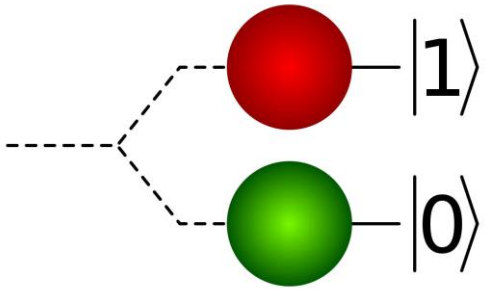
Fazit

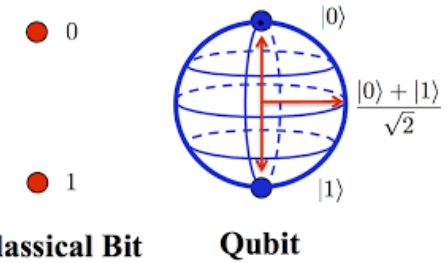
Paul Schöbi

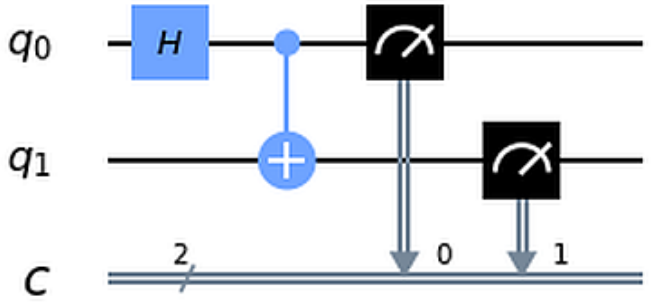
cnlab Herbsttagung 2023: Bits & Qubits
Gleisarena, Zürich, 6. September 2023

