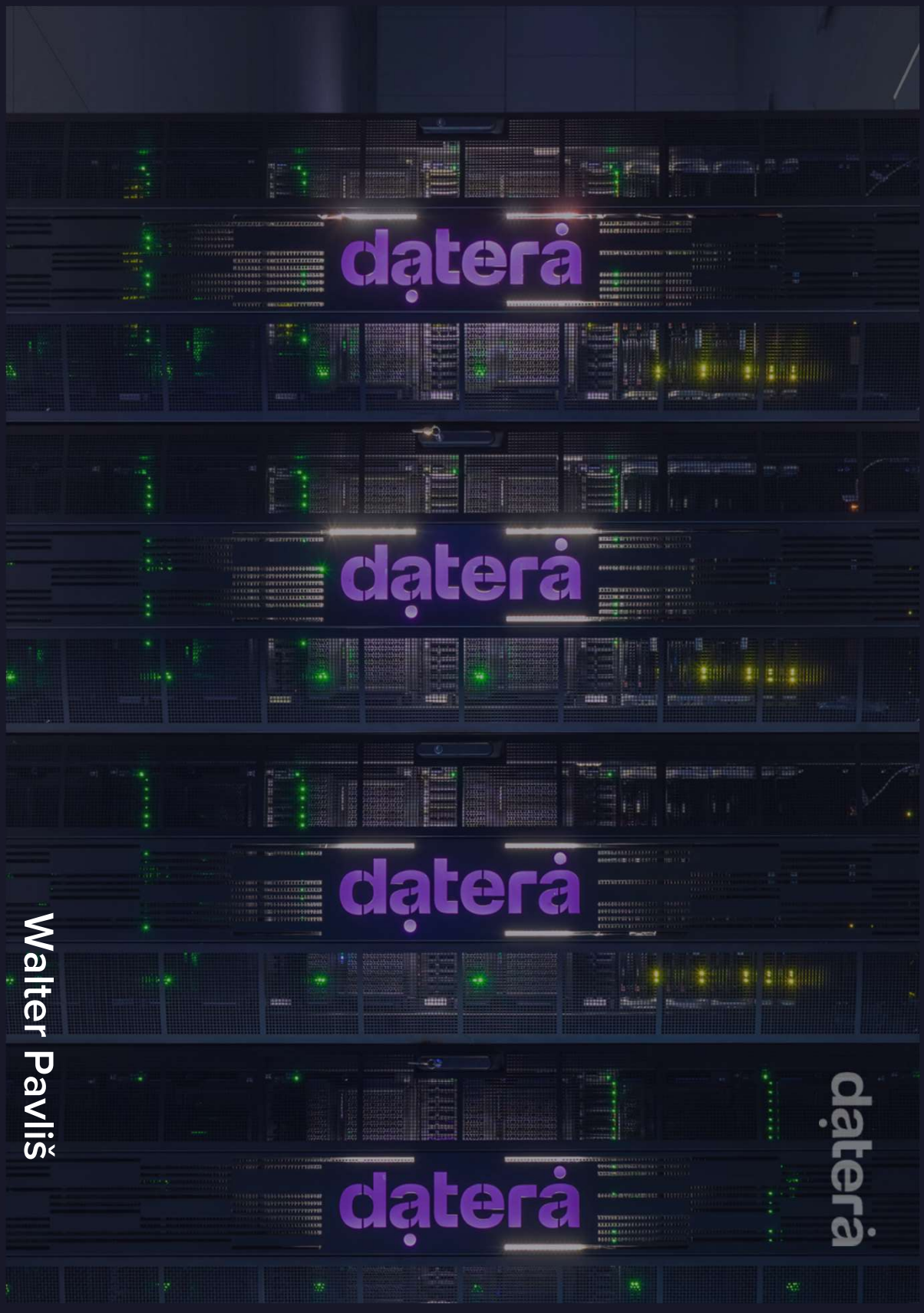
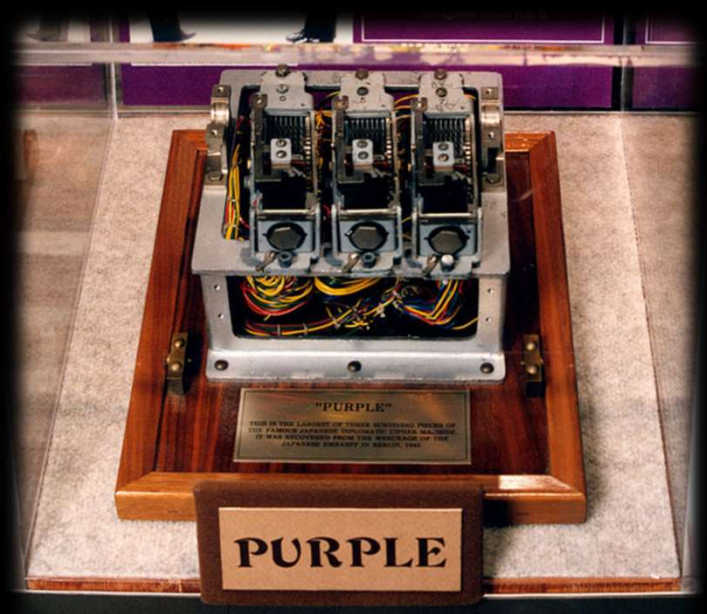
QUANTUM SAFE



