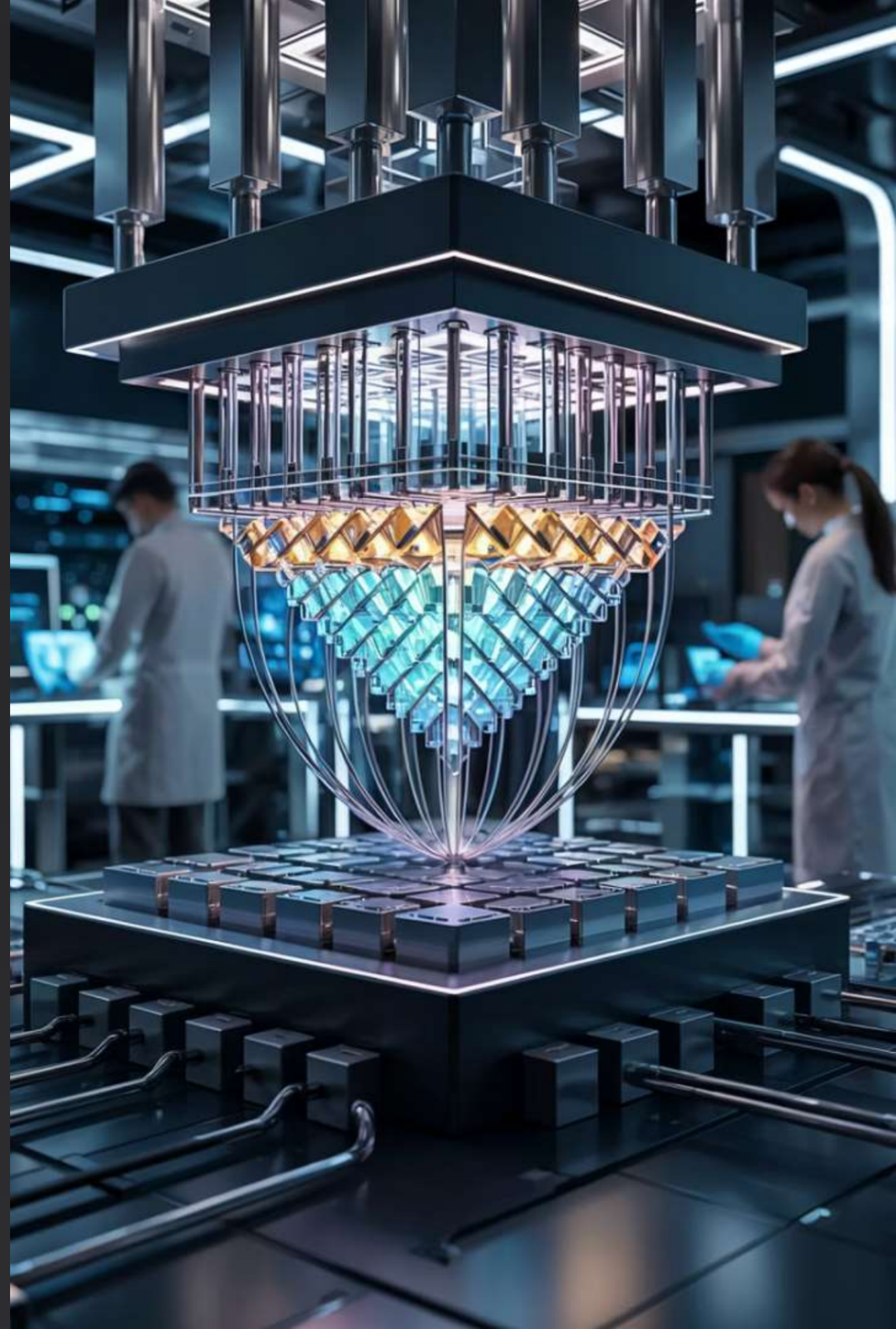
Kvantinės kompiuterijos grėsmės dabartinei kriptografijai: realybė ar nereikalinga baimė?

Kvantinės technologijos - tai naujas mokslo ir inžinerijos laukas, kuris išnaudoja kvantinės mechanikos principus.

Jos tampa vis svarbesnės XXI amžiuje, nes žada revoliuciją skaičiavimuose, komunikacijoje ir saugume.

Dr. Šarūnas Grigaliūnas



Bitai ir kubitai – esminis skirtumas

Klasikinis bitas

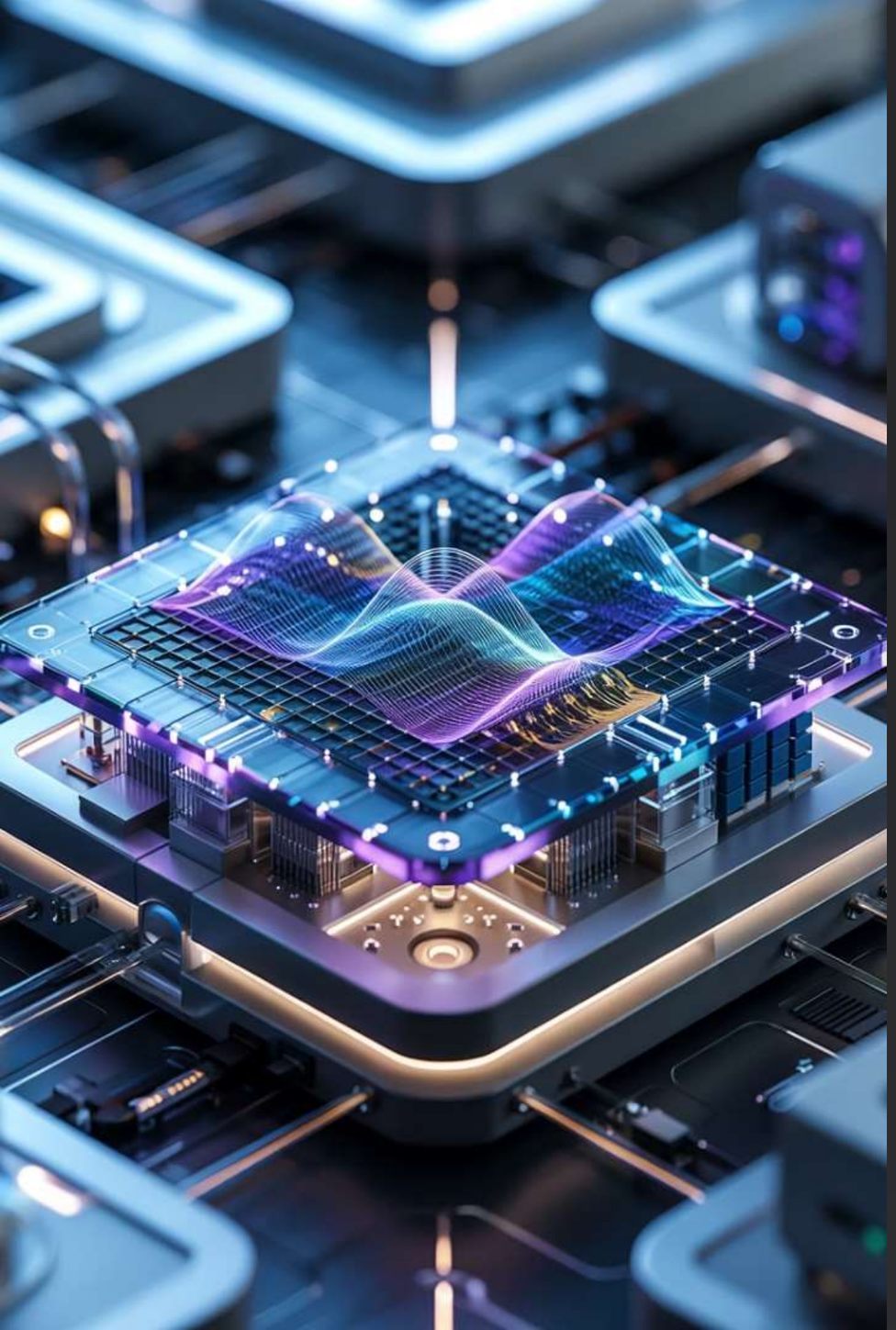
Gali būti tik 0 arba 1.

