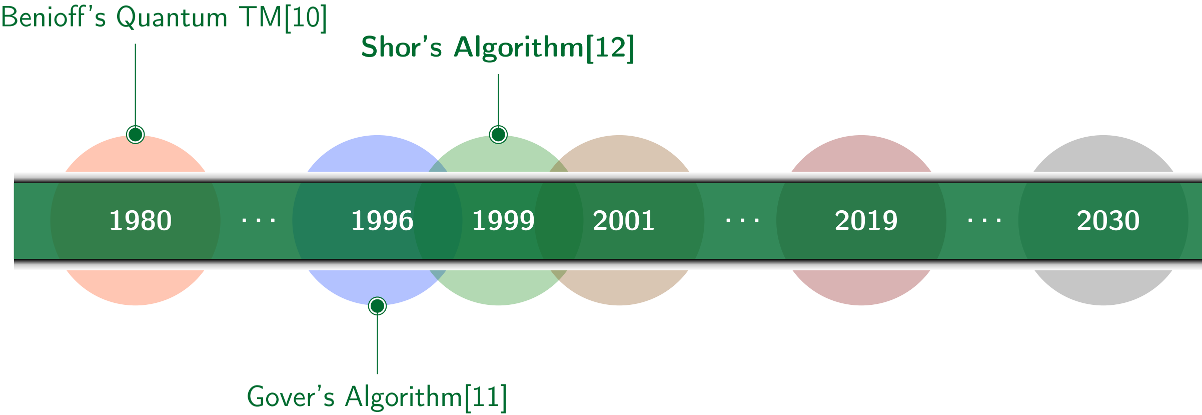
A short history of quantum computing

Benioff's Quantum TM[10]

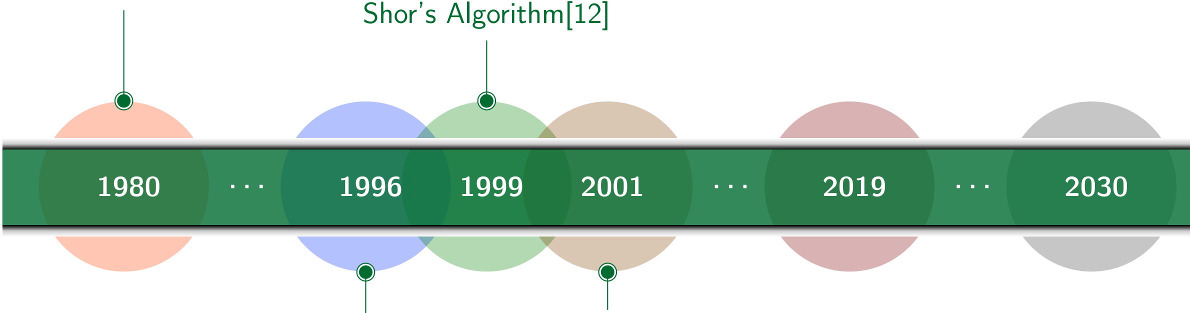


Gover's Algorithm[11]

A short history of quantum computing



A short history of quantum computing



Benioff's Quantum TM[10]

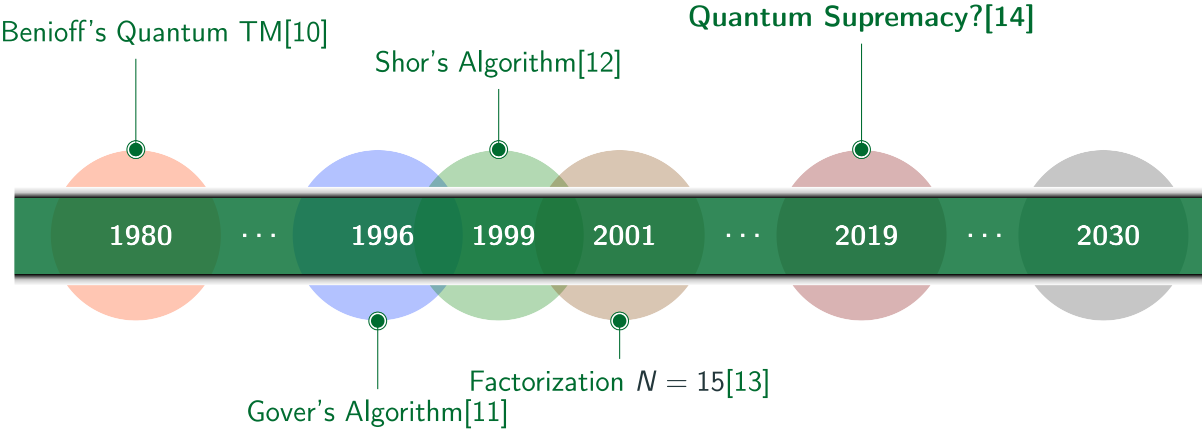
Shor's Algorithm[12]

1980 · · · 1996 1999 2001 · · · 2019 · · · 2030

Factorization $N = 15$**[13]**

Gover's Algorithm[11]

A short history of quantum computing



Benioff's Quantum TM[10]

Shor's Algorithm[12]