Walter Pavliš

Poučení z historie

- Japonská šifra PURPLE byla prolomena již v roce 1940.
- V březnu 1941 o tom Japonsko informoval přes německé diplomaty velvyslanec Sovětského svazu v USA Umansky.
- Japonská reakce.
- Prolomení šifry JN-25 - útok u atolu Midway.
- Německá Enigma - podobný příběh.



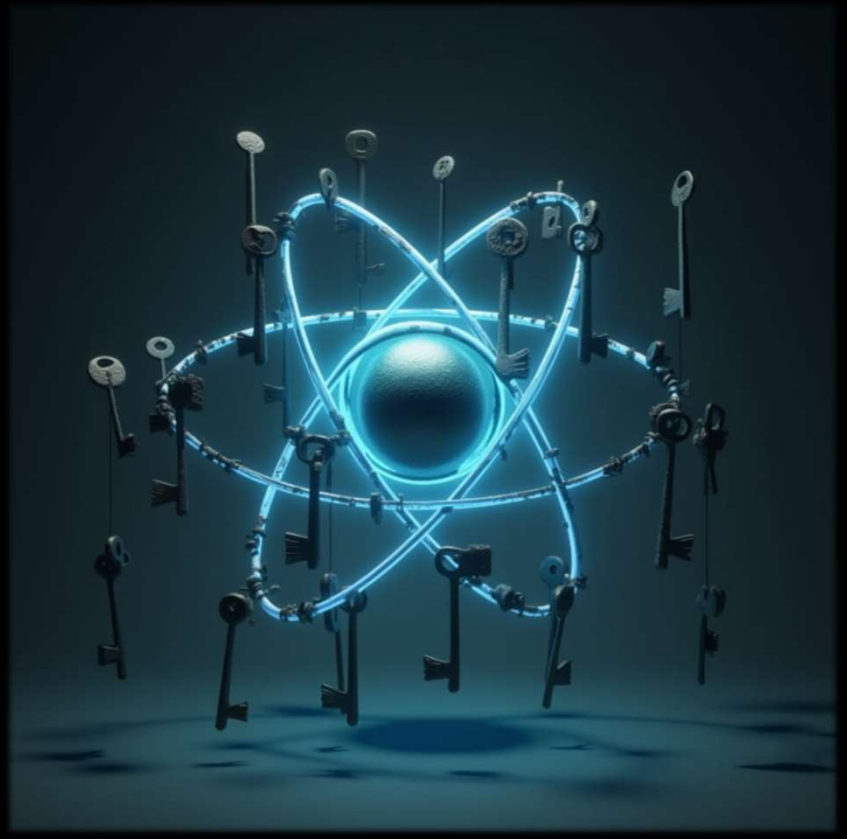
Příchod kvantových počítačů

Kvantové počítače představují hrozbu pro současnou kryptografii, která je základem bezpečnosti digitálního světa.

