Die Kryptokalypse

Post-Quanten-Kryptographie und Open Source Software

Stefan Schumacher

cryptomancer.de

Kieler Open Source und Linux-Tage 2025

$ Id: Kryptokalypse-Input.tex,v 1.35 2025/09/17 15:27:02 stefan Exp $

Inhaltsverzeichnis

1. Einführung
2. Grundlagen
3. Quantencomputer
4. Quantenschlüsselaustausch
5. Quantensichere Algorithmen
6. Stand der Dinge im FLOSSiversum (9/2025)
7. 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
- jetzt Sicherheitsarchitekt bei einem öffentlichen IT-Dienstleister

cryptomancer.de

Über mich

einige Vorträge zum Thema

- CCC2004: Einführung in die Kryptographie
- CLT2004: Anwendung kryptographischer Programme am Beispiel von NetBSD
- CLT2008: Sichere Passwörter
- CLT2011: Kryptographische Dateisysteme im Detail
- CLT2015: Abhörsichere Internet-Telefonie mit OSTN und OSTEL
- CLT2016: Zwei-Faktor-Authentifizierung mit Yubikeys
- CLT2019: Kryptographische Dateisysteme im professionellen Umfeld
- CLT2023: Die Matrix-Verschlüsselung näher betrachtet
- CLT2024: Sichere Datenhaltung und Backup in der Cloud
- CLT2025: Passwortlose Logins mit PassKeys

Über mich

- [1] S. Schumacher, *Einführung in kryptographische Methoden*, 2004. besucht am 19. Apr. 2004. Adresse: `http://www.cryptomancer.de/21c3/21c3-kryptographie-paper.pdf`
- [2] S. Schumacher, „Kryptographische Dateisysteme im Detail,“ in *Chemnitzer Linux-Tage 2011, Tagungsband*, (Technische Universität Chemnitz), Team der Chemnitzer Linux-Tage, Hrsg., Chemnitz: Universitätsverlag, 2011, S. 39–46. Adresse: `https://monarch.qucosa.de/api/qucosa%3A19466/attachment/ATT-0/`
- [3] S. Schumacher, „Zwei-Faktor-Authentifizierung mit Yubikey-Token, Ein kostengünstiges Verfahren,“ *UpTimes*, S. 16–27, 2 2018, ISSN: 1860-7683. besucht am 1. Feb. 2019. Adresse: `https://www.guug.de/uptimes/2018-2/uptimes_2018-02.pdf`

Inhaltsverzeichnis

1 Einführung

2 Grundlagen

3 Quantencomputer

4 Quantenschlüsselaustausch

5 Quantensichere Algorithmen

6 Stand der Dinge im FLOSSiversum (9/2025)

7 Was ist zu tun?

cryptomancer.de

Glossar

- Glossar samt Formelzeichen und Literatur im Handout
- https://www.cryptomancer.de/kryptokalypse/

One Time Pads / Einmalschlüssel

- polyalphabetisches Substitutionsverfahren
- einmalige Verwendung eines kryptographisch zufälligen Schlüssels der gleichen Länge wie m
- k_s muss geheim bleiben, darf nicht wiederverwendet werden
- informationstheoretisch perfekt sicher $\rightsquigarrow$ kann nicht gebrochen werden [4]
- verwandt mit Stromchiffre
- Genutzt u.a. ab 1921 im Auswärtigen Amt als *i-Wurm* im Block-Verfahren [5]
- Für große Datenmengen derzeit nicht praktikabel (k_s >= m)
- https://www.cryptomancer.de/posts/20000713enigmac/

Asymmetrische Kryptographie

- Schlüsselpaar aus privatem und öffentlichem Schlüssel
- Prinzip:
  - Zufallszahl würfeln $\rightsquigarrow$
  - Schlüsselgenerierungsoperation durchführen $\rightsquigarrow k_s + k_p$
  - k_p veröffentlichen
- Anforderungen: Zufallszahl ist möglichst zufällig und groß, Schlüsselgenerierungsoperation ist nicht umkehrbar
- Vorteile: Schlüsselaustausch muss nicht geheimgehalten werden, digitale Signaturen möglich
- Schlüsselgenerierungsoperation: Primfaktoren, diskreter Logarithmus in endlichen Körpern, diskreter Logarithmus in elliptischen Kurven

