Shortpaper/Glossar/Bibliographie

Die Kryptokalypse

Post-Quanten-Kryptographie und Open Source

Stefan Schumacher

$Id: Shortpaper.tex,v 1.3 2025/12/19 16:50:34 stefan Exp $

cryptomancer.de

1 Kurzbeschreibung des Vortrags

Im Vortrag stelle ich die Grundlagen von Quantencomputern und deren Auswirkungen auf die Kryptographie vor. Dabei zeige ich den aktuellen Stand der Forschung zu Quantencomputern und mit welchem Aufwand der Aufbau eines Quantencomputers verbunden ist. Ich stelle die Möglichkeit eines perfekt sicheren Quantenschlüsselaustausch vor und zeige welche bisherigen Krypt-Algorithmen wie betroffen sein werden.

Ich stelle den NIST-Standardisierungsprozess für quantensichere Algorithmen und die Gewinner der ersten Standardisierungsrunde im Details vor und erkläre deren Funktionsweise. Die empfohlenen hybriden Schlüsselkapselungsmechanismen für TLS1.3 werde ich ebenfalls vorstellen.

Zum Abschluss gebe ich einen kleinen aktuellen Überblick über den Stand der Implementierung von quantensicheren Verfahren im Open-Source-Universum und zeige auf was bei der kommenden Migration auf diese Verfahren zu beachten ist.

Außerdem werde ich meine OpenSSL-Benchmark (https://cryptomancer.de/pqcbenchmark) zur PQC und die Ergebnisse zu den veränderten Schlüsselgrößen und Laufzeiten kurz vorstellen.

Gliederung des Vortrages:

- Grundlagen
- Quantencomputer
- Quantenschlüsselaustausch
- Quantensichere Algorithmen
- Stand der Dinge im FLOSSiversum (3/2026)
- Was ist zu tun?

2 Glossar

symmetrisches Kryptosystem ein geteilter geheimer Schlüssel für Verschlüsselung/Entschlüsselung nötig

asymmetrisches Kryptosystem kein geteilter geheimer Schlüssel für Verschlüsselung/Entschlüsselung nötig

Diffie-Hellmann Key Exchange (DH KEX): Protokoll zur Schlüsselvereinbarung, Alice und Bob können über einen öffentlichen (abhörbaren) Kanal einen geheimen Schlüssel für symmetrische Kryptographie vereinbaren

Key Derivation Function Schlüsselableitungsfunktion, leitet $1..n$ neue Schlüssel aus einem geheimen Schlüssel ab

(Perfect) Forward Secrecy (PFS) Sitzungsschlüssel werden so vereinbart, dass nach einem Einbruch *vergangene* Sitzungsschlüssel nicht gebrochen werden können (break-backward protection)

PSK Pre Shared Key, symmetrisches Verfahren mit vorher geteiltem geheimen Schlüssel

HPKE Hybrid Public Key Encryption: Symmetrischer Session-Key wird mit einem asymmetrischen Key-Encryption-Key verschlüsselt

Break-in recovery Sitzungsschlüssel werden so vereinbart, dass nach einem Einbruch auch *zukünftige* Sitzungsschlüssel nicht gebrochen werden können (break-forward protection)

persistent nicht-flüchtig, Langzeitschlüssel/ID-Schlüssel

ephemeral flüchtig, Sizungsschlüssel, wird aus dem Langzeitschlüssel abgeleitet

E2EE / Ende-zu-Ende Verschlüsselung Kommunikation wird zwischen Alice und Bob so verschlüsselt, das niemand dazwischen mitlauschen kann, egal ob ISP oder Server-Betreiber

Merkle-Tree Binärbaum, in dem jeder Knoten den Hash über alle seine Unterbäume bildet

Authentizität Echtheit des Absenders (Web of Trust/Zertifikate)

Integrität Daten wurden nicht verändert (Signatur)

Zurechenbarkeit Nachrichten sind dem zuzuordnen, der sie abgeschickt hat

Verbindlichkeit Sender kann Urheberschaft gesendeter Nachrichten nicht abstreiten

plausible Deniability Gegenteil zu Zurechenbarkeit && Verbindlichkeit, Alice und Bob können sich sicher sein, dass sie mit Bob bzw. Alice kommunizieren, aber Mallory kann nicht beweisen, dass Alice und Bob kommuniziert haben, im Englischen auch Off-the-Record genannt

Malleability Formbarkeit kryptographischer Nachrichten, d.h. Zurechenbarkeit && Verbindlichkeit können ausgehebelt werden

Mitgliedschaftsauthentifizierung jeder Teilnehmer kann alle Mitgliedschaften in der Gruppe überprüfen

Device (Matrix) *alle* End-Geräte eines Nutzers

Client (MLS) Mitglieder einer Gruppe

Epoche (MLS) Zustand einer Gruppe zu einem Zeitpunkt

LeafNode (MLS) Eigenschaft eines jeden Mitglieds mit Identität, Credentials und Fähigkeiten

Attestation Beglaubigung der Integrität und Authentizität von Daten

Formelzeichen M: Message/Nachricht; K: Key S: Secret/Geheimnis *pub*: public *priv*: private *sig*: signature *enc*: decryption

Literatur

Alkhulaifi, A., & El-Alfy, E.-S. M. (2020). Exploring Lattice-based Post-Quantum Signature for JWT Authentication: Review and Case Study. *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 1–5. https://doi.org/10.1109/VTC2020-Spring48590.2020.9129505

Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of statistical physics*, *22*(5), 563–591.

Benioff, P. A. (1982). Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: Application to Turing machines. *International Journal of Theoretical Physics*, *21*(3), 177–201.

Bennett, C. H., & Brassard, G. (1984). An update on quantum cryptography. *Workshop on the theory and application of cryptographic techniques*, 475–480.