Veikia nuosekliai, sprendžiant vieną būseną vienu metu.

Kvantinis kubitas

Gali būti 0 ir 1 vienu metu (superpozicija).

Leidžia išnagrinėti visus labirinto kelius vienu metu.



Revoliucija skaičiavimuose

Kvantiniai paraleliniai skaičiavimai

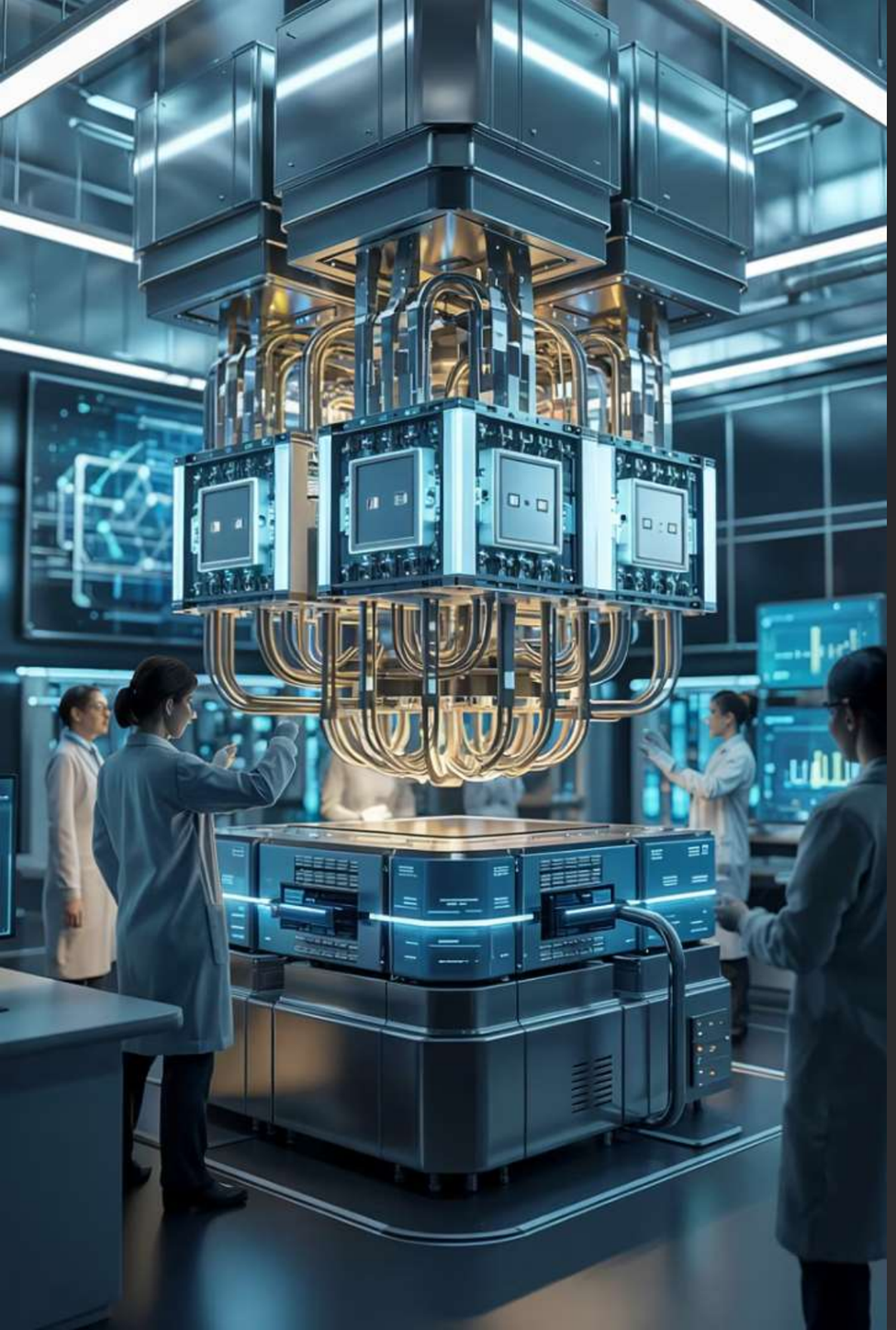
Leidžia atlikti daugybę skaičiavimų vienu metu.

Kvantinė interferencija

Bangų sąveika, stiprinanti teisingus atsakymus.

Dekoherencija

Didžiausias iššūkis - kvantinių būsenų nestabilumas.



Galingiausi kvantiniai kompiuteriai šiandien

1121

IBM CONDOR

Galingiausias IBM kvantinis procesorius.

4158

KOOKABURRA

IBM planuojamas 2025 metais.

