MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

ROBERTAS LAVRENOVAS

KVANTINĖS KOMPIUTERIJOS IR KVANTINIO ŠIFRAVIMO YPATUMAI IR PANAUDOJIMO GALIMYBĖS LIETUVOJE

Magistro baigiamasis darbas

Vadovas

prof. dr. Tadas Limba

VILNIUS, 2022

MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

KVANTINĖS KOMPIUTERIJOS IR KVANTINIO ŠIFRAVIMO YPATUMAI IR PANAUDOJIMO GALIMYBĖS LIETUVOJE

Kibernetinio saugumo valdymo baigiamasis darbas
Studijų programa 6211LX066

Recenzentas

Vadovas
prof. dr. T. Limba
2022 12 05

Atliko
KSVvmis20-1
R. Lavrenovas
2022 12 05

VILNIUS, 2022

TURINYS

LENTELĖS

PAVEIKSLAI

SANTRUMPOS

Atomas - mažiausia elektriškai neutrali cheminio elemento dalelė, turinti jo chemines ir fizikines savybe;
Bitas ir baitas – bitas yra mažiausias elektroninės informacijos saugojimo vienetas kuris saugo 0 ir 1. 8 bitai sudaro baitą;
Blokų grandinė – (*angl. blockchain*) tai nuolat augantis sąrašas, kurio visi įrašai yra susieti vienas su kitu naudojant kriptografiją;
Debesų kompiuterija – tai galimybė naudotis kompiuterine ir programine įranga internete. Dažniausiai mokama ir apmokestinama tik už sunaudotus resursus;
DevOps – IT praktika kuri sujungia programinės įrangos kūrimą ir IT operacijas (*angl. Development and Operations*);
DevSecOps – IT praktika apimanti programinės įrangos kūrimą ir IT operacijas, bet taip pat ir įgyvendinanti saugumo reikalavimus visame programinės įrangos kūrimo etape;
Dictonary attaks – liet. Žodyno atakos. Tai tokia kibernetinė ataka, kuomet bandoma parinkti tam tikrą žodį, frazę ar skaičių ir raidžių kombinaciją neteisėtam prisijungimui. Tokios atakos vykdomos imant žodžius iš tam tikro sudaryto sąrašo, dar kitaip vadinama – žodynu;
Elektronas - sudaro atomų elektroninius sluoksnius, iš kurių gali išsilaisvinti gavę pakankamai energijos;
Faktorialas – tai natūraliojo skaičiaus visų natūraliųjų skaičių suma. Pvz. Skaičiaus 5! Faktorialas yra 120 = 5 x 4 x 3 x 2 x 1 = 120;
Fotonas - elektromagnetinės bangos dažnis;
Integrinis grandynas – iš anglų kalbos integrated circuit. Dar kitaip vadinama mikroschema. Kuris susideda iš neatskiriamų elementų, tokių kaip rezistorius, kondensatorius ar tranzistorius;
IT – Informacinės technologijos;
Kriptovaliuta – skaitmeninė valiuta, dažniausiai mokėjimai atliekami internete ir anonimiškai. Paremta blokų grandinės technologija;
Kvantinė mechanika (kvantinė fizika) - aprašo mikrodaleles (atomus, elektronus, protonus, neutrinus ir kt) ir jų sąveikas;
Mainframe – didelis kompiuteris dažniausiai naudojamas stambių įmonių, pvz. bankų, atlikti vieną ir tą pačią operaciją. Nėra superkompiuterio atitikmuo;
MIT - Masačiusetso technologijų institutas (*angl. Massachusetts Institute of Technology*);
NASA – Jungtinių Amerikos valstijų Nacionaline aeronautikos ir kosmoso agentūra (*angl. National aeronautics and space agency*);
Nestruktūrizuoti duomenys – duomenys kurie neturi jokio duomenų modelio;
Qbitai – dar kitaip kvantinis bitas. Mažiausias kvantinės informacijos saugojimo vienetas. Skirtingai nei bitas, qbitas gali informaciją saugoti trijuose padėtyse 0,1 arba abu kartu.

Absoliutus nulis – žemiausia įmanoma temperatūra kurioje sustoja bet koks atomų ir molekulių judėjimas (kvantinės kompiuterijos pagrindiniai veikimo principai). Ši temperatūra yra lygi -273.15 ^{o}C

Python – programavimo kalba sukurta 1991 m. plačiai naudojama matematiniuose skaičiavimuose, didelių duomenų analizei.

Startuolis – inovatyvi aukštųjų technologijų įmonė, pasižyminti dideliu augimo potencialu.

TLS – (angl. Transport layer security) transporto lygmens apsauga, tai yra kriptografinis protokolas, skirtas saugiai komunikacijai internetu ir kompiuterio tinklu, kuomet perduodamos informacijos srautas yra šifruojamas;

ĮVADAS

Temos aktualumas. Europos kvantiniame manifeste kuri 2016 metais parengė Europos sąjungos komisaras Gunther Oettinger kartu su Niderlandų ministru Henk Kamp yra akcentuojamas kvantinės kompiuterijos ir iš jos sekančio kvantinio šifravimo aktualumas pasaulyje, kadangi sukūrus pilnai be klaidų veikiančius kvantinius kompiuterius jie iš esmės pakeis daug dalykų pasaulyje, pavyzdžiui leis greičiau atrasti naujus vaistus nuo ligų, nuspėti ekonomikos ar orų prognozes tiksliau negu bet kas kitas (Quantum manifesto, 2016). Tačiau nors kvantiniai kompiuteriai ir žada žmonijai suteikti daug naudos, tačiau jie taip pat pakeis visą informacijos saugumo ir konfidencialumo sampratą, tokią kaip mes suprantame ją šiandien. Pasak Jean-Phillippe Aumasson kvantiniai kompiuteriai atneš kvantinį ir post-kvantinį šifravimą, tai reiškia, kad reikės pakeisti visus šiandien naudojamus šifravimo algoritmus - kvantiniams kompiuteriams atspariais algoritmais (Aumasson, 2017). Todėl nenuostabu, kad tiek didžios pasaulio valstybės, tiek didžiausios pasaulio įmonės investuoja labai didelius pinigus į kvantinės kompiuterijos vystymą bei į naujų, kvantiniams kompiuteriams atsparių šifravimo algoritmų sukūrimą.

Kvantinės kompiuterijos temos aktualumas buvo užtvirtintas ir šiais metais per Nobelio premijos fizikos srityje įteikimo ceremoniją, įvykusią 2022 metų spalio 4 dieną, kur lauretai, Alain Aspect, John F. Clauser ir Anton Zeilinger buvo apdovanoti Nobelio premija, už tyrimus atliktus kvantinio susiejimo srityje bei už padėtus pamatus kvantinės informatikos mokslui (The Nobel Prize in Physics 2022).

Temos ištirtinumas. Kvantinė kompiuterija yra sąlyginai neseniai pradėta tyrinėti mokslo šaka. Mokslininkai apie teorinę kvantinę kompiuteriją pradėjo kalbėti dar aštuntajame dešimtmetyje. Pirmasis mokslininkas galima sakyti padėjęs tvirtus pamatus kvantinei kompiuterijai buvo Richard Feynman dar XX a. aštuntajame dešimtmetyje jis pradėjo kelti hipotezes, kaip pasitelkus fizikos mokslą galima būtų atlikti matematinius skaičiavimus, o jau 1994 metais kitas amerikiečių mokslininkas Peter Shor sukūrė algoritmą pavadinimu - Shor`o algoritmas, kuris teoriškai turėjo apskaičiuoti bet kokio natūraliojo skaičiaus faktorialą, tačiau tas algoritmas buvo per sudėtingas net ir galingiausiems tiek tų dienų, tiek netgi šių dienų superkompiuteriams (Shor, 1994). Tačiau Shor`as teigė, kad šis algoritmas turėtų būti labai lengvai apskaičiuojamas teorinės kvantinės skaičiavimo mašinos, taip vadinamo kvantinio kompiuterio (Shor, 1994).

Nuo 1994 metų kelis metus mokslininkai pagrinde dirbo teorinės kvantinės kompiuterijos srityje, tačiau jau 1998 metais buvo sukurtas pirmas mini demonstracinis kvantinis kompiuteris, kuris dar negalėjo atlikti jokių skaičiavimų, bet galėjo trumpai išlaikyti superpoziciją. Didžiausias kvantinės kompiuterijos proveržis prasidėjo XXI a. kuomet į kvantinės kompiuterijos vystymą įsitraukė didžios pasaulio IT bendrovės. 2017 korporacija Google, kartu su NASA sukūrė pirmąjį kvantinį procesorių, o jau 2019 metais Google išleistas kvantinis procesorius sugebėjo atlikti matematinį skaičiavimą per 200

sekundžių, kurį pasak Google galingiausias šiuolaikinis kompiuteris atliktų tik per 10000 metų (Google, 2019).

Šiai dienai didžiausius pasiekimus kvantinės kompiuterijos srityse susišluoja komandos dirbančios tokiuose įmonėse kaip: IBM, Google, Accenture, D-WAWE ar Qbit, todėl sunku išskirti asmeninius mokslininkų indelius vystant kvantinę kompiuteriją, tačiau vertėtų paminėti keletą asmenybių kurios prisidėjo prie kvantinės kompiuterijos vystymo, tai ir Ryan Babbush Google kvantinių algoritmų departamento vadovas ir D-WAWE pirmosios kvantinės kompiuterijos bendrovės įkūrėjas, pagal išsilavinimą teisininkas Haig Farris ar Carl Dukatz Accenture kvantinės programos vadovas turintis tik bakalauro laipsnį iš Mičigano valstybinio universiteto, ir žinoma Alain Aspect, John Clauser ir Anton Zeilinger laimėjusius 2022 metų fizikos Nobelio premiją.

Taigi, nors šiai dienai į kvantinę kompiuteriją daugiausiai investuoja stambios IT kompanijos, tačiau jos dažnai bendradarbiauja ir investuoja į aukštojo mokslo įstaigas bei įvairius mokslininkus. Puikus tokio bendradarbiavimo pavyzdys galėtų būti ir iš netolimos Latvijos, kur JAV aukštųjų technologijų įmonė Accenture bendradarbiauja su Latvijos Universitetu kvantinės kompiuterijos srityse.

Deja Lietuvoje kvantinė kompiuterija ir kvantinis šifravimas, yra labai mažai nagrinėta ir vystyta tema, šiai dienai pavyko rasti informacijos, kad tik Vilniaus Universitete, Dr. Mindaugas Mačernis dėsto kvantinės kompiuterijos įvadą, kvantinės informacijos ir kriptografijos dalykus, fizikos krypties bakalauro ir magistro programų studentams, tačiau tai yra tik pasirenkamas dalykas. Taip pat pavyko identifikuoti kelis Lietuvos mokslininkus dirbančius užsienyje, pavyzdžiui Ieva Čepaitė Strathclyde universitete Škotijoje rengia disertacija kvantinės kompiuterijos srityje.

Lietuvoje taip pat yra mažai diskutuojama ir iškeliama kvantinės kompiuterijos grėsmių problema.

Tyrimo objektas. Kvantinės kompiuterijos ir kvantinio šifravimo galimybės.

Tyrimo problema. Mokslo šaltiniuose nepakankamai plačiai išanalizuota ar Lietuvos verslas ir viešasis sektorius pasiruošęs kvantinių kompiuterių panaudojimui ir galimiems su tuo susijusiems iššūkiams?

Tyrimo hipotezė. Kvantinė kompiuterija nors ir keldama grėsmę informacijos konfidencialumui, atveria daugiau galimybių verslui ir viešajam sektoriui.

Tyrimo tikslas: nustatyti bei apibrėžti kvantinės kompiuterijos ir kvantinio šifravimo panaudojimo galimybes, bei kylančias grėsmes, bei pateikti su tuo susijusias rekomendacijas.

Tyrimo uždaviniai:

1. Išanalizuoti kvantinės kompiuterijos ir kvantinio šifravimo teorinius aspektus;
2. Išnagrinėti kvantinės kompiuterijos ir kvantinio šifravimo praktiką;
3. Atlikti kvantinės kompiuterijos panaudojimo ir kvantinės kompiuterijos grėsmių tyrimą;

Tyrimo metodika. Analizuojant kvantines kompiuterijos ir kvantinio šifravimo ypatumus, keliamas grėsmės ir panaudojimo galimybės Lietuvoje buvo panaudota sisteminė, apibendrinimo, lyginamoji ir aprašomoji mokslinės literatūros analizė bei kokybinis tyrimas - ekspertų apklausa.