Asymmetrische Kryptographie

RSA-Challenge

2009: RSA-768 (768 Bit) in 2000 CPU-Jahren auf 2.2GHz-Opteron-CPU

```
123018668453011775513049495838496272077285356959533479219 7
322452151726400507263657518745202199786469389956474942774 0
638459251925573263034537315482685079170261221429134616704 2
921431160222124047927473779408066535141959745985690214341 3
                                =
334780716989568987860441698482126908177047949837137685689 1
243138898288379387800228761471165253174308773781446799948 9
                                *
367460436667995904282446337996279526322791581643430876426 7
603228381573966651127923337341714339681027009279873630891 7
```

Asymmetrische Kryptographie

Key Encapsulation Mechanism (KEM)

Signifikant langsamer als symmetrische Kryptographie (>Faktor 1000)

- 256 Bit Sitzungsschlüssel x zufallsgenerieren
- m mit Sitzungsschlüssel symmetrisch verschlüsseln $c_1 = Enc_x(m)$
- Sitzungsschlüssel ggf. auffüllen
- Sitzungsschlüssel mit öffentlichem RSA/ECC/ElGamal-Schlüssel k verschlüsseln $c_2 = Enc_k(x)$
- Chiffrat und verschlüsselten Sitzungsschlüssel verschicken $c = c_1 \oplus c_2$

Keine Perfect-Forward-Secrecy! $\rightsquigarrow$ ECDHE

Asymmetrische Kryptographie

Key Encapsulation Mechanism (KEM)

Signifikant langsamer als symmetrische Kryptographie (>Faktor 1000)

- 256 Bit Sitzungsschlüssel x zufallsgenerieren
- m mit Sitzungsschlüssel symmetrisch verschlüsseln $c_1 = Enc_x(m)$
- Sitzungsschlüssel ggf. auffüllen
- Sitzungsschlüssel mit öffentlichem RSA/ECC/ElGamal-Schlüssel k verschlüsseln $c_2 = Enc_k(x)$
- Chiffrat und verschlüsselten Sitzungsschlüssel verschicken $c = c_1 \oplus c_2$

Keine Perfect-Forward-Secrecy! $\rightsquigarrow$ ECDHE

Inhaltsverzeichnis

1 Einführung

2 Grundlagen

3 Quantencomputer

4 Quantenschlüsselaustausch

5 Quantensichere Algorithmen

6 Stand der Dinge im FLOSSiversum (9/2025)

7 Was ist zu tun?

Quantencomputer

- Paul Benioff & Richard Feynman ab 1980 [6], [7], [8]
- arbeiten mit geeigneten quantenmechanischen Systemen
- Superpositionszustände und Quantenverschränkung
- Quantenverschränkung: zusammengesetztes System nimmt einen wohldefinierten Zustand ein, ohne dass man jedem Teilsystem einen wohldefinierten Zustand zuordnen kann [9]
- Quantenparallelismus: mehrere Operationen gleichzeitig ausführen
- Qubit: Quanten-Bit $\rightsquigarrow 2^n$ sicher unterscheidbare (messbare) Zustände
- In der Theorie: 50 Qubits zum Brechen von RSA nötig
- In der Realität: 2022: 433 Qubits (2^{433} Zustände) gebaut [10]

Quantencomputer

- Quantenrauschen: systematische Messfehler
- Laser-Interferometer-Gravitationswellen-Observatorium: 40Kg schwere Spiegel des Gravitationswellen-Detektors um $10^{-20}m$ verschoben $\widehat{=}$ 100 Milliardstel Wasserstoff-Atomdurchmesser [11]
- Quantencomputer kann klassischen Computer simulieren und umgekehrt
- Quanten-Turing-Maschine und Quanten-Komplexität analog zur klassischen Komplexität [12], [13]
- Quantenüberlegenheit: Zeitpunkt, ab dem ein Quantencomputer Probleme lösen kann, die ein klassischer Computer nicht in realisierbarer Zeit lösen kann

