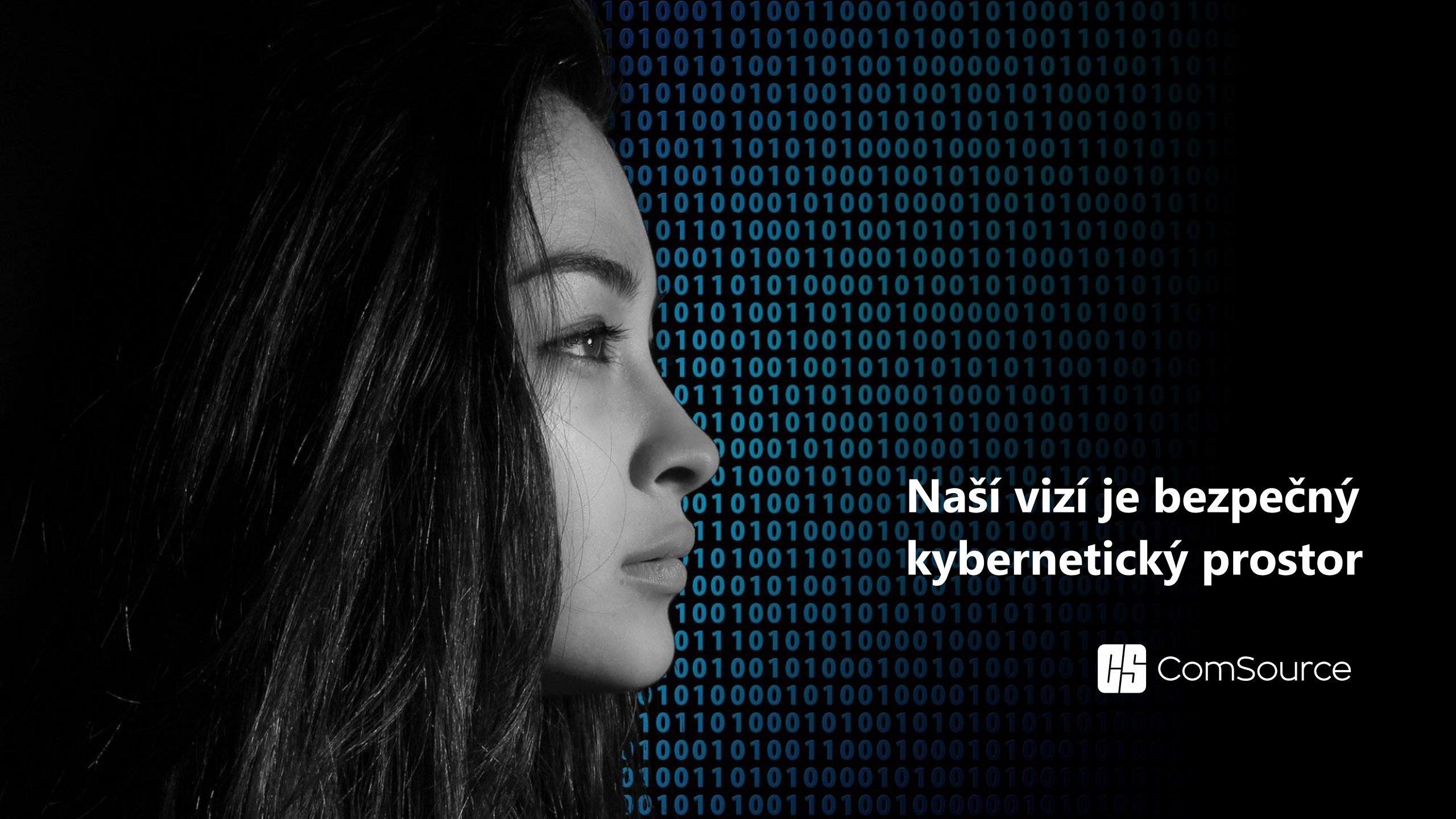
ComSource

Kvantové technologie – aktuální problém nebo máme čas?

Prezentuje: Marek Kocan


Naší vizí je bezpečný
kybernetický prostor
ComSource

ComSource

- Specializace na několik pečlivě vybraných vendorů.