103

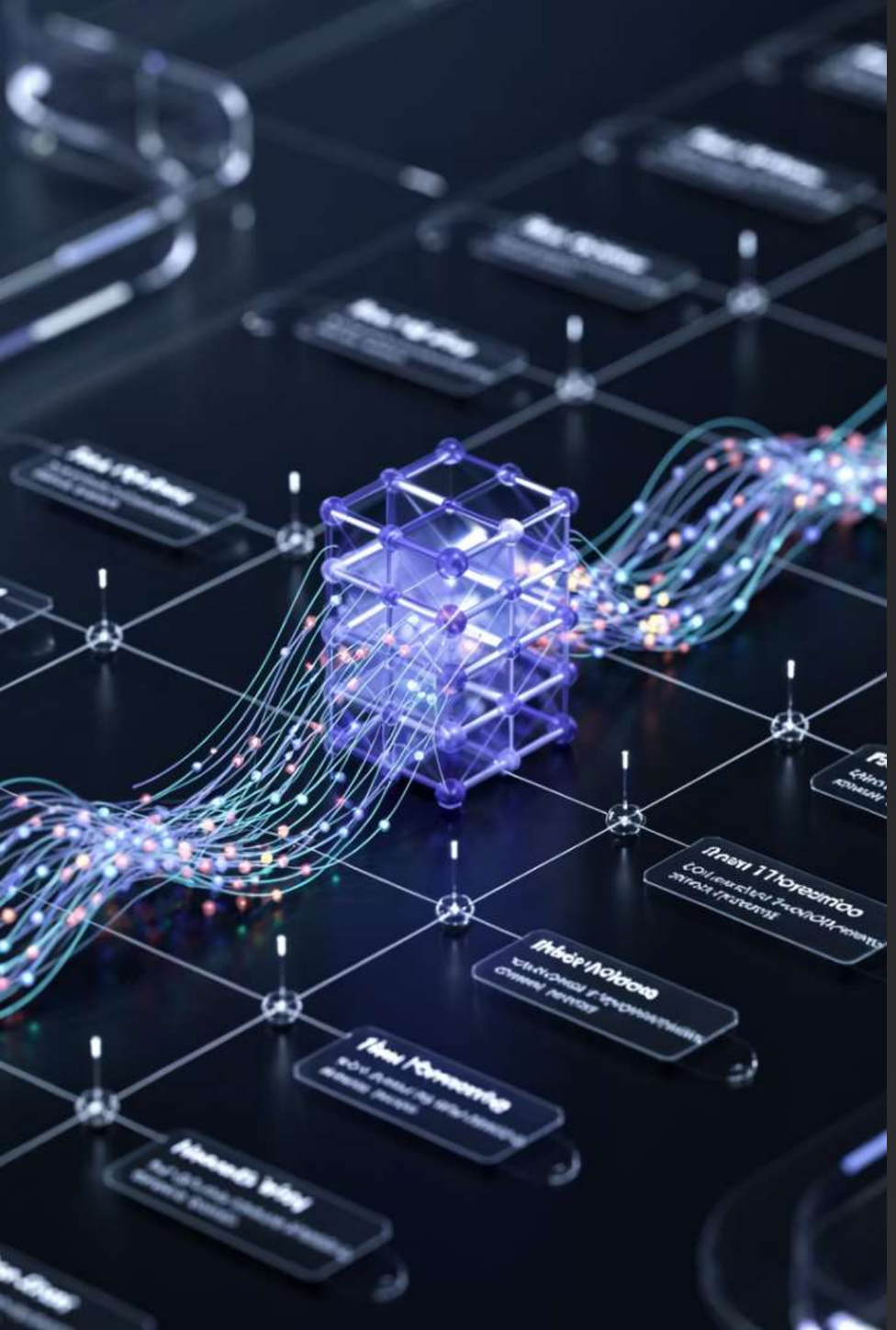
Google Willow

Pristatytas 2024 m. gruodžio 9 d.

32

IAONQ

Jonų spąstų technologija.



Pagrindiniai pasiekimai kvantinių kompiuterių srityje

2019: Kvantinis pranašumas

Google Sycamore atliko skaičiavimą, kuris klasikiniam kompiuteriui užtruktų 10,000 metų.

Shor'o algoritmas

Demonstruoja galimybę efektyviai faktorizuoti didelius skaičius.

Grover'io algoritmas

Žymiai pagreitina paiešką nesutvarkytose duomenų bazėse.

Ateities kvantiniai kompiuteriai

IBM Condor: 1121 kubitų

Pasiektas 2024 metais.

Tarpiniai tikslai

Klaidų korekcijos tobulinimas ir kubitų kokybės gerinimas.

Google: 1 milijono kubitų

Ambicinga vizija iki 2030 metų.

Kvantinių technologijų rinkos dalyviai

Technologijų gigantai

IBM, Google, Intel

Kvantinio verslo atsovai

Rigetti, D-Wave, Quantinuum, PsiQuantum

Startuoliai

Xanadu, IonQ

Quantum AI
Kvantinis kompiuteris + dirbtinis intelektas

Kvantinis mašininis mokymasis (QML)

Kvantiniai algoritmai, pagerinantys mašininio mokymosi efektyvumą.

Duomenų klasifikacija

Žymiai greitesnė didelių duomenų rinkinių analizė.

Kvantiniai neuroniniai tinklai

Naujos architektūros, išnaudojančios kvantinį paralelizmą.

Sinergijos potencialas

Geresni AI sprendimai

Optimizuoti algoritmai realiems iššūkiams spręsti.

Spartesnis mokymas

Kvantiniai kompiuteriai pagreitina neuroninių tinklų mokymą.

Kvantinis optimizavimas

Efektyvesnė sprendimų paieška sudėtingose erdvėse.

9 kubitų tipai – pagrindas kvantinei kompiuterijai

Kubitų tipas	Kubitų tipas (angliškai)	Aprašymas
Superlaidūs kubitai	Superconducting qubits	Dažniausiai naudojami (IBM, Google); greiti, bet reikalauja itin žemos temperatūros.
Jonų spąstų kubitai	Trapped ion qubits	Pavyzdys: IonQ; labai tikslūs, bet lėtesni.
Topologiniai kubitai	Topological qubits	Pavyzdys: Microsoft (teorinis); atsparūs triukšmui.
Fotonių kubitai	Photonic qubits	Naudojami kvantinėje komunikacijoje ir tinkluose.
Spinių kubitai puslaidininkiuose	Spin qubits in semiconductors	Intel projektai; suderinami su klasikine elektronika.
Branduolinio sukimosi kubitai	Nuclear spin qubits	Ilgas gyvavimo laikas; stabilūs, bet sudėtingai valdomi.
Neutralios atomų kubitai	Neutral atom qubits	Startup Xanadu ir kiti; lankstus valdymas ir švietimas lazeriais.
Mechaniniai kubitai	Mechanical qubits	Kvantinės vibracijos; dar tyrimų stadijoje.
Molekuliniai kubitai	Molecular qubits	Tyrinėjami kaip kvantinės informacijos laikmenos molekulėse.

Kibernetinės grėsmės kvantinėje eroje

Shor'o algoritmo grėsmė

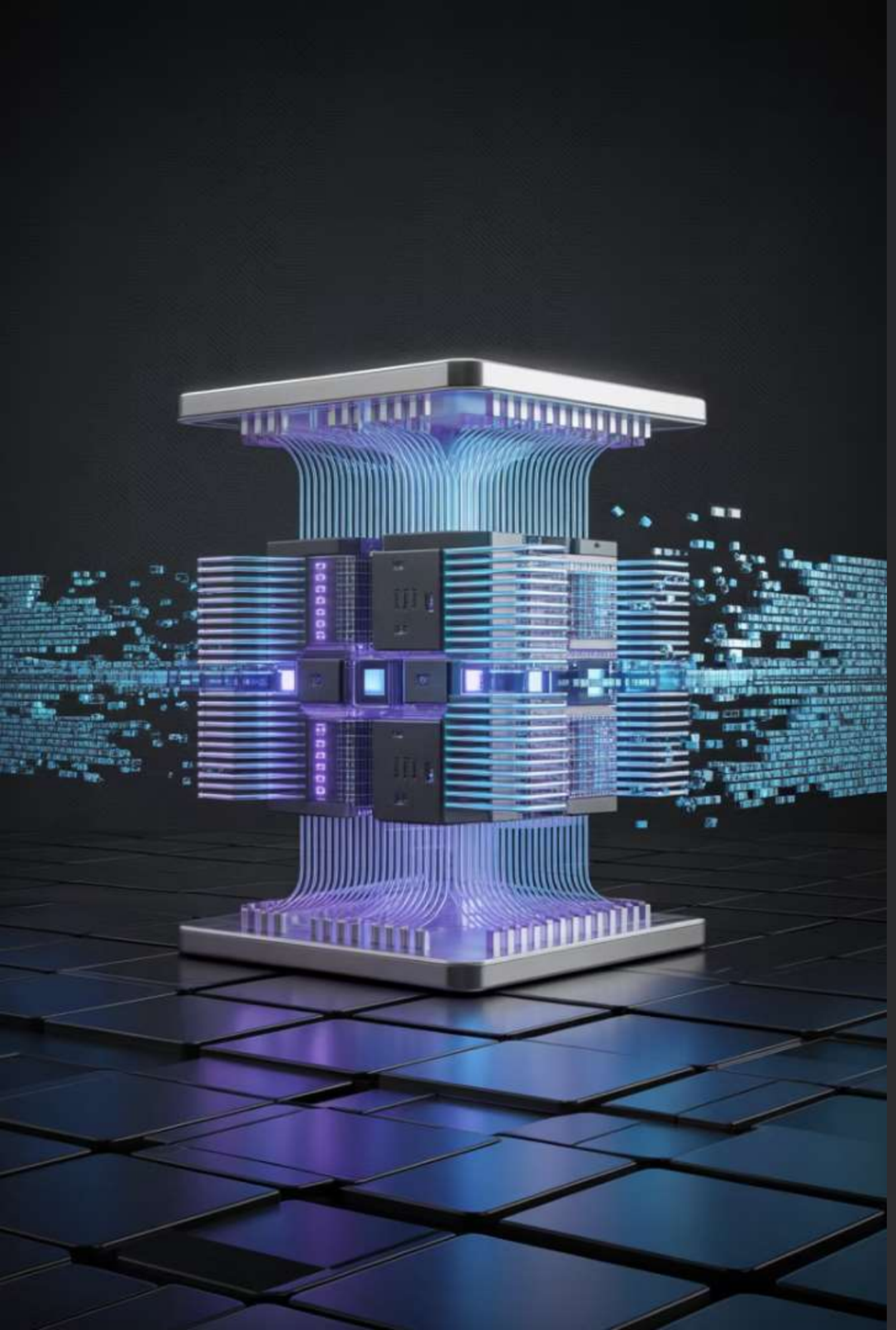
Gali efektyviai sulaužyti RSA ir ECC šifravimo sistemas.

