

Globální **S**standards
interního auditu

Sekce **V** veřejné
správy

Zákon
o řízení a kontrole
veřejných financí

Centrální **J**ednotka
harmonizační
MF ČR

WORKSHOP PRO INTERNÍ AUDITORY Z VEŘEJNÉ SPRÁVY

KOMPAS

pro změny
v interním
auditu

Přerov, 22.–23. říjen 2025

ORGANIZÁTOR



HLAVNÍ PARTNEŘI



PARTNEŘI



Přerov

MEDIÁLNÍ PARTNER



Kvantová hrozba: nové povinnosti a změny v ochraně dat

Lumír SRCH
ITS akciová společnost



pro změny
v interním
auditu

Přerov, 22.–23. říjen 2025



Proč věnovat pozornost kvantovým hrozbám



„Nepokořitelná“ Enigma: K prolomení nerozluštitelné šifry pomohla náhoda

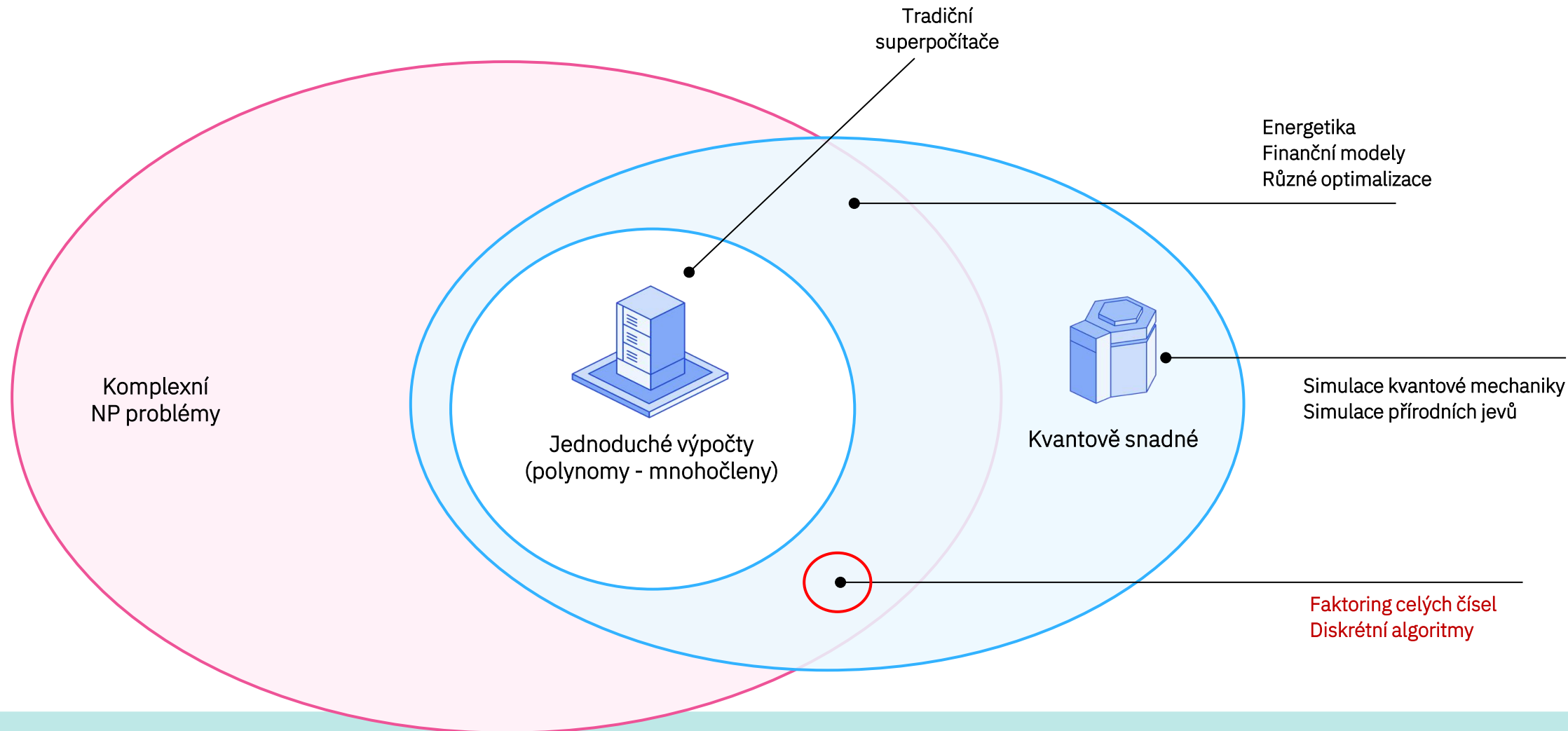


Co je to kvantový počítač

- Kvantový počítač využívá k výpočtům fyzikální jevy a mechanické vlastnosti částic
- Data jsou reprezentována qubity (kvantové bity), které kromě tradičních hodnot 0 a 1 mohou nabývat díky superpozici stavů nulu i jedničku současně
- Pro kvantové počítače neplatí Moorův zákon, ale jejich výkon roste exponenciálně
- Kvantové počítače se hodí pro simulaci přírodních a fyzikálních jevů, mohou se uplatnit v energetice, studiu klimatu, materiálových vědách a neposlední řadě matematice
- Pro kvantové počítače existují nové algoritmy, které využívají jejich fyzikálních schopností a teoreticky převádí exponenciální závislost na polynomiální