ComSource partnerství

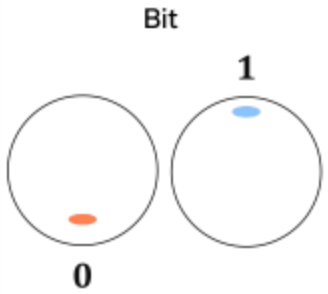
Jsme součástí týmu CSIRT (Computer Security Incident Response Team). Úkolem národního týmu CSIRT.CZ je ve spolupráci s Národním bezpečnostním úřadem reagovat, koordinovat a řešit bezpečnostní incidenty v oblasti bezpečnosti IT.

ComSource je aktivním členem české pobočky AFCEA (Armed Forces Communication and Electronics Association). Členství v této mezinárodní organizaci nám umožňuje sdílet a rozvíjet naše know-how v oblasti kybernetické bezpečnosti a ICT technologií.

ComSource je členem projektu FENIX, který vznikl v roce 2013 na půdě českého peeringového uzlu, sdružení NIX.CZ, jako reakce na intenzivní DDoS útoky, kterým toho roku čelila významná česká média, banky nebo operátoři.

Tradiční počítačový svět

- Analogové technologie
- Digitální technologie
  - využití tranzistorů
  - bity - nuly a jedničky

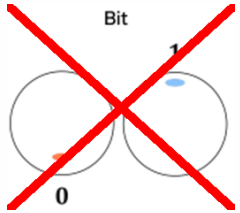


- Přesvědčení, že co nelze v rozumném čase a za rozumných nákladů vyřešit pomocí 0 a 1, nelze vyřešit vůbec
- Různé třídy složitosti:
  - konstantní, lineární … polynomiální, exponenciální, dvojitě exponenciální
  - <= polynomiální … zvládnutelné za rozumný čas/náklady
  - > polynomiální … běžnými ani superpočítači od určité velikosti vstupu prakticky neřešitelné

Tradiční počítačový svět

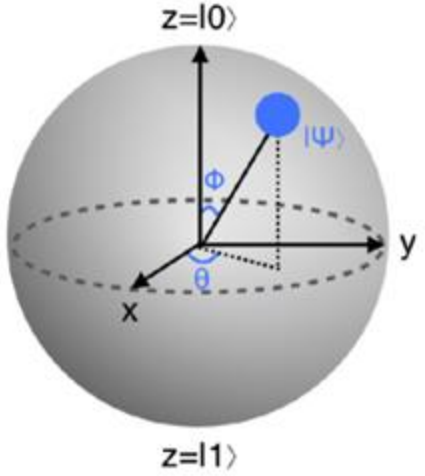
- Náročnost na:
  - zdroje (např. paměť)
  - čas
  - náklady
- Nelze zrychlovat donekonečna
  - fyzikální limity
  - algoritmické limity / rostoucí velikost vstupů

Složitost	Operace pro $n = 2$	Operace pro $n = 4$	Operace pro $n = 10$	Operace pro $n = 100$	Operace pro $n = 1000$
$O(1)$	1	1	1	1	1
$O(\log n)$	1	2	4	7	10
$O(n)$	2	4	10	100	1000
$O(n \log n)$	4	8	40	700	10 000
$O(n^2)$	4	16	100	10 000	1 000 000
$O(n^3)$	8	64	1 000	1 000 000	1 000 000 000
$O(2^n)$	4	16	1 024	$\sim 10^{30}$*	$\sim 10^{301}$*
$O(2^{2^n})$	16	65 536	$\sim 10^{308}$**	Nelze spočítat!	Nelze spočítat!