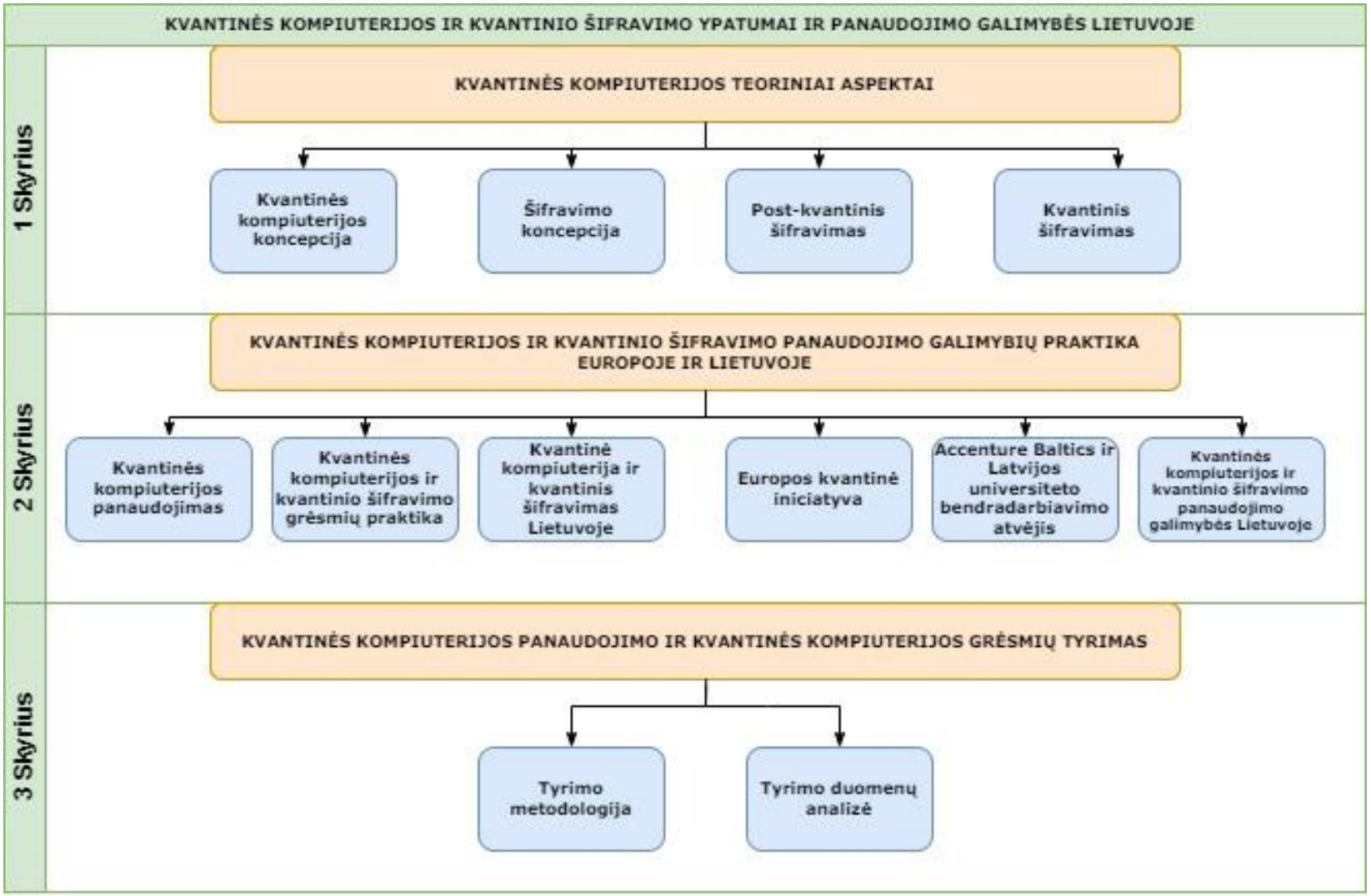
Darbo struktūra. Magistro baigiamasis darbas susideda iš trijų skyrių (žr. 1 pav.). Pirmame skyriuje yra nagrinėjama kvantinės kompiuterijos ir kvantinio šifravimo teorija bei nagrinėjama kvantinės kompiuterijos grėsmių praktika, antrame skyriuje nagrinėjama kvantinės kompiuterijos ir kvantinio šifravimo panaudojimo galimybių praktika, detaliau išnagrinėjant Europos kvantinę iniciatyvą, bei įmonės Accenture ir Latvijos universiteto bendradarbiavimo atvejis kvantinės kompiuterijos srityje. Trečiame skyriuje yra pristatomas ir nagrinėjamas atliktas tyrimas, kurio tikslas aplauksiant ekspertus išsiaiškinti kvantinės kompiuterijos panaudojimo galimybes Lietuvoje, bei pasiruošimą kvantinėms grėsmėms, pristatoma tyrimo metodologija bei tyrimo rezultatai. Darbo pabaigoje pateikiamos išvados ir pasiūlymai.

Darbe pateikta: 22 paveikslai, 3 lentelės. Panaudotas 44 bibliografiniai šaltiniai.

Bendra magistro baigiamojo darbo apimtis be priedų 64 psl..

Darbo praktinis reikšmingumas. Darbo praktinį reikšmingumą atspindi prieš tai Lietuvoje beveik neanalizuota kvantinės kompiuterijos ir kvantinio šifravimo tema. Darbe yra išanalizuota ne tik kvantinės kompiuterijos ir šifravimo teorija, bet taip pat išanalizuotas Europos kvantinis manifestas bei pristatomas praktiškai taikomas kvantinės kompiuterijos taikymo atvejis tiriant rentgenogramas.

Atsižvelgiant į ekspertų nuomonę, išskirtos kvantinės kompiuterijos panaudojimo galimybės Lietuvoje. Šią informaciją galima panaudoti verslui ieškant galimybių plėtrai, norint investuoti į pažangiausias ateities technologijas, taip siekiant apsaugoti informaciją bei duomenis nuo konfidencialumo pažeidimų ir pasiruošti kvantinės kompiuterijos keliamoms grėsmėms.



1 pav. Magistro baigiamojo darbo struktūros loginė schema

1. KVANTINĖS KOMPIUTERIJOS IR KVANTINIO ŠIFRAVIMO TEORINIAI ASPEKTAI

1.1. Kvantinės kompiuterijos koncepcija

Britanikos (*angl. Britannica*) enciklopedija kvantinį kompiuterį įvardina kaip įrankį, kuris patobulina (pagreitina) matematinius skaičiavimus pasitelkiant kvantinės mechanikos principus.

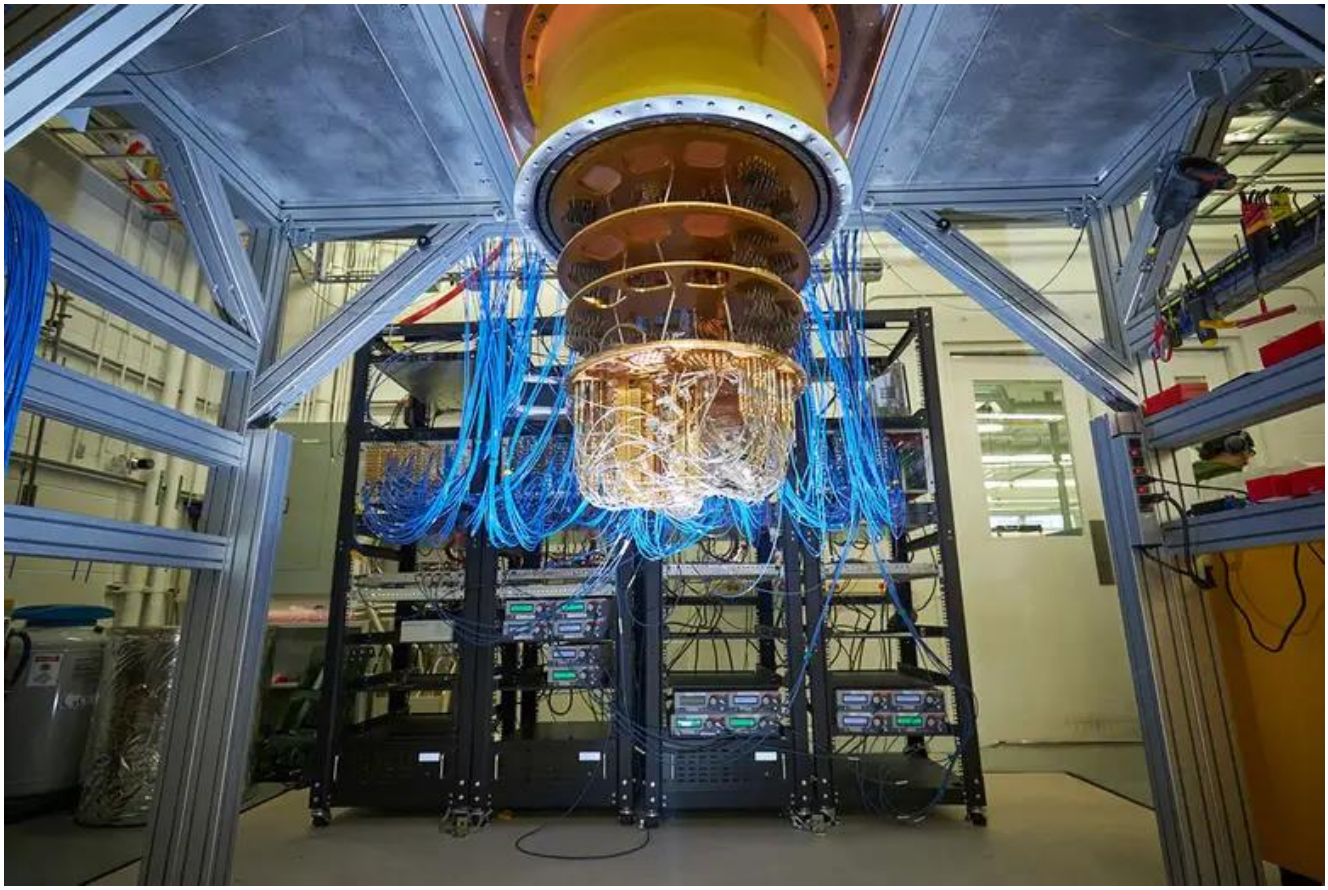
Skirtingai nei paprasti mums žinomi šiuolaikiniai kompiuteriai, veikiantys integrinio grandino, dar kitaip vadinamu mikroschemų (*angl. integrated circuit*) principu (kad atskirti, kuomet yra kalbama apie kvantinius ir kuomet apie integrinio grandino kompiuterius, šiame magistriniame darbe jiems naudosime terminą – klasikiniai kompiuteriai), kvantinių kompiuterių veikimas paremtas fizikos, informatikos ir matematikos mokslais, ir remiasi kvantinės mechanikos mokslu, kuris nagrinėja, kaip mažosios dalelės tokios kaip atomai, elektronai ar fotonai elgiasi visatoje.

Apie atomus ir kitas mažąsias dalelytės veikiančias visą pasaulį pradėta kalbėti dar nuo Demokrito laikų (Aaronson, 2013) , o apie pačią kvantinę kompiuteriją pradėta kalbėti apie 1959m., kuomet dar tik pradėjo rastis pirmieji mikroprocesoriai kompiuteriai. Pirmasis apie tai teoriškai pradėjo kalbėti kvantinės fizikos ir mechanikos pionierius, Nobelio premijos laureatas Richar Freynman, kuris jau 1982 metais pasiūlė kvantinio skaičiavimo algoritmus, kuriuos norint atlikti buvo reikalingas kompiuteris, dirbantis kvantinės mechanikos principais (Feynman, 1984, p. 467-488), o pirmasis mokslininkas 1994m. sukūręs praktiškai pritaikomą tokį algoritmą yra, Masačiusetso technologijos universiteto profesorius Peter Shor (Shor, 1994, p. 28). Shoro algoritmas jau po 7 metų t.y. 2001 metais buvo praktiškai įgyvendintas su IBM sukurtu 7 qbitų kompiuteriu, kuris apskaičiavo skaičiaus 15 faktorialą.

Dar didesnis kvantinės kompiuterijos lūžis įvyko XXI amžiuje, kuomet didžiosios korporacijos, tokios kaip Google ir IBM sugebėjo pagaminti funkcionuojančius kvantinius kompiuterius, gebančius atlikti kompiuterinius skaičiavimus per 200 sekundžių, kai klasikinis superkompiuteris ties tokiu pačiu skaičiavimu užtruktų apytiksliai 10000 metų (Arute, Arya ir k.t. 2019 p. 505-520). Tie patys mokslininkai, vėliau Google Ai tinklaraštyje detaliai paaiškino kokį eksperimentą jie atliko, kad pateikti 10000 metų skaičių (Martinis, Boixo, 2019).

Daugeliui žmonių kvantiniai kompiuteriai gali atrodyti kaip iš mokslinės fantastikos. Tiesą pasakius, jeigu internete pasižiūrėtumėme nuotraukas kaip kvantiniai kompiuteriai iš tiesų atrodo, galbūt ir dalelyte tiesos. 2 paveiksle galite pamatyti kaip atrodo Google kvantinis kompiuteris, pavadinimu Sycamore. Nors iš pirmo žvilgsnio vaizdas gali pasirodyti, kaip iš mokslinės fantastikos, tačiau tiek daug vamzdelių yra skirti aušinti kompiuterį, kadangi manipuliuojant atomais dėl trinties labai pakyla aplinkos temperatūra, taip pat fone matote įrangą panašią į serverius ar tinklo įrangą, jį yra

skirta, tam kad į kvantinius kompiuterius galėtų būti įvedama informacija. Klasikinių kompiuterių ir kvantinių sąveiką išnagrinėsi toliau.