Klasikinių šifravimo sistemų pažeidžiamumas

Dabartiniai saugumo standartai taps nepatikimi.

Skaitmeninių parašų rizika

Elektroninės bankininkystės ir identifikavimo sistemų grėsmės.



Shor’o algoritmas

Klasikinė sauga remiasi sudėtingu matematikos uždaviniu - didelių skaičių faktorizacija. Nors klasikiniais kompiuteriais tai neįtikėtinai lėta užduotis, kvantinis Shor'o algoritmas leidžia ją išspręsti eksponentiškai greičiau.

Shor'o algoritmas veikia pasirenkant atsitiktinį skaičių, kuris yra pirminis su N, tada kvantiniu būdu randamas periodas r iš funkcijos f(x)=a^x mod N. Jei r nelyginis arba a^(r/2) ≡ -1 mod N, procesas kartojamas. Kitu atveju apskaičiuojami gcd(a^(r/2) ± 1, N), kurie yra tikrieji dalikliai.

Šio algoritmo rezultatas - RSA apsaugos pažeidimas, dėl kurio SSL/TLS ryšiai tampa nesaugūs kvantiniame amžiuje.

Kvantinis saugumo valdymas

Kvantiniai įrankiai gali stiprinti ne tik puolimą, bet ir gynybą. Vienas iš metodų - dvipusis pažeidžiamumo grafas, kuriame vienoje pusėje vaizduojamas tinklo turtas (serveriai, duomenys), o kitoje - pažeidžiamumai (silpni slaptažodžiai, programų klaidos).

Tinklo turtas

Serveriai, duomenys, įrenginiai

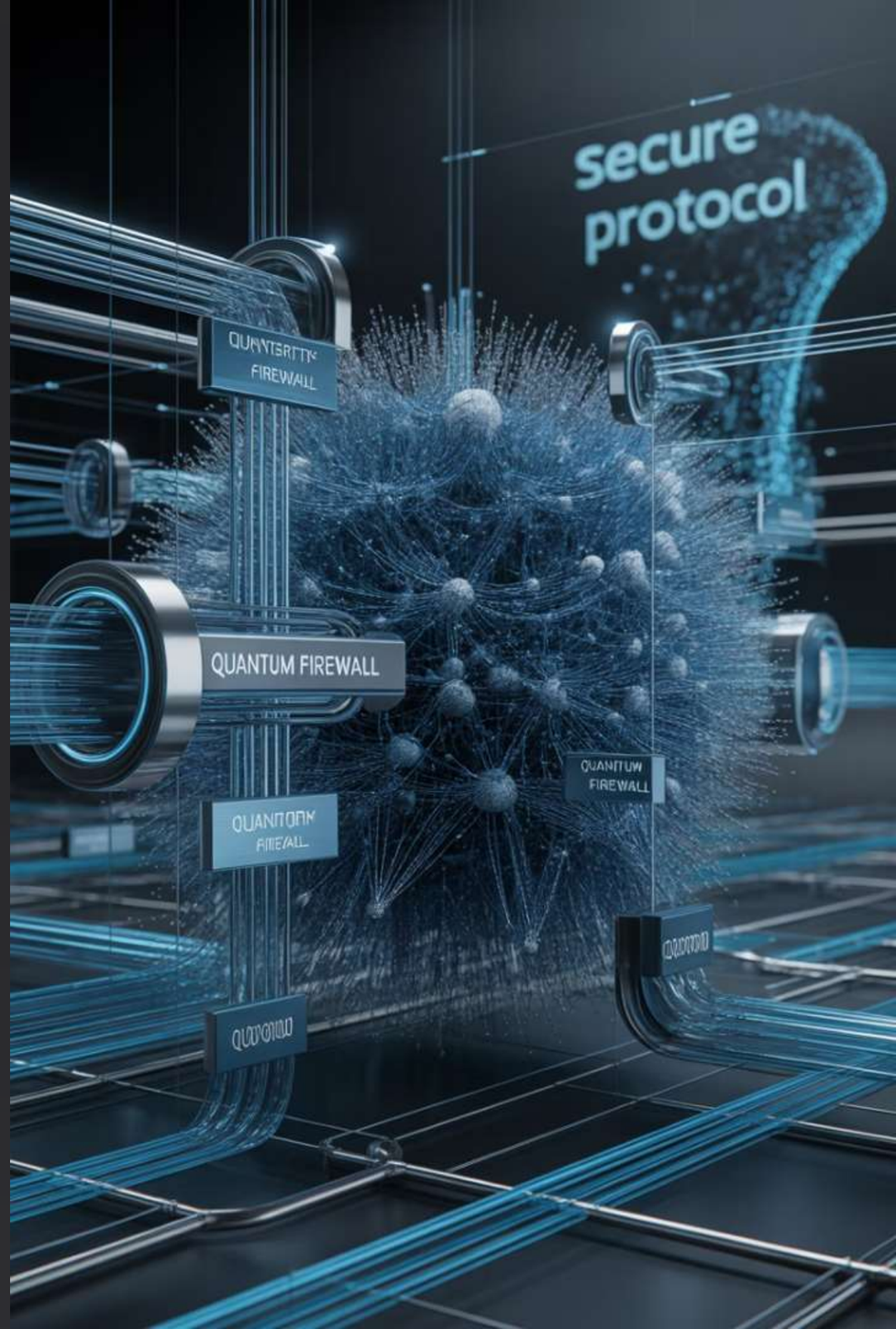
Pažeidžiamumai

Silpni slaptažodžiai, programų klaidos

Kvantinė analizė

Trumpiausi pažeidžiamumo keliai, minimalūs pataisymų rinkiniai

Kvantiniai algoritmai gali greičiau nustatyti trumpiausius pažeidžiamumo kelius ("kill chain") ir minimalius pataisymų rinkinius, reikalingus tinklo saugumui užtikrinti. Šie metodai gali būti integruojami su kibernetinių grėsmių analizės sistemomis, tokiomis kaip SOC ar SIEM, optimizuojant sprendimus per kvantinį grafo padengimo uždavinį.



Kvantinė komunikacija

Quantum Key Distribution (QKD)

Saugus kriptografinių raktų perdavimas, paremtas kvantinės mechanikos principais.

EAGLE-1 palydovas

European Quantum Communication Infrastructure (EuroQCI) kvantinės komunikacijos palydovas - QKD iš kosmoso.

Kvantinis internetas

Ateities vizija - globalus tinklas su neįsilaužiamu ryšiu.

Post-kvantinis atsparumas

Lattice-based šifravimas

Saugumo pagrindas - sudėtingos matematinės gardelių problemos.