cnlab

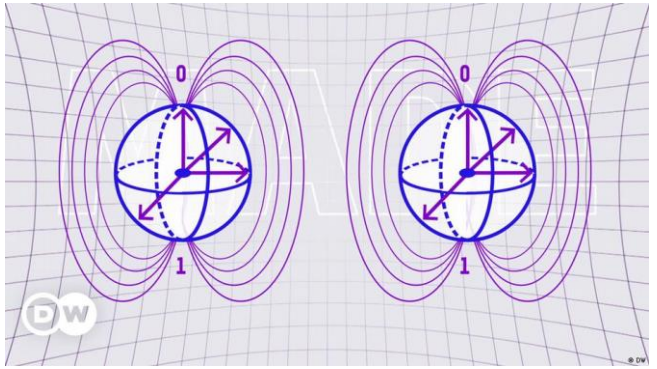
Qubits

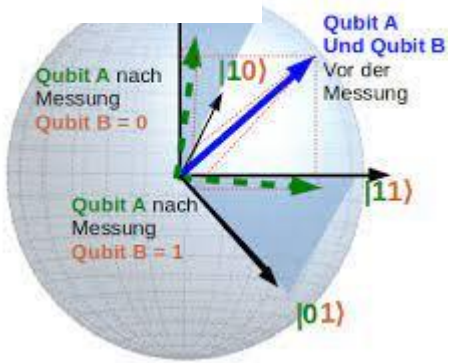




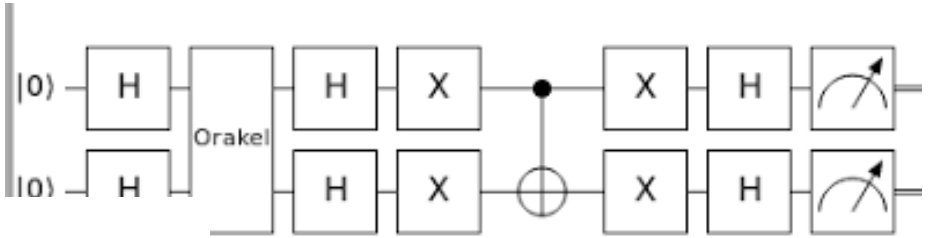


$$|\Phi\rangle\langle\Psi|$$





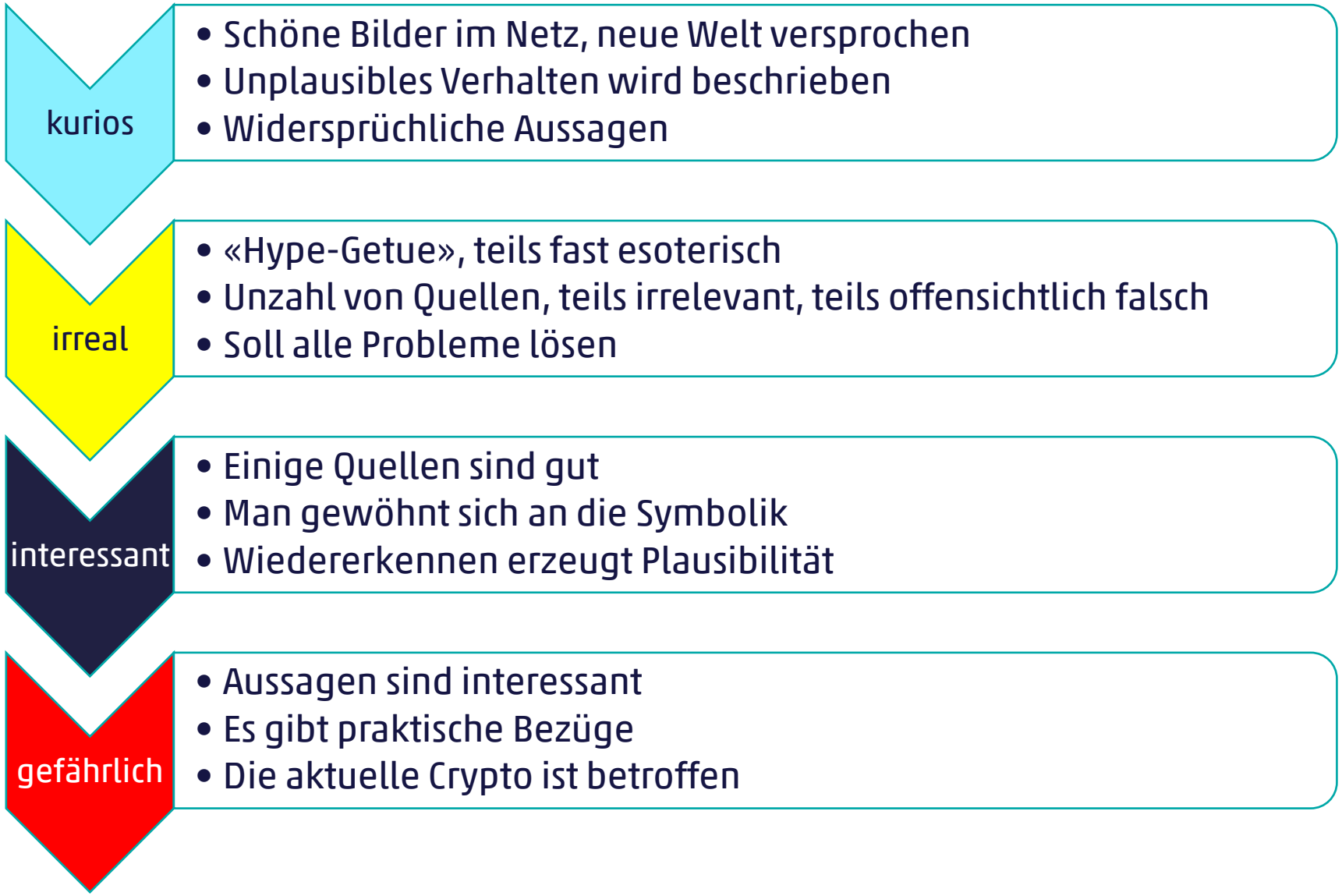
$$\langle\psi_1|\psi_2\rangle = \int_{-\infty}^{\infty} \psi_1^* \psi_2 dx$$



$$\langle A|\alpha = \begin{bmatrix} A_1 & A_2 & A_3 \end{bmatrix} \begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{bmatrix}$$

$$= \begin{bmatrix} A_1\alpha_{11} + A_2\alpha_{21} + A_3\alpha_{31} & A_1\alpha_{12} + A_2\alpha_{22} + A_3\alpha_{32} & A_1\alpha_{13} + A_2\alpha_{23} + A_3\alpha_{33} \end{bmatrix}$$

