

Kvantové hrozby

Ing. Ondřej Navrátil, Ph.D.
MONET+





Kryptografie

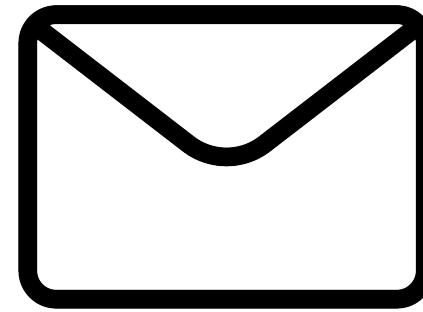
kryptós – skrytý
gráphein – psát

...co ale chceme/můžeme skrývat?

Důvěrnost



Alice



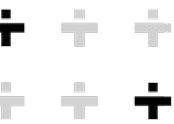
???



Bob



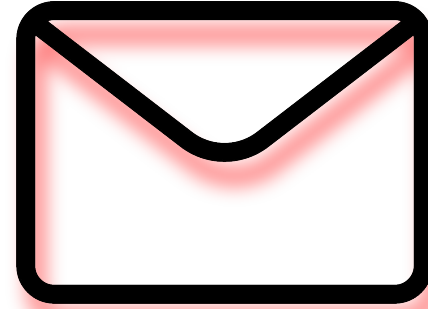
Trudy



Integrita



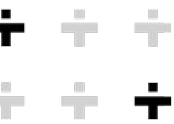
Alice



Bob



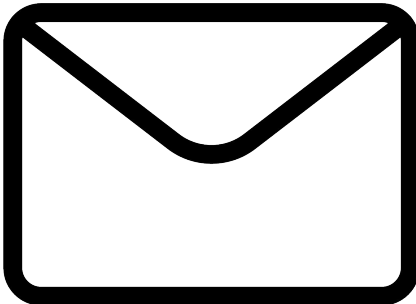
Trudy



Autenticita



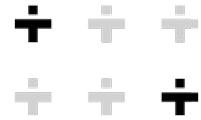
Trudy



od Alice



Bob



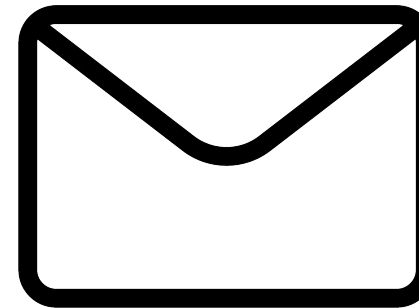
Nepopiratelnost



Trudy



od Trudy



Později...



Bob

Bob: Děkuji za dopis, Trudy!

Trudy: Ale já nic neposlala!

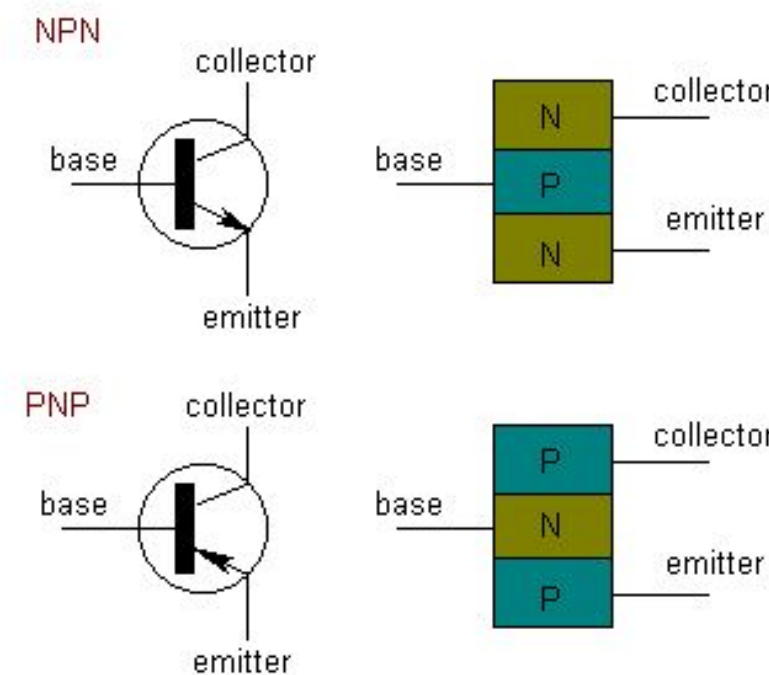
A futuristic quantum computing device is shown, featuring multiple layers of copper plates and intricate wiring. The device is cylindrical and has a complex internal structure with many thin wires and components. The text "Kvantový počítač?" is overlaid on the image in a large, white, sans-serif font.

Kvantový počítač?