Hash-based metodai

Vienkrypčių funkcijų naudojimas, atsparus kvantiniams išpuoliams.

Code-based šifravimas

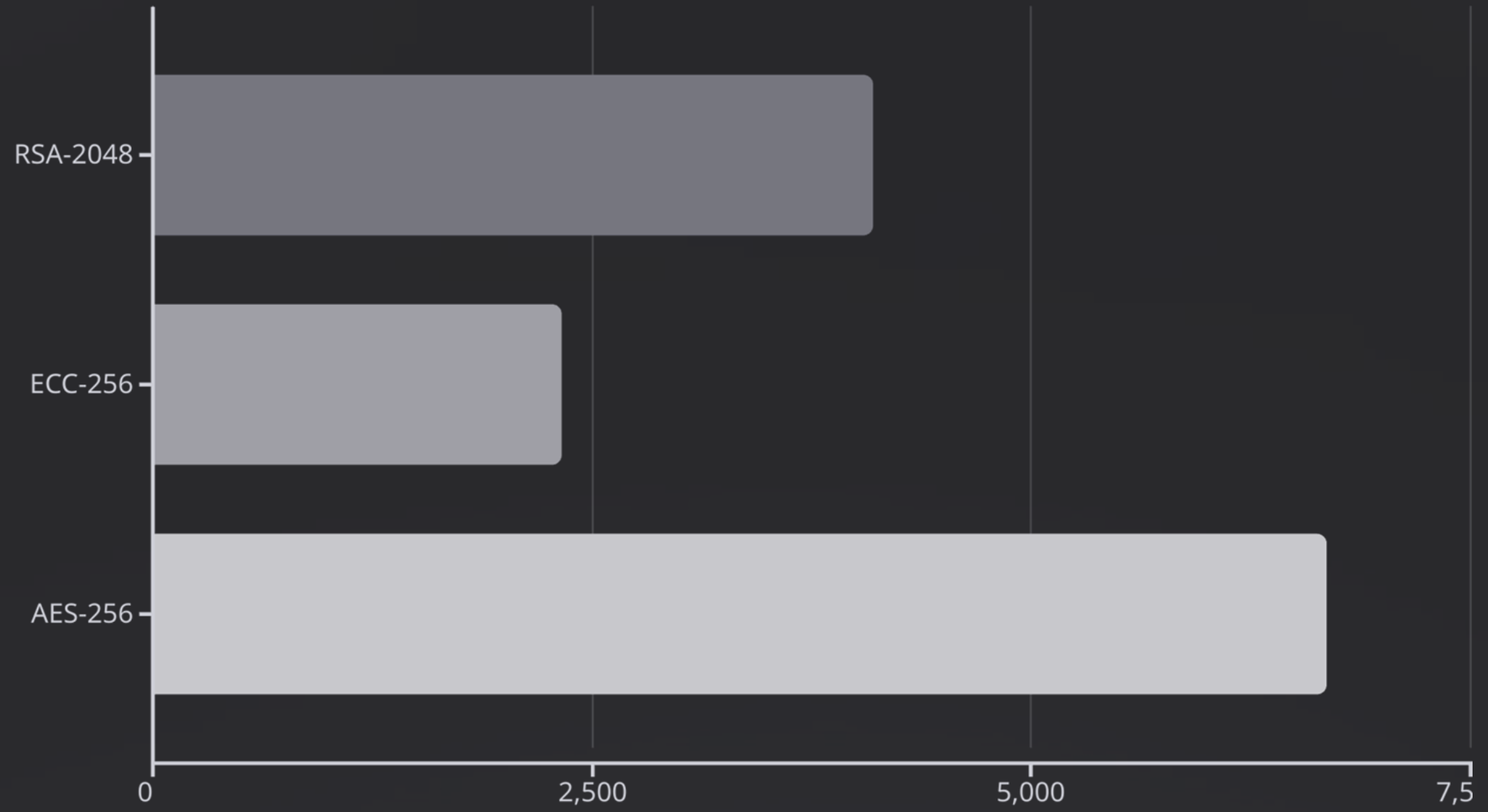
Klaidų korekcijos kodų panaudojimas saugumui užtikrinti.

NIST standartai [5]

Naujų saugumo standartai, atsparūs kvantiniams kompiuteriams.

Kvantiniai hakeriai (#qacker)

Qacker’iai - tai kibernetiniai nusikaltėliai, naudojantys kvantinius kompiuterius šiframs laužyti.



SSL ryšiui, paremtam RSA-2048, sulaužyti reikėtų apie 4100 loginių kubitų.

2025 balandis. Šanchajaus universiteto prof. Wangas Chao su „D-Wave Advantage“ sėkmingai sudaugino **90 bitų RSA sveikąjį skaičių**.

Išvados ir ateities perspektyvos

Revoliuciniai pokyčiai

Kvantinės technologijos keičia saugumo, skaičiavimo ir komunikacijos taisykles.

Pasiruošimas dabar

Būtina ruoštis kvantinei erai jau šiandien.

Filosofinės implikacijos

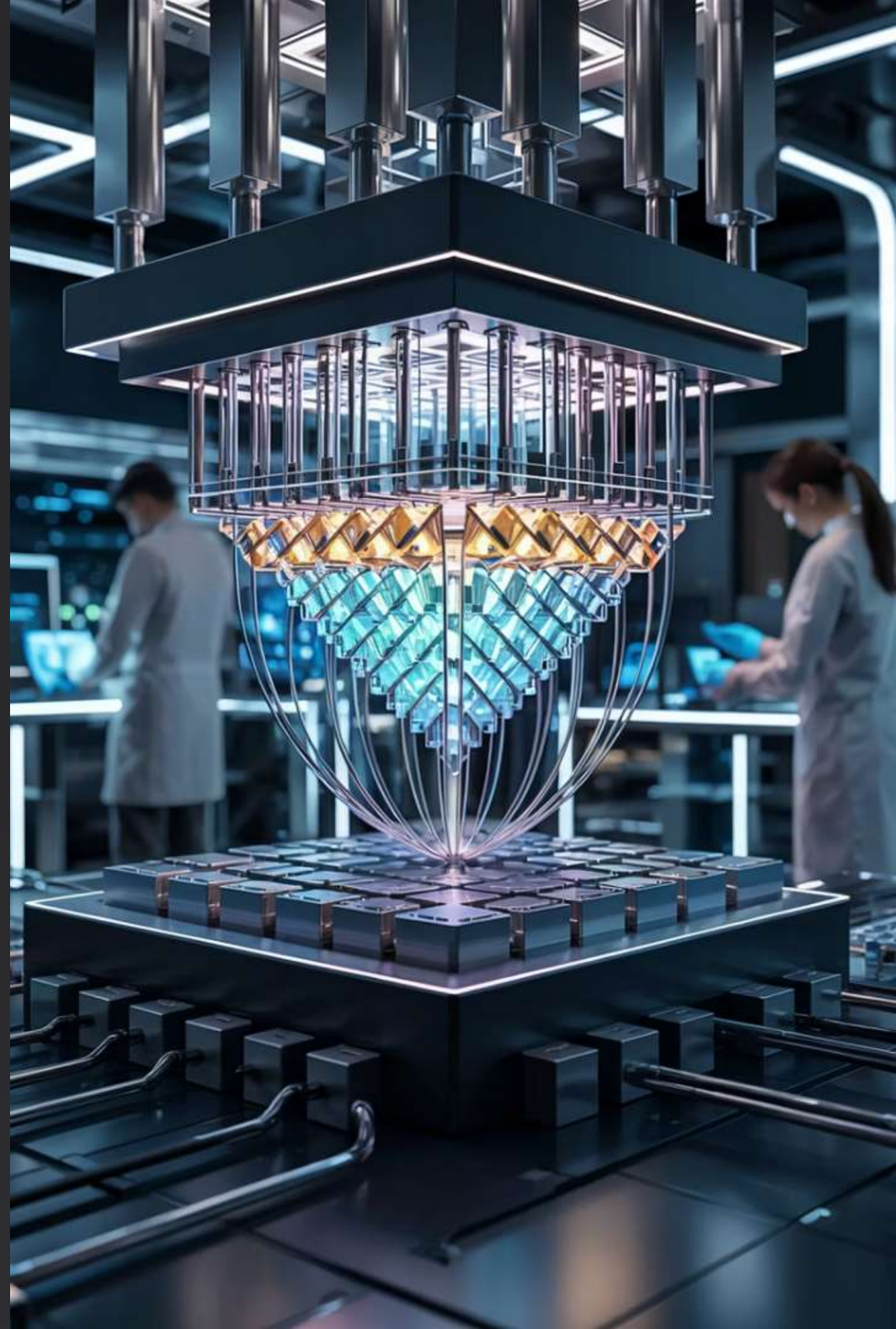
"Google kvantinis čipas įrodo, kad mes gyvename simuliacijoje" – Neil deGrasse Tyson