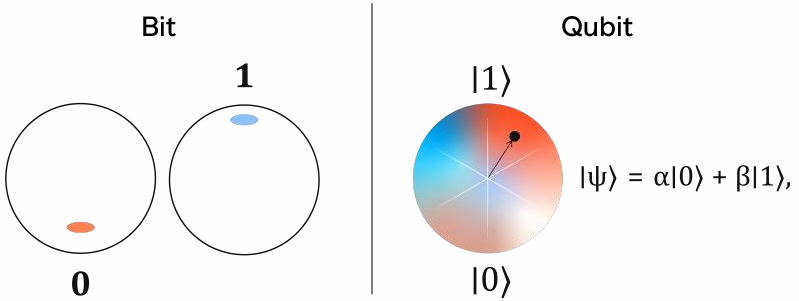


Kvantový svět

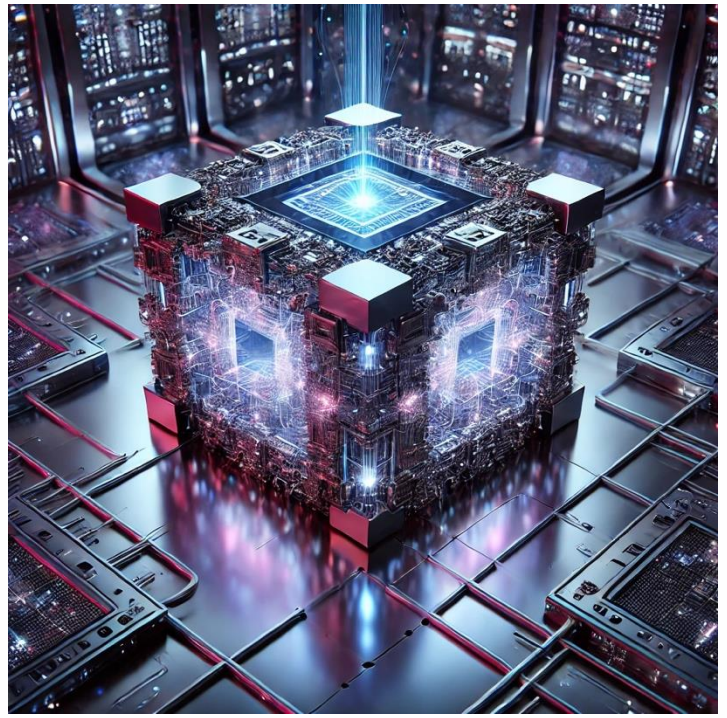
- Zcela nový přístup
- Bity „končí, přichází“ qubity
- Základem kvantových bitů jsou jevy kvantové fyzicky
- Nejde jen o nuly a jedničky, ale o (kvantovou) superpozici těchto dvou stavů
- V konkrétním stavu s určitou pravděpodobností
- Povrch Blochovy koule
- + kvantové provázání



qubit



Kvantový svět



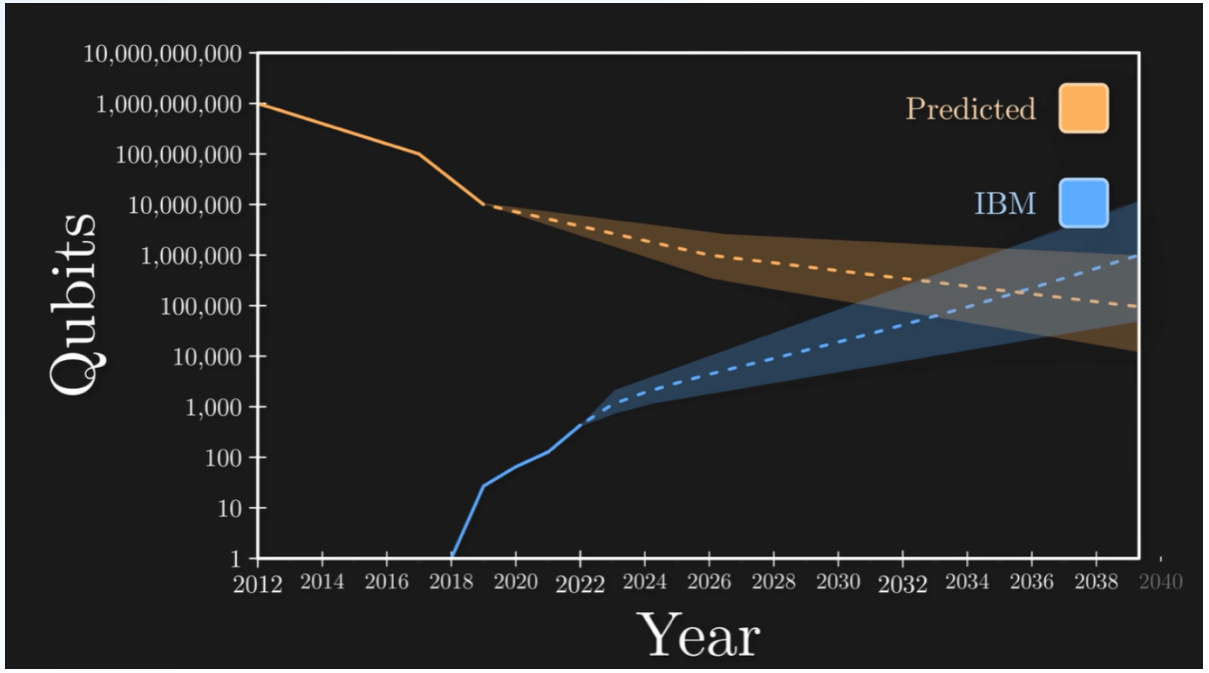
- Neřešitelné pomocí nul a jedniček se stane řešitelným (v rozumném čase a za rozumných nákladů) aneb kvantová nadřazenost
- Současná reprezentace (až) všech 2^n možných stavů
- Qubity tedy mohou být ve více stavech současně a kvantové počítače tak mohou pracovat skutečně paralelně (exponenciální paralelismus)
- Problémy stabilita, chyby, chlazení …
- Speciální algoritmy – Groverův (vyhledávání v nestrukturovaných datech), Shorův (faktorizace velkých čísel na prvočísla) …