- Kvantové počítače využívají kvantové jevy k provádění výpočtů, které jsou pro klasické počítače nemožné.

- Tyto schopnosti umožňují kvantovým počítačům prolomit stávající kryptografické algoritmy, jako je RSA, v řádu hodin, zatímco klasickým počítačům by to trvalo miliony let.

- Hrozba pro širokou škálu oblastí, jako jsou online bankovnictví, elektronické obchodování a důvěrná komunikace.

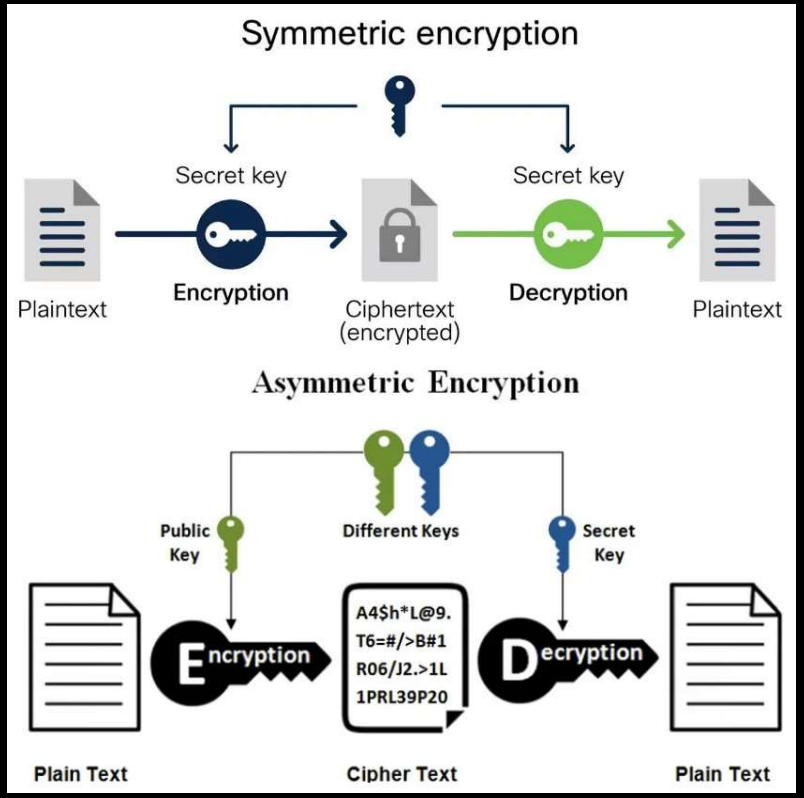


datera

Kvantová hrozba

- Peter Shor kvantový algoritmus.
- Hrozba pro asymetrické algoritmy.

- Kryptoanalyticky relevantní kvantový počítač.



Kde hrozí nebezpečí

Internetové protokoly

Služba DNS (Domain Name Service), Hyper-text Transfer Protocol (HTTP), Telnet, SFTP

Kritická infrastruktura

Řídicí systémy KI, ropovody, elektrické sítě; automobilové systémy,...

Blockchainové aplikace

Kryptoměnové peněženky, Transakce, Autentizace

Digitální podpisy

EiDAS - PDF pokročilý elektronický podpis – (PAdES), zaručené elektronické podpisy (AES), ...

Finanční systémy

Platební systémy (EMV, SWIFT, vypořádací systémy, FinTech, ...)