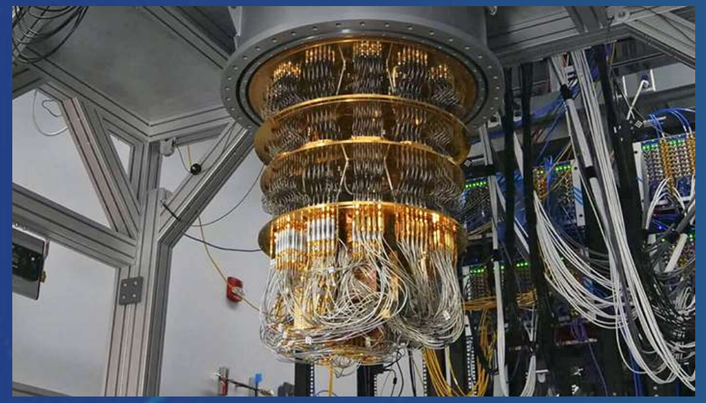
Kvantinės technologijos – ateities revoliucija

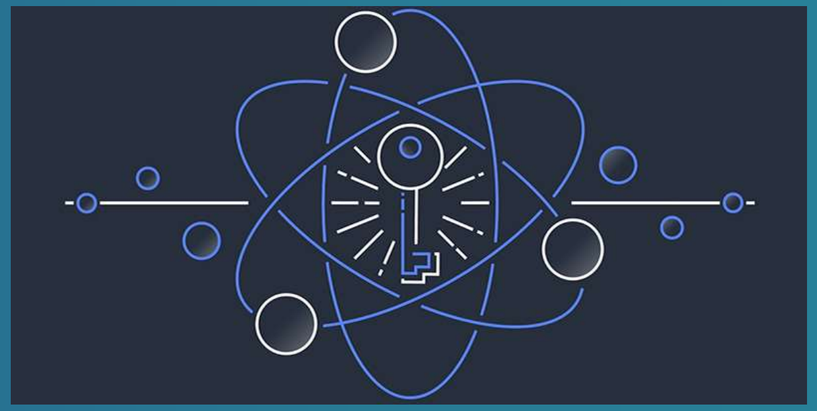
Bendraukime...

Prof. dr. Šarūnas Grigaliūnas

sarunas.grigaliunas@ktu.lt







PASIRENGIMAS Q DIENAI:
DABARTINĖ SITUACIJA IR ATEITIES PERSPEKTYVOS

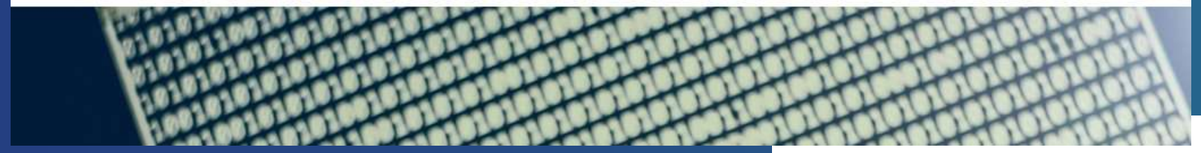
Raimonda Andrijauskienė, Krašto apsaugos ministerija

Q DIENA

Data, kai kvantiniai kompiuteriai taps tokie galingi, kad galės nulaužti šiandieninę kriptografiją

Chinese Scientists Report Using Quantum Computer To Hack Military-Grade Encryption

National, Quantum Computing Business, Research Matt Swayne • October 11, 2024



As of October 2024, China has the largest investment with $15 billion spent on quantum computing research of the estimated $42 billion funding for quantum computing worldwide, according to QURECA. The United States comes second, with $4.98 billion from the National Quantum Initiative.

Finansų sektorius

Energetikos sektorius

Pramonė

Sveikatos sektorius

Gamybos sektorius

Gynybos sektorius

KAM TAI AKTUALU?

Skaitmeninės paslaugos

Daiktų internetas

Telekomunikacijų sektorius

Transporto sektorius

Žemės ūkis

Kiti sektoriai

RENGIMASIS Q DIENAI

Kuriami kvantinių kompiuterių **grėsmėms atsparūs** kriptografiniai algoritmai – **postkvantiniai algoritmai**

JAV Nacionalinis standartų ir technologijų institutas **standartizavo 3 postkvantinius algoritmus:**

- **ML-KEM (CRYSTALS-Kyber)**
  - *raktų apsikeitimui*
- **ML-DSA (CRYSTALS-Dilithium)**
  - *skaitmeniniams parašams*
- **SLH-DSA (SPHINCS+)**
  - *skaitmeniniams parašams*

Family of Algorithms	Parameters	Examples	Transition
Classical Asymmetric Cryptography	112 bits of security strength	RSA (≤2048), ECDH (≤256 bits), ECDSA (≤256 bits)	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	RSA (>2048), ECDH (>256 bits), ECDSA (>256 bits)	Disallowed after 2035
Post-Quantum Asymmetric Cryptography	NIST post-quantum security categories 1 to 5	ML-KEM, ML-DSA, SLH-DSA	Allowed
Symmetric Cryptography	112 bits of security strength	SHA-224	Disallowed after 2030
	≥ 128 bits of security strength	SHA-256, AES-128	Allowed

RENGIMASIS Q DIENAI

Google's PQC Commitments

Google takes these risks seriously, and is taking steps on multiple fronts. Google began testing PQC in Chrome in 2016 and has been using PQC to protect internal communications since 2022. In May 2024, Chrome enabled ML-KEM by default for TLS 1.3 and QUIC on desktop. ML-KEM is also enabled on Google servers. Connections between Chrome Desktop and Google's products, such as Cloud Console or Gmail, are already experimentally protected with post-quantum key exchange.

Starting with quantum-resilient encryption support for the Linux application, NordVPN aims to implement post-quantum cryptography for all applications

NordVPN, a leading cybersecurity company, launches its first VPN application with quantum-resilient encryption. The first iteration of post-quantum cryptography support for NordLynx is now available on the NordVPN Linux application. Additionally, the company plans to implement post-quantum algorithms on all NordVPN applications by 2025 Q1 at the latest.

Microsoft Is Adding New Cryptography Algorithms

Microsoft is updating SymCrypt, its core cryptographic library, with new quantum-secure algorit
Microsoft's details are here. From a news article:

> The first new algorithm Microsoft added to SymCrypt is called ML-KEM. Previously known as CRYSTALS-Kyber, ML-KEM is one of three post-quantum standards formalized last month by the National Institute of Standards and Technology (NIST).