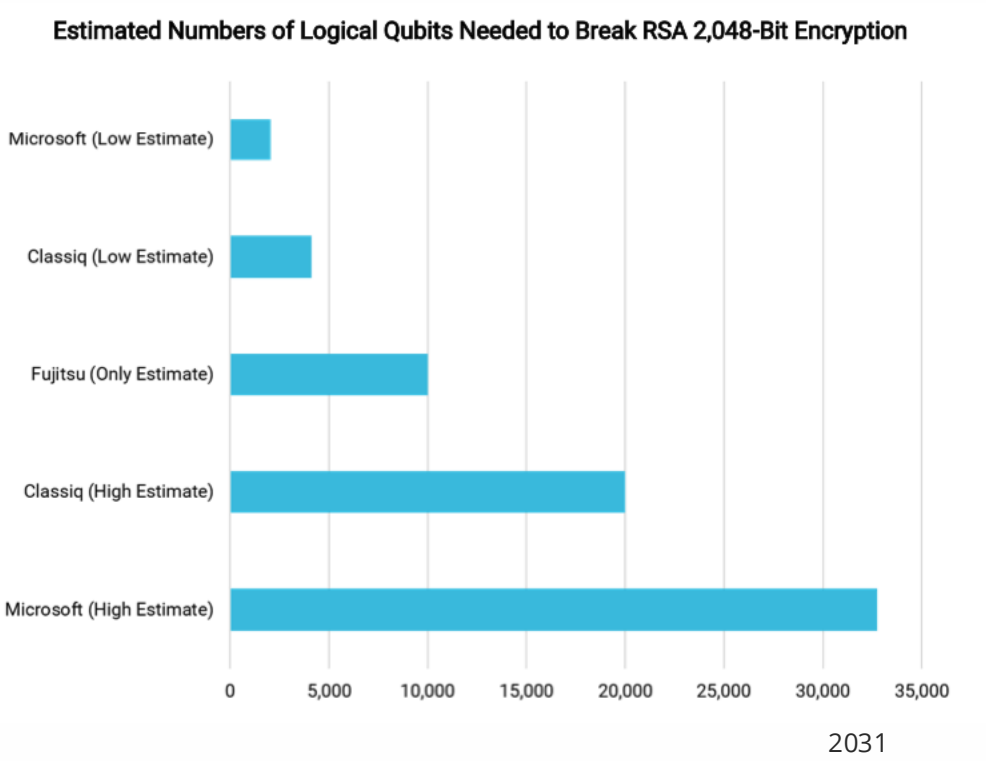
Kryptografie a kvantový svět

- Symetrické šifry – při dostatečné délce klíčů OK
  - AES-128, 192 nebo 256
- Asymetrické šifry – problém je paralelní výkon
  - RSA, ECC, DSA … nebudou bezpečné
- Uložená data -> relativně snadná opatření
- Přenášená data -> stávající algoritmy nebudou stačit
- Máme se bát?
  - RSA-2048, potřeba cca 4000 qubitů, IBM cca 10k qubitů do konce této dekády