Podnikové aplikace

EMAIL – PGP, Identity Management PKI/LDAP/.., Antivirové vzory, PKI služby

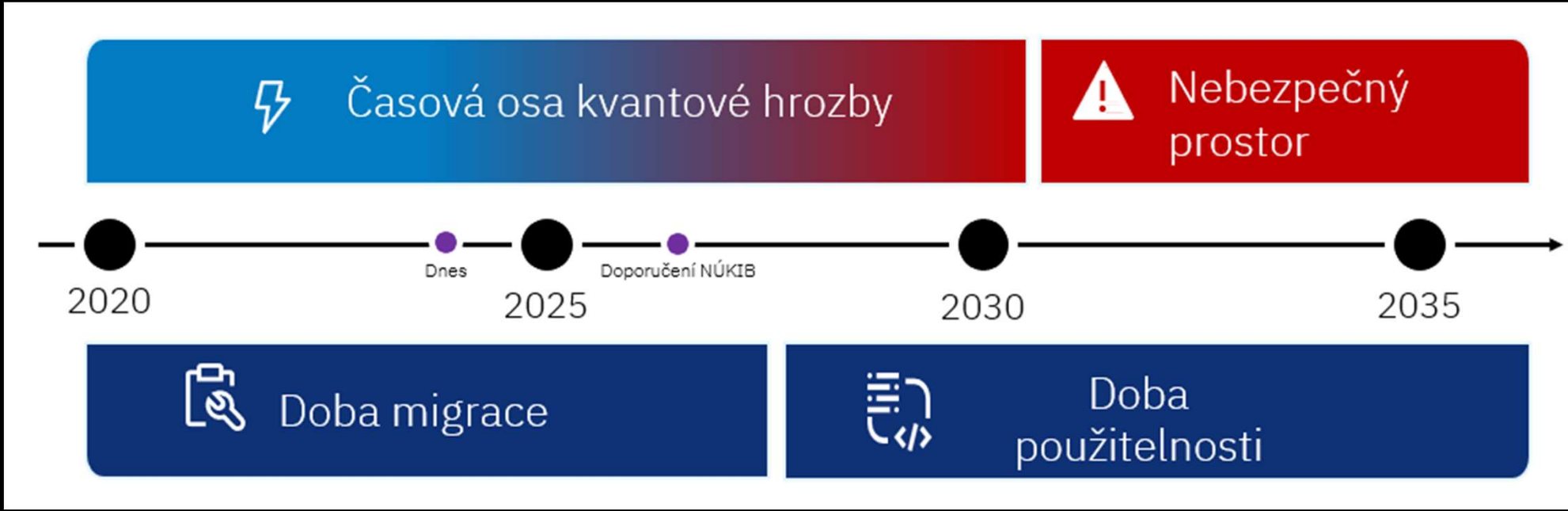
datera

Co nám hrozí a co s tím?

- Sklízejte dnes, dešifrujte později
- Migrace bude trvat dlouho
- NÚKIB – dokument o kvantové hrozbě
- Přechod na kvantově odolné algoritmy

datera

Kdy začít?



datera

Post-Quantum Cryptography

- Quantum-safe cryptography (QSC),Post-Quantum Cryptography (PQC)
- V letech 2017 až 2022 - “National Institute of Standards and Technology” (NIST) prošel třemi koly výběrového řízení na vytvoření standardů pro kvantově bezpečné šifrování
- 2022 – NIST vybral PQC algoritmy a doporučil dva primární CRYSTALS KYBER a CRYSTALS Dilithium
- 2024 – NIST uveřejnil Federal Information Processing Standards (FIPS) standardy:
  - FIPS 203 / CRYSTALS-Kyber
    - **Šifrování klíčů**
    - “Public key Encryption” a “Key establishment Algorithms”
  - FIPS 204 / CRYSTALS-Dilithium
    - D**igitální podpisy**
    - “Digital Signature Algorithms”

datera

Historie šifrování

- symetrické X asymetrické šifrování
- Dříve symetrické, závislost na fyzické bezpečnosti
- Nyní asymetrické, závislost na výpočetní obtížnosti – OHROŽENO