Kdy je vhodné použít kvantový počítač?



Na co spoléhá současná kryptografie

<p>Primární faktor</p> <p>$= p \times q$</p>	<p>2048-bit složené celé číslo</p> <pre>2519590847565789349402718324004839857142928212620403202777137836 04366202070759555626401852588078440691829064124951508218929855914 9176184502808489120072844992687392807287767359714183472702618963 75014971824691165077613379859095700097330459748808428401797429100 64245869181719511874612151517265463228221686998754918242243363725 90851418654620435767984233871847744479207399342365848238242811981 63815010674810451660377306056201619676256133844143603833904414952 63443219011465754445417842402092461651572335077870774981712577246 79629263863563732899121548314381678998850404453640235273819513786 3656439212010397122822120720357</pre>	<p>Očekávaná doba výpočtu</p> <hr/> <p>Na tradičních nejvýkonnějších systémech:</p> <p>Milióny let</p>
---	---	---

Šifrování veřejným klíčem • Digitální podpisy • Algoritmy výměny klíčů

RSA • DSA • ECC • ECDSA • DH



pro změny
v interním
auditu

Přerov, 22.–23. říjen 2025



Na co spoléhá současná kryptografie

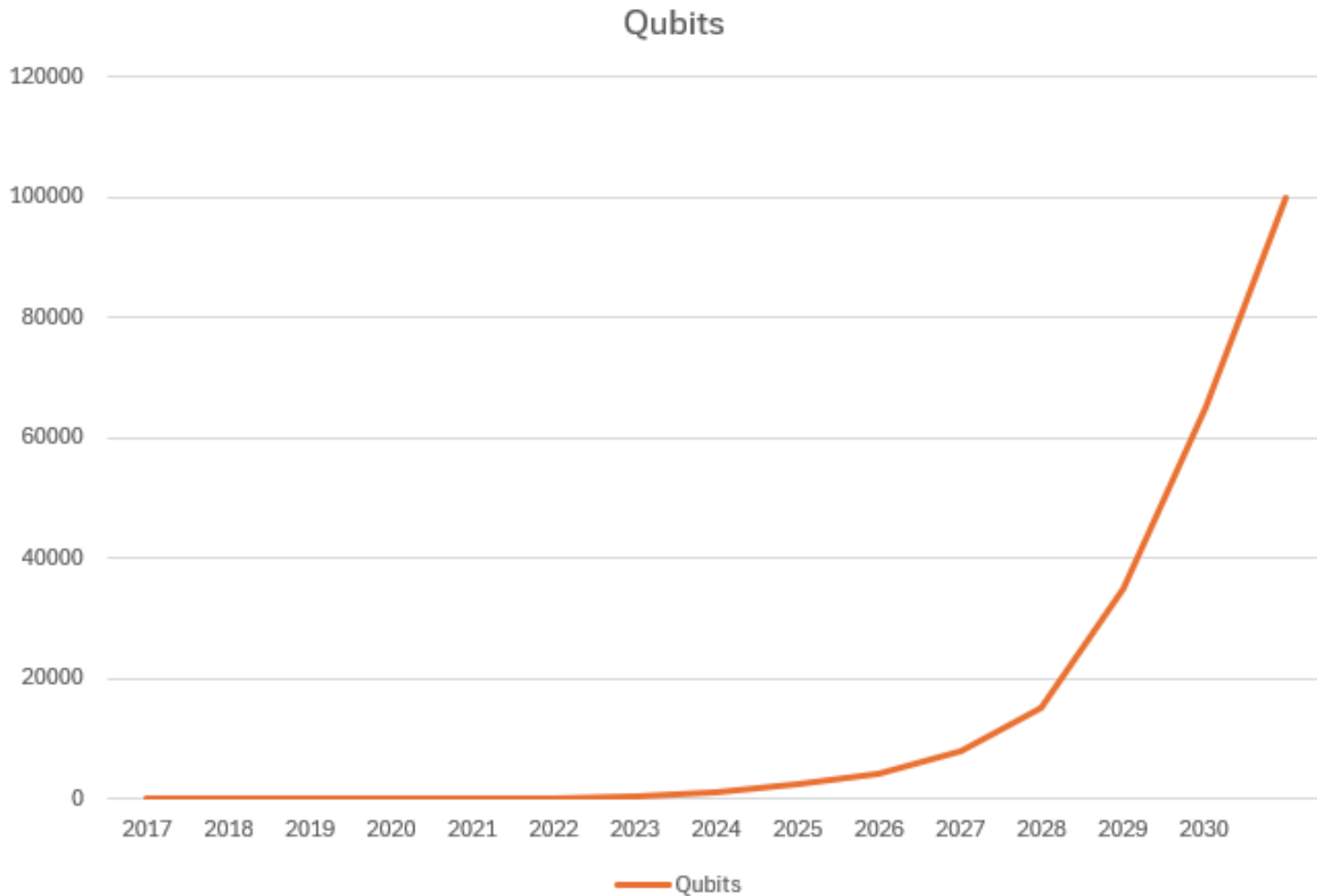
kvantové počítače zahajují novou kryptografickou éru