Shor-Algorithmus

- Faktorisierungsverfahren, probabilistisch, Monte-Carlo-Algorithmus [14]
- berechnet einen nichttrivialen Teiler einer zusammengesetzten Zahl
- polynomielle Laufzeit für Primfaktorzerlegung und zur Berechnung des diskreten Logarithmus
- Schätzung: Brechung von RSA2048 ca. 10 bis 100 Millionen Qubits benötigt [15]
- Shors Algorithmus versagt für hinreichend große Primfaktoren durch Quantenrauschen fast sicher [16]

cryptomancer.de

Grovers Algorithmus

- Suche in unsortierter Datenbank in $\mathcal{O}\left(\sqrt{N}\right)$
- z.B. erschöpfende Suche des Schlüsselraumes, Kollisionsangriff, Urbild-Angriffe
- quadratische Beschleunigung gegenüber $\mathcal{O}\left(N\right)$
- signifikante Beschleunigung für sehr große $\mathcal{N}$ [17]
- Sicherheitsniveau symmetrischer Verfahren wird ca. halbiert: AES-128 $\rightsquigarrow$ AES-64
- c.f. Pollard-Rho-Methode

cryptomancer.de

Inhaltsverzeichnis

1 Einführung

2 Grundlagen

3 Quantencomputer

4 Quantenschlüsselaustausch

5 Quantensichere Algorithmen

6 Stand der Dinge im FLOSSiversum (9/2025)

7 Was ist zu tun?

cryptomancer.de

Quantenschlüsselaustausch

informationstheoretisch sicher

- stellt Alice und Bob eine Zufallszahl als k_s zur Verfügung
- nutzt quantenmechanische Kohärenz zur Absicherung
- Messung: Verschränkung mit dem Messapparat $\rightsquigarrow$ Veränderung der Messung [18]
- Abhörvorgänge werden immer bemerkt, d.h. k_s wird verworfen
- macht One-Time-Pads praktikabel (verifizierbar sicher)
- Implementierung z.B. im BB84-Protokoll [19]
- 2017: Satellitenübertragung zwischen Wien und Peking gelungen
  in 2 großen Forschungslabors
- Zukunftsmusik ...
- Wir brauchen neue asymmetrische Krypto-Systeme
- Post-Quanten-Kryptographie [20]
- Sofort! (Migration dauert siehe DES $\rightsquigarrow$ 3DES $\rightsquigarrow$AES, Hardwareimplementierungen? IoT?)

cryptomancer.de

Quantenschlüsselaustausch

informationstheoretisch sicher

- stellt Alice und Bob eine Zufallszahl als k_s zur Verfügung
- nutzt quantenmechanische Kohärenz zur Absicherung
- Messung: Verschränkung mit dem Messapparat $\rightsquigarrow$ Veränderung der Messung [18]
- Abhörvorgänge werden immer bemerkt, d.h. k_s wird verworfen
- macht One-Time-Pads praktikabel (verifizierbar sicher)
- Implementierung z.B. im BB84-Protokoll [19]
- 2017: Satellitenübertragung zwischen Wien und Peking gelungen in 2 großen Forschungslabors
- Zukunftsmusik ...
- Wir brauchen neue asymmetrische Krypto-Systeme
- Post-Quanten-Kryptographie [20]
- Sofort! (Migration dauert siehe DES $\rightsquigarrow$ 3DES $\rightsquigarrow$AES, Hardwareimplementierungen? IoT?)

cryptomancer.de

Inhaltsverzeichnis

1 Einführung

2 Grundlagen

3 Quantencomputer

4 Quantenschlüsselaustausch

5 Quantensichere Algorithmen

6 Stand der Dinge im FLOSSiversum (9/2025)

7 Was ist zu tun?

Symmetrische Verfahren

- Sicherheitsniveau durch Grover halbiert
- Verdoppelung der Schlüsselgrößen
- derzeit empfohlenes Sicherheitsniveau: 120 Bit
- Schlüsselgrößen größer 240
- geeignete elliptische Kurven auswählen
- Brainpool 384/521, SecP 384/521, SecT 409/571

Standardisierungsprozess

- US NIST startet Standardisierungsprozess auf der PQCrypto 2016
- offener Standardisierungsprozess von AES 1997-2000 als Vorbild
- nach der Kritik am DES/3DES-Standardisierngsprozess 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 [21], [22], [23], [24]
- 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

Standardisierungsprozess

- US NIST startet Standardisierungsprozess auf der PQCrypto 2016
- offener Standardisierungsprozess von AES 1997-2000 als Vorbild
- nach der Kritik am DES/3DES-Standardisierngsprozess 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 [21], [22], [23], [24]
- 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