Šaltinis: Rocco Ceselin, Google.

2 pav. Google kvantinis kompiuteris Sycamore

Kad galima būtų pradėti nagrinėti kvantinės kompiuterijos panaudojimo teoriją, reikėtų išsiaiškinti esminius kvantinių kompiuterių skirtumus nuo klasikinių kompiuterių. Pats didžiausias kvantinių kompiuterių skirtumas lyginant su klasikiniais namų ar super kompiuteriais yra tai, kaip juose yra saugoma ir apdorojama informacija. Klasikiniuose kompiuteriuose mažiausias informacijos saugojimo ir perdavimo vienetas yra bitas, turintis tik dvi reikšmes 0 ir 1, arba galima panaudoti elektros srovės perdavimo alegoriją, kai yra leidžiama tekėti elektrai arba neleidžiama.

Greičiausiai daugeliui teko matyti panašią į sekančią skaičių seką:

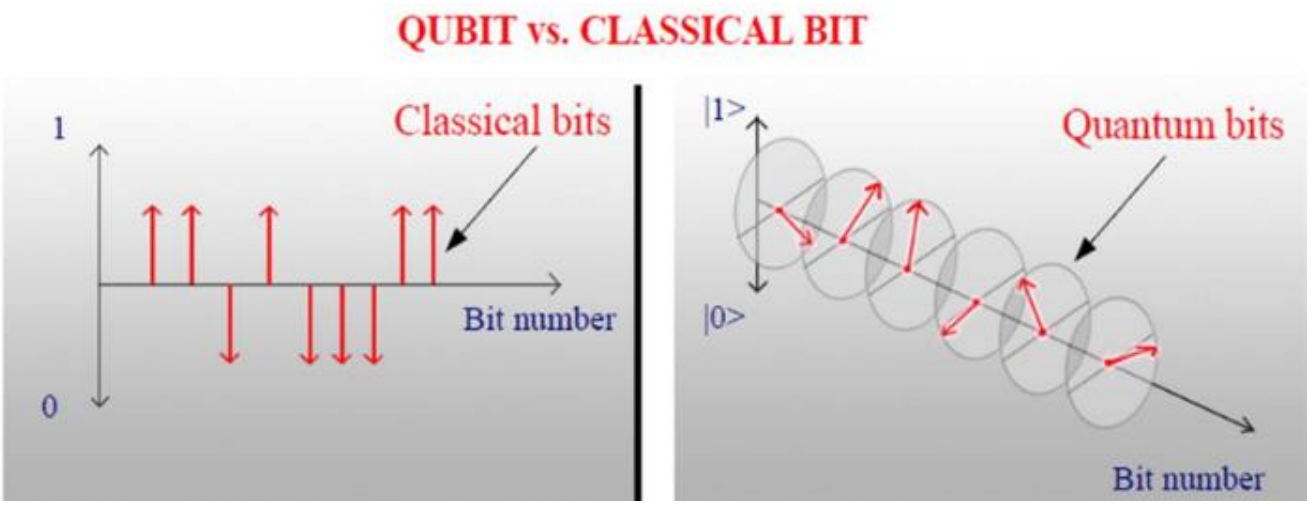
0101110001101010101010111100001110101010101010101010111111000110101010101010101

tai yra taip vadinamas - binarinis kodas. Binarinis kodas daugeliui gali atrodyti kaip atsitiktinė skaičių seka, tačiau tai yra kompiuteriui suprantama skaičių seka, kurioje yra saugoma ar perduodama informacija ir kurią gali suprasti kompiuteriai veikiantys elektros impulsų pagalba.

Tuo tarpu kvantiniuose kompiuteriuose informacija yra saugoma kvantiniuose bituose arba dar kitaip vadinamuose kubituose (*angl. Qbit*) - informacijos vienetuose, kurie gali turėti tas pačias dvi reikšmes 0 ir 1, ir dar kartu bet kuria reikšmė tame tarpe, tai yra taip vadinama - **superpozicija**.

Superpozicija, yra vienas iš dviejų reikšmingiausių kvantinės mechanikos principų pritaikomų kvantiniuose kompiuteriuose, leidžiančių atlikti kompiuterinius skaičiavimus (*angl. computing*) daug greičiau, nei klasikiniai kompiuteriai.

Vizualiai iliustruoti kubito nuo bito skirtumą pasitelksime Michael Agbaje iliustracija (žr. 3 pav.) išspausdinta 2019 metais Caribien Journal of Science . Kaip matome klasikinis bitas būna arba 0 arba 1, kai tuo tarpu kvantinis bitas turi skirtingas pozicijas.



Šaltinis: Michael Agbaje, 2019, Caribien Journal of Science.

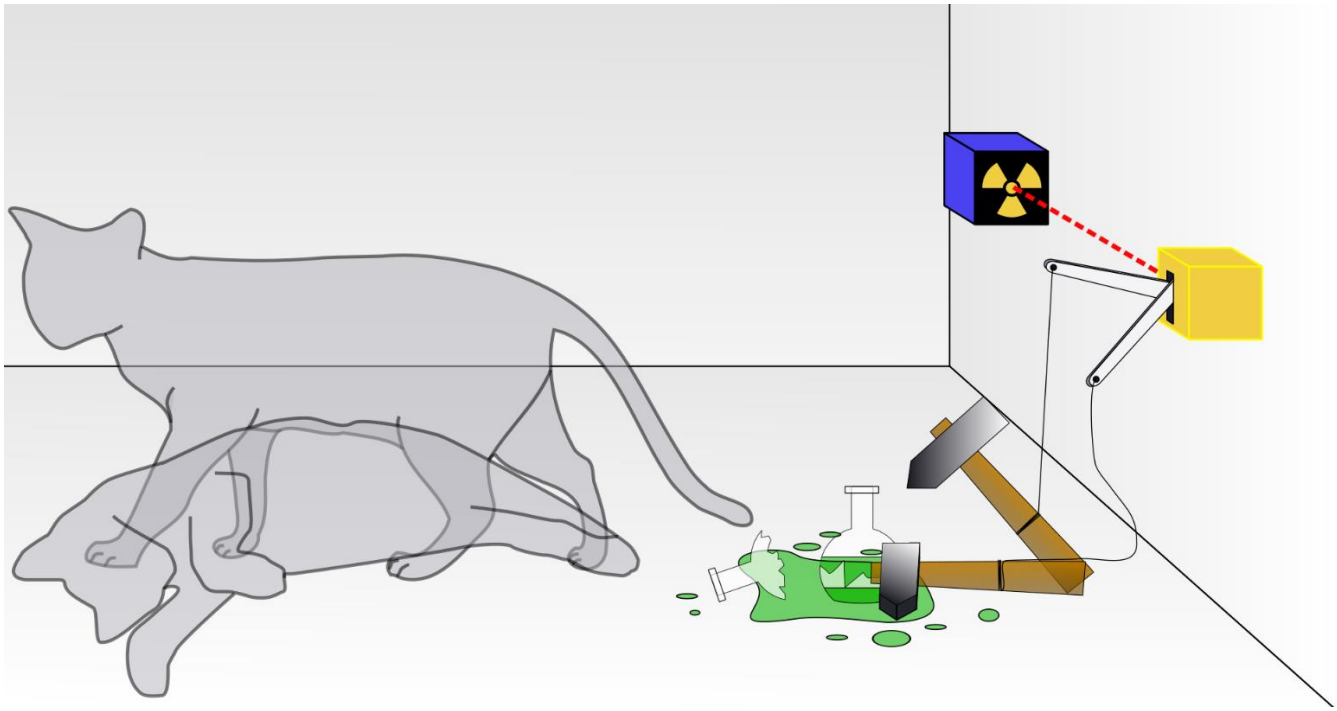
3 pav. Klasikinio bito ir kvantinio bito palyginimas

Pirmasis superpozicijos, kaip kvantinės mechanikos paradoksą pademonstravo austrų mokslininkas Erwin Shrodinger, atlikęs daugeliui greičiausiai girdėtą Shrodingerio katės eksperimentą, kurio metu katė vienu metu buvo ir gyva, ir mirusi (Shrodinger, 1935, p.823-829). Kaip tai įmanoma? Ogi paprasčiausiai pasitelkus kvantinės mechanikos vieną iš principų, kad kol stebimas dalykas nėra išmatuotas, mes negalime atsakyti koks yra matuojamo dalyko būvis.

Taigi kaip ten su ta kate. Šriodingeris pasiūlė eksperimentą, kuomet katė yra įdedama į nepermatomą dėžę su radioaktyvia medžiaga, nuodais ir Geigerio skaitikliu, kuris yra pajungtas prie plaktuko. Pasak Shriodingerio tikimybė, kad medžiaga kuri spinduliuoja radioaktyvias daleles išspinduliuos jų tiek, kad po valandos juos galėtų aptikti Geigerio skaitiklis yra lygi penkiasdešimt ant penkiasdešimt procentų, tad jeigu Geigerio skaitiklis nustato radiaciją yra atlaisvinamas plaktukas, kuris sudaužo kolbą su nuodais ir šie akimirksniu nužudo katę.

Taigi pasak Shriodinger, eksperimento tikimybė, kad katė po valandos vis dar yra gyva, lygi penkiasdešimt ant penkiasdešimt, tačiau kad būti šimtu procentų tikriems eksperimento atlikėjui reikia atidaryti dėžę ir pamatyti (išmatuoti) ar katė gyva ar ne (žr. 4 pav.) (Shrodinger, 1935, p.844).

Reikia pabrėžti, kad istoriniai šaltiniai sako, kad eksperimentas buvo tik teorinis ir Shrodingeris nenumarino nei vienos katės, tiesą pasakius teigiama, kad jis buvo joms alergiškas ir jų apskritai neaugino.



Šaltinis: internetas

4 pav. Shriodinger katės eksperimentas

Kitas galbūt humaniškesnis būdas paaiškinti superpozicijos veikimą yra vadinamasis monetos metimo eksperimentas. Kuomet metame monetos burtą, mes spėjame ar moneta iškris herbu ar skaičiumi į viršų t.y. 0 arba 1 (panašų į prieš tai aprašytus bitus), bet kol moneta dar nenusileido ir ji sukasi ore, ji vis dar turi abu galimus baigties variantus, tai yra vienu metu yra ir skaičius, ir herbas, taigi moneta turi taip vadinamą superpoziciją (Mishima 2018), ir galutinį rezultatą galime pamatyti (išmatuoti), tik tada kai moneta yra nukritusi ant žemės, arba ją jau turime rankoje.

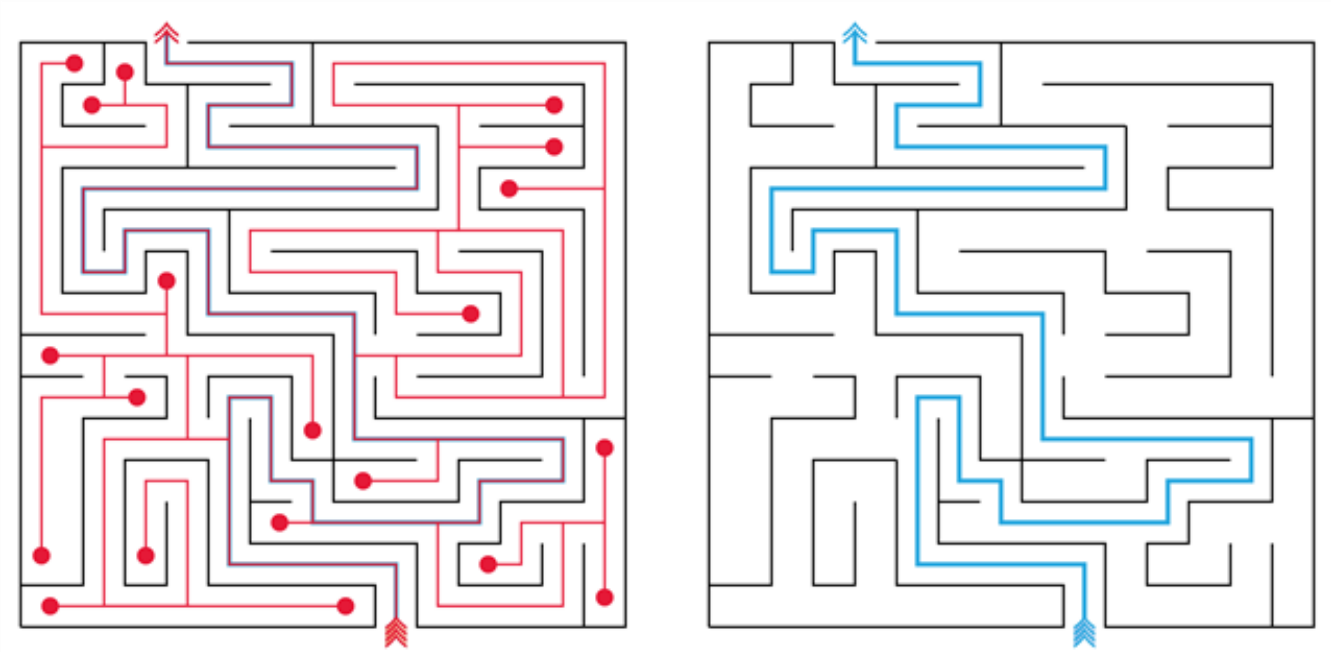
Nors mokslinėje literatūroje dažnai galime rasti monetos burto, kaip superpozicijos pavyzdį, manome, kad tokio eksperimento negalime laikyti pilnu superpozicijos paaiškinimu, nes skirtingai nuo Shriodingerio katės eksperimento, kur tikimybė dėl dviejų galimų baigčių yra netoli 100 procentų (dėl to Shrodingerio eksperimentas gali pasirodyti šiek tiek komplikuotas), monetos burto metimo eksperimento metu vis tiek yra teorinė galimybė, kad moneta nukris ant briaunos (Mishima 2018 m.).

