T.I.S.P./T.P.S.S.E. Community Meeting 2024

Berlin, 05. – 06.11.2024

Quantum-sichere Verschlüsselung:

Beispiele praktischer Anwendungen - Das Warum, Wie und Wann für eine sichere digitale Kommunikation

Dietmar Wyhs, SSH (Communications Security Oyj)

SSH - Deja Vu

- 1995: Inventor of the SSH protocol
- 2020: 

customer implementation of PQC
- Certified vendor 4 PQC
  - Traficom NCSA-FI Level III
  - NATO

Gartner Top-Ten Trends 2025

von Michael Cooney
Senior Editor

Gartner's Top-Ten: Die wichtigsten Technologietrends für 2025

News
23 Oktober 2024 • 9 Minuten
Big Data

Agentic AI, Post-Quantum-Kryptografie, KI-Governance und Hybrid-Computing gehören laut Gartner zu den dringlichsten und potenziell disruptivsten Trends, mit denen Unternehmen ab 2025 konfrontiert sind.

4. Post-Quanten-Kryptographie

Gartner prognostiziert, dass bis 2029 die meisten herkömmlichen asymmetrischen Kryptographieverfahren aufgrund von Fortschritten im Quantencomputing nicht mehr sicher genug sein werden. Dies unterstreiche die Bedeutung der Post-Quanten-Kryptographie, die einen Datenschutz bietet, der den Entschlüsselungsrisiken von Quantencomputern standhält.

Timeline: PKI Crypto vs Quantum Computers

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

RSA
1977

The first public-key cryptosystem

Quantum computer concept
1980

Quantum computer as a purely theoretical concept

Quantum computer live
1998

The first live Quantum computer with 2 qubits

Quantum threat
2025?

Quantum computers capable of breaking RSA

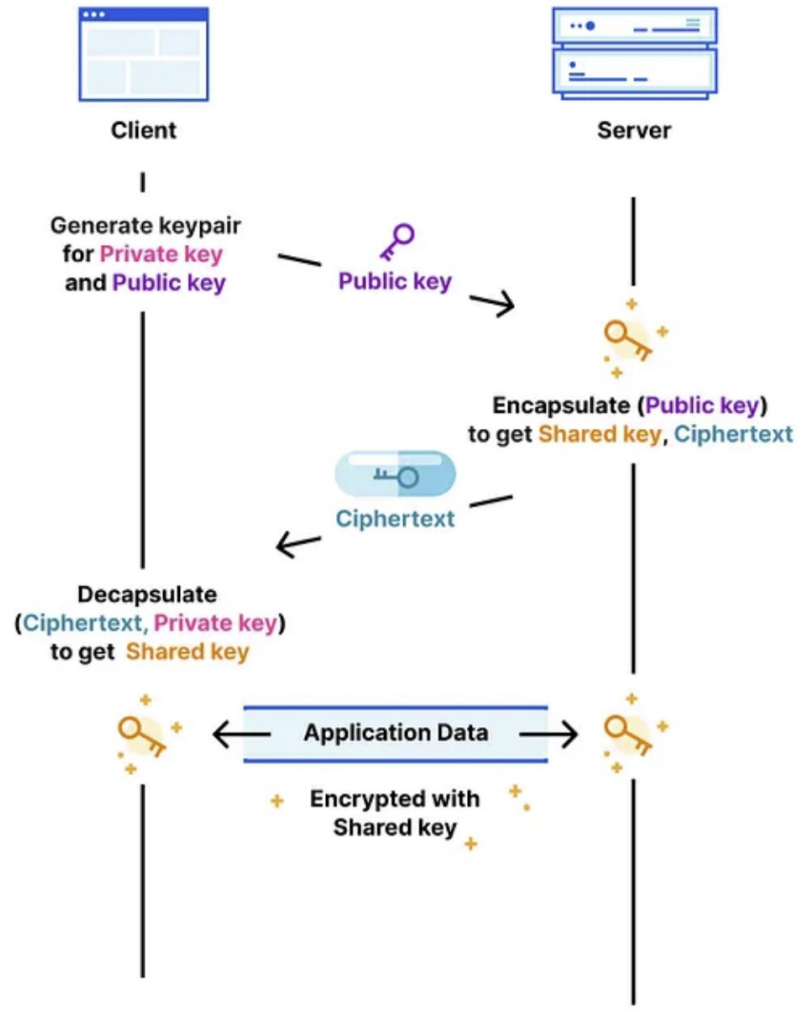
- Public-key cryptosystems predate even the concept of Quantum Computers.
  ⟶ They are obsolete by design to survive during the Quantum Age!

