Rainer W. Gerling
Datenschutz und IT-Sicherheit

HM

Web-Server mit quantensicherer Verschlüsselung betreiben

Prof. Dr. Rainer W. Gerling
https://www.rainer-gerling.de

33. DFN-Konferenz „Sicherheit in vernetzten Systemen“
Hamburg, 27. Januar 2026

Rainer W. Gerling
Datenschutz und IT-Sicherheit

HM

Wann wird es einen kryptographisch relevanten Quantencomputer (CRQC) geben?

- „Damit ist es wahrscheinlich, dass selbst ohne Disruptionen ein krypotanalytisch relevanter Quantencomputer in höchstens 16 Jahre realisierbar ist “
  (BSI, Entwicklungsstand Quantencomputer, Deutsche Zusammenfassung, Version 2.1, August 2024)

- Kölsches Risikomanagement:

  Et hätt noch emmer joot jejange.
  (Es ist noch immer gut gegangen.)

  ist suboptimal.

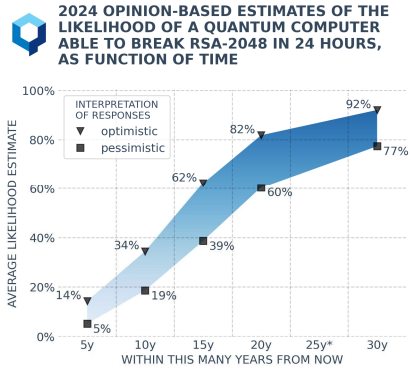


Abb.: Quantum Threat Timeline Report 2024, Global Risk Institute, Dezember 2024

- **Besser jetzt vorbereiten!**

Rainer W. Gerling
Datenschutz und IT-Sicherheit

HM

Wo setzen wir Verschlüsselung ein?

- Digitale Signaturen
  - Banking, Verträge, E-Mail-S…
  - Umstellu… benötigen
  - PKI-Strukturen müssen angepasst werden
- Schlüsselvereinbarung (Data in Motion) und Schlüsselspeicherung (Key Wrapping; Data at Rest)
  - Basiert meist auf den gleichen Algorithmen wie Digitale Signaturen
  - Umstellung ist standardisiert und durchführbar
  - Keine PKI-Anpassungen erforderlich!
- Speicherung und Übertragung verschlüsselter Daten
  - Data at Rest: Festplatten, USB-Sticks, Cloud-Speicher, …
  - Data in Motion: https, E-Mail-Verschlüsselung, …
  - Angriff: **Harvest now, decrypt later** (Jetzt sammeln, später entschlüsseln)

Der lange Weg zur quantenresistenten PKI
Knobloch/Freising, 32. DFN Konferenz 2025

Rainer W. Gerling
Datenschutz und IT-Sicherheit

HM

Post-Quanten-Kryptographie

- Man muss auf die mögliche Bedrohung der Sicherheit durch Quantencomputer vorbereitet sein.
- Verschlüsselungsalgorithmen, die mit Quantencomputern nicht gebrochen werden können, werden als Post-Quanten-Kryptographie (PQK oder PQC) bezeichnet.
- In den USA sind einige Standardisierungsprozesse für PQC beim NIST bereits abgeschlossen:
  - FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard (Kyber, 13.8.2024)
  - FIPS 204 Module-Lattice-Based Digital Signature Standard (Dilithium, 13.8.2024)
  - FIPS 205 Stateless Hash-Based Digital Signature Standard (Sphincs+, 13.8.2024)
  - FIPS 206 *Falcon Digital Signature Standard* (Falcon, für Ende 2025 angekündigt)
  - *FIPS 207 HQC Key-Encapsulation Mechanism Standard (HQC, 2026?)*
    - Backup für FIPS 203, falls ML-KEM gebrochen wird (NIST, 11.3.2025)

Schlüsselvereinbarung/Key Wrapping; Digitale Signaturen

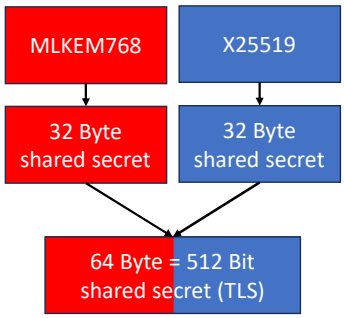
Rainer W. Gerling
Datenschutz und IT-Sicherheit

HM

Sicher ist sicher

- Wenn wir jetzt die neuen PQC-Algorithmen einführen und die werden dann geknackt … ☹
- Deshalb wurden die Hybriden Verfahren definiert: ein klassischer und ein PQC-Algorithmus werden kombiniert: wird einer geknackt, schützt der andere!
  - Klassisch: Curve 25519 ; PQC: ML-KEM oder NTRU Prime
  - Für TLS 1.3 und für SSH in RFC-Entwürfen standardisiert

Erstellt mit ChatGPT



 Web-Server mit quantensicherer Verschlüsselung betreiben 5

Rainer W. Gerling
Datenschutz und IT-Sicherheit

HM

Unterstützung von PQC (Auswahl)