Klasický počítač



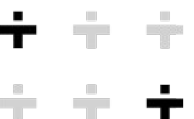
Základní jednotkou je bit



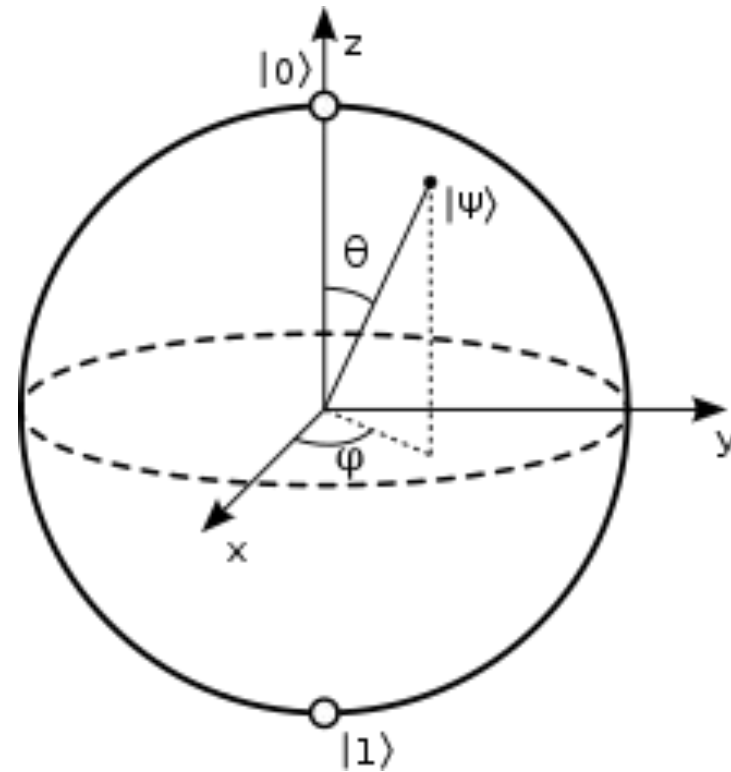
Založeny na polovodičích



Pracují s principy klasické fyziky a elektrodynamiky



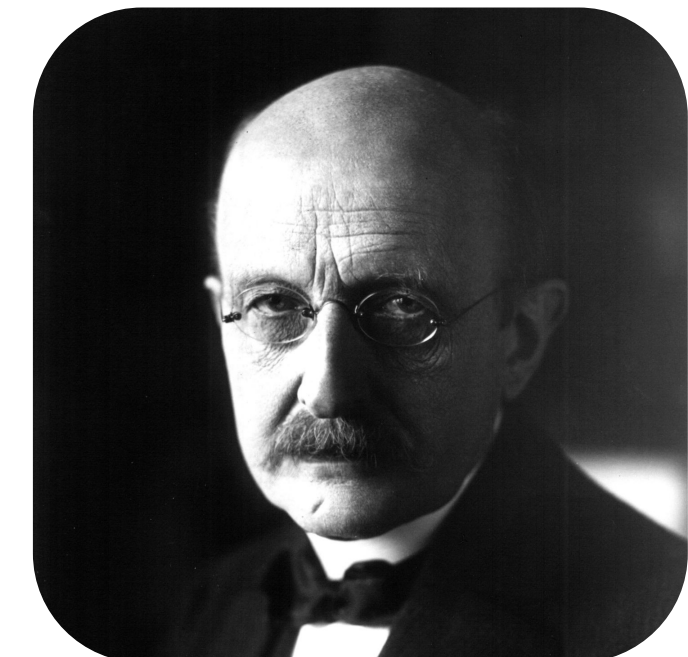
Kvantový počítač



Základní
jednotkou
je qubit



Založeny
na supravodičích



Pracují s principy
kvantové mechaniky
(superpozice,
provázané stavy)

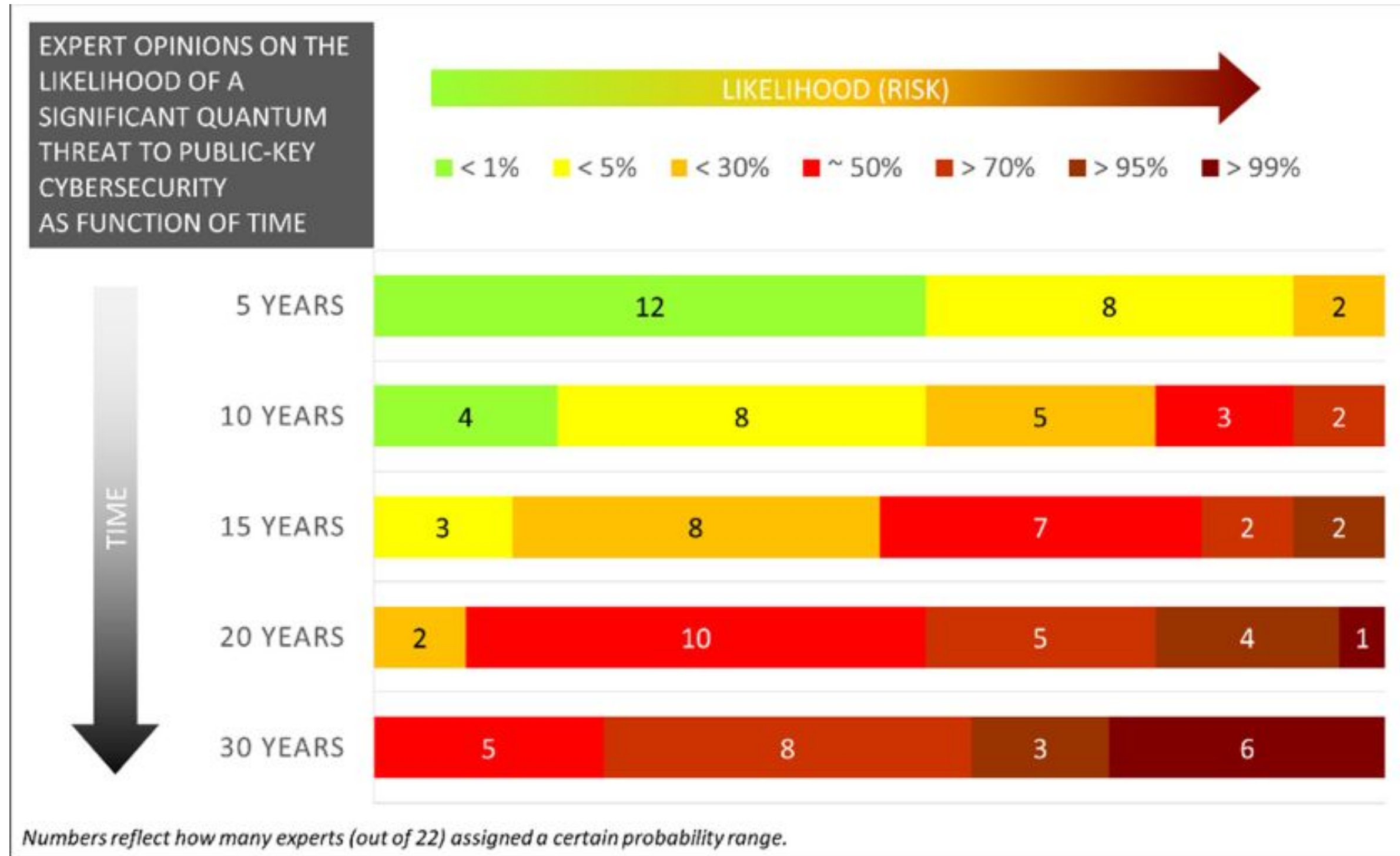
A close-up shot of Captain Archer from Star Trek: Enterprise. He is wearing a red Starfleet uniform with a gold and silver Starfleet insignia on his chest. He has a serious expression and is gesturing with his right hand, pointing upwards with his index finger. The background is a blurred interior of a ship.