Qubits: Zugang



Interpellation: Quantensichere Systeme beim Bund (14.6.2023)

Die Bundesversammlung — Das Schweizer Parlament

Die Forschung zu Quantencomputing macht derzeit grosse Fortschritte. Zwar lässt sich heute nicht vorhersagen, wann der Durchbruch leistungsfähiger resp. stabiler Quantencomputer bevorsteht, aber einig ist man sich über die damit zusammenhängenden neuen Sicherheitsprobleme. Gewisse Verschlüsselungstechnologie werden für Angriffe von Quantencomputern im grossen Stil angreifbar werden, und es wird vermutet, dass Kriminelle bereits heute verschlüsselte Daten stehlen, um sie dereinst mit Quantentechnologie zu entschlüsseln (steal now, decrypt later). In diesem Zusammenhang wird der Bundesrat gebeten, folgende Fragen zu beantworten:

1. Hat sich der Bundesrat mit den Gefahren des Quantencomputings für die verschlüsselten Daten der Verwaltung und Behörden, inkl. der Armee, der Staatsbetriebe und systemkritischer Institutionen wie etwa die SNB auseinandergesetzt?
2. In welchen Bereichen identifiziert der Bundesrat Handlungsbedarf in Zusammenhang mit dieser Gefahr?
3. Ist der Bundesrat bereit, die derzeit eingesetzte Technologien resp. Datenbestände und Systeme auf quantensichere Standards zu prüfen resp. grundsätzlich darauf auszurichten?
4. In welchem Zeitrahmen plant der Bundesrat diese Prüfung resp. Umstellung?

BELLAICHE JUDITH

Grünliberale Fraktion
Grünliberale Partei

https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20233689

14.06.2023

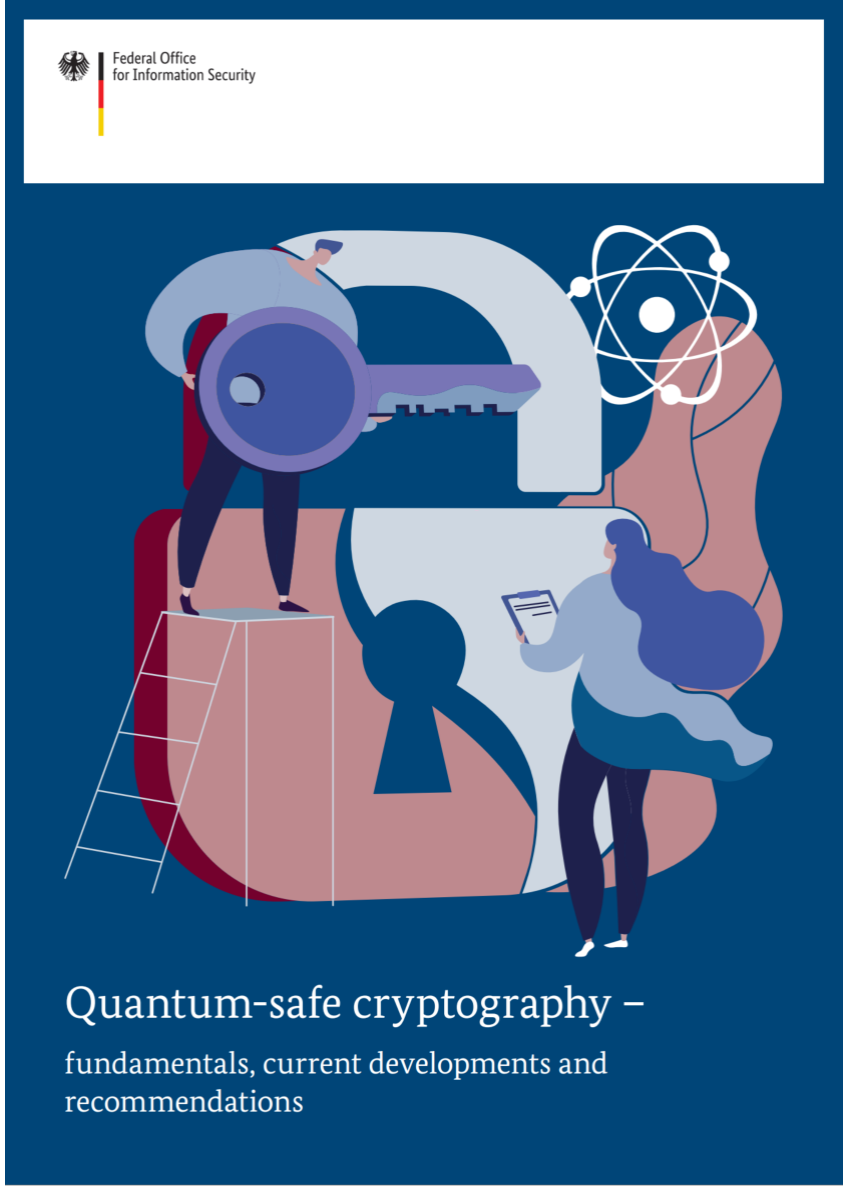
Stellungnahme des Bundesrats (23.8.2023)