The key problem is the “KEY” problem !

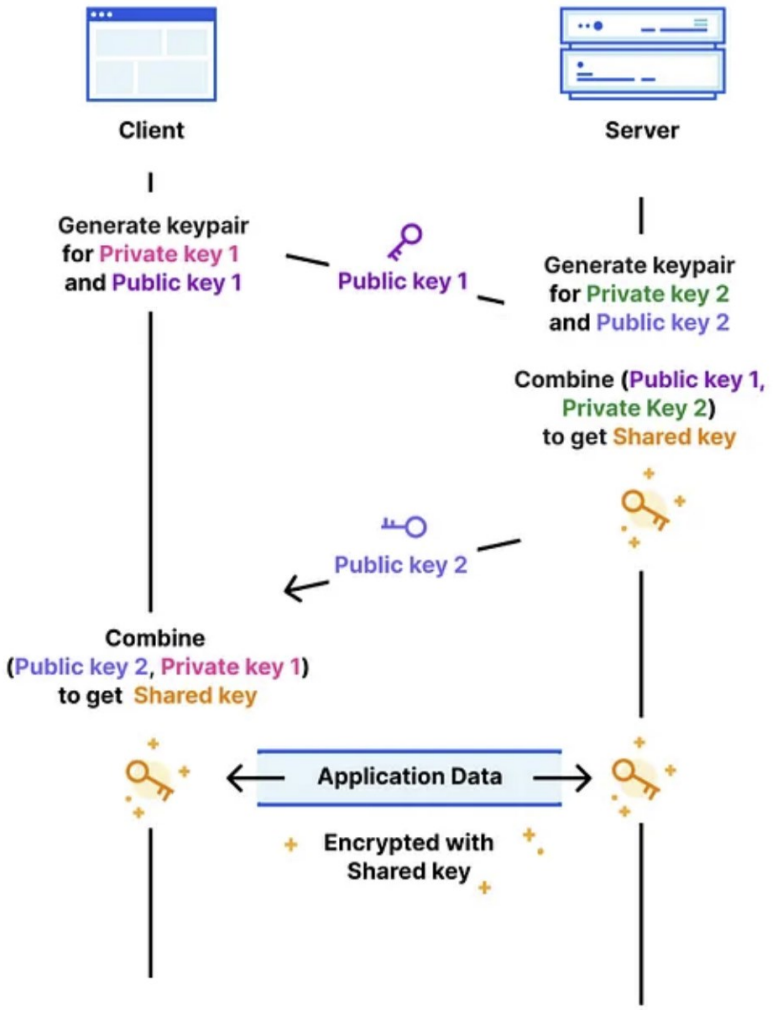
- Public-Key Cryptography
  - Cornerstone of modern cryptosystems and protocols since the late 70’s
  - Not just encryption, also authentication
  - Public-private key pairs:
    - Encryption, by anyone, with the recipient’s public key
    - Decryption, by the recipient, with his/her private key
  - Examples: RSA, Diffie-Hellman
  - Every connection begins with an asymmetrically encrypted key exchange, followed by the payload symmetrically encrypted with the exchanged key
    - Symmetric encryption examples: AES, Poly1305