Cisco PQC hardware based on the new NIST standards is expected to become available in late 2025 or 2026. The availability of Cisco products that utilize standard industry components, such as CPUs or TPMs, will be dependent on their availability. This will likely delay their availability until late 2026 or 2027.

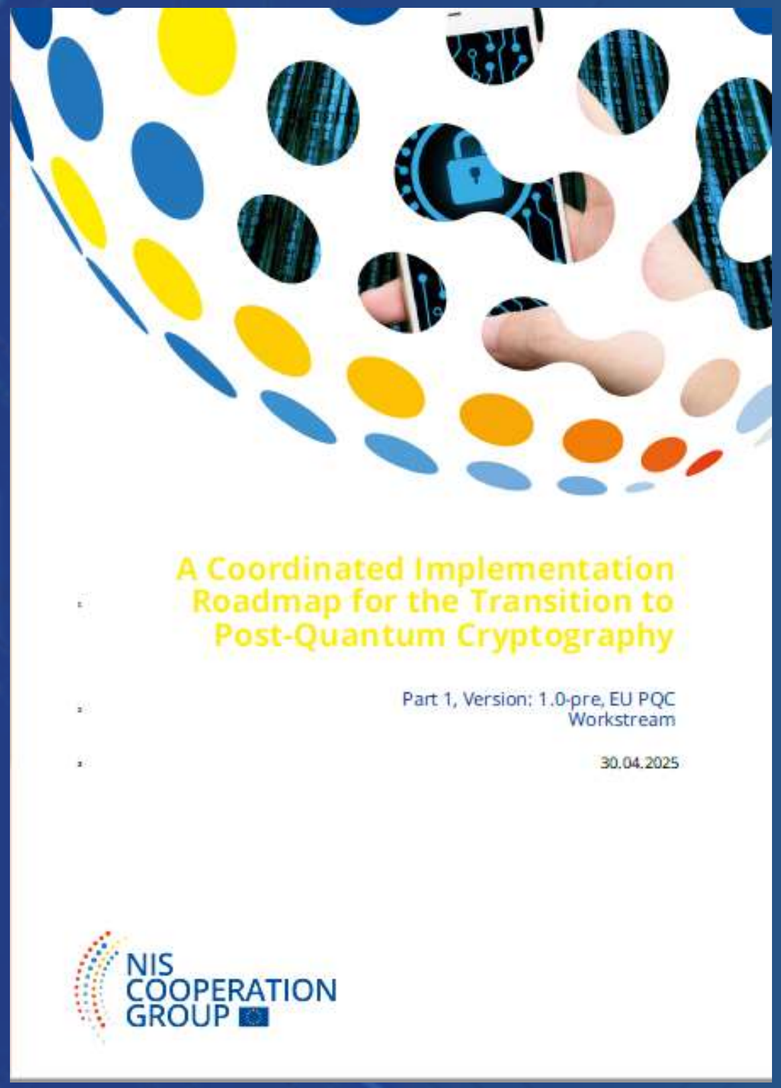
RENGIMASIS Q DIENAI

2024-04-11 Komisijos rekomendacija (ES) 2024/1101 dėl Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairių

Įsteigta Postkvantinės kriptografijos darbo grupė

Parengtos koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairės

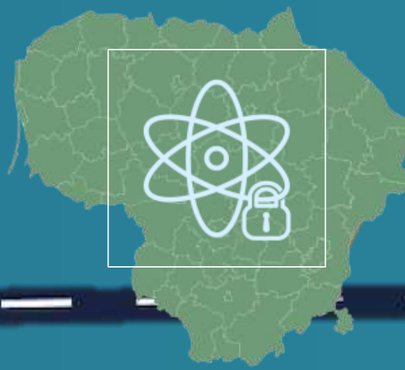
KOORDINUOTŲ PERĖJIMO PRIE POSTKVANTINĖS KRIPTOGRAFIJOS VEIKSMŲ GAIRĖS



Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high and medium risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high risk use cases has been completed.
   - PQC transition planning and pilots for medium risk uses cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium risk use cases has been completed.
   - The PQC transition for low risk use cases has been completed as much as feasible.

Q-DAY



Organizacijų perėjimo prie postkvantinės kriptografijos planų parengimas

Lietuvos perėjimo prie postkvantinės kriptografijos plano parengimas

Organizacijų faktinis perėjimas prie postkvantinės kriptografijos

Grėsmių supratimo didinimas

Nacionalinės perėjimo prie postkvantinės kriptografijos koordinacinės grupės sudarymas

AČIŪ!

PQC MIGRACIJA ORGANIZACIJOJE

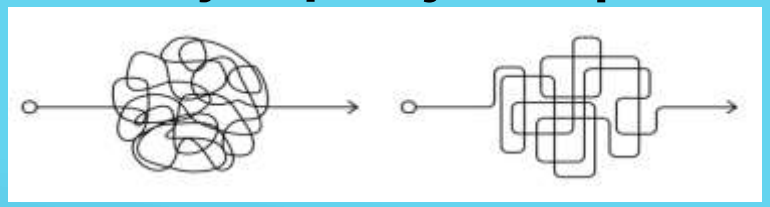
KODĖL REIKIA RUOŠTIS PQC MIGRACIJAI?

- **Kvantinė grėsmė:** kvantiniai kompiuteriai gebės nulaužti dabartinius kriptografinius algoritmus.
- **„Saugok dabar – dekoduok vėliau“:** Priešininkai jau dabar gali kaupti šifruotus duomenis, kad atšifruotų juos vėliau.
- **Ilgalaikės sistemos ir duomenys:** Sistemos, kurių duomenys turi išlikti konfidencialūs dešimtmečius, jau šiandien yra pažeidžiami.
- **PQC sprendimas:** Post-kvantinė kriptografija siūlo atsparius algoritmus, kuriuos būtina pradėti diegti laiku.

Nacionalinis kelrodis (planas)

2030 M.

Organizacijos perėjimas prie PQC



Kriptografijos inventorizacija

Rizikos vertinimas

Prioritetų nustatymas

Migracijos plano sudarymas

Testavimas

Postkvantinės kriptografijos diegimas

INVENTORIZACIJA

PQC MIGRACIJOS PIRMASIS ŽINGSNIS – KRIPTOGRAFINIO TURTO ANALIZĖ

Kriptografinio turto apžvalga
Identifikuojami visi algoritmai, raktai, sertifikatai ir protokolai, naudojami organizacijos sistemose.

Trys inventorizacijos sritys
Kriptografinio turto,
Informacijos/kibernetinės apsaugos vertė,
Produkto/paslaugos tiekėjų.

Atsakingi specialistai
Sistemų administratoriai, IT saugumo komanda.

Trukmė ir sudėtingumas
Didelėse organizacijose pilna inventorizacija gali trukti iki 1–2 metų.

RIZIKOS VERTINIMAS

PRIORITETŲ NUSTATYMAS REMIANTIS KVANTINE GRĖSME

Kvantinio scenarijaus analizė
Vertinama, kokią žalą sukeltų kriptografinių aktyvų pažeidžiamumas kvantinio priešininko atveju.

Prioritetų nustatymas
Pirmiausia apsaugomos sistemos, kurių kompromitavimas turėtų kritines pasekmes.

Atsakingi asmenys
IT saugumo ir organizacijos procesų valdymo atstovai, įvertinantys duomenų svarbą ir rizikos apetitą.