Doba kvantová?

Jak vzdálená je *kvantová doba*?

- 1998 – úspěšná demonstrace
- 2007 – specializovaný počítač s 128 qubity
- 2011 – D-Wave One – komerčně dostupný (\$10m)
- 2019 – Google AI Quantum – Quantum Supremacy
- 2021 – IBM Eagle (127 qubitový univerzální procesor)

Názor expertů



Enigma

- 1941 – první prolomení
- 1945 – spojenci dokáží vyluštit prakticky všechny zprávy šifrované Enigmou během jednotek dní
- Němci zůstávají přesvědčeni o bezpečnosti Enigmy
- Informace zveřejněny v 70. letech

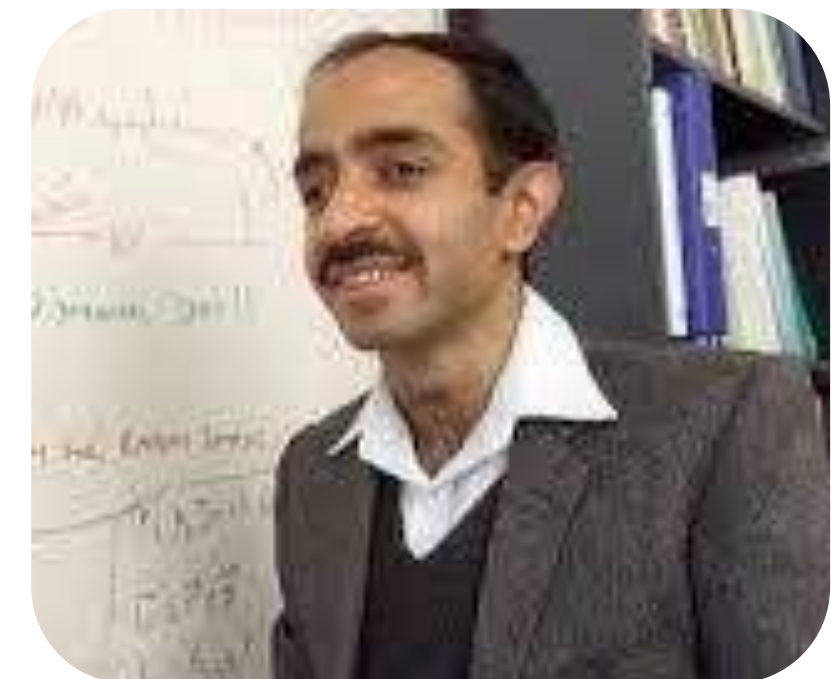
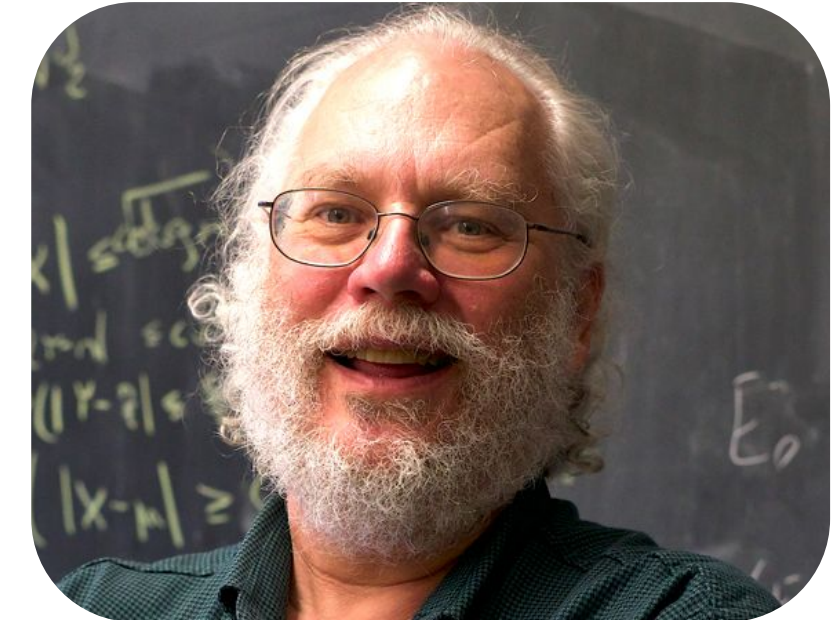


