Die Kryptokalypse

Post-Quanten-Kryptographie und Open Source Software

Stefan Schumacher

cryptomancer.de

Quantenkryptographie-Symposium ITZBund
29.04.2026

$ Id: Kryptokalypse-Input.tex,v 1.53 2026/04/26 21:17:27 stefan Exp $

cryptomancer.de

Inhaltsverzeichnis

1 Einführung

2 Quantensichere Algorithmen

3 Stand der Dinge im FLOSSiversum (4/2026)

4 CBOMs

5 Was ist zu tun?

cryptomancer.de



- Robotron KC85/3 Mitte der 80er Jahre
- Geek, Nerd, Hacker
- Kryptographie seit 30 Jahren
- einige Jahre NetBSD-Entwickler
- ehem. Sicherheitsforscher u.a. Fach-Didaktik der Kryptographie
- bis 2020 Hrsg. Magdeburger Journal zur Sicherheitsforschung
- jetzt Sicherheitsarchitekt bei Dataport AöR in Magdeburg

cryptomancer.de

- Chemnitzer Linux-Tage 2025: Open-Source-Software BSI-Grundschutzfähig machen
- https://media.ccc.de/v/clt25-190-open-source-software-bsi-grundschutzfahig-machen
- https://gitlab.opencode.de/StefanSchumacher/phoenixflossquellenrichtlinie

Glossar

- Glossar samt Formelzeichen und Literatur im Handout
- https://www.cryptomancer.de/kryptokalypse/
- Video und Foliensatz aus Chemnitz
- Videos in der CCC Mediathek

Inhaltsverzeichnis

1 Einführung

2 Quantensichere Algorithmen

3 Stand der Dinge im FLOSSiversum (4/2026)

4 CBOMs

5 Was ist zu tun?

cryptomancer.de

Standardisierungsprozess

- US NIST startet Standardisierungsprozess auf der PQCrypto 2016
- offener Standardisierungsprozess von AES 1997-2000 als Vorbild
- nach der Kritik am DES/3DES-Standardisierungsprozess durch die NSA
- CfP zum Ende 2017
- 23 Signaturverfahren und 59 KEM-Verfahren eingereicht
- Analyse der Verfahren in 3 Runden
- 2022: Bekanntgabe der ersten 4 Gewinner [1], [2], [3], [4]
- 2025: Bekanntgabe des Ersatz-Algorithmus für KEM (Hamming Quasi-Cyclic)
- Dritte Runde des Standardisierungsprozesses für Digitale Signaturverfahren läuft
- Oktober 2024: 14 Kandidaten für Runde 3 ausgewählt

cryptomancer.de

Standardisierungsprozess

- US NIST startet Standardisierungsprozess auf der PQCrypto 2016
- offener Standardisierungsprozess von AES 1997-2000 als Vorbild
- nach der Kritik am DES/3DES-Standardisierungsprozess durch die NSA
- CfP zum Ende 2017
- 23 Signaturverfahren und 59 KEM-Verfahren eingereicht
- Analyse der Verfahren in 3 Runden
- 2022: Bekanntgabe der ersten 4 Gewinner [1], [2], [3], [4]
- 2025: Bekanntgabe des Ersatz-Algorithmus für KEM (Hamming Quasi-Cyclic)
- Dritte Runde des Standardisierungsprozesses für Digitale Signaturverfahren läuft
- Oktober 2024: 14 Kandidaten für Runde 3 ausgewählt

cryptomancer.de

FIPS203 - ML-KEM (Kyber)

- Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)
- Learning with errors: Schwierigkeit, aus einer Reihe von Gleichungen mit fehlerbehafteten Variablen die ursprünglichen Variablen zu bestimmen
- z.B. Fehlerrate in der Vektor-/Matrix-Multiplikation
- Module/Gitter: diskrete Untergruppe des euklidischen Raumes
- Key Encapsulation zum Austausch eines geteilten Geheimnisses
- Zufälligkeit wird von beiden Parteien beigesteuert, geteiltes Geheimnis kann genutzt werden, ohne weitere Schlüsselableitung
- keine Authentifizierung der Kommunikationspartner!
- Aber: ohne PFS, da keine ephemeralen Schlüssel!