- Browser: Firefox 132+, Chrome 131+, Safari 26+, Edge 131+, TOR Browser 15+, aktueller Opera und Brave, … (ML-KEM)
- Webserver: Apache, NGINX, lighttpd, node.js, Caddy, … (ML-KEM)
- Anwendungen: OpenSSL 3.5.0+ (ML-KEM, ML-DSA und SLH-DAS), OpenSSH* 9.8+, Putty 0.83+, Winscp 6.4.2+, (ML-KEM, NTRU Prime) GnuPG 2.5.16+ (ML-KEM)
- Apple: ab iOS 26, iPadOS 26, macOS Tahoe 26 und visionOS 26
  - Unterstützen TLS 1.3 mit ML-KEM
- Google: Android 15+ (ML-KEM)

- Kleiner Test: HM👍, TUM👎, LMU👎, DFN👎, DFN-cert👎, Google👍, Amazon👎, Cloudflare👍

*Windows erst ab OpenSSH 10.0

 Web-Server mit quantensicherer Verschlüsselung betreiben 6

Rainer W. Gerling
Datenschutz und IT-Sicherheit

HM

Test (TLS 1.3 mit ML-KEM)

- MacOS: `nscurl --tls-diagnostics https://rainer-gerling.de`
- Windows*/Linux: `openssl s_client -brief -connect rainer-gerling.de:443`
- Qualys SSL Labs: noch nicht ☹
- testssl.sh: ja ☺ (mit Version 3.2.2 getestet)

```
Connecting to 217.154.78.54
CONNECTION ESTABLISHED
Protocol version: TLSv1.3
Ciphersuite: TLS_AES_256_GCM_SHA384
Peer certificate: CN=rainer-gerling.de
Hash used: SHA256
Signature type: ecdsa_secp256r1_sha256
Verification: OK
Negotiated TLS1.3 group: X25519MLKEM768
```

```
============================================================

Negotiated TLS version (codepoint): 0x0304
Negotiated TLS key exchange group (name): X25519MLKEM768
Negotiated TLS ciphersuite (codepoint): 0x1302

============================================================
```

Android 13/14 (native)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Android 15 (native)	TLSv1.3	TLS_AES_128_GCM_SHA256	X25519MLKEM768
Chrome 101 (Win 10)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Chromium 137 (Win 11)	TLSv1.3	TLS_AES_128_GCM_SHA256	X25519MLKEM768
Firefox 100 (Win 10)	TLSv1.3	TLS_AES_128_GCM_SHA256	253 bit ECDH (X25519)
Firefox 137 (Win 11)	TLSv1.3	TLS_AES_128_GCM_SHA256	X25519MLKEM768
IE 8 Win 7	No connection		
IE 11 Win 7	TLSv1.2	ECDHE-ECDSA-AES256-GCM-SHA384	256 bit ECDH (P-256)
IE 11 Win 8.1	TLSv1.2	ECDHE-ECDSA-AES256-GCM-SHA384	256 bit ECDH (P-256)

*OpenSSL muss für Windows erst installiert werden: `winget install openssl`

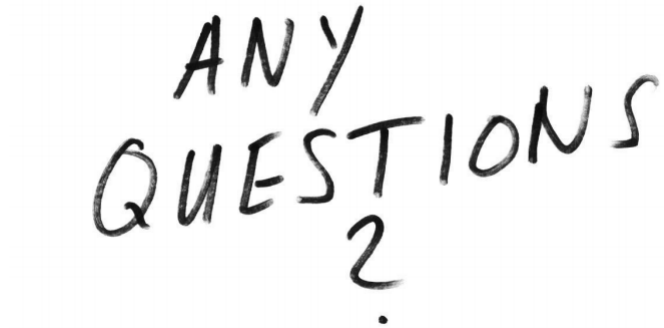
Rainer W. Gerling
Datenschutz und IT-Sicherheit

HM

Mögliche Probleme

- TLS 1.3 ist erforderlich
- IPv6: kein Problem
- Direkte Verbindung Klient-Server: kein Problem
- Firewall:
  - bei „deep packet inspection“ möglicherweise Unterstützung erforderlich, da sich der TLS-Handshake beim Aufbau der Verbindung ändert
  - Die Datenpakete beim TLS-Handshake beim Aufbau der Verbindung werden deutlich größer -> Fragmentierung der IP-Pakete
- „Middle-Boxen“ zur Kontrolle der verschlüsselten Inhalte müssen u.U. angepasst werden.
- Proxy-Server müssen u.U. angepasst werden

Rainer W. Gerling
Datenschutz und IT-Sicherheit



Weitere Info: https://tipps4it.de/PQC

Rainer W. Gerling
Datenschutz und IT-Sicherheit

WEB-Server Konfiguration

- Apache
  - In Datei: `/etc/apache2/mods-enabled/ssl.conf`
  - ```
    SSLProtocol           -all +TLSv1.2 +TLSv1.3
    SSLOpenSSLConfCmd     Curves X25519MLKEM768:X25519:X448:prime256v1:secp384r1
    ```
- Lighttpd (1.79) mit OpenSSL (3.5.4)
  - In Datei: `/etc/lighttpd/conf-enabled/10-ssl.conf`
  - ```
    ssl.openssl.ssl-conf-cmd = ("MinProtocol" => "TLSv1.2")
    ssl.openssl.ssl-conf-cmd += ("Curves" => "X25519MLKEM768:X25519:X448:prime256v1;secp384r1“)
    ```
- NGINX (1.29.x) mit OpenSSL (3.5.x)
  - ```
    ssl_protocols      TLSv1.2 TLSv1.3;
    ssl_conf_command   Curves "X25519MLKEM768:X25519:X448:prime256v1:secp384r1";
    ```
- …


    ```