Graphical examples of Key Exchange (KEX)

Key Encapsulation Mechanism (KEM)

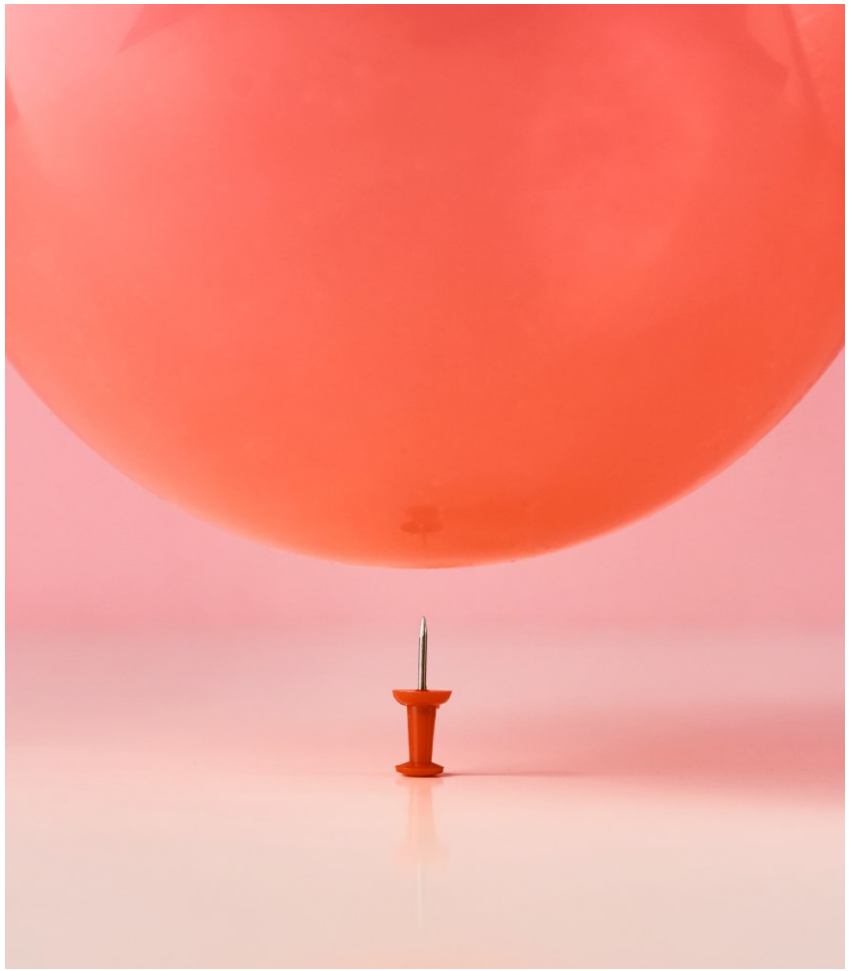


Diffie–Hellman (DH)