<p>Primární faktor</p> $= p \times q$	<p>2048-bit složené celé číslo</p> <pre>25195908475657893494027183240048398571429282126204032 02777713783604366202070759555626401852588078440691829 06412495150821892985591491761845028084891200728449926 8739280728776735971418347270261896375014971824691165 07761337985909570009733045974880842840179742910064245 86918171951187461215151726546322822168699875491824224 33637259085141865462043576798423387184774447920739934 23658482382428119816381501067481045166037730605620161 96762561338441436038339044149526344321901146575444541 78424020924616515723350778707749817125772467962926386 35637328991215483143816789988504044536402352738195137 863656439212010397122822120720357</pre>	<p>Očekávaná doba výpočtu</p> <hr/> <p>Na kvantových počítačích:</p> <h1>Hodiny</h1>
---------------------------------------	--	--

~~Čifrování veřejným klíčem Digitální podpisy Algoritmy výměny klíčů~~

~~RSA DSA ECC ECDSA DH~~

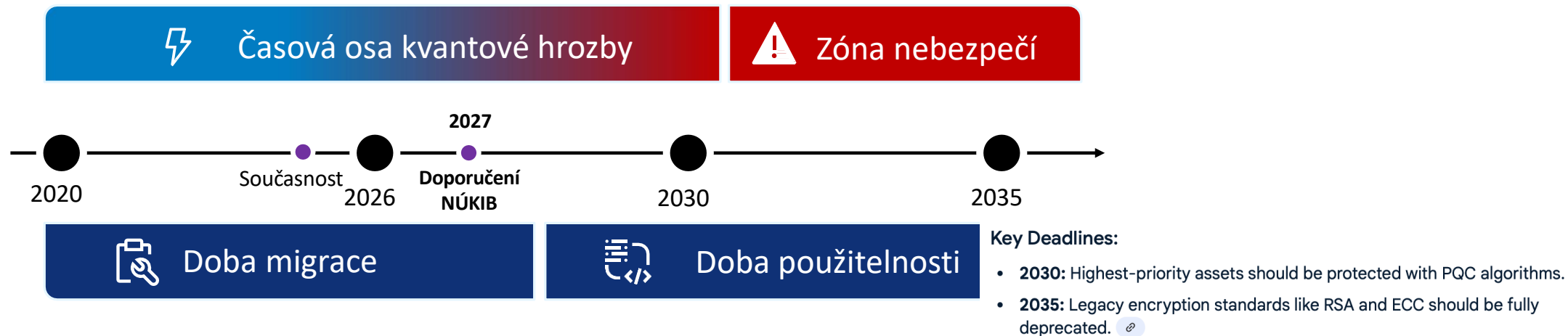
Kdy dosáhneme 100.000 qubitů?