FIPS203 - ML-KEM - Kyber

Schlüsselgrößen

```
openssl genpkey -algorithm ML-KEM-512 -out priv.pem
openssl pkey -in priv.pem -pubout -out pub.pem
```

ML-KEM:	512	768	1024	RSA:	3072	7680	X25519	BP384
sec lvl	128	192	256		128	192	128	192
K_{sec}	2399	3439	4479		2484	6002	113	310
K_{pub}	1166	1686	2206		625	1405	119	223

Vergleich mit ECDH/Curve25519: [5]

- Laufzeit Faktor 2,5
- Energieverbrauch Faktor 2,5
- Metadaten x70

https://www.cryptomancer.de/pqcbenchmark

cryptomancer.de

FIPS204/FIPS205

Signaturverfahren

- FIPS204: Module-Lattice-Based Digital Signature Standard
  ML-DSA-44 ML-DSA-65 ML-DSA-87
- FIPS205: Stateless Hash-Based Digital Signature Standard
  SLH-DSA-SHA2-128 SLH-DSA-SHA2-192 SLH-DSA-SHA2-256
  SLH-DSA-SHAKE-128 SLH-DSA-SHAKE-192 SLH-DSA-SHAKE-256
- f == fast; s == small
- stateless: keine Zustandsübergänge zwischen den Operationen
- Einmal-Signatur für jedes Blatt eines Merkle-Baumes
- konservativer »Ersatz« für ML-DSA
- Wenn möglich, beides verwenden

Inhaltsverzeichnis

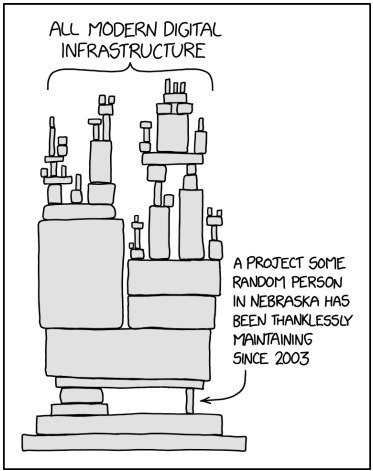
1 Einführung

2 Quantensichere Algorithmen

3 Stand der Dinge im FLOSSiversum (4/2026)

4 CBOMs

5 Was ist zu tun?


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

AI Slop

- AI Slop
- Daniel Stenberg: curl-Maintainer

OpenSSL

- Open Quantum Safe Project
- während des Auswahlprozesses parallel Implementierung der Kandidaten
- als Engine für OpenSSL 3.0
- als OpenSSL-Bibliothek ab OpenSSL 3.5 (April 2025) unterstüzt
- OpenSSL 4.0 April 2026 erschienen

OpenSSL 4.0

- SSLv2 und SSLv3 entfernt; API gestrafft
- Engine-Konzept abgeschafft
- Encrypted Client Hello nach RFC 9849 $\rightsquigarrow$ SNI verschlüsselt
- ShangMi (SM) Cipher Suites implementiert (`curveSM2MLKEM768`)
- KDFs für SNMP und SRTP

TLS1.3

- TLS1.3 führt 3 neue Hybridverfahren ein
  X25519MLKEM768, SecP256r1MLKEM768, SecP384r1MLKEM1024
- X25519MLKEM768: wird wahrscheinlich nicht durch BSI empfohlen werden
- alle Web-Browser unterstützen X25519MLKEM768
- https://pq.cloudflareresearch.com/
- https://tls.support/
- https://browserleaks.com/tls

Beispiel-Verbindung mit X25519MLKEM768

```
openssl s_client -connect apache.org:443 -groups X25519MLKEM768
...
Peer signing digest: SHA256
Peer signature type: rsa_pss_rsae_sha256
Negotiated TLS1.3 group: X25519MLKEM768
...
```

Beispiel-Verbindung ohne X25519MLKEM768

```
openssl s_client -connect openssl.org:443
...
Peer signing digest: SHA256
Peer signature type: rsa_pss_rsae_sha256
Peer Temp Key: X25519, 253 bits
...
```