  - *Kryptoanalyticky relevantní kvantový počítač (Cryptographically Relevant Quantum Computers, CRQC) je takový kvantový počítač, který je dostatečně výkonný na to, aby dokázal prolomit reálné kryptografické systémy, jež není možné prolomit klasickými počítači.* (nukib.gov.cz)

My nevíme …

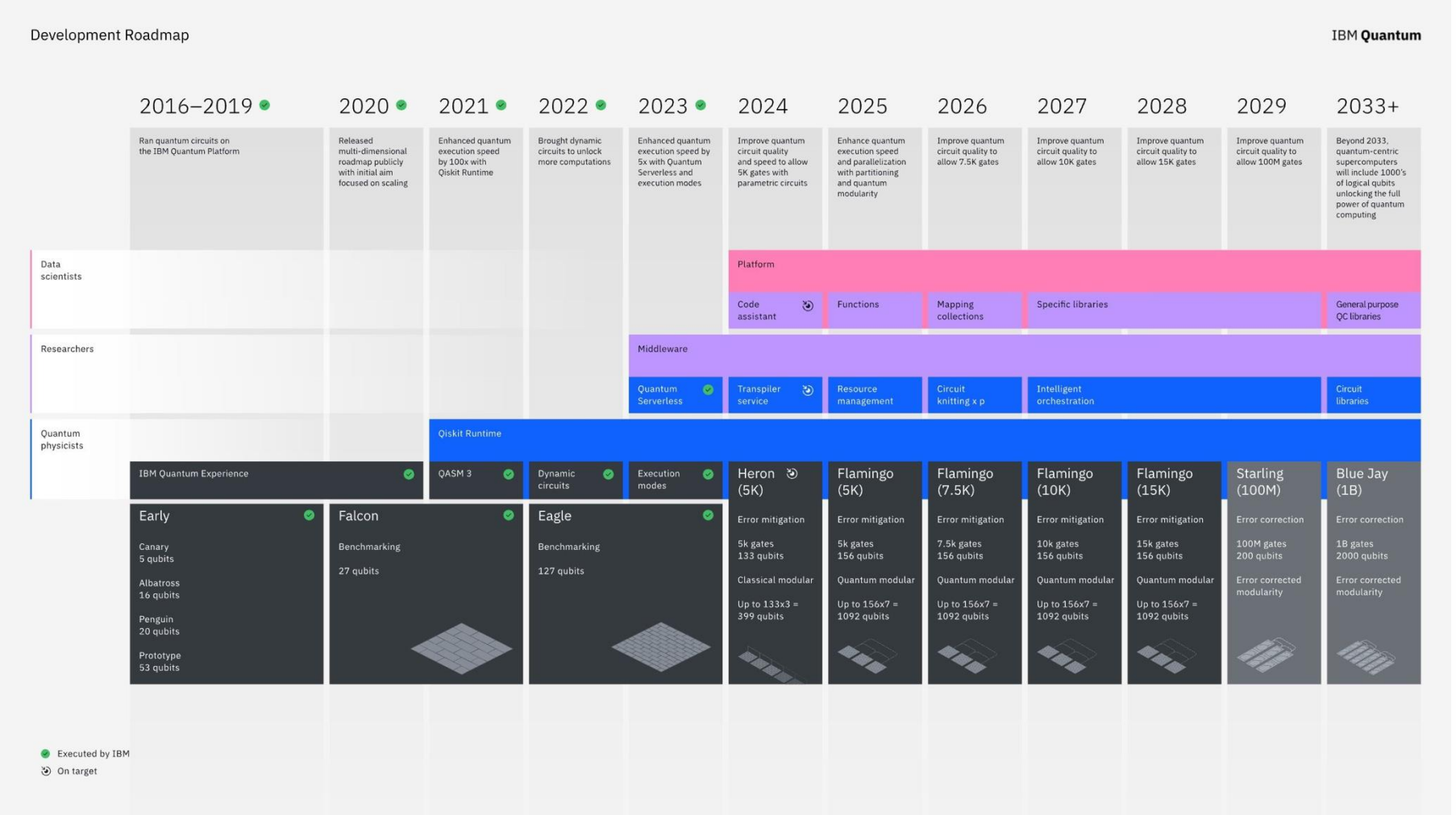
Máme se tedy bát?