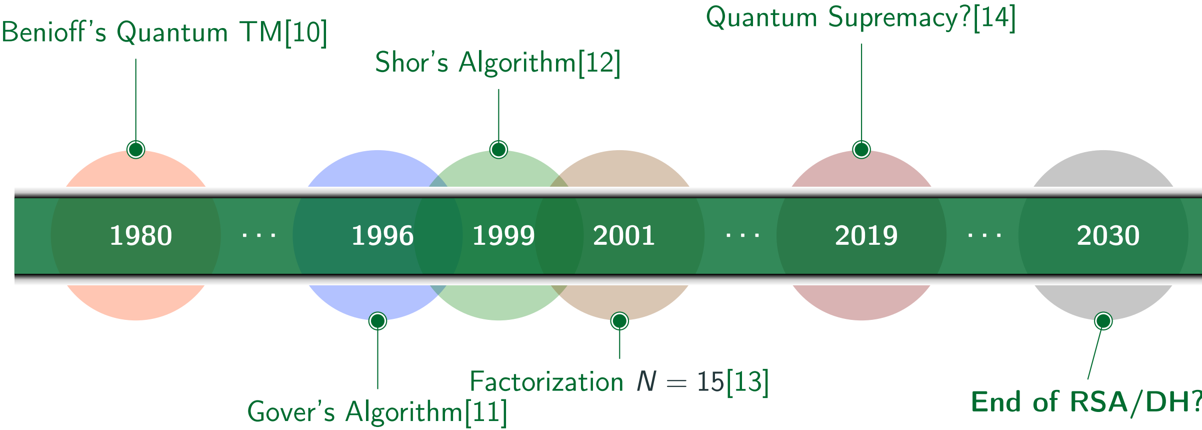
Quantum Supremacy?[14]

1980 · · · 1996 1999 2001 · · · 2019 · · · 2030

Gover's Algorithm[11]

Factorization $N = 15$[13]

A short history of quantum computing



1980 Benioff's Quantum TM[10]

· · ·

1996 Gover's Algorithm[11]

1999 Shor's Algorithm[12]

2001 Factorization $N = 15$[13]

· · ·

2019 Quantum Supremacy?[14]

· · ·

2030 **End of RSA/DH?**

References I

[1] T. Häner, M. Roetteler, and K. M. Svore, "Factoring using 2n+ 2 qubits with toffoli based modular multiplication," *arXiv preprint arXiv:1611.07995*, 2016.

[2] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, "Quantum resource estimates for computing elliptic curve discrete logarithms," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2017, pp. 241–270.

[3] D. Steblia, S. Fluhrer, and S. Gueron, "Hybrid key exchange in TLS 1.3," Internet Engineering Task Force, Internet-Draft draft-ietf-tls-hybrid-design-00, Apr. 2020, Work in Progress, 34 pp. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design-00.

References II

[4] W. Whyte, Z. Zhang, S. Fluhrer, and O. Garcia-Morchon, "Quantum-Safe Hybrid (QSH) Key Exchange for Transport Layer Security (TLS) version 1.3," Internet Engineering Task Force, Internet-Draft draft-whyte-qsh-tls13-06, Oct. 2017, Work in Progress, 19 pp. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-whyte-qsh-tls13-06.

[5] J. M. Schanck and D. Stebila, "A Transport Layer Security (TLS) Extension For Establishing An Additional Shared Secret," Internet Engineering Task Force, Internet-Draft draft-schanck-tls-additional-keyshare-00, Apr. 2017, Work in Progress, 10 pp. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-schanck-tls-additional-keyshare-00.

References III

[6] F. Kiefer and K. Kwiatkowski, “Hybrid ECDHE-SIDH Key Exchange for TLS,” Internet Engineering Task Force, Internet-Draft draft-kiefer-tls-ecdhe-sidh-00, Nov. 2018, Work in Progress, 13 pp. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-kiefer-tls-ecdhe-sidh-00.

[7] J. M. Schanck, W. Whyte, and Z. Zhang, “Quantum-Safe Hybrid (QSH) Ciphersuite for Transport Layer Security (TLS) version 1.2,” Internet Engineering Task Force, Internet-Draft draft-whyte-qsh-tls12-02, Jul. 2016, Work in Progress, 19 pp. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-whyte-qsh-tls12-02.

References IV

[8] Q.-R. K. Exchange, "Towards a verifiably secure quantum-resistant key exchange in ikev2,",

[9] M. Braithwaite, *Experimenting with post-quantum cryptography*, https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html, Accessed: 2020-05-13.

[10] P. Benioff, "The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines," *Journal of statistical physics*, vol. 22, no. 5, pp. 563–591, 1980.

References V

[11] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.

[12] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[13] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, R. Cleve, and I. L. Chuang, “Experimental realization of an order-finding algorithm with an nmr quantum computer,” *Physical Review Letters*, vol. 85, no. 25, p. 5452, 2000.

References VI

[14] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[15] D. Stebila and M. Mosca, "Post-quantum key exchange for the internet and the open quantum safe project," in *International Conference on Selected Areas in Cryptography*, Springer, 2016, pp. 14–37.

[16] D. J. Bernstein and T. L. (editors), *Ebacs: Ecrypt benchmarking of cryptographic systems*, https://bench.cr.yp.to, Accessed: 2020-06-25.