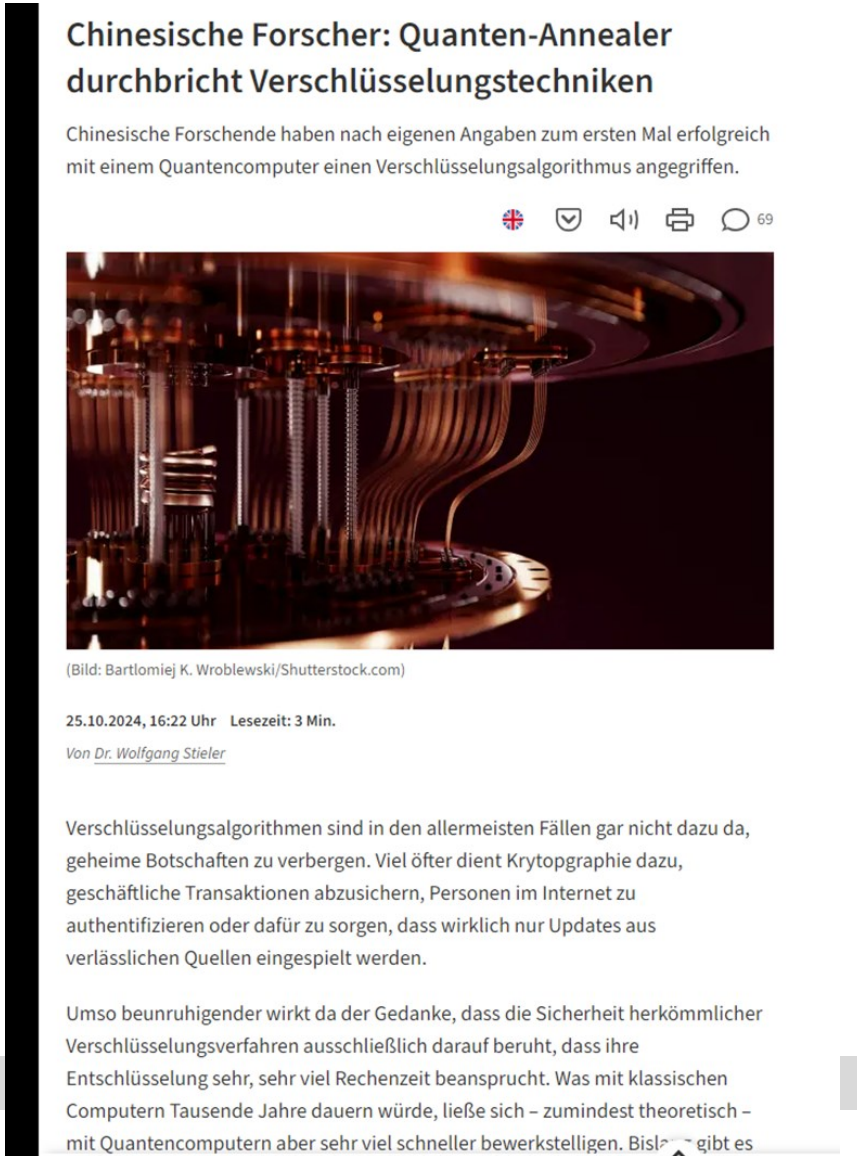
Key-Exchange in Danger

- The asymmetric key exchange is very vulnerable towards prime factoring with Shor's algorithm
- The symmetric payload encryption, and other parts of the protocol, are much less vulnerable
- However, compromising the key exchange will also compromise the payload, since the key for the symmetric payload encryption is now known!
- Grover's alg. –> Symmetric Key Cryptosystems



How acute is the threat?

- Quantum computer processing power is measured in qubits
- The number of quantum bits with multiple possible simultaneous states that can be processed within one calculation
- Currently most powerful computers have ~1000 qubits
- A quantum computer with +4000 (“high-fidelity”) qubits could theoretically break RSA-2408 within seconds
- Quantum annealing algorithms running on classical computers can dramatically lower this limit
- Estimates on the threat timeline vary from 2 to 20 years
- However, the potential of recording attacks means the Quantum Threat is acute during the present day!



Chinesische Forscher: Quanten-Annealer durchbricht Verschlüsselungstechniken

Chinesische Forschende haben nach eigenen Angaben zum ersten Mal erfolgreich mit einem Quantencomputer einen Verschlüsselungsalgorithmus angegriffen.