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

ML-KEM:	512	768	1024	RSA:	3072	7680	X25519
security level	128	192	256		128	192	192
C	768	1088	1568				
K_p	1632	1184	1568		625	1405	119
K_s	800	2400	3168		2484	6002	113

Vergleich mit ECDH/Curve25519: [25]

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

https://www.cryptomancer.de/pqcbenchmark

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 Grundlagen

3 Quantencomputer

4 Quantenschlüsselaustausch

5 Quantensichere Algorithmen

6 Stand der Dinge im FLOSSiversum (9/2025)

7 Was ist zu tun?

X.509-Zertifikate, JWT

- X.509-Zertifikate: 7. Draft offen bis Mitte Dezember 2025, ML-KEM Identifiers Draft offen bis Januar 2026
- OIDs für Algorithmen enthalten diverse hybride Verfahren
- `https://pkic.org/pqccm/` PKI PQC Capabilities Matrix
- JWT: Ebenfalls noch kein neuer Standard vorhanden [26]
- FIDO2 (Passkeys): IANA CBOR Object Signing and Encryption (COSE) und JSON Object Signing and Encryption (JOSE): ML-DSA aufgenommen

TLS1.3

- TLS1.3 führt 3 neue Hybridverfahren ein
  X25519MLKEM768, SecP256r1MLKEM768, SecP384r1MLKEM1024
- derzeit nur X25519MLKEM768 als Gruppe in OpenSSL unterstützt
- alle aktuellen Desktop-Browser unterstützen X25519MLKEM768
- auf iOS noch nicht unterstützt
- Android: Chrome ja, Firefox nein
- 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

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

OpenSSH/GnuPG

- OpenSSH 10: `mlkem768x25519-sha256` als Standard-KEX
- GnuPG: u.a. Brainpool512 und NIST P521
  - LibrePGP: Alternativer *Standard* zu OpenPGP (RFC 4880)
  - ML-KEM-768+BrainpoolP256r1 und ML-KEM-1024+BrainpoolP384r1
- Yubico Yubikeys / Nitrokey3: u.a. Brainpool512 und NIST P521, Token2: NIST P521

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`

Inhaltsverzeichnis

1 Einführung

2 Grundlagen

3 Quantencomputer

4 Quantenschlüsselaustausch

5 Quantensichere Algorithmen

6 Stand der Dinge im FLOSSiversum (9/2025)

7 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*!

Fragen?

- cryptomancer.de
- kaishakunin.com
- `https://mastodon.social/@0xKaishakunin`
- 7B2B 45B1 330E 579E 3C3E 9B34 089D 8068 8050 ECCF
- Matrix: @SchumaSte:matrix.org

BSI TR I

- https://github.com/gematik/ecc-brainpool-how-to
- [27] *Migration zu Post-Quanten-Kryptografie. Handlungsempfehlungen des BSI*
- [28] *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*
- [29] *Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)*
- [30] *Kryptographische Verfahren: Verwendung von Secure Shell (SSH)*
- [31] *Kryptographische Verfahren: X.509 Zertifikate und Zertifizierungspfadvalidierung*
- [32] *TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government: Vertrauensniveaus und Mechanismen*
- [33] *Elliptic Curve Cryptography*
- [34] *TR-03116-4 Kryptographische Vorgaben für Projekte der Bundesregierung: Kommunikationsverfahren in Anwendungen*
- [35] *TR-03124-1eID-Client – Part 1: Specifications*
- [36] *TR-03175 Infrastruktur zur Absicherung von Dokumenten mit digitalen Siegeln*
- [37] *Certificate Policy 2024: Root-CA der PKI-1-Verwaltung*

cryptomancer.de

Literatur I

[1] S. Schumacher, *Einführung in kryptographische Methoden*, 2004. besucht am 19. Apr. 2004. Adresse: http://www.cryptomancer.de/21c3/21c3-kryptographie-paper.pdf.

[2] S. Schumacher, „Kryptographische Dateisysteme im Detail,“ in *Chemnitzer Linux-Tage 2011, Tagungsband*, (Technische Universität Chemnitz), Team der Chemnitzer Linux-Tage, Hrsg., Chemnitz: Universitätsverlag, 2011, S. 39–46. Adresse: https://monarch.qucosa.de/api/qucosa%3A19466/attachment/ATT-0/.