Benchmarking Post Quantum Cryptography with OpenSSL 3.5

NetBSD 10, Intel Atom 230, SATA-HDD, OpenSSL 3.5.2

- https://www.cryptomancer.de/pqcbenchmark
- md5: sign 16G in 392.39s
- SLH-DSA-SHAKE-256f: sign 16G in 01.87s
- SLH-DSA-SHAKE-256s: sign 16G in 10.51s
- ML-DSA-87: sign 16G in 00.62s
- x25519: 5031 connections in 601 real seconds
- 25519MLKEM768: 4976 connections in 601 real seconds

cryptomancer.de

Benchmarking Post Quantum Cryptography with OpenSSL 3.5

NetBSD 10, Intel Atom 230, SATA-HDD, OpenSSL 3.5.2

- https://www.cryptomancer.de/pqcbenchmark
- md5: sign 16G in 392.39s
- SLH-DSA-SHAKE-256f: sign 16G in 01.87s
- SLH-DSA-SHAKE-256s: sign 16G in 10.51s
- ML-DSA-87: sign 16G in 00.62s
- x25519: 5031 connections in 601 real seconds
- 25519MLKEM768: 4976 connections in 601 real seconds

cryptomancer.de

GnuPG

Fork-Drama

- LibrePGP: Alternativer *Standard* zu OpenPGP (RFC 4880)
  - draft-koch-librepgp-05
  - GnuPG ab 2.5 implementiert
  - ML-KEM-768+BrainpoolP256r1, ML-KEM-1024+BrainpoolP384r1, ML-KEM-768+X25519, ML-KEM-1024+X448
  - überarbeitet komplettes Schlüssel-/Paketformat
- OpenPGP: draft-ietf-openpgp-pqc-17
  - Sig: ML-DSA-65+Ed25519 (MUST), ML-DSA-87+Ed448 (SHOULD)
  - Enc: ML-KEM-768+X25519 (MUST), ML-KEM-1024+X448 (SHOULD)
- LibrePGP bisher in keiner Mainstream-Distro unterstützt
- `cdrtools` again and again ...
- Yubico Yubikeys / Token2 / Nitrokey3 als GnuPG-Smartcard: neue Firmware nötig

cryptomancer.de

GnuPG

Fork-Drama

- LibrePGP: Alternativer *Standard* zu OpenPGP (RFC 4880)
  - draft-koch-librepgp-05
  - GnuPG ab 2.5 implementiert
  - ML-KEM-768+BrainpoolP256r1, ML-KEM-1024+BrainpoolP384r1, ML-KEM-768+X25519, ML-KEM-1024+X448
  - überarbeitet komplettes Schlüssel-/Paketformat
- OpenPGP: draft-ietf-openpgp-pqc-17
  - Sig: ML-DSA-65+Ed25519 (MUST), ML-DSA-87+Ed448 (SHOULD)
  - Enc: ML-KEM-768+X25519 (MUST), ML-KEM-1024+X448 (SHOULD)
- LibrePGP bisher in keiner Mainstream-Distro unterstützt
- `cdrtools` again and again ...
- Yubico Yubikeys / Token2 / Nitrokey3 als GnuPG-Smartcard: neue Firmware nötig

cryptomancer.de

OpenSSH, X.509-Zertifikate, JWT

- OpenSSH 10: `mlkem768x25519-sha256` als Standard-KEX
- X.509-Zertifikate: RFC9935 - 6.2.2026
- OIDs für Algorithmen enthalten diverse hybride Verfahren
- `https://pkic.org/pqccm/` PKI PQC Capabilities Matrix
- JWT: Ebenfalls noch kein neuer Standard vorhanden [6]
- FIDO2 (Passkeys): IANA CBOR Object Signing and Encryption (COSE) und JSON Object Signing and Encryption (JOSE): ML-DSA aufgenommen

cryptomancer.de

Software

- Open Quantum Safe Project `oqsprovider`
- OpenSSL ab 3.5, GnuTLS, BoringSSL, rustls
- Bouncy Castle Java 1.79 / C# .NET 2.6.1
- Nginx, Rpxy, Traefik, Caddy
- C: liboqs, C++ Botan, Zig, Go, Node
- OpenVPN und Wireguard arbeiten an PQC
- `crypto-policies(7) FUTURE`