Year	Qubits	Key Milestone
2016	5	IBM Q 5 Tenerife - First cloud quantum computer
2017	20	IBM Q 20 Austin
2018	72	Google Bristlecone
2019	65	IBM Q System One
2020	65	IBM Q Network expansion
2021	127	IBM Eagle processor
2022	433	IBM Osprey processor
2023	1180	Atom Computing + IBM Condor breakthrough
2024	2500	Current leading systems
2025	4000	Industry leaders reach 4K qubits
2026	8000	Error correction scaling begins
2027	15000	Multiple vendors exceed 10K
2028	35000	Fault-tolerant systems deployed
2029	65000	Commercial quantum advantage
2030	100000	100K milestone achieved

Kdy skutečně nastane kvantová hrozba?

U dat, která vyžadují dlouhodobou ochranu existuje hrozba již dnes s dopadem v budoucnu



"Přesná časová osa hrozeb, na kterou byste se měli zaměřit, závisí na vaší toleranci k riziku. U velmi kritických systémů a aktiv se pravděpodobnost kvantových útoků do pěti let stává významnou a u většiny kritických systémů a aktiv se domnívám, že je třeba asertivně řešit desetiletou pravděpodobnost."

Dr. Michele Mosca, University of Waterloo, Canada

"Zkušenosti ukazují, že v nejlepším případě bude k implementaci těchto standardů stále zapotřebí 5 až 15 nebo více let po zveřejnění kvantově odolných kryptografických standardů s veřejným klíčem."

National Cybersecurity Center of Excellence (NCCoE)

Kde všude se používá kryptografie

Internetové protokoly



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

Kritická infrastruktura



Aktualizace kódu; Řídicí systémy -
ropovody, elektrické sítě;
Automobilové systémy,...

Blockchain aplikace



Elektronické peněženky,
Transakce, Autentizace

Digitální podpisy a související zákony



EiDAS - PDF Advanced Electronic
Signature – (PADES), Advanced
Electronic Signatures (AES), ...

Finanční systémy



Platební systémy: (EMV, SWIFT,
Sídlní systémy, FinTech, ...)

Enterprise aplikace



EMAIL – PGP, Identity
Management PKI/LDAP/.., Virus
scanning patterns, PKI Services

Kde všude se používá kryptografie

Internetové protokoly



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

Kritická infrastruktura



Aktualizace kódu; Řídicí systémy -
ropovody, elektrické sítě;
Automobilové systémy,...

Blockchain aplikace



Mincovní peněženky,
Transakce, Autentizace

Digitální podpisy a související zákony



EiDAS - PDF Advanced Electronic
Signature – (PAES), Advanced
Electronic Signatures (AES), ...

Finanční systémy



Platební systémy: (EMV, SWIFT,
Sídlní systémy, FinTech, ...)

Enterprise aplikace



EMAIL – PGP, Identity
Management PKI/LDAP/.., Virus
scanning patterns, PKI Services

**Bude potřeba
změnit/aktualizovat/uzákonit**

Jaká známe dnes konkrétní rizika?

Čeho jsou dnes kyberzločinci schopni?

 sběru dat s dešifrováním později

 podvodných ověření

 padělání digitálních podpisů

- Výměna většiny v současnosti používaných systémů veřejných klíčů bude trvat **5 až 10 let.**
- Všechna data, která nejsou chráněna kvantově bezpečnou kryptografií **jsou ohrožena.**

NÚKIB doporučení

- Instituce jako ENISA a lokální NÚKIB doporučují přechod na post-kvantově odolné algoritmy do roku **2027**



Minimální požadavky
na kryptografické
algoritmy



Příloha k dokumentu
Minimální požadavky
na kryptografické
algoritmy

NÚKIB



KVANTOVÁ HROZBA A KVANTOVĚ ODOLNÁ KRYPTOGRAFIE

Příloha k dokumentu:
Minimální požadavky na kryptografické algoritmy



pro změny
v interním
auditu

Přerov, 22.–23. říjen 2025



Co je to Quantum safe?

- Quantum safe (kvantově bezpečné) je označení pro šifrovací metody a bezpečnostní opatření, která jsou odolná vůči útokům jak klasických, tak i budoucích kvantových počítačů
- Jedná se o náhradu současné kryptografie, která je zranitelná díky schopnosti kvantových počítačů v přiměřeně době vyřešit matematické úlohy, na nichž je založena
- Termín se často zaměňuje za spojení post-quantum cryptography (PQC), tedy kryptografií odolnou vůči kvantovým počítačům



Quantum safe framework



Otázka není jestli, ale **kdy**

- Kvantová hrozba **není IT problém**
- **Nečekejte** a vyvolejte svými otázkami **diskuzi** napříč vaší organizací
- Přejít na kvantově odolné algoritmy je dlouhodobý proces, ale **zodpovědnost za bezpečnost dat máte již teď**