Dažnai kalbant apie kvantinę kompiuteriją kyla klausimai, tai kur gi (kokiuose skaičiavimuose) gali būti panaudota superpozicija? Kvantinė kompiuterija gali būti pritaikoma informacijos paieškai nestruktūrizuotuose duomenų bazėse. Čia pasitarnaus superpozicijos principas. Dažnai kaip superpozicijos panaudojimo pavyzdys pateikiama keliaujančio pardavėjo problema, ar labirinto užduotis (nestruktūrizuota paieška).

Labirinto užduotis, tai paprasčiausias galvosūkis, kuomet bandoma rasti išėjimą iš labirinto.

Klasikiniai kompiuterių algoritmai norint rasti reikiamą išėjimo iš labirinto kelią bando visus galimus kelius (variantus) po vieną, kol galiausiai yra randamas išėjimas iš labirinto. Programuotojams puikiai pažįstamos komandos: while, if, break ir t.t.

Tuo tarpu kvantiniai kompiuteriai pasitelkdami superpoziciją, iškarto mato visą labirintą ir gali rasti tą vienintelį kelią iš karto (žr. 5 pav.).



Šaltinis IMA x IBM: Quantum Computing renginio prezentacija.

5 pav. Kairėje matome kaip operacijas atlieka klasikinis kompiuteris, dešinėje kaip kvantinis

Antras kvantinės mechanikos principas, kuris irgi yra esminis kvantinėje kompiuterijoje yra kvantinis susiejimas (*angl. Entanglement*). Tai yra toks kvantinės fizikos fenomenas, kuomet esant tam tikroms sąlygoms kvantinės dalelės (pavyzdžiui fotonai) yra labai stipriai susiejamos, net ir esant labai dideliems atstumams. Pavyzdžiui turint dvi kvantiškai susietas dalelytes ir pakeitus jų būsenas, pavyzdžiui viena iš jų pasukus pagal laikrodžio rodyklę, kitos būsena pasikeis priešingai – pradės suktis prieš laikrodžio rodyklę (Shrodinger, 1935 m.).

Taigi iš to kas buvo išsiaiškinta, galima susisteminti ir padaryti sekančias išvadas, kad klasikiniai namų kompiuteriai ir net super kompiuteriai veikia elektros pagalba (elektros impulsais, kas iš esmės irgi yra fizikos reiškinys), tačiau tuo tarpu kvantiniai kompiuteriai veikia veikdami mažiausias mums žinomas dalelės protonus, elektronus, neutronus ar fotonus iš to savaime darytina išvada, kad kvantinis kompiuteris nepakeis namų ar net super kompiuterių, bet juos tik papildys, kadangi atlikti manipuliacinius veiksmus su mažosiomis visatos dalelytėmis reikalinga laboratorijos lygmens aplinka. Pavyzdžiui iš fizikos mokyklos kurso žinome, kad atomai turi savybę vibruoti, o atomų vibravimas kelia

aplinkos temperatūrą, todėl kad sumažinti atomų vibraciją kvantiniai kompiuteriai yra laikomi netoli absoliutaus nulio (−273.15 °C) temperatūros.

Taip pat į kvantinius kompiuterius informacija vis tiek turės būti įvedama naudojant klasikinius kompiuterius.

Nagrinėjant kvantinės kompiuterijos teoriją, reikėtų paminėti, kad šiai dienai kvantiniai kompiuteriai dažniausiai naudoja dvi skirtingas kvantines architektūras: kvantinių vartų (*angl. quantum gates),* dar dažnai sutinkamas terminas - skaitmenine (*angl. digital*), apie ją daugiausiai ir yra koncentruojamasi šiame magistro baigiamajame darbe bei kvantinio atkaitinimo (angl. *quantum annealing*), dažnai sutinkamas terminas - analogine (Amercenkova, 2021). Ir nors esminiai kvantinės architektūros konceptai yra tapatūs, yra ir labai daug skirtumų. Didžiausias jų skirtumas yra tai, kad kvantinio atkaitinimo kompiuteriai naudoja kitokius algoritmus skaičiavimams (*adiabatinius*) ir jie apskaičiuoja (randa) minimalų „sprendimą“ kuris yra „ganėtinai geras“ ar „priimtinas“, todėl jie negali būti naudojami ten kur yra reikalingas labai didelis tikslumas pavyzdžiui baltymų sintezėje (Crssson & Lidar, 2021 m.).

Šiai dienai kvantinio atkaitinimo kompiuteriai yra labiau pritaikomi praktikoje, tačiau didžios korporacijos į jų vystymą nėra linkusios investuoti ir pasaulyje yra tik keletas įmonių kurios vysto kvantinio atkaitinimo kompiuterius. Viena iš jų yra kanadiečių *D-WAWE Systems,* kuri plėtoja kvantinio atkaitinimo kompiuterius, tačiau jie patys greta kvantinio atkaitinimo kompiuterių investuoja ir į kvantinių vartų technologijos kvantinius kompiuterius.

Analizuojant kvantine kompiuterija reikėtų nenustebti, kad jeigu ieškotume informacijos apie greičiausius kvantinius kompiuterius pasaulyje rasime labai skirtingus skaičius. Pavyzdžiui kai kuriuose šaltiniuose rašoma, kad šiai dienai galingiausias kvantinis kompiuteris yra laikytinas Borelis su 216 Qb procesoriumi, tačiau šaltiniuose galima rasti, kad D-WAWE kvantiniai procesoriai siekia iki 5000 Qb, tačiau kaip ir buvo prieš tai paminėta, tokių kvantinių kompiuterių rezultatai būna „priimtini“.

Tokias skirtingas architektūras manome, kad galima būtų palyginti su kažkada vykusiu „vaizdo kasečių formato karu“, kurį savo studijoje aprašo Christ & Slovak, kuomet du pasauliniai elektronikos gigantai Sony ir JVS septyniasdešimtaisiais rinkai pateikė du skirtingus vaizdo kasečių formatus Betamax ir visiems puikiai žinomą VHS. Galiausiai JVS su VHS formatu laimėjo ir Betamax buvo pašalintas iš rinkos. Taip įvyko dėl to, kad VHS labiau atitiko naudotojų lūkesčius, todėl manome, kad kai atsiras be klaidų veikianti kvantinių vartų architektūra, kompiuteriai, jie tikrai išstums kvantinio atkaitinimo kompiuterius (Christ & Slovak, 2009).

Chris & Slovak taip pat patvirtina, kad kvantiniai kompiuteriai nepakeis šiuolaikinių namų ar super kompiuterių, bet juos papildys, kadangi kvantiniai kompiuteriai negali atlikti operacijų einamuoju laiku, pavyzdžiui valdyti procesus kur reikia kažką įjungti ir išjungti (bitų operacijos). Taip pat kvantiniai kompiuteriai gali dirbti tik tam tikroje laboratorijos lygmens aplinkoje – būti apsaugoti nuo vibracijos,

tinkamai aušinami (beveik absoliutaus nulio temperatūroje), taip pat duomenys į kvantinį kompiuterį vis tiek turi būti įvedami naudojant klasikinius kompiuterius (Christ & Slovak, 2009)..

Vis dėl to kvantine kompiuterija susidomėjimas yra be galo milžiniškas, ją domisi didžiausios pasaulio finansų, farmacijos energetikos kompanijos, taip pat valstybių vyriausybės, įvairūs mokslininkai. Tačiau akivaizdu, kad ištekliai pagaminti kvantinį kompiuterį yra dideli, reikia ne tik pinigų, bet ir talentų, todėl, kad kvantinė kompiuterija taptų prieinama kiekvienam, IBM dar 2016 metais padarė savo kvantinius kompiuterius prieinamus visuomenei ir įkėlė juos į IBM debesijos (*angl. cloud*) paslaugą kur juos pasiekti gali bet kas. Maža to IBM prieigą prie kvantinio kompiuterio, su tam tikromis išlygomis siūlo nemokamai. Taip pat IBM siūlo ir nemokamus mokymus bei pirmąjį pasaulyje kvantinės kompiuterijos programuotojo sertifikatą. Programuoti kvantinius kompiuterius nereikalingos kažkokios specifinės fizikos ar kvantinės mechanikos žinios. Užtenka mokėti Python programavimo kalbą ir kažkiek linijinės algebros. IBM tam yra sukūrusi specialų Python karkasą (*angl. framework*) pavadinimu Qiskit, kad būtų galimybė programuoti operacijas kvantiniams kompiuteriams (https://qiskit.org/).

Kadangi kaip ir buvo paminėta prieš tai, kvantiniams kompiuteriams reikalinga labai saugi ir specifinė aplinka, todėl faktas, kad jie niekada netaps namų kompiuteriais, tačiau tikrai ateityje jų naudotojų skaičius tik didės, todėl manome, kad kvantinių kompiuterių pasiekiamumas per debesį yra prieinamiausias sprendimas. Įkeliant savo kvantinius kompiuterius į debesį neatsilieka ir kitos technologijų kompanijos, pavyzdžiui Google Cloud, Microsoft Azure, Amazon AWS debesų platformose yra pasiekiamas Ionq startuolio 32 qbitų kvantinis kompiuteris. Šią teoriją patvirtina Ruane J., McAfee A, & . Oliver, D.W. kurie teigia, kad verslas norės sutaupyti naudojant ir kvantinius kompiuterius, kaip dabar taupo perkeldamos didžiąją dalį savo paslaugų į debesijos paslaugas, todėl ateityje tik kelios didžios korporacijos bus išvysčiusios kvantinius kompiuterius ir leis juos pasiekti visiems norintiems už pinigus

Nagrinėjant kvantinės kompiuterijos temą noretusi trumpai apžvelgti šiai dienai esančius galingiausius pasaulyje kvantinius kompiuterius. Taigi galingiausias kvantinis kompiuteris pasak šaltinių yra 127 qbitų, IBM sukurtas kvantinis kompiuteris pavadinimu Eagle· Google šiai dienai turi 72 qbitų kvantinį kompiuterį pavadinimu Bristlecone (grupė mokslininkų 2022m. liepos 1 dieną paskelbė, kad Kanadiečių kvantinių kompiuterių bendrovė Xanadu yra paskelbusi, kad 2022 metų spalį bus išleistas 216 qbitų kvantinis kompiuteris) (Madsen, Laudenbash, Askarini et al. 2022 m.)

Daugelis įmonių dirbančių ir vystančių kvantinę kompiuteriją aktyviai dirba ties galingesnio, nei 1000 Qbitų kompiuterio tyrimais ir produkcija. Pilnai be klaidų veikiantis, daugiau kaip 1000 Qbitų kvantinis kompiuteris reikštų didžiulį proveržį kvantinės kompiuterijos pasaulyje. IBM planuose yra dar 2023 metais pristatyti 1121 Qbito kvantinį kompiuterį. Žvelgiant į šiuos skaičius galima daryti išvadą, kad iš esmės vyksta savotiškos kvantinės kompiuterijos lenktynės.

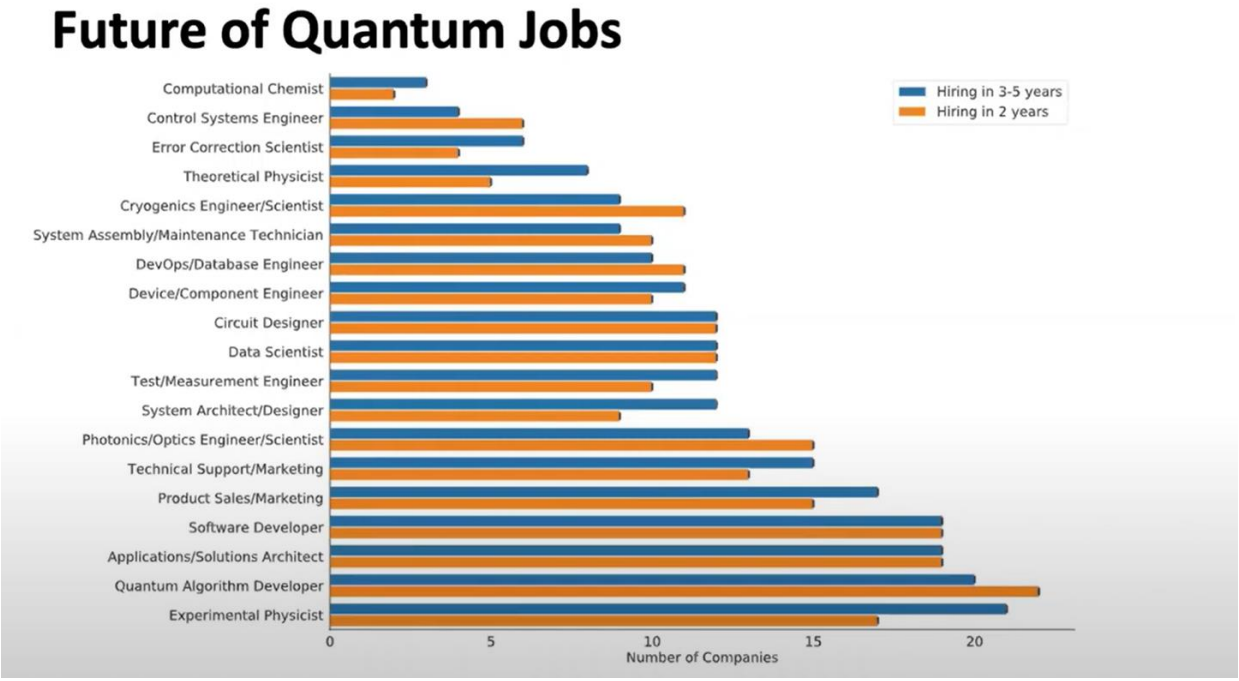
Toliau pateiktoje lentelėje (1 lentelė) pateikiame informacija apie galingiausius pasaulyje kvantinius kompiuterius, naudojančius kvantinių vartų technologiją ir jų išleidimo metus.