cryptomancer.de

Inhaltsverzeichnis

1 Einführung

2 Quantensichere Algorithmen

3 Stand der Dinge im FLOSSiversum (4/2026)

4 CBOMs

5 Was ist zu tun?

cryptomancer.de

Cryptographic Bill of Materials

- riesiges Problem: wo wird welche Form der Verschlüsselung wie eingesetzt?
- Netzwerkverkehr? TLS kann ich relativ einfach scannen und inventarisieren
- aber: TrueCrypt 6 Container von 2006 irgendwo im Cold Storage Backup ...
- *verschlüsselte Daten sind von Zufallsdaten nicht sinnvoll zu unterscheiden*
- Wie finde ich verschlüsselte Artefakte
- `---ORTVA CEVINGR XRL---`
- `---BEGIN PRIVATE KEY---`
- CycloneDX als OWASP-Standard für CBOMs

cryptomancer.de

Cryptographic Bill of Materials

- riesiges Problem: wo wird welche Form der Verschlüsselung wie eingesetzt?
- Netzwerkverkehr? TLS kann ich relativ einfach scannen und inventarisieren
- aber: TrueCrypt 6 Container von 2006 irgendwo im Cold Storage Backup ...
- *verschlüsselte Daten sind von Zufallsdaten nicht sinnvoll zu unterscheiden*
- Wie finde ich verschlüsselte Artefakte
- `---ORTVA CEVINGR XRL---`
- `---BEGIN PRIVATE KEY---`
- CycloneDX als OWASP-Standard für CBOMs

cryptomancer.de

Inhaltsverzeichnis

1 Einführung

2 Quantensichere Algorithmen

3 Stand der Dinge im FLOSSiversum (4/2026)

4 CBOMs

5 Was ist zu tun?

cryptomancer.de

Was ist zu tun?

- Krypto-Kataster: Wo findet Verschlüsselung statt?
  Datenflussdiagramme, Schnittstellendefinitionen
  TLS, Backups, Datenbanken, Firmware ...
- Jetzt: Hybrid – später Ersetzen: Prä- und Post-QC kombinieren (z.b. tunneln oder überschlüsseln)
- Kryptoagilität: Algorithmen und Cipher-Suiten austauschbar einbinden
- Data at Rest und Data in Motion: Datenbanken, Dateisysteme, Storage, Backups, VPNs, SSH, QUIC, WebRTC, Zertifikate, HSM
- Hardwaretoken: FIDO2 Passkeys, Yubikey, Nitrokey, Token2 ...
- Entwicklung: Frameworks und Bibliotheken beobachten, Interoperabilität überwachen, Schlüssel rotierbar halten
- Maßnahmenplan: Compliance erfordert Migrationspläne mit Umsetzungsplan *jetzt*!

cryptomancer.de

Fragen?

- https://www.cryptomancer.de/posts/kryptokalypse/
- https://cryptomancer.de/pqcbenchmark/
- https://cryptomancer.de/posts/20260418kryptokalypse-artikel/
- https://fediverse.cryptomancer.de/cryptomancer
- https://mastodon.social/@0xKaishakunin *deprecating*
- 7B2B 45B1 330E 579E 3C3E 9B34 089D 8068 8050 ECCF
- public [at] cryptomancer [dot] de

cryptomancer.de

Fragen?

- https://www.cryptomancer.de/posts/kryptokalypse/
- https://cryptomancer.de/pqcbenchmark/
- https://cryptomancer.de/posts/20260418kryptokalypse-artikel/
- https://fediverse.cryptomancer.de/cryptomancer
- https://mastodon.social/@0xKaishakunin *deprecating*
- 7B2B 45B1 330E 579E 3C3E 9B34 089D 8068 8050 ECCF
- public [at] cryptomancer [dot] de

cryptomancer.de

BSI TR I

- https://github.com/gematik/ecc-brainpool-how-to
- [7] *Migration zu Post-Quanten-Kryptografie. Handlungsempfehlungen des BSI*
- [8] *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*
- [9] *Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)*
- [10] *Kryptographische Verfahren: Verwendung von Secure Shell (SSH)*
- [11] *Kryptographische Verfahren: X.509 Zertifikate und Zertifizierungspfadvalidierung*
- [12] *TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government: Vertrauensniveaus und Mechanismen*
- [13] *Elliptic Curve Cryptography*

