# Update Post-Quanten-Kryptographie für Langzeitsicherheit

Tanja Lange

Eindhoven University of Technology

Handelsblatt Jahrestagung Cybersecurity 2022

# Post-Quanten Kryptographie

# Post-Quanten Kryptographie

## Kryptographie mit Angriffs-Modell Quantencomputer

# National Academy of Sciences (US)

4. Dezember 2018: Studie zu Quanten-Computern

**Kein Stress.** "Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade."

# National Academy of Sciences (US)

4. Dezember 2018: Studie zu Quanten-Computern

**Kein Stress.** "Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade."

**Panik!** "Key Finding 10: Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster."

"[Section 4.4:] In particular, all encrypted data that is recorded today and stored for future use, will be cracked once a large-scale quantum computer is developed."

# Post-Quanten Kryptographie – Zeitleiste

- 1994: Shors Algorithmus. 1996: Grovers Algorithmus. Für viele weitere Quanten-Algorithmen siehe quantumalgorithmzoo.org.
- 2003: Daniel J. Bernstein prägt Ausdruck Post-Quanten Kryptographie.
- 2006: Erster internationaler Workshop zu Post-Quanten Kryptographie. PQCrypto 2006, 2008, 2010, 2011, 2013, 2014, 2016 – 2022 (jährlich).
- 2015: erster Workshop bei NIST zu Post-Quanten Kryptographie.
- 2016: NIST kündigt ein Standardisierung-Projekt zum Thema PQC an.
- 2017: Deadline für Einreichungen zum NIST ~~Wettbewerb~~ Projekt.
- 2017 – 69 Kandidaten, viele Angriffe (13 gebrochen).
- 2019: Zweite Runde des NIST Wettbewerbs beginnt.
- 2019 – 26 Kandidaten, mehr Angriffe (2 gebrochen).
- 2020: Dritte Runde des NIST Wettbewerbs begint.
- 2020 – 15 Kandidaten im Brennpunkt; zwei etablierte Systeme wackeln.
- 2021 "Ende Dezember": NIST kündigt die Auswahl an.

# Post-Quanten Kryptographie – Zeitleiste

- 1994: Shors Algorithmus. 1996: Grovers Algorithmus. Für viele weitere Quanten-Algorithmen siehe quantumalgorithmzoo.org.
- 2003: Daniel J. Bernstein prägt Ausdruck Post-Quanten Kryptographie.
- 2006: Erster internationaler Workshop zu Post-Quanten Kryptographie. PQCrypto 2006, 2008, 2010, 2011, 2013, 2014, 2016 – 2022 (jährlich).
- 2015: erster Workshop bei NIST zu Post-Quanten Kryptographie.
- 2016: NIST kündigt ein Standardisierung-Projekt zum Thema PQC an.
- 2017: Deadline für Einreichungen zum NIST ~~Wettbewerb~~ Projekt.
- 2017 – 69 Kandidaten, viele Angriffe (13 gebrochen).
- 2019: Zweite Runde des NIST Wettbewerbs beginnt.
- 2019 – 26 Kandidaten, mehr Angriffe (2 gebrochen).
- 2020: Dritte Runde des NIST Wettbewerbs begint.
- 2020 – 15 Kandidaten im Brennpunkt; zwei etablierte Systeme wackeln.
- ~~2021~~ 2022 “not later than the end of March” NIST kündigt die Auswahl an.