1 lentelė 10 galingiausių kvantinių kompiuterių 2022 spalio 1 d.

Gamintojas	Pavadinimas	Qbitų skaičius	Išleidimo data
Xanadu	Borelis	216 QB	2022
IBM	IBM Eagle	127 QB	2021 lapkritis
USTC	Jiuzhang	76 QB	2020
Google	Bristlecone	72 QB	2018 kovo 5 d.
IBM	IBM Manhattan [17]	65 QB	
Google	Sycamore	53 QB	2019
IBM	IBM Q 53	53 QB	2019 spalis
IBM	IBM Q 50 prototype	50 QB	
Google	N/A	49 QB	2017, 4 ketvirtis
Intel	Tangle Lake	49 QB	2018 sausio 4 d.

Nagrinėjant kvantinės kompiuterijos teoriją verta paminėti, kad pasak kai kurių autorių plėtojantis kvantinei kompiuterijai ateityje galime tikėtis naujų „kvantinių“ specialybių atsiradimo, pavyzdžiui, pasak Thankaraj per artimiausius 10 metų darbo skelbimuose atsiras nauja profesija, kurios ieškos verslas, tai kvantinio mašinų mokymosi analitikas (*angl. Quantum machine learning analytic*) ir k.t.

Taigi galima teigti, kad kaip šalia sistemų administratoriaus profesijos kažkada atsiradę DevOps ar DevSecOps taip pat ir ateityje galime tikėtis, kad atsirandant plėtojantis pažangioms technologijoms atsiras ir naujos dar negirdėtos profesijos (Regupathi Thankaraj 2021). Tačiau dirbti su kvantiniais kompiuteriais nebūtinai reikės naujų specializacijų specialistų. 2021 metais gan išsamų tyrimą apie aukštojo mokslo institucijų galimybes patobulinti savo studijų programas ir pritaikyti jas „kvantiniam verslui“ atlikusi H.J.Lewandowski tyrimo metu apklausė 25 įmones, kurios jau šiandien investuoja į kvantinę kompiuteriją ir klausė jų atstovų nuomonės, kokios netolimoje ateityje (2-5 metai) bus paklausiausios profesijos įmonėms, kurių specialistai dirbs su kvantiniais kompiuteriais. Pateiktas tyrimo metu identifikuotų specialybių sąrašas, kurios pasak verslo subjektų bus reikalingos verslui siekiančiam dirbti su kvantinėmis technologijomis (žr. 6 pav.)



Šaltinis: H.J. Lewandowski QTC21 | Education and Training Workshop: Higher Education

6 pav. Ateities kvantinės specialybės

Kaip matome iš 6 pav. pirmą vietą pagal paklausą užėmė Eksperimentinės fizikos specialistas (*angl. Experimental Physicist*), kitos seka „klasikinės“ IT specialybės t.y. programuotojai, IT architektas bei „klasikinės“ verslo vadybos specialybės – marketingo, pardavimų specialistai.

Taigi atsižvelgus į H.J.Lewandowski atlikto tyrimo rezultatus galima daryti išvadą, kad iš esmės vystant kvantinę kompiuteriją bus reikalingi tiek aukštųjų technologijų specialistai, tiek vadybos ir marketingo specialistai. Tačiau savaime aišku, kad tokie specialistai norintys būti konkurencingi turės turėti tam tikras žinias susijusias su kvantine kompiuterija, todėl jau šiandien keli Europos universitetai (*Sorbonos, TU Eindhoven, Universite de Strasbourg, Karlsruher Insitut fur Technologie* ir k.t.) yra parengę vienerių metų EFEQT (*Enpowering the Future Experts in Quantum Science and Technology*

for Europe) programą Europos universitetų magistrantūros studijų studentams, kurios tikslas praplėsti studijuojamą magistrantūros studijų programą ir parengti ateities lyderius besiformuojančiai kvantines kompiuterijos darbo jėgai.

1.2. Šifravimo koncepcija

Nagrinėjant kvantinę kompiuteriją būtina išnagrinėti kvantinio šifravimo ir post – kvantinės kriptografijos teoriją. Pasak Gregory Mone kvantinis ir post – kvantinis šifravimas kelia daugiausiai klausimų, bei taip pat daugiausiai rizikų pasaulyje, susijusių su kvantinės kompiuterijos plėtra (Mone, 2020).

Pirmiausiai, kad pradėti nagrinėti kvantinį šifravimą, iš esmės būtina išsiaiškinti ir susipažinti su pagrindine šifravimo dar kitaip vadinamos kriptografija teorija.

Šifravimas yra labai senai naudojamas metodas, kuomet visiems suprantamas tekstas, failas, paveiksliukas ar bet kokie kiti duomenys yra pakeičiami taip, kad be tam tikro rakto jų negalima butu perskaityti ar panaudoti pagal paskirtį.

Dar senovės Romos laikais šifravimui buvo naudojamas taip vadinamas Cezario šifras (žr. 7 pav.). Elementarus kriptografijos metodas, kuomet norimos užkoduoti žinutės raidės yra perstumiamos per kelias pozicijas (dažniausiai tris) į dešinę, o norintys atšifruoti žinutę, turi perstumti per tam tikrą pozicijų skaičių į kairę. Kad tai atlikti buvo reikalingas raktas, šiuo atveju – per kiek pozicijų perstumti raides. Toks šifravimo būdas kuomet naudojamas vienas ir tas pats raktas užšifruoti ir atšifruoti yra vadinamas simetriniu.

S	E	C	R	E	T	M	E	S	S	A	G	E
V	H	F	U	H	W	P	H	V	V	D	J	H

7 pav. Cezario šifras

Deja toks šifras ne tik kad, bet kokiam šiuolaikiniam kompiuteriui iššifruoti yra sekundžių darbas, bet netgi žmogus su geromis matematinėmis žiniomis galėtų priklausomai nuo teksto ilgio iššifruoti ji per kelias valandas ar net minutes.

Pirmas sudėtingesnis simetrinio šifravimo būdas atsirado tik apie 1553 metus jis pavadintas prancūzų mokslininko Blaise de Vigenere vardu. Šis šifras yra daug kartų sudėtingesnis, kadangi Vinegere šifro esmė yra perkelti šifruojamo teksto raides į dešinę, per tiek pozicijų, kokia yra rakto raidė abėcėlėje. Raktas naudojamas ratu. Pavyzdžiui: jeigu turime tekstą HELLO_WORLD ir naudojame trijų

raidžių raktą YES, tai šifras bus: EICISRTSIIH t.y raidę H žodyje HELLO perkeliame per 25 vietas, kadangi Y anglų abėcėlėje yra 25 raidė (įvertiname, tai kad pagal nutylėjimą paskutinis ženklas yra tarpas ir t.t.).

Kuo daugiau raktas turi simbolių, tuo sunkiau yra atspėti užšifruotą tekstą. Pavyzdžiui anglų abėcėlėje panaudojus raktą iš 14 simbolių gali būti, net 64,509,974,703,297,150,976 kombinacijų.

Tačiau vėl gi, toks šifras turi nemažai trūkumų, nes pasinaudojus šiuolaikinėmis žodynų atakomis (*angl. dictonary attaks*) jį gali nesunkiai įveikti net paprastas namų kompiuteris.

Taigi nors gali atrodyti, kad visi simetriniai šifravimo metodai yra nesaugūs, tačiau tiesą pasakius kai kurie simetriniai šifravimo metodai yra vieni saugiausių pasaulyje, tai yra taip vadinami Pažangusis šifravimo standartas (*angl. Advanced Encryption Standart – AES*) ar vienos spynos (*angl. one time pad*) metodas. Pavizdžiui vienos spynos šifro esmė yra ta, kad raktas turi būti ne trumpesnis nei pats šifruojamas tekstas ir jis turi būti vienkartinis ir unikalus, t.y. pritaikytas konkrečiai norimai perduoti žinutei. Pavyzdžiui . norima perduoti žodį HELLO, o raktas yra pvz. X, M, C, K, L. Taigi kadangi raidė H yra septinta abėcėlės raidė, o X 23 (angliškoje abėcėlėje) sudėję gauname 30, bet kadangi angliškoje abėcėlėje yra tik 25 raidės, tai 26 pradedame skaičiuoti vėl nuo A, todėl užkoduota raidė yra E na ir t.t. Pavyzdį pateikiame toliau pateiktoje lentelėje.

2 lentelė Vigenere šifras

	H	E	L	L	O	žinutė
	7	4	11	11	14	abėcėles skaičiaus eilės numeris
+	X	M	C	K	L	raktas
	23	12	2	10	11	
=	30	16	13	21	25	žinutė + raktas
=	4	16	13	21	25	žinutė + raktas moduliu 26.
	E	Q	N	V	Z	užkoduota žinutė

Taigi atsižvelgus į tai, kad šifro raktas turi būti tokio pat ilgio kaip ir pranešimas, o dar priedo, kad užtikrinti visišką pranešimo saugumą, pats raktas taip pat turi būti perduodamas saugiai, toks raktas yra labai nepraktiškas.

Daug patogesnis ir praktiškesnis yra taip vadinamas asimetrinis šifravimas, dažniau sutinkamas terminų viešojo ir privataus rakto kriptografija – kuris padedantis išlaikyti labai aukštą šifro saugumą.

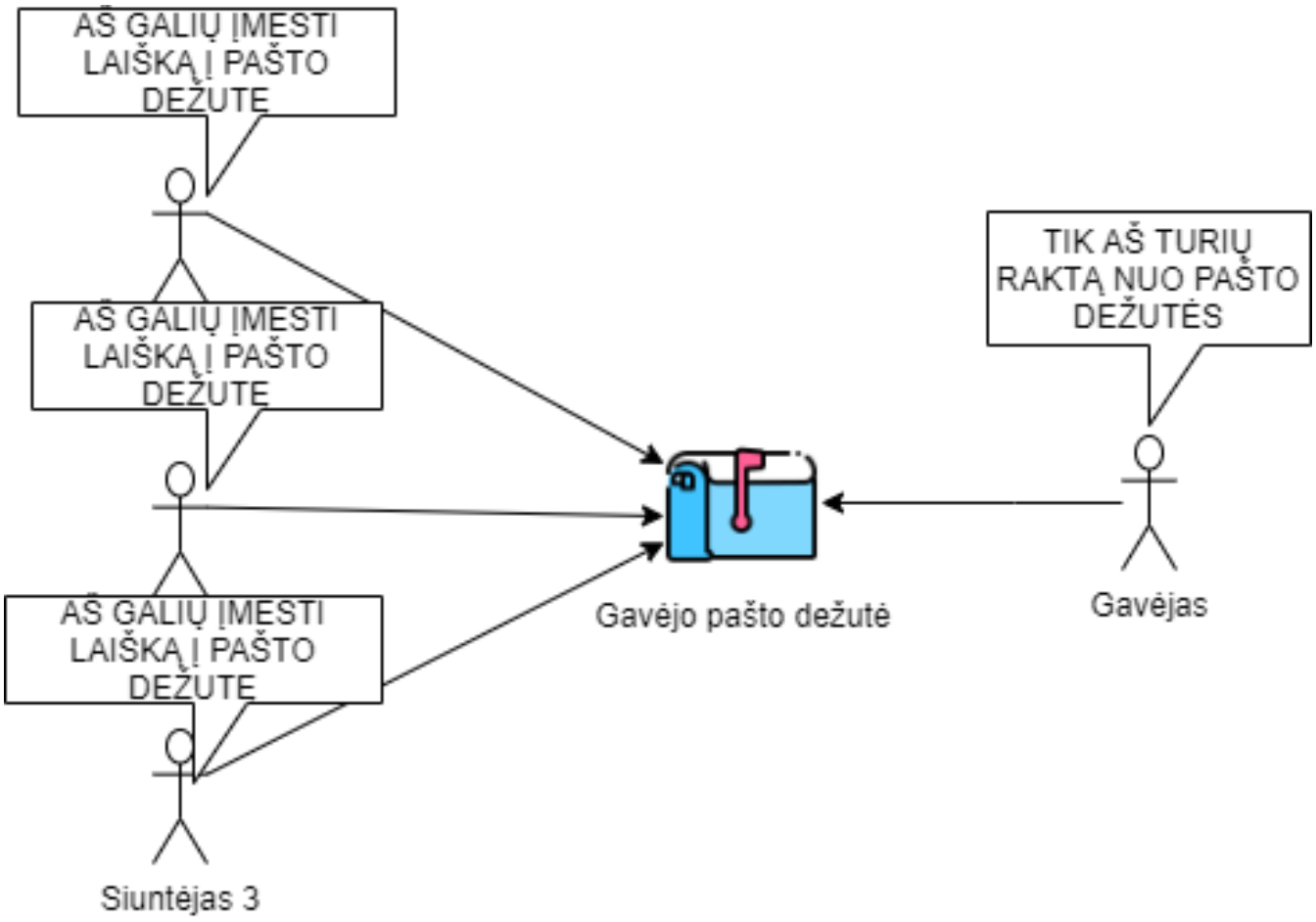
Pagrindinius asimetrinio šifravimo principus (du vienas nuo kito nepriklausantys būdai informacijai iššifruoti ir užšifruoti) dar 1976 metais aprašė JAV mokslininkai Whitfield Diffie and Martin Hellman, kurių vardu ir yra netgi vienas iš šifravimo algoritmų - (Diffie & Hellman 1976 m.).