69

(Bild: Bartlomiej K. Wroblewski/Shutterstock.com)

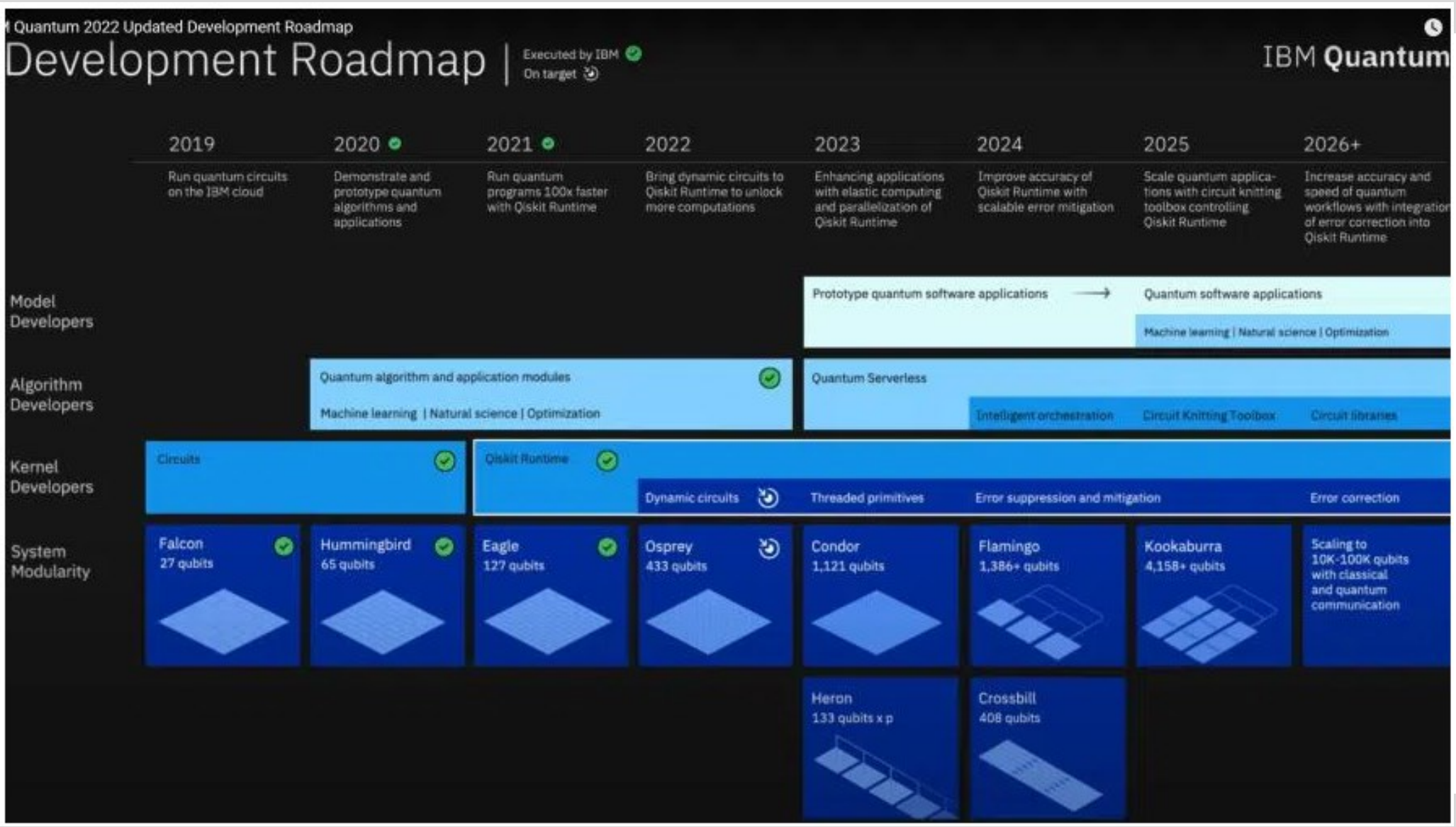
25.10.2024, 16:22 Uhr Lesezeit: 3 Min.

Von Dr. Wolfgang Stieler

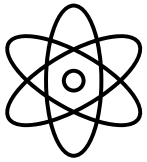
Verschlüsselungsalgorithmen sind in den allermeisten Fällen gar nicht dazu da, geheime Botschaften zu verbergen. Viel öfter dient Krytopgraphie dazu, geschäftliche Transaktionen abzusichern, Personen im Internet zu authentifizieren oder dafür zu sorgen, dass wirklich nur Updates aus verlässlichen Quellen eingespielt werden.