# Post-Quanten Kryptographie – Zeitleiste

- 1994: Shors Algorithmus. 1996: Grovers Algorithmus. Für viele weitere Quanten-Algorithmen siehe quantumalgorithmzoo.org.
- 2003: Daniel J. Bernstein prägt Ausdruck Post-Quanten Kryptographie.
- 2006: Erster internationaler Workshop zu Post-Quanten Kryptographie. PQCrypto 2006, 2008, 2010, 2011, 2013, 2014, 2016 – 2022 (jährlich).
- 2015: erster Workshop bei NIST zu Post-Quanten Kryptographie.
- 2016: NIST kündigt ein Standardisierung-Projekt zum Thema PQC an.
- 2017: Deadline für Einreichungen zum NIST ~~Wettbewerb~~ Projekt.
- 2017 – 69 Kandidaten, viele Angriffe (13 gebrochen).
- 2019: Zweite Runde des NIST Wettbewerbs beginnt.
- 2019 – 26 Kandidaten, mehr Angriffe (2 gebrochen).
- 2020: Dritte Runde des NIST Wettbewerbs begint.
- 2020 – 15 Kandidaten im Brennpunkt; zwei etablierte Systeme wackeln.
- ~~2021~~ 2022 ~~"not later than the end of March"~~ July NIST Ankündigung.
- 2023/2024?: NIST gibt Standards in Post-Quanten Kryptographie heraus.

# NISTs Ankündigung vom 5. Juli 2022 ($\hat{=}$ 127. März 2022)

https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

Die Gewinner sind:

- Kyber, ein Verschlüsselungs-System basierend auf strukturierten Gittern
- Dilithium, ein Signaturverfahren basierend auf strukturierten Gittern
- Falcon, ein Signaturverfahren basierend auf strukturierten Gittern
- SPHINCS+, ein Signaturverfahren basierend auf

# NISTs Ankündigung vom 5. Juli 2022 ($\hat{=}$ 127. März 2022)

https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

Die Gewinner sind:

- Kyber, ein Verschlüsselungs-System basierend auf strukturierten Gittern
- Dilithium, ein Signaturverfahren basierend auf strukturierten Gittern
- Falcon, ein Signaturverfahren basierend auf strukturierten Gittern
- SPHINCS+, ein Signaturverfahren basierend auf Hash-Funktionen

# NISTs Ankündigung vom 5. Juli 2022 (≙ 127. März 2022)

https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

Die Gewinner sind:

- Kyber, ein Verschlüsselungs-System basierend auf strukturierten Gittern
- Dilithium, ein Signaturverfahren basierend auf strukturierten Gittern
- Falcon, ein Signaturverfahren basierend auf strukturierten Gittern
- SPHINCS+, ein Signaturverfahren basierend auf Hash-Funktionen

Systeme für die 4. Runde, möglicherweise spätere Gewinner:

- BIKE, ein Verschlüsselungs-System basierend auf fehlerkorrigierenden Codes.
- Classic McEliece, ein Verschlüsselungs-System basierend auf fehlerkorrigierenden Codes.
- HQC, ein Verschlüsselungs-System basierend auf fehlerkorrigierenden Codes.
- SIKE, ein Verschlüsselungs-System basierend auf Isogenien.

# NISTs Ankündigung vom 5. Juli 2022 (≙ 127. März 2022)

https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

Die Gewinner sind:

- Kyber, ein Verschlüsselungs-System basierend auf strukturierten Gittern
- Dilithium, ein Signaturverfahren basierend auf strukturierten Gittern
- Falcon, ein Signaturverfahren basierend auf strukturierten Gittern
- SPHINCS+, ein Signaturverfahren basierend auf Hash-Funktionen

Systeme für die 4. Runde, möglicherweise spätere Gewinner:

- BIKE, ein Verschlüsselungs-System basierend auf fehlerkorrigierenden Codes.
- Classic McEliece, ein Verschlüsselungs-System basierend auf fehlerkorrigierenden Codes.
- HQC, ein Verschlüsselungs-System basierend auf fehlerkorrigierenden Codes.
- ~~SIKE, ein Verschlüsselungs-System basierend auf Isogenien~~

30. Juli: SIKE vollständig gebrochen, keinen Monat nach NISTs Ankündigung.

# Populäre Software mit PQC Optionen (Zeitleiste)

2016.07: Chrome bietet `newhope1024` an.
Teil eines Experiments mit Google-Servern.