Šiandien su asimetriniu šifravimu vienaip ar kitaip susiduria didžioji pasaulio gyventojų dalis, ar tai būtų susirašinėjimas elektroniniais laiškais ar tiesiog naršymas internetu, visur siekiant apsaugoti

perduodamus duomenis ir išlaikyti konfidencialumą, informacija yra šifruojama naudojant būtent asimetrinį šifravimą.

Pagrindinė asimetrinio šifravimo esmė, yra šifravimas naudojantis dviem šifro raktais - viešuoju ir privačiuoju. Viešas raktas yra prieinamas daugeliui ir gali būti pasiekiamas dviem būdais: pirma - jį „duoda“ informacijos gavėjas, kad siunčiantysis asmuo galėtų su juo užkoduoti perduodamą informaciją, antra – jis saugomas specialiuose visiems prieinamuose viešuose viešų raktų infrastruktūros serveriuose (*angl. public key infrastructure server*), o tuo tarpu privatų raktą, su kuriuo turėtų būti iššifruojama perduodama informacija, turi tik pats gavėjas ir jis jį saugo tik sau žinomoje vietoje, arba jei tai internetu perduodama informacija, kaip pvz. TLS šifravimas, jis yra saugomas taip vadinamuose sertifikatų tarnybose (*angl. certificate authority*).

Kad suprasti asimetrinio šifravimo principus galima panaudoti labai paprastą alegoriją su pašto dėžute. Pašto dėžutės pagal savo pagrindinį „veikimo“ principą yra prieinamos visiems ir ten jums gali palikti pranešimą (laišką, reklamą, ir t.t.) bet kas, (t.y. viešojo rakto principas), tačiau atidaryti ją galite tik jūs, nes tik jūs turite raktą į ją (privatus raktas) (žr. 8 pav.).



8 pav. Asimetrinio šifravimo pavyzdys

Asimetriniuose šifruose šiai dienai populiariausi šifravimo algoritmai yra: RSA , DSA, Elipsinės tiesės ir Diffie Hellman-DH.

Nagrinėjant magistrinio darbo pagrindinę temą, truputį labiau reikėtų susipažinti su šiais šifravimo algoritmais, kad suprasti jų pažeidžiamumą prieš kvantinius kompiuterius.

RSA yra vienas pirmųjų dar 1977 metais pristatytų šifravimo algoritmų ir šiai dienai tai yra labiausiai paplitęs šifravimo algoritmas pasaulyje, kurio veikimo principas yra paremtas dviejų labai didelių pirminių skaičių sandauga ir sakydami labai didelių, mes kalbame apie labai labai didelius skaičius. Pavyzdžiui jeigu paimtume skaičius 23 ir 29 jų sandauga yra 667. Greičiausiai skaičiaus 667 pirmini skaičių rasti būtų nesudėtinga, tačiau ar lengvai pavyktų apskaičiuoti skaičiaus 3139 pirminį skaičių? Taigi, kaip matome kuo skaičiai ilgėja, tuo sudėtingesnis tampa pats šifravimo algoritmas, pavyzdžiui RSA 1024 bitų šifras yra 309 skaitmenų ilgio, tokio ilgio šifrą net ir galingiausiam šiuolaikiniam kompiuteriui iššifruoti prireiktų kelių milijonų metų.

Antras pagal populiarumą pasaulyje yra elipsinės tiesės algoritmas, kuris naudoja kiek kitokius matematinius skaičiavimus, o tiksliau elipsines kreivės metodą. Matematiškai šie skaičiavimai yra sudėtingesni, todėl greičiausiai dėl to RSA yra populiaresnis algoritmas pasaulyje, tačiau ECC gali suteikti tokį patį šifro saugumą su mažesniu raktų dydžiu, pvz. 2048 bitų RSA, rakto dydis yra apie 224 bitai EEC. Vėlgi ar šiais laikais, kai vienas interneto svetainės puslapis užima kelis gigabaitus ir daugiau atminties, verta sukti galvą dėl naudojamo šifro rakto dydžio?

Taigi kaip matome du patys populiariausi pasaulyje šifravimo algoritmai yra paremti paprasčiausiais matematiniais veiksmais – skaičiavimais, kurie dėl savo kompleksiškumo yra neįveikiami šiuolaikiniams kompiuteriams, tačiau nieku darbas yra kvantiniams kompiuteriams.

1.2.1. Post-kvantinis šifravimas

Šiai dienai, pasaulyje jau retai kur sutiksime RSA 1024, dažniausiai yra sutinkamas RSA 2048 bitų raktas kurį iššifruoti klasikiniam kompiuteriui prireiktų apie 300 trilijonų metų arba 4096 bitų RSA raktas kuriam dvigubai daugiau laiko reikėtų iššifruoti. Taigi iš esmės tai yra neįveikiami šifravimo algoritmai.

Bet nors ir atrodo, kad jau daugiau kaip keturiasdešimt metų turime nenulaužiamą kriptografinį algoritmą plačiai naudojamą pasaulyje, tačiau jau prieš tai išsiaiškinome, kad kvantiniai kompiuteriai skaičiavimus atlieka kitaip nei mums įprasti klasikiniai kompiuteriai, t.y. naudodami superpoziciją, todėl jiems tokie skaičiavimai kaip rasti sveikojo skaičiaus faktorialo pirminį sveikąjį skaičių, būtų kelių sekundžių darbas.

Forbes žurnale 2021 gegužės mėnesį išėjo Lila Kee straipsnis pavadinimu *RSA Is Dead — We Just Haven't Accepted It Yet* - RSA mirė, mes tik dar to nepripažįstame (Forbes 2021). Straipsnyje yra

rašoma apie tai, kad paprasčiausias kvantinis kompiuteris 2048 bitų RSA šifrą sugebės nulaužti per 8 valandas, todėl jau beveik visi specialistai sako, kad RSA tikrai atėjo galas, nes nors ir RSA šifro raktai gali būti ir ilgesni tačiau, ilgesnių RSA raktų naudojimas taptų tiesiog nepraktiškas, reikalautų daug daugiau resursų (vis dėl to manome, kad ši nuostata yra diskutuotina, kadangi jau dabar kai kurių interneto tinklapių pirmi puslapiai užima po kelis megabaitus naršyklėje, todėl papildomas apdorojimas kelių šimtų kilobaitų neturėtų ženkliai apkrauti įrenginių) (Kee, 2021).

Tai gal elipsinės kreivės algoritmas yra saugesnis? Deja, čia atrodo žinios dar prastesnės, kadangi kvantiniai kompiuteriai labiau remiasi į simbolių apdorojimą, 256 bitų EEC raktą, kvantinis kompiuteris iššifruotų per 2 valandas.

Taigi kvantiniai kompiuteriai įrašydami į pasaulio istorijos vadovėlius visiems žinomus šiandieninius šifravimo algoritmus iškelia labai didelę konfidencialumo problemą ir čia atsiranda taip vadinamas post-kvantinis šifravimas (*angl. post-quantum cryptography*).

Post-kvantinė kriptografija, tai kvantiniams kompiuteriams atsparus viešojo ir privataus rakto algoritmai. Tokie algoritmai pirmiausiai turi būti atsparūs Shor`o algoritmui.

Pasak Jean-Phillipe Aumasson teoriškai simetriniai algoritmai, tokie kaip blokų grandinės ir maišos funkcijos, turėtų būti atsparūs kvantiniams kompiuteriams arba bent jau neprarasti viso savo saugumo, todėl šiandien mokslininkai yra įvardiję keturis kriptografinius metodus, kuriais gali būti paremti kvantiniams kompiuteriams atsparūs algoritmai: maišos (*angl. hash*), daugiamatė kriptografija (*angl. multivariate*), grotelių (*angl. lattice*) ir kodu paremti (*angl. code-based*). (Aumasson 2017).

Šiuos keturis kriptografijos algoritmus, kaip pamatinius kvantiniams kompiuteriams atspariems 2016 metais įvardino ir Jungtinių Valstijų Nacionalinė Standartų ir Technologijų Agentūra – NIST (*angl. National Institute of Standards and Technology*), paskelbusi pasaulinį kvietimą teikti mokslininkams, verslo atstovams paraiškas, dėl naujų kriptografinių reikalavimų - algoritmų, kurie galėtų pakeisti šiuolaikinius viešojo rakto principu veikiančius kriptografijos standartus ir būti atsparūs kvantinės kompiuterijos grėsmėms (NIST 2016). Šiai dienai (2022 Spalio 16 d.) jau yra atrinktas vienas šifravimo algoritmas viešojo ir privataus rakto kriptografijos sistemai ir trys algoritmai užtikrinantys elektroninio parašo saugumą (žr. 3 lentelė).

3 lentelė Atrinkti post-kvantiniai algoritmai

Algoritmas	Algoritmo tipas	Pastabos
CRYSTALS-Kyber	Paremtas plokštelių metodu.	Viešojo ir privataus rakto
CRYSTALS-DILITHIUM	Paremtas plokštelių metodu.	Elektroninio parašo
FALCON	Paremtas plokštelių metodu.	Elektroninio parašo
SPHINCS+	Maišos metodas.	Elektroninio parašo

1.2.2. Kvantinis šifravimas

Kaip jau prieš tai išsiaiškinome, kvantiniai kompiuteriai veikia remdamiesi kvantinės fizikos, o ne matematikos mokslu, dėl to jiems dabartiniais matematiniais skaičiavimais paremti šifravimo algoritmai yra labai lengvai įveikiami.

Tačiau nepaisant to, teoriškai greta mums žinomo klasikinio šifravimo gali egzistuoti ir kvantinis šifravimas.

Pasak Alexander S. Grillis (2022 m.) kvantinio šifravimo pagrindinis skirtumas nuo simetrinio ar asimetrinio šifravimo yra vientisumas t.y. jeigu užšifruota informacija būtų kompromituota, juos fizikinis būvis būtų pakitęs ir tai galėtų pastebėti tiek informacijos siuntėjas, tiek gavėjas. Kodėl taip yra? Vėlgi čia veikia superpozicijos ir kvantinio susiejimo principai:

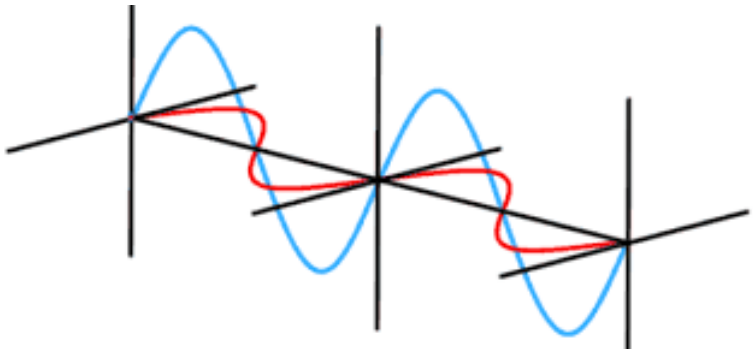
- kvantinės dalelytės vienu metu gali būti keliose vietose ir būviuose;
- kvantinė būsena negali būti išmatuota nepakeičiant juos būvio;
- dalelytės negali būti nukopijuotos;

Šios sąlygos neleidžia perimti informacijos nepaveikiant kvantinės sistemos, taip neinformuojant dalyvių (Grillis, S.A. 2022).

Pats kvantinio šifravimo veikimo modelis irgi yra paremtas viešojo ir privataus rakto principais, tik ten skaitmeninius raktus atstoja fotonai, o patys raktai yra saugomi kvantiniuose raktų saugyklose (*angl. quantum key distribution – QKD*).