dațerá

QKD

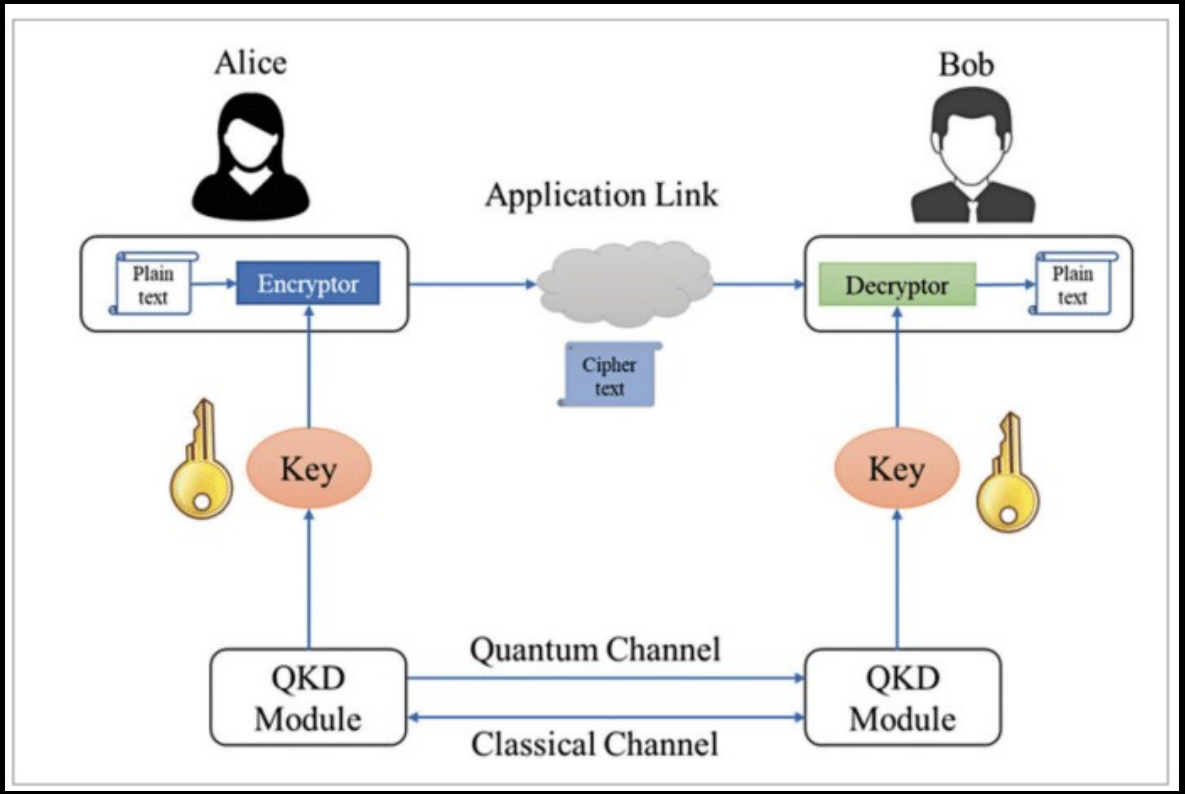
- QKD X kryptografie veřejného klíče
- výpočetní náročnost X kvantová mechanika
- Nejde o náhradu asymetrického kódování, ale o odlišnou technologii

SCEPTRE DUO

SCEPTRE LINK qRx SCEPTRE LINK qTx

QKD

- Pouze výměna klíče
- V praxi použito s algoritmy symetrických klíčů (AES, ...)
- Různé fyzikální přístupy
  - Kvantová neurčitost (BB84)
  - Kvantové provázání (E91)
- Znemožňuje získání klíče
  - Nemožnost klonování
  - Princip neurčitosti



datera

Další vývoj problematiky

- Quantum Key Distribution (QKD) as a Service - QaaS
- DIQKD (MDIQKD) – QKD nezávislý na zařízení
  - Začlenění odchylek do systému
  - Překonání limitu vzdálenosti (TFQKD)
- Kvantové opakovače

- **QKD přináší další vrstvu bezpečnosti**

datera

Kroky které je třeba podniknout

- **Vytvořte povědomí na úrovni vedení**, aby vaše organizace programově a strategicky reagovala na potřebu kvantové bezpečnosti. Získejte podporu od svého vedení.
- **Komunikujte potřebu stát se kvantově bezpečným**, a tím povýšit kvantovou bezpečnost na společnou obchodní a IT iniciativu. Identifikujte zúčastněné strany a získejte jejich podporu.
- **Začněte připravovat plán** pro transformaci vaší organizace na kvantovou bezpečnost. Odhadněte investice potřebné po dobu trvání cesty.

Děkuji za pozornost

Walter Pavliš
Kontakt: walter.pavlis@datera.cz

datera