A Klingon Bird-of-Prey is shown firing two bright blue quantum torpedoes towards the USS Enterprise (NCC-1701). The Enterprise is positioned in the upper left, and the Bird-of-Prey is in the lower left. The background is a dark space filled with stars. The text "Kvantová torpéda!" is overlaid in the center in a large, white, bold font.

Kvantová torpéda!

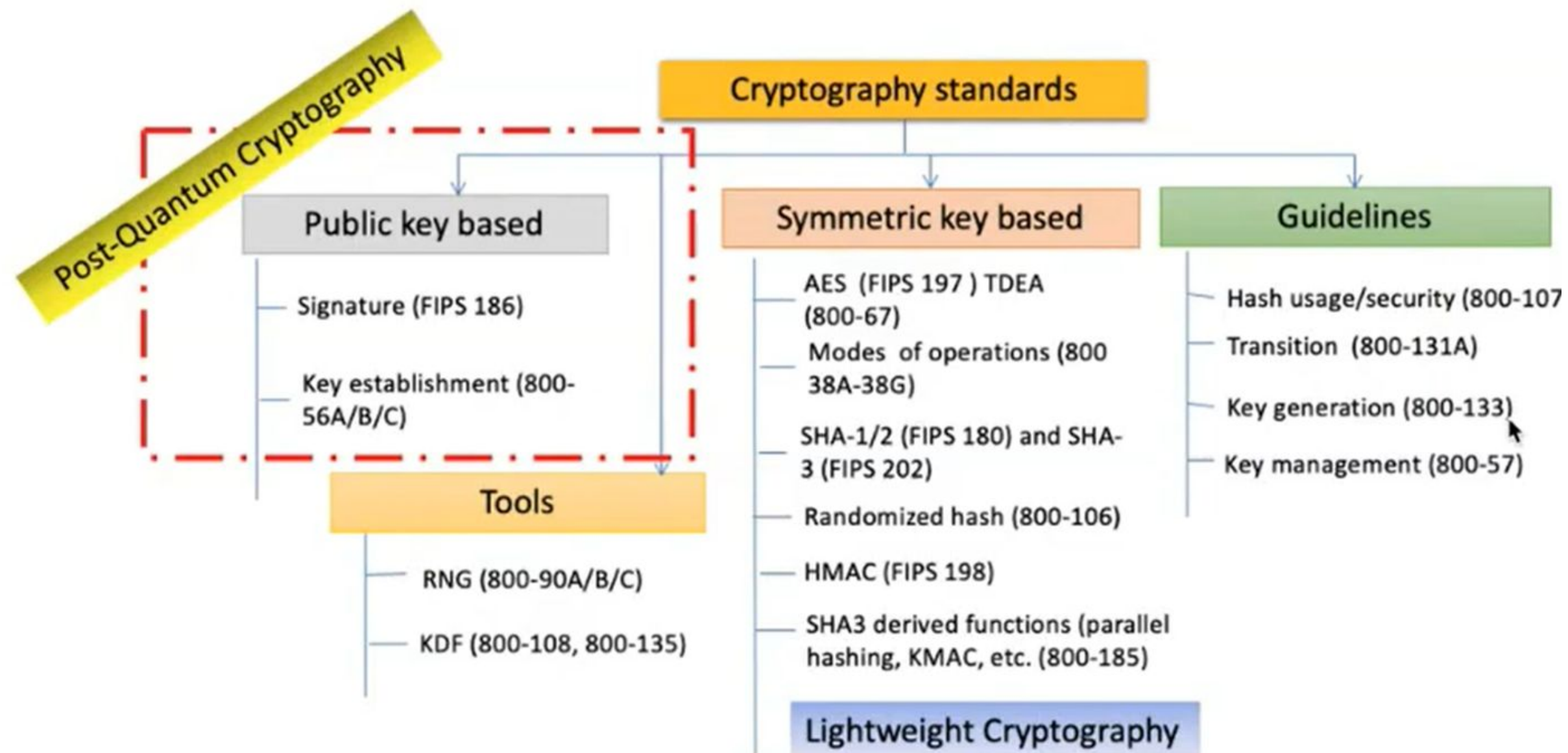
Dopady do kryptografie (1/2)

- Shorův algoritmus (1994)
 - Faktorizace přirozených čísel (RSA)
 - Diskrétní logaritmus (EC)
 - tranzitivně Diffie–Hellman výměna klíčů
- Groverův algoritmus (1996)
 - Prohledávání stavového prostoru (délky klíčů etc.)



