Internet Key Exchange v2

Secure Key Agreement in a Quantum World

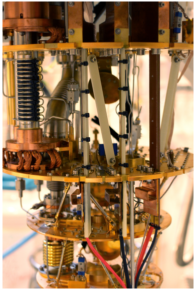
Stefan-Lukas Gazdag
<Stefan-Lukas_Gazdag@genua.eu>

Tobias Heider
<Tobias_Heider@genua.eu>

Berlin, Crypto Meetup, 3rd of September 2019

Living in a quantum era

- **Quantum Computing**
  - Quantum Computers
  - Quantum Supremacy
  - Quantum Advantage
- **Quantum Cryptography**
  - Quantum Key Distribution (QKD)
- **Post-Quantum Cryptography (PQC)**
  - aka Quantum-Safe Cryptography (QSC)
  - aka Quantum-Resistant Cryptography (QRC)



by UCL Mathematical

and Physical Sciences

CC BY 2.0

Post-Quantum Cryptography

Use Cases (not exhaustive)

- Digital signatures
  - Software updates / code signing
  - E-mail signatures
  - Qualified electronic signatures (eIDAS)
- Secure communication
  - Websites (online banking, ...)
  - Remote work
- Securing data
  - Passports / IDs
  - Health data
  - Payment data
- ...

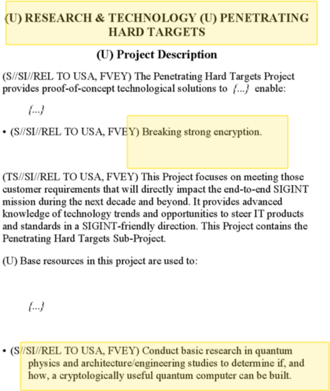
Use Cases (not exhaustive)

- Digital signatures
  - Software updates / code signing
  - E-mail signatures
  - Qualified electronic signatures (eIDAS)
- Secure communication
  - Websites (online banking, ...)
  - Remote work

- Securing data
  - Passports / IDs
  - Health data
  - Payment data
- ...

Consider different attack scenarios:
e.g. an intelligence agency could record and store encrypted data today and break it once they are able to do so.

NSA loves Quantum Computing



(U) RESEARCH & TECHNOLOGY (U) PENETRATING HARD TARGETS

(U) Project Description

(S//SI//REL TO USA, FVEY) The Penetrating Hard Targets Project provides proof-of-concept technological solutions to *{...}* enable:

{...}

- (S//SI//REL TO USA, FVEY) Breaking strong encryption.

(TS//SI//REL TO USA, FVEY) This Project focuses on meeting those customer requirements that will directly impact the end-to-end SIGINT mission during the next decade and beyond. It provides advanced knowledge of technology trends and opportunities to steer IT products and standards in a SIGINT-friendly direction. This Project contains the Penetrating Hard Targets Sub-Project.

(U) Base resources in this project are used to:

{...}

- (S//SI//REL TO USA, FVEY) Conduct basic research in quantum physics and architecture/engineering studies to determine if, and how, a cryptologically useful quantum computer can be built.

Excerpt from the documents revealed by Edward Snowden and published by the Washington Post on 2nd of January 2014

NSA loves Post-Quantum Crypto

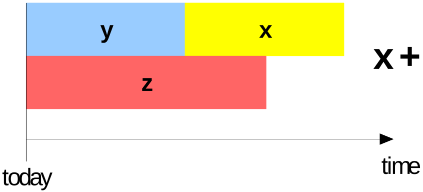
NSA Information Assurance Directorate MFQ U/OO/815099-15

- Published early 2016
- Suite B to be updated (crypto suite for U.S. agencies and algorithm recommendation for U.S. companies)
- NSA recommends to use more secure classical parameter sets
- Suite B to recommend post-quantum crypto in the near future