Rizikos vertinimo ataskaita
Sudaromas prioritetizuotas aktyvų sąrašas, kuris naudojamas planavimui.

MIGRACIJOS PLANAVIMAS

STRATEGIJA, KOMANDOS SUDARYMAS IR SPRENDIMŲ PASIRINKIMAS

Migracijos strategija
Nustatoma, ką ir kuo keisti, kokia seka, atsižvelgiant į priklausomybes tarp sistemų.

Sprendimų pasirinkimas
Parenkami PQC algoritmai, numatomi sprendimai ir Kriptografinio lankstumo architektūra.

Komandos suformavimas
PQC migracijos vadovas ir komanda

Resursai ir biudžetas
Planuojami ištekliai, terminai, įrangos poreikiai ir tiekėjų vertinimai.

TESTAVIMAS

BANDOMOJI APLINKA IR POST-KVANTINIŲ ALGORITMŲ PATIKRINIMAS

Laboratorinis testavimas: PQC algoritmai išbandomi kontrolinėse sąlygose, naudojant reprezentatyvias sistemas.

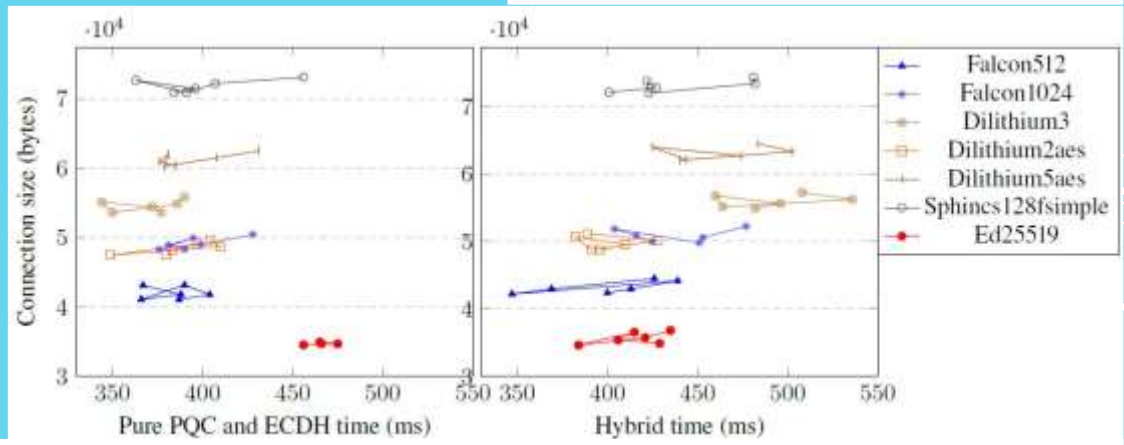
Suderinamumo tikrinimas: įvertinama kaip algoritmai veikia su esama programine ir aparatine įranga.

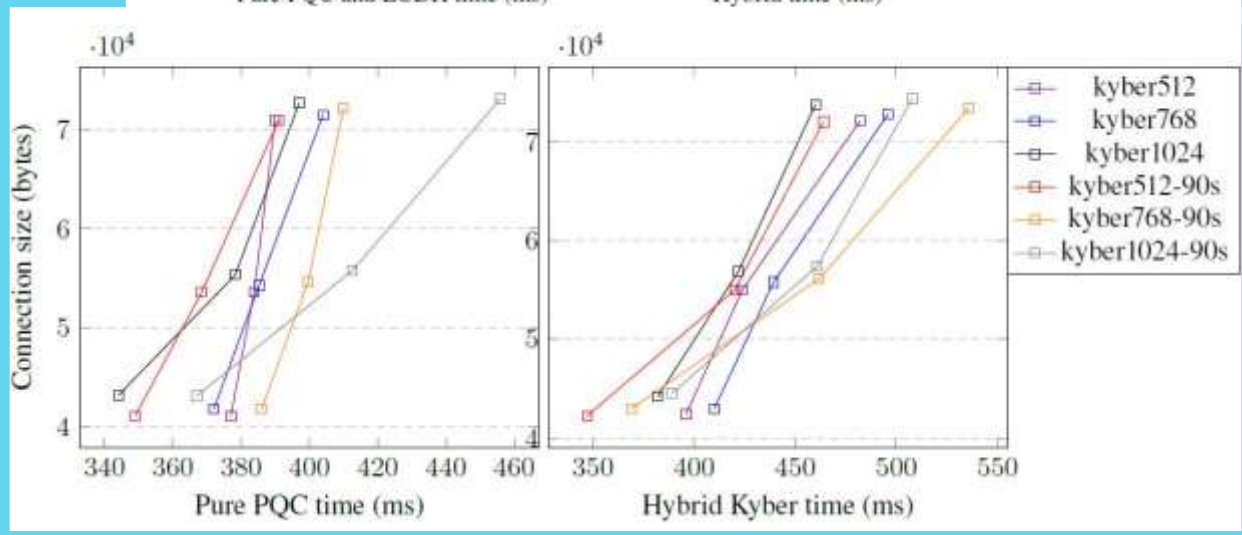
Našumo analizė: Stebimas algoritmų poveikis greičiui, tinklo apkrovai ir operacijų delsimui.

Probleminių vietų identifikavimas: Ankstyvas testavimas leidžia ištaisyti nesklandumus prieš produkcinį diegimą.

Diffie-Hellman with digital signature Ed25519 implementation

Ed25519 signature with:	time (ms)	size (bytes)
Ecdh-nistp256	459	34540
Ecdh-nistp384	475	34700
Ecdh-nistp521	465	34942
Average:	**466**	**34727**





ĮGYVENDINIMAS

PALAIPSNIS DIEGIMAS IR KRIPTO LANKSTUMO UŽTIKRINIMAS

Palaipsnis diegimas: Nauji algoritmai diegiami pirmiausia ten, kur rizika didžiausia, o sistemos kritinės.

Rizikos kontrolė: Svarbu išvengti naujų spragų – kiekvienas pakeitimas testuojamas ir audituojamas.

Minimizuoti trikdžius: Atnaujinimai planuojami taip, kad netrukdytų veiklai; pritaikomi BCP/DR planai.

Kripto lankstumas: Architektūra turi leisti greitai keisti algoritmus, reaguojant į naujus iššūkius.

APIBENDRINIMAS

1. Etapai
Migracija vykdoma struktūriškai: inventorizacija, rizikos vertinimas, planavimas, testavimas, įgyvendinimas.

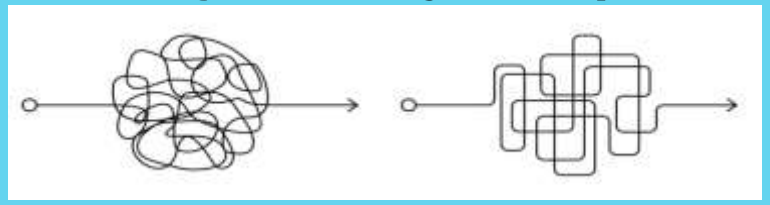
2. Komandos darbas
Sėkmei būtinas koordinuotas darbas tarp IT, teisės, saugumo ir vadovybės.

3. Ekosistemos svarba
Tiekėjų, partnerių ir klientų įsitraukimas nulemia bendrą saugumo lygį.

4. Veikti reikia dabar
Kvantinė grėsmė artėja – organizacijos turi ruoštis jau šiandien.

Nacionalinis kelrodis (planas)

Organizacijos perėjimas prie PQC



Kriptografijos inventorizacija

Rizikos vertinimas

Prioritetų nustatymas

Migracijos plano sudarymas

Testavimas

Postkvantinės kriptografijos diegimas