- říjen 2024 – prolomení RSA-50 (Chine University Shanghai)

Máme se tedy bát?



ComSource

Ano, musíme se bát!

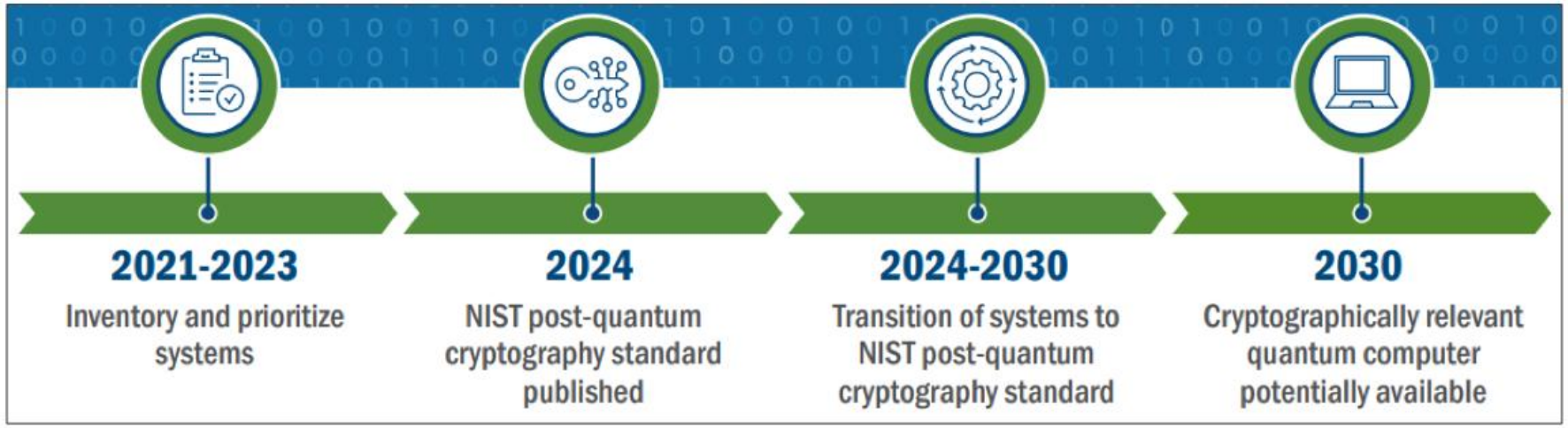
- Harvest now, decrypt later
- Žádné nebo jen minimální informace o současném stavu
- Lepší alespoň něco než nic
  - zvyšování povědomí
  - audit
  - zohlednění platných doporučení
  - …

Postkvantová kryptografie

- Kryptografie odolná vůči útokům pomocí kvantových počítačů
- Využití tradičních počítačů a lepších algoritmů
- Nejde tedy o kvantovou kryptografii (např. Quantum Key Distribution)
- Standardy NIST (jsou zdarma i pro komerční užití):
  - Úsilí od začátku druhé poloviny minulé dekády
  - 8/2024: FIPS 203 - Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)
  - 8/2024: FIPS 204 - Module-Lattice-Based Digital Signature Standard (ML-DSA)
  - 8/2024: FIPS 205 - Stateless Hash-Based Digital Signature Standard (SLH-DSA)
  - FN-DSA - FFT over NTRU lattices Digital Signature Standard
- EK: Doporučení pro koordinovanou implementaci přechodu na PQC (4/2024)
- NÚKIB: Kvantová hrozba a kvantově odolná kryptografie, příloha dokumentu *Minimální požadavky na kryptografické algoritmy* (7/2023)