Tempus fugit

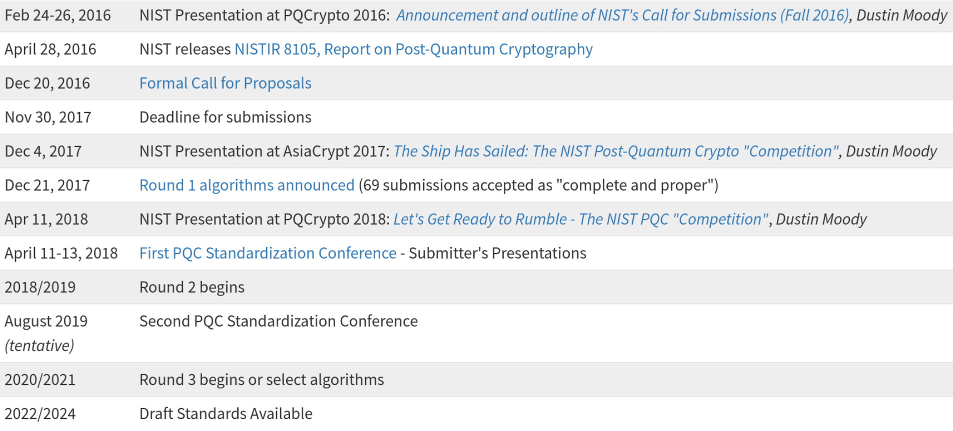
How soon do we need to worry?
(Michele Mosca, University of Waterloo)

- How long do you need encryption to be secure? (x years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (y years)
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance)? (z years)



x + y > z ?

NIST Process - Timeline



Feb 24-26, 2016	NIST Presentation at PQCrypto 2016: *Announcement and outline of NIST's Call for Submissions (Fall 2016)*, *Dustin Moody*
April 28, 2016	NIST releases NISTIR 8105, Report on Post-Quantum Cryptography
Dec 20, 2016	Formal Call for Proposals
Nov 30, 2017	Deadline for submissions
Dec 4, 2017	NIST Presentation at AsiaCrypt 2017: *The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition"*, *Dustin Moody*
Dec 21, 2017	Round 1 algorithms announced (69 submissions accepted as "complete and proper")
Apr 11, 2018	NIST Presentation at PQCrypto 2018: *Let's Get Ready to Rumble - The NIST PQC "Competition"*, *Dustin Moody*
April 11-13, 2018	First PQC Standardization Conference - Submitter's Presentations
2018/2019	Round 2 begins
August 2019 *(tentative)*	Second PQC Standardization Conference
2020/2021	Round 3 begins or select algorithms
2022/2024	Draft Standards Available

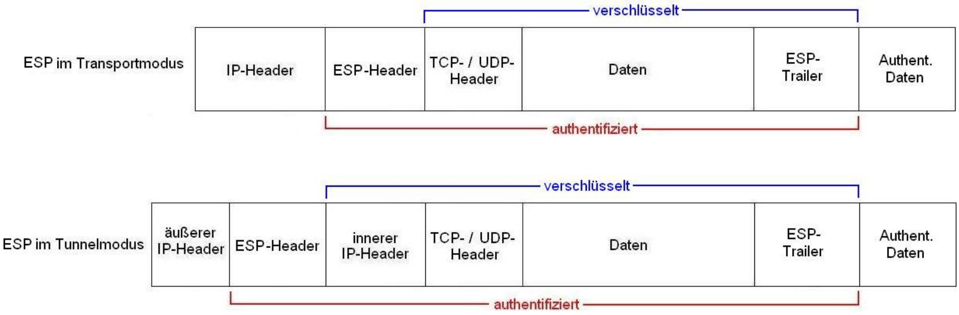
https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline

IPsec

Internet Protocol Security

- Protocol suite for securing traffic (VPN)
- IETF RFCs
- IP level (OSI layer 3)
- Symmetric cryptography
- *Independent* of key exchange
- Confidentiality, Authenticity, Integrity
- e.g. protection mechanisms for replay attacks, IP spoofing, ...

Protocols



verschlüsselt

ESP im Transportmodus

IP-Header | ESP-Header | TCP- / UDP-Header | Daten | ESP-Trailer | Authent. Daten

authentifiziert

verschlüsselt

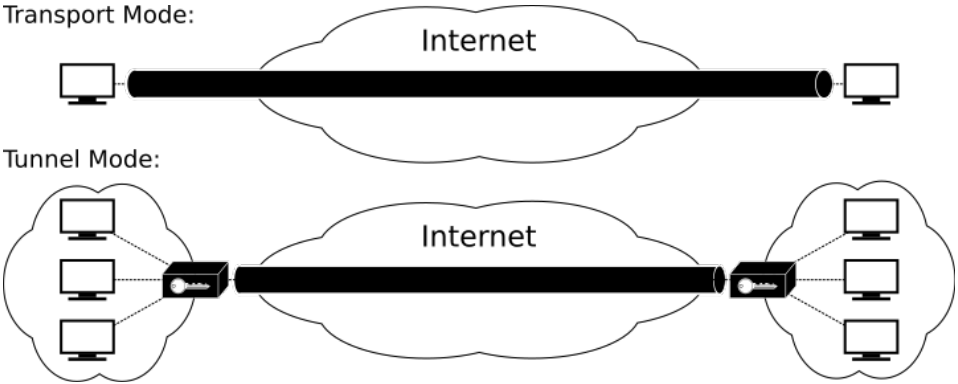
ESP im Tunnelmodus

äußerer IP-Header | ESP-Header | innerer IP-Header | TCP- / UDP-Header | Daten | ESP-Trailer | Authent. Daten