BSI TR II

- [14] *TR-03116-4 Kryptographische Vorgaben für Projekte der Bundesregierung: Kommunikationsverfahren in Anwendungen*
- [15] *TR-03124-1eID-Client – Part 1: Specifications*
- [16] *TR-03175 Infrastruktur zur Absicherung von Dokumenten mit digitalen Siegeln*
- [17] *Certificate Policy 2024: Root-CA der PKI-1-Verwaltung*

Literatur I

[1] „Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 203,“ 2024. besucht am 17. Aug. 2025. Adresse: https://doi.org/10.6028/NIST.FIPS.203

[2] „Module-Lattice-Based Digital Signature Standard, FIPS 204,“ 2024. besucht am 17. Aug. 2025. Adresse: https://doi.org/10.6028/NIST.FIPS.204

[3] „Stateless Hash-Based Digital Signature Standard, FIPS 205,“ 2024. besucht am 17. Aug. 2025. Adresse: https://doi.org/10.6028/NIST.FIPS.205

Literatur II

[4] „Recommendation for Stateful Hash-Based Signature Schemes, NIST Special Publication 800-208,“ 2020. besucht am 19. Aug. 2025. Adresse: https://doi.org/10.6028/NIST.SP.800-208

[5] I. Duits, „The post-quantum Signal protocol: Secure chat in a quantum world,“ Magisterarb., University of Twente, 2019.

[6] A. Alkhulaifi und E.-S. M. El-Alfy, „Exploring Lattice-based Post-Quantum Signature for JWT Authentication: Review and Case Study,“ in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, S. 1–5. DOI: 10.1109/VTC2020-Spring48590.2020.9129505

Literatur III

[7] „Migration zu Post-Quanten-Kryptografie. Handlungsempfehlungen des BSI,“ 2020-08-01. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=1

[8] „Kryptographische Verfahren: Empfehlungen und Schlüssellängen,“ 2024-02-02. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=5

Literatur IV

[9] „Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS),“ Technische Richtlinie des BSI, 2024-01. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=4

[10] „Kryptographische Verfahren: Verwendung von Secure Shell (SSH),“ Technische Richtlinie des BSI, 2024-02-29. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.pdf?__blob=publicationFile&v=3

Literatur V

[11] „Kryptographische Verfahren: X.509 Zertifikate und Zertifizierungspfadvalidierung,“ Technische Richtlinie des BSI, 2020. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02103/BSI-TR-02103.pdf?__blob=publicationFile&v=2

[12] „TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government: Vertrauensniveaus und Mechanismen,“ Technische Richtlinie des BSI, 2019-05-07. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf?__blob=publicationFile&v=1

cryptomancer.de

Literatur VI

[13] „Elliptic Curve Cryptography,“ 2018-06-01. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.pdf?__blob=publicationFile&v=1

[14] „TR-03116-4 Kryptographische Vorgaben für Projekte der Bundesregierung: Kommunikationsverfahren in Anwendungen,“ Technische Richtlinie des BSI, 2023-03-07. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf?__blob=publicationFile&v=5

Literatur VII

[15] „TR-03124-1eID-Client – Part 1: Specifications,“ Technische Richtlinie des BSI, 2021-10-08. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03124/TR-03124-1.pdf?__blob=publicationFile&v=2

[16] „TR-03175 Infrastruktur zur Absicherung von Dokumenten mit digitalen Siegeln,“ Technische Richtlinie des BSI, 2022-05-13. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03175/BSI-TR-03175.pdf?__blob=publicationFile&v=4

Literatur VIII

[17] „Certificate Policy 2024: Root-CA der PKI-1-Verwaltung,“ 2024-12-31. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/VerwaltungsPKI/Certificate_Policy_2024.pdf?__blob=publicationFile&v=3