Hlavní doporučení

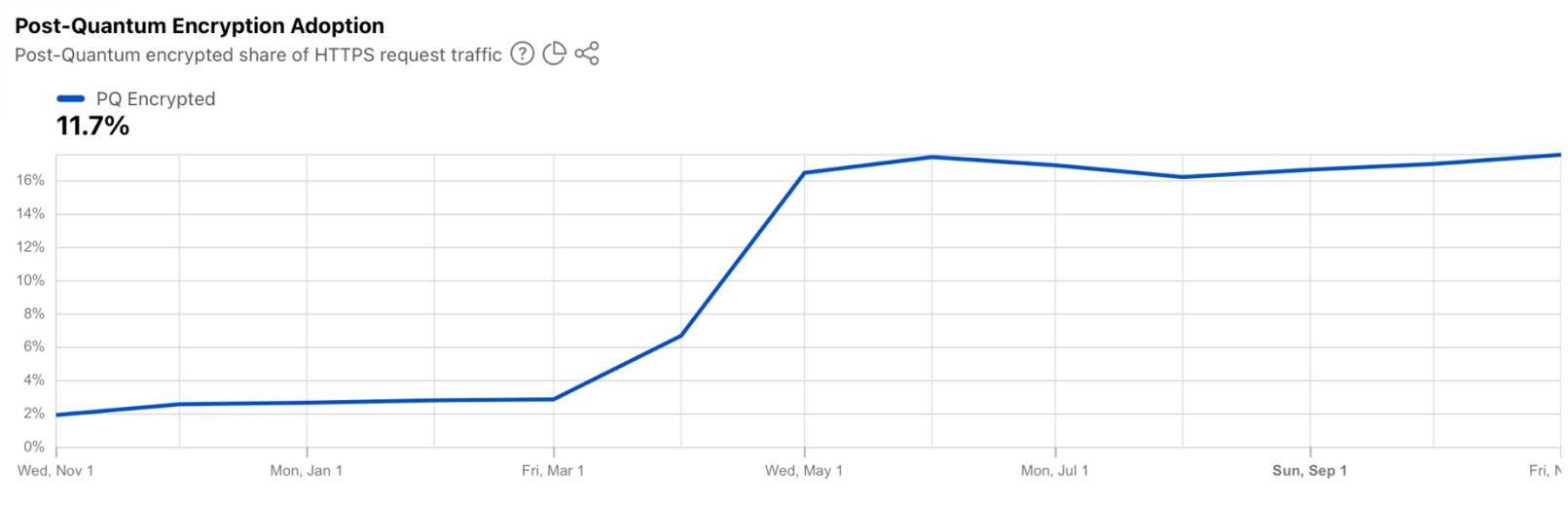
- Vnímání reálnosti hrozby útoků pomocí kvantových počítačů
- Zvyšování délky klíčů (zejména u symetrických šifer)
- Používání hybridních algoritmů (my totiž pořád nevíme!!!)
  - X25519Kyber768 (X25519 + Kyber768)
- Příprava plánu přechodu na PQC
- NIS2



Příklady aktuálního stavu

- Podpora PQC:
  - TLS protokol: Google Chrome v131, Firefox v125
  - Apple iOS, iPadOS, MacOS, WatchOS
  - iMessage, Signal
  - BoringSSL, OpenSSH
  - Aplikace Google
  - Microsoft Azure Key Vault

Cloudflare Radar



ComSource

Pár postřehů …

- Historie kvantové mechaniky spadá staletí zpět, moderní od 1925, existuje velmi dobrý matematický aparát
- První úvahy o kvantových počítačích – Richard Feynman, 1982
- Zvyšování počtu qubitů je nelineární problém
- Kvantový čip Willow od Googlu prokázal možnost snižování chybovosti s nárůstem výkonu (mimochodem výpočet z 10^25 let zvládl za pouhých pět minut)
- Provoz ideální v teplotách blížící se absolutní nule
- Budoucnost kryptoměn? Uvidíme …

Harvest now, decrypt later

Otázky?

Děkuji za pozornost

Email: marek.kocan@comsource.cz

Tel: 604 766 243