Bernstein, E., & Vazirani, U. (1993). Quantum complexity theory. *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, 11–20.

Buchmann, J., Coronado, C., Döring, M., Engelbert, D., Ludwig, C., Overbeck, R., Schmidt, A., Vollmer, U., & Weinmann, R.-P. (2004). Post-quantum signatures. *Cryptology ePrint Archive*. https://eprint.iacr.org/2004/297.pdf

Cai, J.-Y. (2024). Shor's algorithm does not factor large integers in the presence of noise. *Science China Information Sciences*, *67*(7). https://doi.org/10.1007/s11432-023-3961-3

Certificate Policy 2024: Root-CA der PKI-1-Verwaltung (V. 1.0.0). (2024, 31. Dezember). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/VerwaltungsPKI/Certificate_Policy_2024.pdf?__blob=publicationFile&v=3

Deutsch, D. (1985). Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, *400*(1818), 97–117.

Duits, I. (2019). *The post-quantum Signal protocol: Secure chat in a quantum world* [Magisterarb., University of Twente].

Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical review*, *47*(10), 777.

Elliptic Curve Cryptography (V. 2.1.0). (2018, 1. Juni). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.pdf?__blob=publicationFile&v=1

Feynman, R. P. (1986). Quantum mechanical computers. *Found. Phys.*, *16*(6), 507–532.

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*, 433. https://doi.org/10.22331/q-2021-04-15-433

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 212–219.

Halang, W. A., & Fitz, R. (2018). Informationstheoretisch sichere Datenverschlüsselung. In *Nicht hackbare Rechner und nicht brechbare Kryptographie* (S. 147–156). Springer.

Kryptographische Verfahren: Empfehlungen und Schlüssellängen (2024-01). (2024, 2. Februar). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=5

Kryptographische Verfahren: Verwendung von Secure Shell (SSH) (2024-01, Technische Richtlinie des BSI). (2024, 29. Februar). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.pdf?__blob=publicationFile&v=3

Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS) (TR-02102-2 2022-01, Technische Richtlinie des BSI). (2024, Januar). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=4

Kryptographische Verfahren: X.509 Zertifikate und Zertifizierungspfadvalidierung (V. 1.0.0, Technische Richtlinie des BSI). (2020). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02103/BSI-TR-02103.pdf?__blob=publicationFile&v=2

Migration zu Post-Quanten-Kryptografie. Handlungsempfehlungen des BSI. (2020, 1. August). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=1

Module-Lattice-Based Digital Signature Standard: FIPS 204. (2024). National Institute of Standards & Technology. Verfügbar 17. August 2025 unter https://doi.org/10.6028/NIST.FIPS.204

Module-Lattice-Based Key-Encapsulation Mechanism Standard: FIPS 203. (2024). National Institute of Standards & Technology. Verfügbar 17. August 2025 unter https://doi.org/10.6028/NIST.FIPS.203

Preskill, J. (2012). Quantum computing and the entanglement frontier. https://arxiv.org/abs/1203.5813

Recommendation for Stateful Hash-Based Signature Schemes: NIST Special Publication 800-208. (2020). National Institute of Standards & Technology. Verfügbar 19. August 2025 unter https://doi.org/10.6028/NIST.SP.800-208

Schumacher, S. (2004). Einführung in kryptographische Methoden. Verfügbar 19. April 2004 unter http://www.cryptomancer.de/21c3/21c3-kryptographie-paper.pdf

Schumacher, S. (2011). Kryptographische Dateisysteme im Detail. In Team der Chemnitzer Linux-Tage (Hrsg.), *Chemnitzer Linux-Tage 2011: Tagungsband* (S. 39–46). Universitätsverlag. https://monarch.qucosa.de/api/qucosa%3A19466/attachment/ATT-0/

Schumacher, S. (2018). Zwei-Faktor-Authentifizierung mit Yubikey-Token: Ein kostengünstiges Verfahren. *UpTimes*, 16–27. Verfügbar 1. Februar 2019 unter https://www.guug.de/uptimes/2018-2/uptimes_2018-02.pdf

Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, *26*(5), 1484–1509. https://doi.org/10.1137/s0097539795293172

Stateless Hash-Based Digital Signature Standard: FIPS 205. (2024). National Institute of Standards & Technology. Verfügbar 17. August 2025 unter https://doi.org/10.6028/NIST.FIPS.205

TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government: Vertrauensniveaus und Mechanismen (Technische Richtlinie des BSI). (2019, 7. Mai). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf?__blob=publicationFile&v=1

TR-03116-4 Kryptographische Vorgaben für Projekte der Bundesregierung: Kommunikationsverfahren in Anwendungen (Technische Richtlinie des BSI). (2023, 7. März). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf?__blob=publicationFile&v=5

TR-03124-1eID-Client – Part 1: Specifications (Technische Richtlinie des BSI). (2021, 8. Oktober). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03124/TR-03124-1.pdf?__blob=publicationFile&v=2

TR-03175 Infrastruktur zur Absicherung von Dokumenten mit digitalen Siegeln (Technische Richtlinie des BSI). (2022, 13. Mai). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03175/BSI-TR-03175.pdf?__blob=publicationFile&v=4

Von Neumann, J. (1932). Mathematische Grundlagen der Quantenmechanik. https://gdz.sub.uni-goettingen.de/id/PPN379400774

Weierud, F., & Zabell, S. (2020). German mathematicians and cryptology in WWII. *Cryptologia*, *44*(2), 97–171.

Yu, H., McCuller, L., Tse, M., Kijbunchoo, N., Barsotti, L., & Mavalvala, N. (2020). Quantum correlations between light and the kilogram-mass mirrors of LIGO. *Nature*, *583*(7814), 43–47.