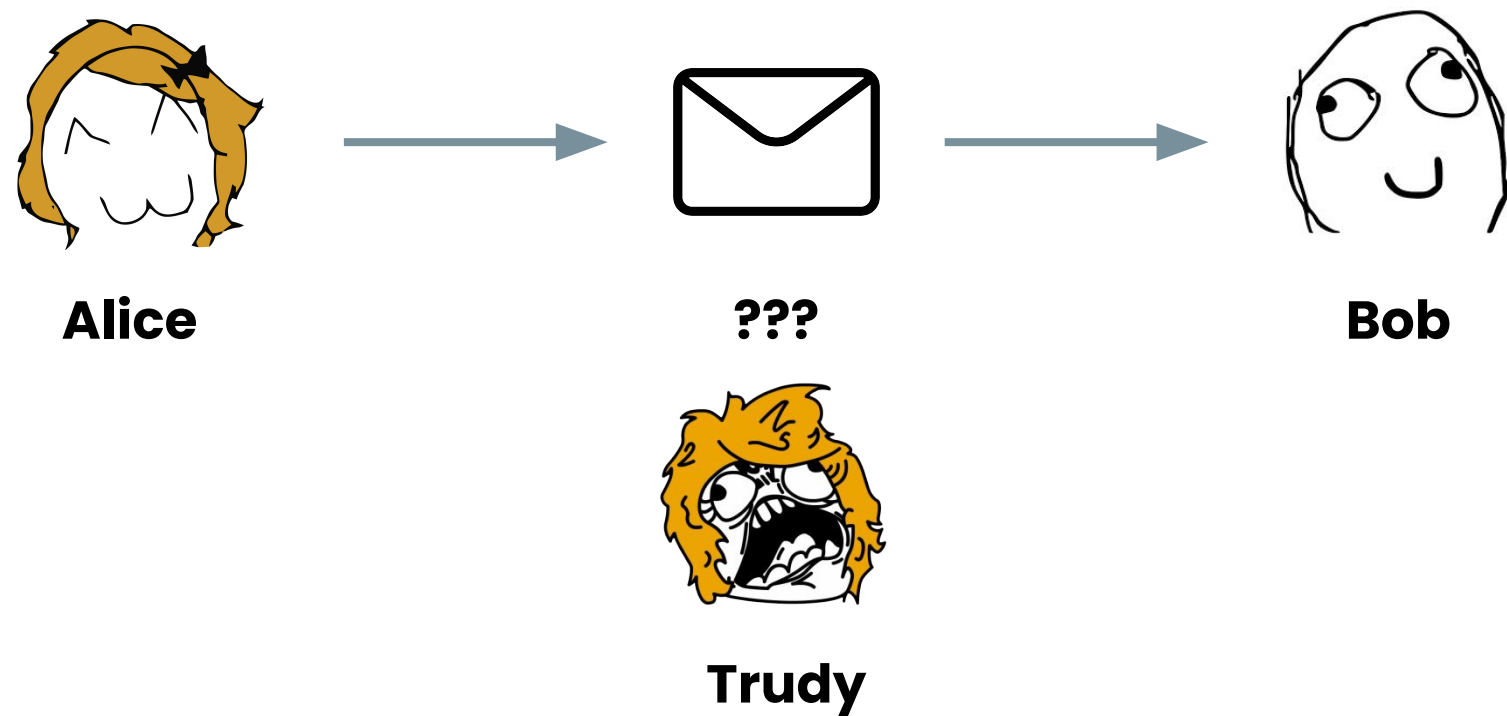
Dopady do kryptografie (2/2)