[3] S. Schumacher, „Zwei-Faktor-Authentifizierung mit Yubikey-Token, Ein kostengünstiges Verfahren,“ *UpTimes*, S. 16–27, 2 2018, ISSN: 1860-7683. besucht am 1. Feb. 2019. Adresse: https://www.guug.de/uptimes/2018-2/uptimes_2018-02.pdf.

Literatur II

[4] W. A. Halang und R. Fitz, „Informationstheoretisch sichere Datenverschlüsselung,“ in *Nicht hackbare Rechner und nicht brechbare Kryptographie*, Springer, 2018, S. 147–156.

[5] F. Weierud und S. Zabell, „German mathematicians and cryptology in WWII,“ *Cryptologia*, Jg. 44, Nr. 2, S. 97–171, 2020.

[6] 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*, Jg. 22, Nr. 5, S. 563–591, 1980.

[7] P. A. Benioff, „Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: Application to Turing machines,“ *International Journal of Theoretical Physics*, Jg. 21, Nr. 3, S. 177–201, 1982.

[8] R. P. Feynman, „Quantum mechanical computers.,“ *Found. Phys.*, Jg. 16, Nr. 6, S. 507–532, 1986.

Literatur III

[9] A. Einstein, B. Podolsky und N. Rosen, „Can quantum-mechanical description of physical reality be considered complete?“ *Physical review*, Jg. 47, Nr. 10, S. 777, 1935.

[10] J. Preskill, *Quantum computing and the entanglement frontier*, 2012. arXiv: 1203.5813 [quant-ph]. Adresse: https://arxiv.org/abs/1203.5813.

[11] H. Yu, L. McCuller, M. Tse, N. Kijbunchoo, L. Barsotti und N. Mavalvala, „Quantum correlations between light and the kilogram-mass mirrors of LIGO,“ *Nature*, Jg. 583, Nr. 7814, S. 43–47, 2020.

[12] D. Deutsch, „Quantum theory, the Church–Turing principle and the universal quantum computer,“ *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, Jg. 400, Nr. 1818, S. 97–117, 1985.

[13] E. Bernstein und U. Vazirani, „Quantum complexity theory,“ in *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, 1993, S. 11–20.

Literatur IV

[14] P. W. Shor, „Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,“ *SIAM Journal on Computing*, Jg. 26, Nr. 5, S. 1484–1509, Okt. 1997, ISSN: 1095-7111. DOI: 10.1137/s0097539795293172. Adresse: http://dx.doi.org/10.1137/S0097539795293172.

[15] C. Gidney und M. Ekerå, „How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,“ *Quantum*, Jg. 5, S. 433, Apr. 2021, ISSN: 2521-327X. DOI: 10.22331/q-2021-04-15-433. Adresse: http://dx.doi.org/10.22331/q-2021-04-15-433.

[16] J.-Y. Cai, „Shor’s algorithm does not factor large integers in the presence of noise,“ *Science China Information Sciences*, Jg. 67, Nr. 7, Juni 2024, ISSN: 1869-1919. DOI: 10.1007/s11432-023-3961-3. Adresse: http://dx.doi.org/10.1007/s11432-023-3961-3.

Literatur V

[17] 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, S. 212–219.

[18] J. Von Neumann, „Mathematische Grundlagen der Quantenmechanik,“, 1932. Adresse: https://gdz.sub.uni-goettingen.de/id/PPN379400774.

[19] C. H. Bennett und G. Brassard, „An update on quantum cryptography,“ in *Workshop on the theory and application of cryptographic techniques*, Springer, 1984, S. 475–480.

[20] J. Buchmann u. a., „Post-quantum signatures,“ *Cryptology ePrint Archive*, 2004. Adresse: https://eprint.iacr.org/2004/297.pdf.

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

Literatur VI

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

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

[24] „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.

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

[26] 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.

cryptomancer.de

Literatur VII

[27] „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.

[28] „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.

[29] „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.

Literatur VIII

[30] „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.

[31] „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.

Literatur IX

[32] „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.

[33] „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.

[34] „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.

cryptomancer.de

Literatur X

[35] „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.

[36] „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.

[37] „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.