# Populäre Software mit PQC Optionen (Zeitleiste)

2016.07: Chrome bietet `newhope1024` an.
Teil eines Experiments mit Google-Servern.
Ein Patent-Inhaber kontaktiert Google, fragt nach Geld

# Populäre Software mit PQC Optionen (Zeitleiste)

2016.07: Chrome bietet `newhope1024` an.
Teil eines Experiments mit Google-Servern.
Ein Patent-Inhaber kontaktiert Google, fragt nach Geld

2016.11: Chrome entfernt `newhope1024`.

# Populäre Software mit PQC Optionen (Zeitleiste)

2016.07: Chrome bietet `newhope1024` an.
Teil eines Experiments mit Google-Servern.
Ein Patent-Inhaber kontaktiert Google, fragt nach Geld

2016.11: Chrome entfernt `newhope1024`.

2019.04: OpenSSH 8.0 bietet `sntrup761` an.
Nur genutzt, wenn Client und Server es anfragen.

# Populäre Software mit PQC Optionen (Zeitleiste)

2016.07: Chrome bietet `newhope1024` an.
Teil eines Experiments mit Google-Servern.
Ein Patent-Inhaber kontaktiert Google, fragt nach Geld

2016.11: Chrome entfernt `newhope1024`.

2019.04: OpenSSH 8.0 bietet `sntrup761` an.
Nur genutzt, wenn Client und Server es anfragen.

2019.07: Chrome und Cloudflare Experimente mit `ntruhrss701` und `sikep434`.

# Populäre Software mit PQC Optionen (Zeitleiste)

2016.07: Chrome bietet `newhope1024` an.
Teil eines Experiments mit Google-Servern.
Ein Patent-Inhaber kontaktiert Google, fragt nach Geld

2016.11: Chrome entfernt `newhope1024`.

2019.04: OpenSSH 8.0 bietet `sntrup761` an.
Nur genutzt, wenn Client und Server es anfragen.

2019.07: Chrome und Cloudflare Experimente mit `ntruhrss701` und `sikep434`.

2021.05: OpenBSD bietet `sntrup761` für IPsec an.
Nur genutzt, wenn Client und Server es anfragen.

# Populäre Software mit PQC Optionen (Zeitleiste)

2016.07: Chrome bietet `newhope1024` an.
Teil eines Experiments mit Google-Servern.
Ein Patent-Inhaber kontaktiert Google, fragt nach Geld

2016.11: Chrome entfernt `newhope1024`.

2019.04: OpenSSH 8.0 bietet `sntrup761` an.
Nur genutzt, wenn Client und Server es anfragen.

2019.07: Chrome und Cloudflare Experimente mit `ntruhrss701` und `sikep434`.

2021.05: OpenBSD bietet `sntrup761` für IPsec an.
Nur genutzt, wenn Client und Server es anfragen.

2022.02: OpenSSH 8.9 schaltet `sntrup761` auf Servern automatisch an.
Genutzt sobald der Client es anfragt.

# Populäre Software mit PQC Optionen (Zeitleiste)

2016.07: Chrome bietet `newhope1024` an.
Teil eines Experiments mit Google-Servern.
Ein Patent-Inhaber kontaktiert Google, fragt nach Geld

2016.11: Chrome entfernt `newhope1024`.

2019.04: OpenSSH 8.0 bietet `sntrup761` an.
Nur genutzt, wenn Client und Server es anfragen.

2019.07: Chrome und Cloudflare Experimente mit `ntruhrss701` und `sikep434`.

2021.05: OpenBSD bietet `sntrup761` für IPsec an.
Nur genutzt, wenn Client und Server es anfragen.

2022.02: OpenSSH 8.9 schaltet `sntrup761` auf Servern automatisch an.
Genutzt sobald der Client es anfragt.

2022.04: OpenSSH 9.0 schaltet `sntrup761` auf Clients automatisch an.

# Populäre Software mit PQC Optionen (Zeitleiste)

2016.07: Chrome bietet `newhope1024` an.
Teil eines Experiments mit Google-Servern.
Ein Patent-Inhaber kontaktiert Google, fragt nach Geld

2016.11: Chrome entfernt `newhope1024`.

2019.04: OpenSSH 8.0 bietet `sntrup761` an.
Nur genutzt, wenn Client und Server es anfragen.