Umso beunruhigender wirkt da der Gedanke, dass die Sicherheit herkömmlicher Verschlüsselungsverfahren ausschließlich darauf beruht, dass ihre Entschlüsselung sehr, sehr viel Rechenzeit beansprucht. Was mit klassischen Computern Tausende Jahre dauern würde, ließe sich – zumindest theoretisch – mit Quantencomputern aber sehr viel schneller bewerkstelligen. Bisl… gibt es

Why PQC now? Store/Steal Now, Decrypt Later!



Game plan is going to change



2010	2015	2019	2020	2022	2023	2025
IBM QC	27 Qubits	65 Qubits	433 Qubits	1121 Qubits	4158 Qubits	
2048 Bit RSA key estimated 1 billion Qubits required to break RSA key	**2048 Bit RSA key** Could be cracked in 8 hours Require 20 million noisy Qubits, new mathematical method (modular exponentiation).			Cracking PKC key would require ~2x modulus length high fidelity Qubits	Quantum software applications. Open-source platforms.	

RSA 232 bit Key cracked

Breaking the key took 2000 computing Core years

RSA 240 bit Key cracked

12/2019

900 computing core years. breaking the key used thousands computers simultaneously. Enhancement with new algorithms 3-4 time faster..

RSA 250 bit Key cracked

2/2020

2700 computing core years. breaking the key used several distributed systems. – tens of thousands cores.

You don’t need new fiber cables to be Quantum Safe

- Quantum Cryptography
  - Utilizes novel quantum mechanical phenomena for security
  - Designed to be tamper proof
  - Requires heavy infrastructure investment and special quantum processing hardware (including a dedicated fiber cable or optical link)
  - Infeasible for most practical use cases