Toliau pateiksime pavyzdį kaip pasak mokslininkų Charles Bennett ir Gillles Brassard sukūrusių pirmąjį kvantinį šifravimo algoritmą BB84, kvantinis šifravimas veiktų praktikoje (žr. 10 pav.). Pateikiamas modelis buvo sukurtas dar 1984 m.

Įsivaizduokite, kad turime du žmones Alice ir Bob, kurie nori apsikeisti informacija saugiai. Pirmiausiai Alice norėdama išsiųsti žinutę kuri yra užšifruota kvantiniu šifru, Bobui turi perduoti privatų raktą. Privatus raktas yra ne kas kitas, o fotonų grandinė. Fotonų grandinė iš esmės simbolizuoja 0 ir 1, tačiau, priedo to tokia grandis banguoja arba vibruoja, t.y. ir turi tam tikrą seką (žr. 9 pav.).

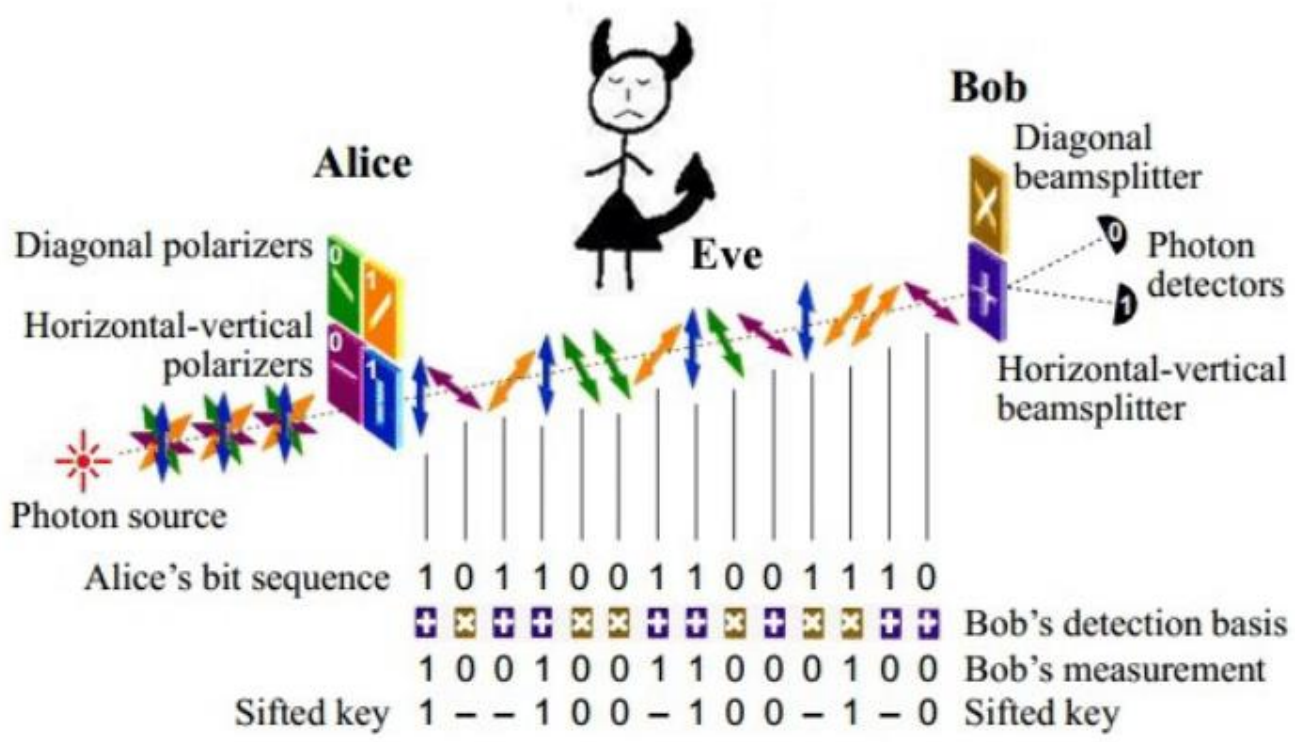


Šaltinis: ResearchGate.

9 pav. Fotonų grandis

Taigi, prieš perduodant informaciją fotonai keliauja per poliarizatorius (optinis filtras skirtas praleisti tam tikrus šviesos srautus) kuris praleidžia fotonus, kurie yra vertikalūs (1 bitas), horizontalūs (0 bitas) 45 laipsniai į dešinę (1 bitas), 45 laipsniai į kairę (0 bitas). Poliarizatorius praėję fotonai toliau keliauja optiniais kabeliais iki gavėjo kur informacijos gavėjo pusėje yra du spindulio skeltuvai (*angl. beam spliter*) kurių vienas yra horizontalus, kitas vertikalus ir jų tikslas yra perskaityti kiekvieno fotono poliarizaciją. Tačiau gavėjas nežino kurį poliarizatorių kuriam fotonui naudoti, todėl jis siuntėjui perduoda atgal, kurį poliarizatorių kuriam fotonui naudojo, taip siuntėjas sulygina duomenis su išsiųstų fotonų pozicijomis. Fotonai kurie buvo perskaityti ne per reikiamą spindulio skeltuvą yra panaikinami, o iš likusių yra sudaromas privatus raktas.

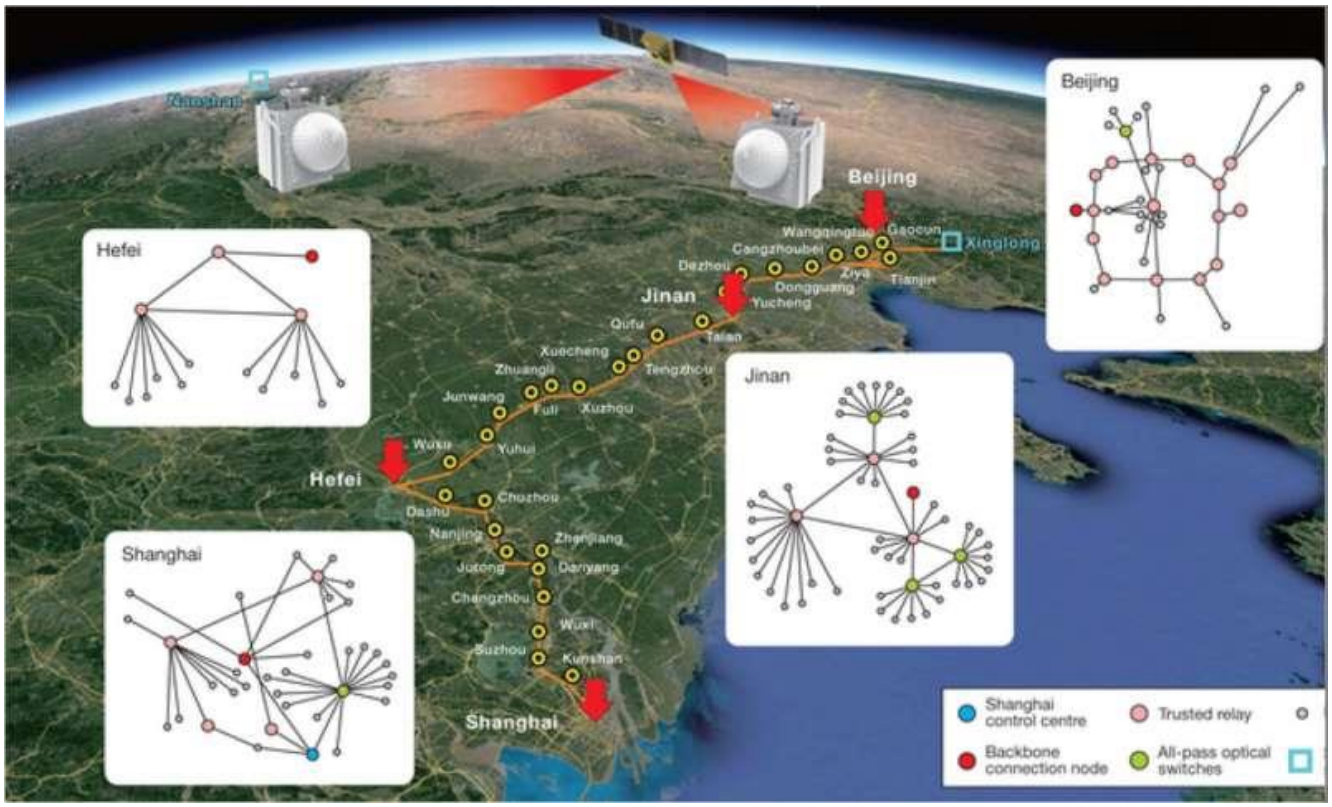
Jeigu šiame informacijos perdavimo sraute atsirastų piktavalis norintis perimti informacijos srautą (*angl. eavesdropper*) tarkim vardu Eva, kuri norėtų perskaityti užšifruotą informaciją, ji teoriškai turėtų perskaityti kiekvieno fotono būvį ir toliau perduoti tą patį fotoną Bobui. Tačiau kaip jau išsiaiškinome prieš tai, kad skaitant fotono būvį (poziciją) yra pakeičiama ne tik jo pozicija, bet ir kito su juo susieto fotono pozicija, todėl yra pakeičiama visa rakto grandis ir apie tokį pasikeitimą nedelsiant sužino tiek Alice tiek Bobas ir nedelsiant sunaikina raktą, toliau yra generuojamas naujas raktas siekiant toliau saugiai perduoti informaciją.



Šaltinis: ResearchGate.

10 pav. Kvantinės kriptografijos pavyzdys

Taigi kaip matome, kvantinis šifravimas, kalbant apie informacijos saugumą, yra pranašesnis už šiuolaikinius viešojo ir privataus rakto kripto sistemomis paremtais šifravimo algoritmais. Teoriškai daugelis mokslininkų teigia, kad tai yra nenulaužiama kriptografijos sistema, kadangi informacijos perėjimas galimas tik realiu laiku, kurio pagal kvantinės fizikos taisykles tokio mėginimo nepastebėti neįmanoma. Tačiau vien tik iš pateikto kvantinės kompiuterijos pavyzdžio matome, kad tai yra labai komplikuotas šifravimo būdas, reikalaujantis atskiros infrastuktūros, tokios kaip atskiras kvantinis tinklas (literatūroje kartais dar sutinkamas terminas – kvantinis internetas) sudarytas iš optinių kabelių, kuriais keliauja fotonai, o taip pat ir kvantinių maršrutizatorių, retransliuotojo ir t.t. Vėl gi, kadangi tokio tinklo veikimas yra paremtas kvantinės fizikos principais, optinių kabelių ilgis (t.y. perduodamos informacijos atstumas) negali būti didesnis nei 600 kilometrų, tačiau kvantiniu šifravimu užšifruota gali būti sėkmingai perduodama naudojantis palydovais. Kaip skelbia Kinijos mokslo ir technologijų universitetas, Kinijoje jau sėkmingai yra išbandytas 4600 kilometrų ilgio kvantinis tinklas jungiantis Šanchajų su Pekinu, susidedantis iš daugiau kaip 700 optinių kabelių ir palydovų (žr. 11 pav.).



Šaltinis: Kinijos mokslų ir technologijų universitetas.

11 pav. Kinijos pirmas kvantinis tinklas

Europos sąjunga taip pat turi tikslus plėtoti kvantinį tinklą. 2019 metais tarp Europos sąjungos narių buvo pasirašytas memorandumas, dėl kvantinio tinklo plėtojimo - (EuroQCI). Memorandumo

tikslas yra suvienyti EU nares ir kurti vieną bendrą saugų informacijos perdavimo tinklą. Tikimasi, kad toks tinklas pradės veikti 2030 metais.

Reikėtų pabrėžti, kad toks kvantinis tinklas nepakeis dabartinio interneto, o jį tik papildys, kaip ir kvantiniai kompiuteriai papildys klasikinius. Taip pat, kvantinis internetas greičiausiai nebus pasiekiamas paprastiems namų naudotojams.

Kaip memorandume paminėta, pirminis tikslas yra juo sujungti valdžios, finansų, sveikatos apsaugos institucijas, kad jos galėtų saugiai dalintis informacija.

2. KVANTINĖS KOMPIUTERIJOS IR KVANTINIO ŠIFRAVIMO PANAUDOJIMO GALIMYBIŲ PRAKTIKA EUROPOJE IR LIETUVOJE

2.1. Kvantinės kompiuterijos panaudojimas

Nors mūsų įprasti namų kompiuteriai puikiai susitvarko ir tikrai toliau puikiai susitvarkys su visais paprastam namų naudotojui kylančiais iššūkiais, tačiau jau ir dabar yra daug sričių kur net ir patys galingiausi pasaulio super kompiuteriai nebe susitvarko, pvz. sudėtingi finansiniai skaičiavimai, vaistų gamyba ir atrodytų toks savaime paprastas dalykas, kaip viešojo transporto maršrutų planavimas ir optimizavimas.