- Risiko bewusst
- Empfehlung für GEHEIM-klassifizierte Daten seit 2014 (symmetrische Verfahren)
- Spezifisches Monitoring ab 2023
- Teilnahme am Auswahlprozess zur Standardisierung von Post-Quanten-Kryptografie (NIST)
- Prüfung der Standards vorgesehen

https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20233689

BSI-Empfehlungen

1. Preparation
2. Cryptographic agility
3. Short-term protective measures
4. Key lengths for symmetric encryption
5. Hybrid solutions
6. Post-quantum algorithms for key agreement
7. Hash-based signature schemes for firmware updates
8. General signature schemes for authentication
9. Adaption of cryptographic protcols
10. Migration to quantum-safe public key infrastructure
11. Recommendations for quantum key distribution
12. Migration to post-quantum cryptography has priority over the use of QKD
13. Need for further research on quantum-safe cryptography



BSI: Der «Preparation»-Schritt

The first step before migration is a survey of the existing situation and the development of a migration plan. This should include answering the following questions:

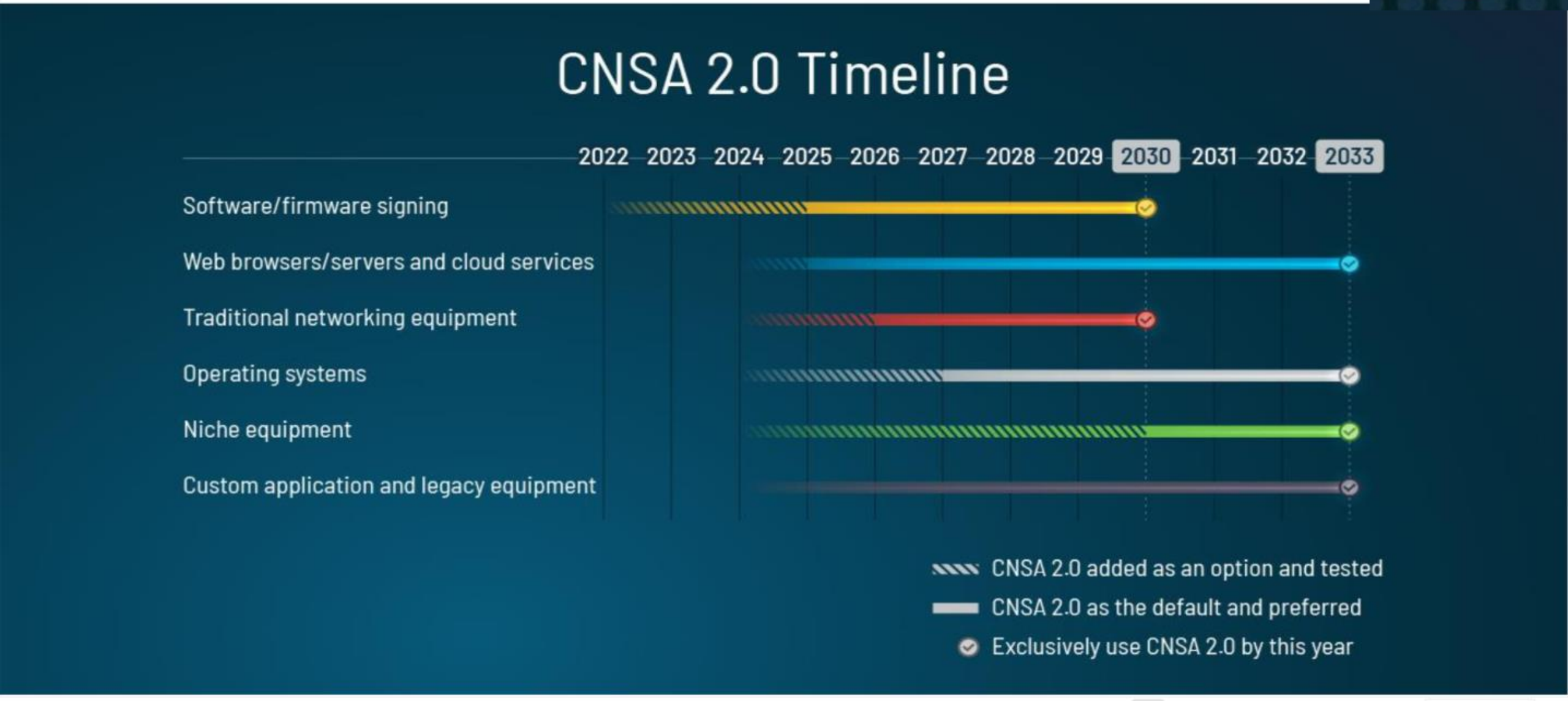
- What cryptographic algorithms or products are used in my organization?
- How critical is the data that is being processed and how long is its lifespan?
- Where is there an immediate need for action?
- Do the protocols used need to be adapted?
- Are there already solutions for this?
- ...

NIST: Quantum-Readiness: Migration to Post-Quantum Cryptography (17.8.2023)

- ESTABLISH A QUANTUM-READINESS ROADMAP
- PREPARE A CRYPTOGRAPHIC INVENTORY
- DISCUSS POST-QUANTUM ROADMAPS WITH TECHNOLOGY VENDORS CRYPTOGRAPHIC INVENTORY
- SUPPLY CHAIN QUANTUM-READINESS
- TECHNOLOGY VENDOR RESPONSIBILITIES

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

NSA: Commercial National Security Algorithm Suite (CNSA)



Es läuft schon einiges

- … As a step down this path, Chrome will begin supporting X25519Kyber768 for establishing symmetric secrets in TLS, starting in Chrome 116, and available behind a flag in Chrome 115…

  https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html

- .. the first quantum resilient FIDO2 security key implementation as part of OpenSK, our open source security key firmware ..

  https://security.googleblog.com/2023/08/toward-quantum-resilient-security-keys.html

Cnlab-Empfehlungen für kommerzielle Anwender

Das ist **jetzt** fällig (2023)

Kritische Daten

in 10 Jahren noch heikel, exponiert

- Daten identifizieren
- Krypto-Mechanismen analysieren
- Mechanismen anpassen
- Daten neu chiffrieren
- alte Kopien löschen

Vertrauliches

Personendaten, Kundendaten

- Standard-Produkte aktuell halten,
- Spezialentwicklungen PQ-sicher bauen

Wichtige Signaturen

In 10 Jahren noch relevant

- Daten identifizieren
- Sichere Timestamps setzen

Vielen Dank für Ihre Aufmerksamkeit_

Paul Schöbi

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

cnlab