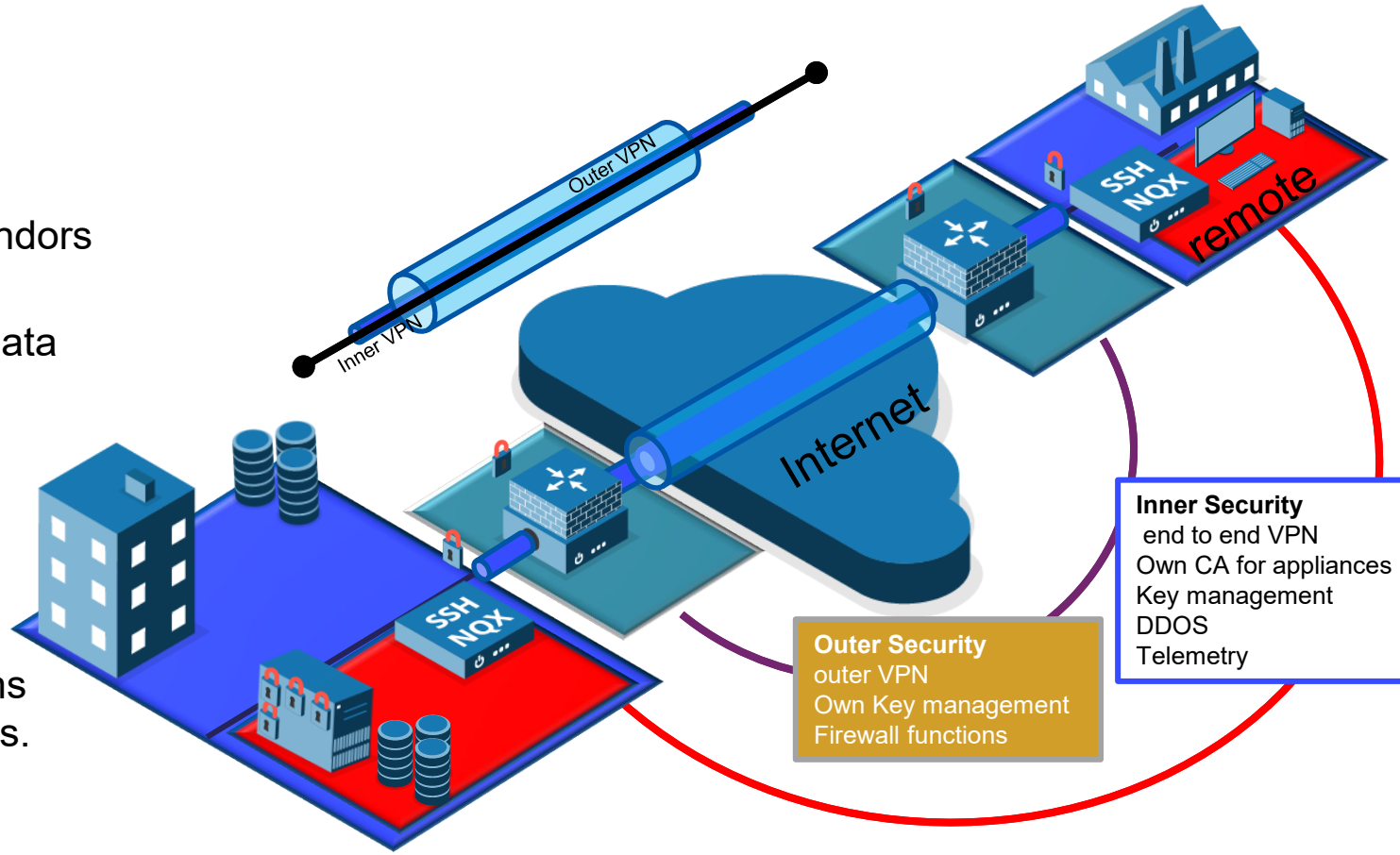
- Post-Quantum Cryptography
  - Utilizes existing communication protocols and networks
  - Affordable and easy to take into use
  - Most likely, this is what you are looking for!

Post-quantum algorithms overview

- NIST (US): Hybrid Encryption: Crystals-Kyber (ML-KEM) + ECDH
  - Backup: FireSaber
  - BTW: Crystals-Dilithium for Digital Signatures (ML-DAS)
- BSI (Germany): FrodoKEM
- Crypto agility: Post-Quantum algorithms are ongoing rapid development. As a user of PQC you should always have the most relevant algorithms in use by default!

Tiered encryption for transporting classified data

- Tiered encryption
  - Encryption procedures made in separate entities
  - Solution is required to utilize separate vendors or at least the sec libraries need differ
  - Use different SW / algorithms to secure data even case of breach in one system
- Secure service availability
  - DDoS resiliency and rule functionalities required on both tiers
- Separate security functions
  - One use case is to separate FW functions and strong encrypted VPN on own entities.
    - Performance advantage
    - Reduce complexity



U.S. NSA Commercial solutions Multi Site Connectivity capability package define procedure to transport classified data over untrusted networks.

PQC use cases and benefits

- Remote access, nomadic and mobile sites
  - Mobile 4G and 5G as transport, nomadic devices or fixed-wireless
  - Vehicles with 12 VDC power source, usage temperature from -10 to +50ºC
  - “Wearable Device” on the way
- Data should be “secure 4 ever”
  - Military
  - Public Departments (e.g. Department of Foreign Affairs & Embassy)
  - Finance
  - Healthcare
  - Critical Infrastructure
  - “Long Term IPR” (e.g. Aero-Space, Automotive, ….)
- USA
  - Quantum Cybersecurity Preparedness Act (21. Dec. 2022)
    - Law H.R.7535 to: “federal government agencies to adopt technology that will protect against quantum computing attacks.”

Thank you for your questions (with disclaimer)