- Důvěrnost
- Nepopiratelnost

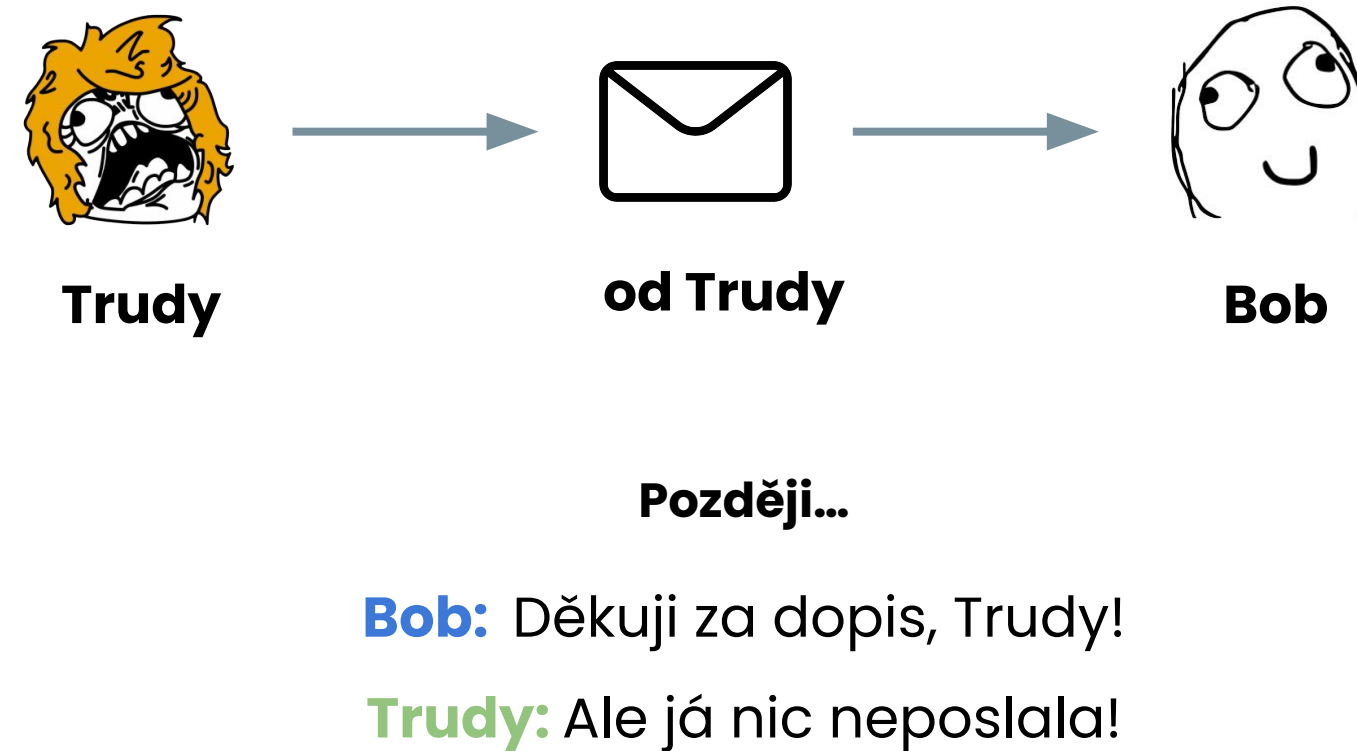


Pro připomenutí

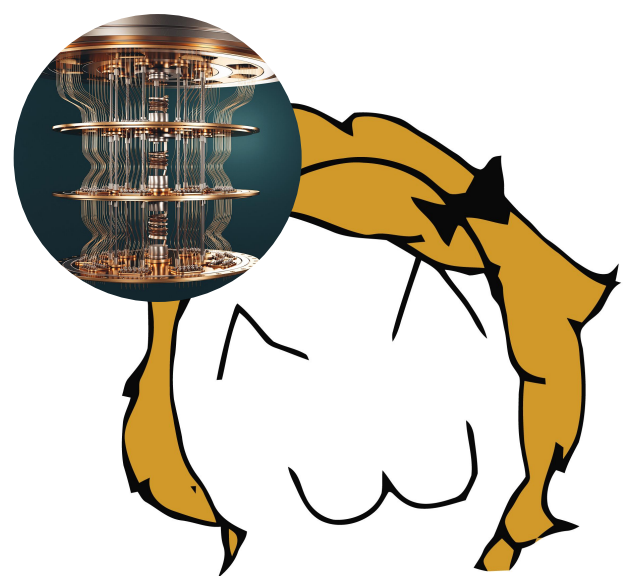
Důvěrnost



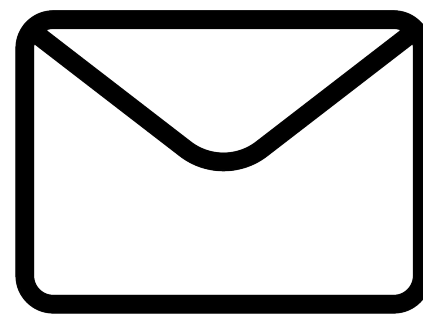
Nepopiratelnost



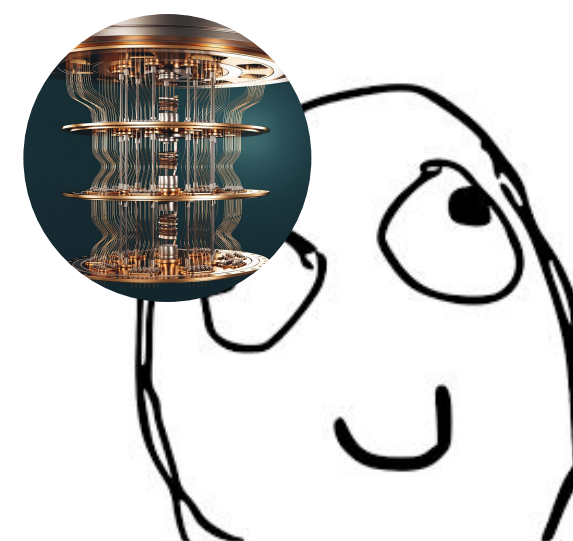
Kvantová kryptografie



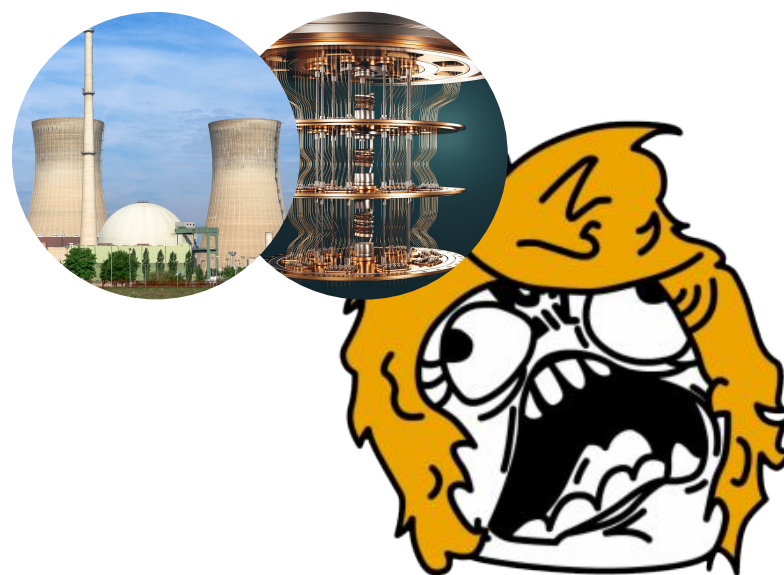
Alice



???



Bob

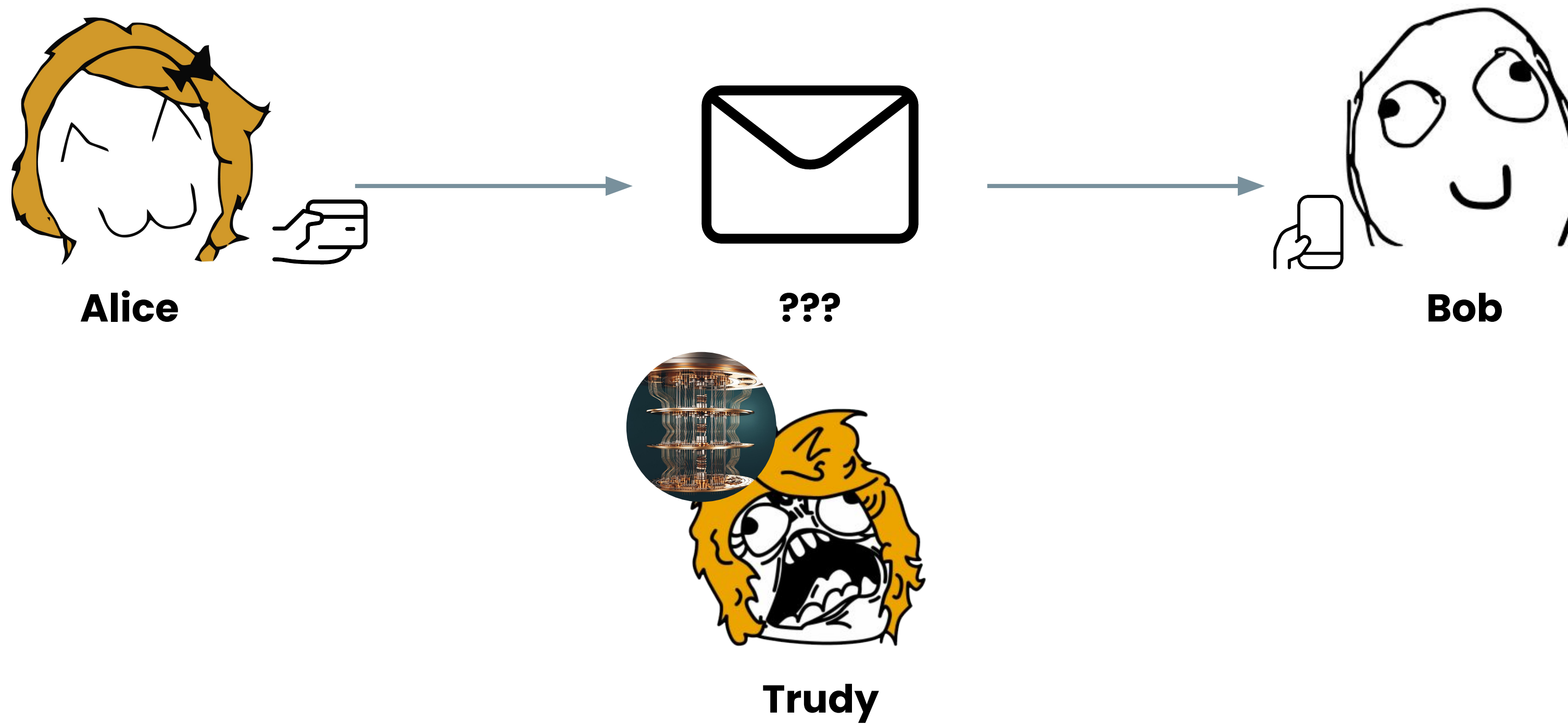


Trudy



Co ted'?

Postkvantová kryptografie



NIST soutěž



- 2017 začátek, předpokládaný konec 2024
- Dvě kategorie – **Podpisy** a **Šifrování (ustanovení klíče)**
- Červenec 2022 – finalisté ke standardizaci:
 - Crystals–KYBER
 - Crystals–Dillithium
 - Falcon
 - SPHINCS+
- Alternativy do 4. Kola: BIKE, Classic McEliece, HQC
 - **SIKE**
- NIST dál aktivně hledá zejména ne-mřížkové alternativy

ENISA

- Publikace týkající se PQC (únor 2021, aktualizováno)
- Pravděpodobně bude kopírovat NIST
- Doporučuje aplikaci hybridních schémat



Jak na to?