2019.07: Chrome und Cloudflare Experimente mit `ntruhrss701` und `sikep434`.

2021.05: OpenBSD bietet `sntrup761` für IPsec an.
Nur genutzt, wenn Client und Server es anfragen.

2022.02: OpenSSH 8.9 schaltet `sntrup761` auf Servern automatisch an.
Genutzt sobald der Client es anfragt.

2022.04: OpenSSH 9.0 schaltet `sntrup761` auf Clients automatisch an.

All diese Systeme nutzen PQC *zusätzlich* zu X25519 Verschlüsselung.
ECC sichert alles ab (bis Quanten-Computer kommen).

# US Regierung gegen die Nutzung von PQC

2021.07 Matthew Scholl, Chief of the Computer Security Division in NIST's Information Technology Laboratory: "Don't let folks start to buy and implement unstandard, unknown, potentially unsecured implementations before we as a general community have agreed upon standardization."

2021.08 NSA: "The intention is to update CNSA to remove quantum-vulnerable algorithms and replace them with a subset of the quantum-resistant algorithms selected by NIST ... NSA is waiting for the NIST process to be completed and for standards to be published. ... NSS customers are reminded that NSA does not recommend and policy does not allow implementing or using unapproved, non-standard or experimental cryptographic algorithms. The field of quantum-resistant cryptography is no exception."

2021.09 DHS: Do not use "post-quantum cryptographic industry products until standardization, implementation, and testing of replacement products with approved algorithms are completed by NIST."

# HYBRID?

CYBERSECURITY

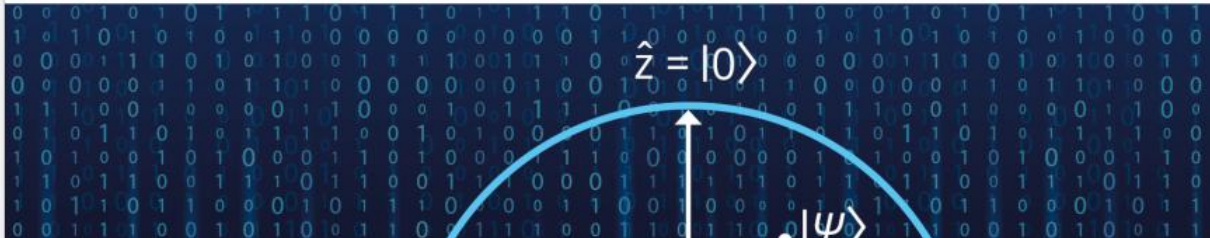
- NSA does not expect to approve post-quantum algorithms with any kind of “but just to be safe, combine with an older algorithm” guidance
- While some argue that deploying a post-quantum algorithm in addition to an existing solution cannot make things less secure, experience shows this to be false
  - CVE 2021-3450 OpenSSL X509_V_FLAG-STRICT
    - Extra check to see if curves were named (relates to NSA discovered Windows CVC 2020-0601)
    - Additional checks shouldn’t hurt…but this one overwrote the “The CA isn’t valid” result
  - “in cryptographic libraries…system level bugs are a greater security concern than the actual cryptographic procedures” (arXiv 2107.04940)
    - Don’t muck with trusted crypto for a temporary fix

Upshot: Don’t use temporary hybrids, and invest in implementation robustness before crypto redundancy

# Post-Quantum Cryptography: Current state and quantum mitigation

Ward Beullens, Jan-Pieter D'Anvers, Andreas Hülsing, Tanja Lange, Lorenz Panny, Cyprien de Saint Guilhem, Nigel P. Smart.
Evangelos Rekleitis, Angeliki Aktypi, Athanasios-Vasileios Grammatopoulos.

EUROPEAN UNION AGE
FOR CYBERSECU



# ENISA Studien: Current state and quantum mitigation (2021)
# Post-Quantum Cryptography - Integration study (2022)

Inhaltsverzeichnisse





Die Studien sind hier und hier verfügbar.