authentifiziert

Public Domain: `https://de.wikipedia.org/w/index.php?title=Datei:Ipsec_esp.jpg`

Modes



Author: Ford prefect (Wikipedia) `https://de.wikipedia.org/wiki/Datei:Ipsec-modes.svg` under `https://creativecommons.org/licenses/by/3.0/deed`

State

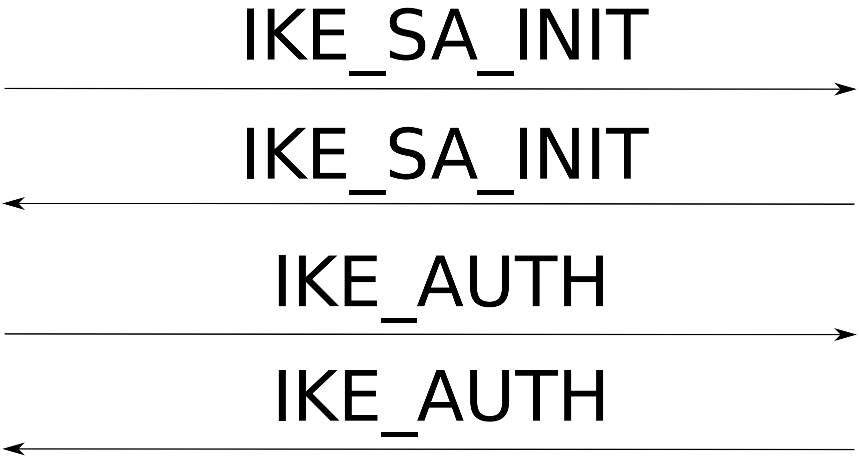
- Peer Authorization Database
- Secure Policy Database
- Security Association Database

IKEv2

Internet Key Exchange Version 2

- Key agreement protocol
- Sets up a Security Association (SA)
- Diffie-Hellman Key Exchange
- Two round trips

Key Agreement



IKE_SA_INIT

IKE_SA_INIT

IKE_AUTH

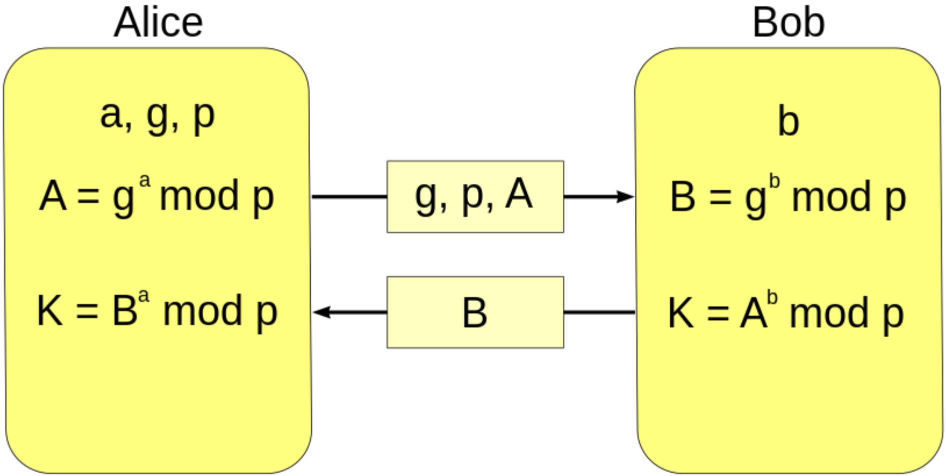
IKE_AUTH

IKE_SA_INIT

```
HDR, SAi1, KEi, Ni  -->

                           <--  HDR, SAr1, KEr, Nr, [CERTREQ]
```

Diffie-Hellman



Alice

a, g, p

$A = g^a \bmod p$

$K = B^a \bmod p$

g, p, A

B

Bob

b

$B = g^b \bmod p$

$K = A^b \bmod p$

$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$$

Authentication

- Public Key (Signature)
- Pre-Shared Key
- Extensible Authentication Protocol (EAP)

Questions?

Get in touch:

Stefan-Lukas_Gazdag@genua.eu

www.genua.eu