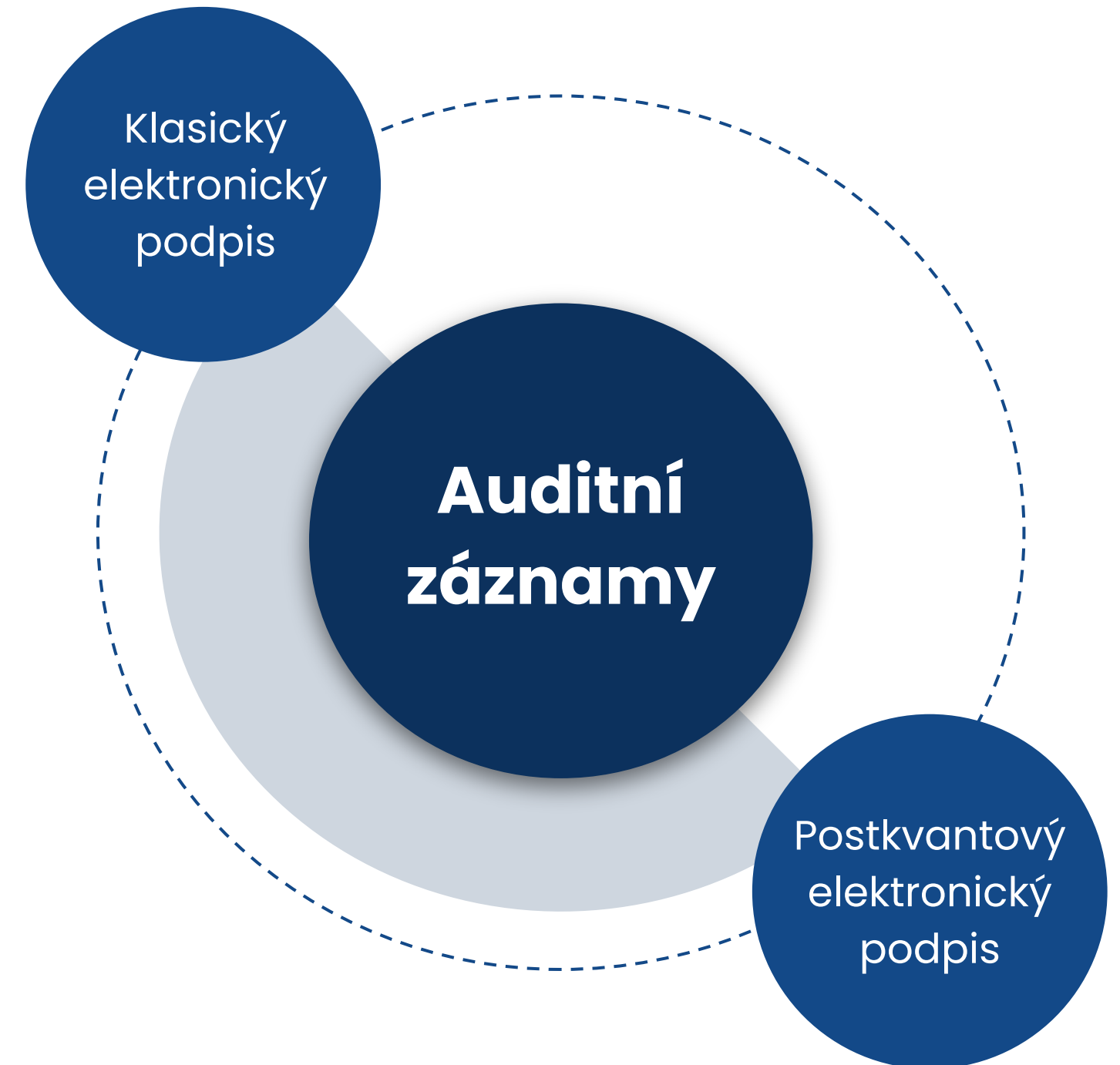
- Hybridní model
- Projekty implementující kandidáty
 - [Cortex M4](#), [Open Quantum Safe](#)
- Pracovní skupiny pro jednotlivé technologie (např. TLS)
- Migrační plány a manuály
- Problémy
 - Výpočetní a latenční overhead
 - Omezení hardware, protokolů
 - Kompatibilita, podpora
 - *Kontroverze* NIST
 - Intellectual Property

A co dělá M+?



Aktivity MONET+

- Pilotní projekt
- Integrace PQC algoritmů pro auditní záznamy
 - Hybridní model
 - Integrace PQC knihoven
 - Bez výrazných technických limitů
 - Nutnost dlouhé retence
- Možnost rozšíření na další typy podepisovaných dat
- Čekáme na standardizaci a podporu v hardware



Aktivity MONET+

- Sledujeme novinky a trendy, účastníme se konferencí a akcí
 - PQC Summer School
 - NIST konference
 - IACR *Crypt konference
 - Santa's Crypto



Aktivity MONET+

- Pravidelně pořádáme interní i veřejné přednášky
 - Czechitas
 - CyberRangers
 - Webinars, podcasts



A modern office interior with a man on a phone, a man on stairs, and a man and woman talking.

Děkuji!

Potřebujete vyřešit kryptografii
ve vaší organizaci?

Kontaktujte nás.

www.proid.cz | info@proid.cz