# US ANSI X9 zu PQC hybrids

2021: "As we transition from classical cryptography to post-quantum cryptography (PQC), there is a need to understand the proper ways to use both methods simultaneously. PQC methods will not be able to be used as a direct replacement in all cases. And the confidence and broad acceptance of PQC methods will not be as great as classical cryptography. **Simultaneous use of both classical cryptography and PQC methods for both security and acceptance** is required during a transition and may be required long term as well. There are improper and insecure ways of implementing a hybrid of classical and PQC methods. Specifying the proper methods of using both are required." (Hervorhebungen ergänzt)

# ANSSI (französische Behörde) zu PQC hybrids

2022: "Although this new post-quantum toolbox may seem handy for developers, the maturity level of the post-quantum algorithms presented to the NIST process should not be overestimated. Many aspects lack cryptanalytical hindsight or are still research topics, e.g. analysis of the difficulty of the underlying problem in the classical and quantum computation models, dimensioning, integration of schemes in protocols and more importantly the design of secure implementations. This situation will probably last some time after the publication of NIST standards. **Acknowledging the immaturity of PQC is important: ANSSI will not endorse any direct drop-in replacement of currently used algorithms in the short/medium term.** However, this immaturity should not serve as an argument for postponing the first deployments." (Hervorhebungen ergänzt)

# Was tun? Hybrids kombinieren pre & post-quanten Systeme

**Signaturen:**

*Alle* Signaturen müssen gültig sein, damit die hybride Signatur gültig ist.

**Verschlüsselung:**

Mehrere Systeme erzeugen einen Schlüssel *gemeinsam*.

Sichere Kombinationen für Verschlüsselungen

- PQC Information wird pre-quanten verschlüsselt als “payload” geschickt (einfachere Integration).
- Pre-quanten Information wrid PQC verschlüsselt als “payload” geschickt (der Quanten-Angreiffer hat keinen Zugang zu pre-quanten Information).

**Empfehlungen zum Umstieg sind risikoabhängig:**

- Um den Umstieg so unbemerkbar wie möglich zu machen, nurtzt man die schnellsten / kleinsten PQC Systeme zusammen mit ECC oder RSA.
- Um schnellstmöglich die beste Sicherheit zu schaffen, nutzt man die am besten studierten PQC Systeme zusammen mit ECC oder RSA.

# Mehr Information

- NISTs PQC Wettbewerb.
- Quantum Threat Timeline vom Global Risk Institute, 2019; 2021 update.
- Status of quantum computer development (vom deutschen BSI).
- ENISA Studie Post-Quantum Cryptography: Current state and quantum mitigation
- ENISA Studie Post-Quantum Cryptography - Integration study

- YouTube Kanal Tanja Lange: Post-quantum cryptography.
- `https://2017.pqcrypto.org/school`: PQCRYPTO summer school mit 21 Vorlesungen auf Video und jeweils Folien und Übungsblättern.
- `https://2017.pqcrypto.org/exec` and `https://pqcschool.org/index.html`: Executive school (weniger Mathe, mehr Perspektive).

# Bonus Folien

# 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

# Erste Empfehlungen von PQCRYPTO

- **Symmetrische Verschlüsselung** Grover erfordert 256-Bit Schlüssel:
  - AES-256
  - Salsa20 mit 256-Bit Schlüssel

  Forschung: Serpent-256, ...
- **Symmetrische Authentisierung** Informationstheoretische MACs (weder Shor noch Grover finden Anwendung):
  - GCM mit 96-Bit nonce und 128-Bit Ausgabe
  - Poly1305
- **Public-key Verschlüsselung** McEliece mit binären Goppa Codes:
  - Länge $n = 6960$, Dimension $k = 5413$, $t = 119$ Fehler

  Forschung: QC-MDPC, Stehlé-Steinfeld NTRU, ...
- **Public-key Signaturen** Hash-basiert (minimale Annahmen):
  - XMSS mit Parametern aus dem CFRG Draft
  - SPHINCS-256

  Forschung: HFEv-, ...