Daug keliaujantiems žmonėms dažnai tenka susidurti su situacija kuomet vėlavo skrydis, todėl labai dažnai nuo vieno vėluojančio skrydžio susidaro vėluojančių veiksmų grandinė, kadangi, jei ir lėktuvas vėluoja pradžioje tik į vieną skrydį, jis automatiškai vėluos ir į sekantį savo skrydį, o taip pat pilotai dažnai keičia ir lėktuvus, arba kiti lėktuvai laukia vėluojančių keleivių skrendančių jungiamaisiais skrydžiais. Pasak skrydžių monitorinimo platformos Flightradar24.com, pasaulyje kas dieną įvyksta virš 200000 skydžių, taigi matome, kad gali susidaryti labai didelė veiksmų grandis, dėl vėluojančių skrydžių, todėl jau dabar Amerikos oro linijos tokios kaip Delta bendradarbiauja su IBM ir ieško kvantinio sprendimo, kad greičiau ir efektyviau perskirstyti skrydžių maršrutus (Witner 2022).

CERN instituto esančio Šveicarijoje mokslininkai sukūrė didįjį hadronų greitintuvą, pasirašė bendradarbiavimo sutartį su IBM, dėl kvantinės kompiuterijos taikymo tiriant visatą. Pasak programos inovacijų vadovo Federico Carminiti jau dabar yra susiduriama su iššūkiais atliekant tam tikrus skaičiavimus ir klasikiniai super kompiuteriai kuo toliau, tuo labiau susiduria su pajėgumų trūkumais. Yra apskaičiuota, kad norint sėkmingai tęsti programą, 2026 metais reikės 50 ar net 100 kartų didesnės skaičiavo galios, todėl kvantinė kompiuterija suteikia daug vilčių dėl programos tęstinumo. (Carminati 2019). Korporacija Daimler gaminanti automobilius taip pat bendradarbiauja su IBM. Daimler mokslininkai tikisi, kad kvantiniai kompiuteriai padės sukurti naujos kartos elektros baterijas elektromobiliams (Jeannetter 2020). Tuo tarpu, Jungtinės Karalystės startuolis Cambridge Quantum specializuojasi specifinės kvantinės programinės įrangos būtent skirtos kvantiniams kompiuteriams kūrimui. Šiandien kurti jų produktai jau yra pritaikomi tokiuose srityse, kaip vaistų gamyba, medžiagų mokslas, dirbtinis intelektas ar kibernetinis saugumas (Cembridge Quantum 2021).

Taip pat pasak Jacob Biamonte kvantinė kompiuterija suteikia daug didesnį proveržį dirbtinio intelekto (*angl. artificial intelligence*) ir mašinų mokymosi (*angl. machine learning*) srityse. Skirtingai nuo klasikinių kompiuterių, kvantiniai kompiuteriai gali apdoroti netipinius duomenų modelius ir kas svarbiausia daug greičiau nei klasikiniai. Vis dėl to nors ir neseniai atlikti tyrimai parodė, kad kvantiniai

algoritmai gali kurti naujus mašinų mokymosi blokus, tačiau pritaikyti praktikoje vis dar yra labai daug iššūkių (Biamonte 2017 m.).

2.2. Kvantinės kompiuterijos grėsmių praktika

Dorthy E. Denning (2019 m.) informacijos saugumo mokslininkė, 2019 metais American Scientist žurnale paskelbtame straipsnyje „*Is Quantum Computing a Cybersecurity Threat*“ teigia, kad kai pasaulyje atsiras pakankamai galingi kvantiniai kompiuteriai, tai sukels labai didelę saugumo grėsmę. Autorė teigia, kad šiuo metu standartinė populiariausio pasaulyje šifravimo algoritmo RSA raktų pora kuri yra 2048 bitų ilgio arba 617 skaitmenų, šiuolaikiniam kompiuteriui iššifruoti prireiktų apie 300 trilijonų metų, tačiau kvantinis kompiuteris pasitelkdamas Šoro algoritmą tai atliktų per kelias valandas, todėl autorė straipsnyje ragina atsparumą kilsiančioms kvantinės kompiuterijos grėsmėms pradėti planuoti jau dabar.

Šioms grėsmėms dar 2016 metais pirmieji pradėjo ruoštis amerikiečiai. JAV Nacionalinis standartų ir technologijų institutas NIST, 2016 metais išleido kvietimą teikti mokslininkams, verslo atstovams pasiūlymus, dėl naujų kriptografinių reikalavimų, kurie galėtų pakeisti šiuolaikinius viešojo rakto principu veikiančius kriptografijos standartus ir būti atsparūs kvantinės kompiuterijos grėsmėms. Kaip buvo paminėta 1.2.1 poskyryje šį rudenį NIST jau atrinko post-kvantinius šifravimo algoritmus ir yra planuojama, kad naujas šifravimo standartas bus parengtas dar šiais metais arba 2023 metų pradžioje.

Tačiau kvantinių kompiuterių panaudojimas blogiems tikslams gali neapsiribot tik informacijos konfidencialumo pažeidimais. Manoma, kad kvantiniai kompiuteriai gali būti naudojami ir automatizuotoms atakoms, ypač jeigu kvantiniai kompiuteriai bus plačiai pasiekiami per debesų kompiuteriją. Puikus pavyzdys yra kai dirbtinis intelektas naudojamas automatizuotoms atakoms.

Nagrinėjant kvantinės kompiuterijos temą, beveik nėra informacijos, dėl galimybės panaudoti kvantinius kompiuterius DOS atakoms, vis dėl to jeigu jų panaudojimo galimybės prieš klasikinius kompiuterius ir būtų ribotos, manoma, kad DOS atakų grėsmė gali kilti tik kitiems kvantiniams kompiuteriams, kurie būtų sujungti į vieną kvantinį tinklą.

Taip pat būtina įvertinti ir tokias rizikas, kad kaip jau minėjome, kad kvantiniai kompiuteriai vis tiek turės veikti sąveikoje su klasikiniais kompiuteriais ar kitais elementais, kurie gali būti pažeidžiami klasikiniams atakų metodams (*angl. supply chain attacks*) .

Taip pat saugumo specialistai turėtų jau dabar tinkamai saugoti saugomą informaciją, kadangi net jei bus nutekinta užšifruota informacija, piktavaliai ją gali pasilaikyti kuriam laikui ir kai tik jiems bus pasiekiamas kvantinis kompiuteris laisvai ją iššifruoti.

2.3. Kvantinė kompiuterija ir kvantinis šifravimas Lietuvoje

Lietuvos akademinės elektroninės bibliotekos (toliau – Elaba) paieškoje nepavyko rasti nei vieno straipsnio, disertacijos ar bent bakalauro darbo šia tema. T.y. nei kvantinės kompiuterijos, nei juo labiau apie kvantinio šifravimo temas. Viešoje interneto paieškoje pasinaudojus Google paieška, taip pat nepavyko rasti daug informacijos Lietuvių kalba, apart kelių verstinių straipsnių nagrinėjama tema iš užsienio mokslinių žurnalų.

Apžvelgus aukštųjų mokyklų studijų programas susijusias su informatika, fizika ar matematika, pavyko rasti informacijos, kad Vilniaus Universitete Dr. Mindaugas Mačernis dėsto kvantinės kompiuterijos įvadą, kvantinės informacijos, ir kriptografijos dalykus fizikos krypties bakalauro ir magistro programų studentams, tačiau tai yra pasirenkami dalykai.

Nagrinėjant kvantinės kompiuterijos ir kvantinio šifravimo populiarumą ir pritaikomumą Lietuvoje vertėtų pažvelgti į mums artimiausius kaimynus Latvius ir Lenkus, kur Latvijos Universitete jau yra įsteigtas kvantinės kompiuterijos mokslo centras prie informatikos fakulteto, o Lenkijoje tikimasi, kad kitąmet pradės veikti pirmas kvantinis kompiuteris (šiuos atveju plačiau apžvelgsime sekančiame skyriuje).

Taigi, kaip matome Latvijoje skirtumas, nuo Lietuvos yra tas, kad Latvijoje kvantinė kompiuterija jau yra priskiriama prie informatikos mokslo, tuo tarpu Vilniaus Universitete ji yra dėstoma fizikos studentams. Taip pat verta paminėti, kad Latvijos kvantinės kompiuterijos centras aktyviai bendradarbiauja su aukštųjų technologijų įmonėmis, 2021 metais aukštųjų technologijų pasaulinė konsultacijų bendrovė Accenture į Latvijos Universiteto kvantinės kompiuterijos centrą investavo 100 mln. eurų ir investicija per metus jau davė apčiuopiamus rezultatus, nes šiais metais bendradarbiaujant buvo sukurtas kvantinis algoritmas, kuris rentgenogramose ir tomografijose gali aptikti įvairius pakitimus ir anomalijas.

Taigi atsižvelgus į informacijos Lietuvių kalba apie kvantinę kompiuteriją ir kvantinį šifravimą paieškos rezultatus, galima teigti, kad kvantinė kompiuterija ar kvantinis šifravimas yra beveik nenagrinėta arba labai mažai nagrinėta tema Lietuvoje, tačiau pati kvantinė kompiuterija, o iš jos išsivystantis kvantinio šifravimo mokslas (manome, kad tiek kvantinė kompiuterija ir kvantinis šifravimas ilgainiui turėtų tapti atskira mokslo disciplina) yra kvantinės mechanikos dalis, o čia, bent jau iš viešai prieinamos informacijos matyta, kad Lietuva tikrai yra pionieriai šioje mokslo srityje. Vien Elaba sistemoje mums pavyko rasti virš 2400 įrašų šia tema, tame tarpe ir 75 disertacijas. Taigi daroma išvada, kad Lietuvoje kvantinės fizikos ir mechanikos srityse turime mokslininkų potencialą, tad ne veltui Lietuva dažnai pristatoma, kaip lyderė lazerių technologijų pasaulyje (2020.02.19 dienos LRT televizijos reportažas apie tris Vilniaus universiteto Lazerinių tyrimų centro profesorius, šiais metais buvo įvertinti Lietuvos nacionaline mokslo premija „Lietuva – lazerių srities lyderė: mokslininkai tikisi,

kad jų žinios gali būti panaudotos ir organų auginimui“). Tačiau magistro baigiamajame darbe labiausiai domina kvantinės kompiuterijos ir kvantinio šifravimo būklė Lietuvoje, o kadangi viešai prieinamos informaciją sunku rasti, magistrinio darbo metu bus atliktas tyrimas ir pateiktos atlikto tyrimo išvados. Tyrime bus siekiama apklausti IT specialistus - kibernetinio saugumo ekspertus ir išsiaiškinti kokia yra situacija Lietuvoje, kvantinės kompiuterijos ir kvantinio šifravimo srityse.

Kadangi kvantinė kompiuterija yra dar palyginti menkai nagrinėta ir tyrinėta sritis Lietuvoje, todėl tikėtis, kad kvantinio šifravimo tema bus labiau nagrinėta, nei kvantinė kompiuterija yra nelogiška, tačiau vėlgi kaip ir kvantinės kompiuterijos taip ir kvantinio šifravimo srityje nagrinėjant prieinama medžiaga manome, kad Lietuva turi potencialo. Visų pirma dėl prieš tai aprašytų kvantinės mechanikos srityje dirbančių mokslininkų ir mokslo darbuotojų įsitraukimo, o taip pat ir dėl galimo vyriausybės palaikymo. Pavyzdžiui, Lietuvoje po 2014 ir 2022 įvykusios Rusijos agresijos prieš Ukraina, buvo ženkliai susirūpinta nacionaliniu saugumu: padidintas gynybos biudžetas, vėl pradėti šaukti šauktiniai į kariuomenę, įkurtas Nacionalinis kibernetinio saugumo centras - NKSC. NKSC Lietuvoje tvarko įslaptintos informacijos ir ryšių informacinę sistemą, taip pat vertina kriptografinių metodų ir produktų, skirtų informacijos apsaugai ĮIRIS vertinimą ir tvirtinimą, priedo to NKSC užsiima ir moksliniais tyrimais ir inovacijomis. Pvz. Šifruoto ryšio balso ir trumpųjų žinučių perdavimo sistemos programinio kodo veikimo ir funkcionalumo mobiliajame įrenginyje palaikymą.

Teoriškai galima teigti, kad Lietuvoje kriptografines priemones plačiai naudoti ir vystyti gali ir kitos valstybės institucijos, tokios kaip Kertinis valstybės telekomunikacijų centras atsakingas už saugųjį valstybės duomenų tinklą, Valstybės saugumo departamentas bei Lietuvos kariuomenė su antruoju operatyvinių tyrimų departamentu bei Informacinių technologijų tarnyba prie krašto apsaugos ministerijos.

2.4. Europos kvantinė iniciatyva

Nepaisant to, kad Lietuvoje susidomėjimas kvantine kompiuterija šiai dienai yra menkas, Europos sąjungos lygmenyje ji turi labai didelį susidomėjimą. 2016 metais Europos sąjungos skaitmeninės ekonomikos ir visuomenės komisaras Gunther Oettinger kartu su Niderlandų ekonomikos ministrų Henk Kamp išleido Kvantinį manifestą, kurio tikslas buvo nustatyti bendrą Europos sąjungos kvantinę strategiją ateinantiems metams bei iškelti Europos, kaip lyderės vaidmenį antrosios kvantinės revoliucijos priešakyje. Manifeste buvo iškelti reikalavimai Europos komisijai skirti nemažiau nei vieną milijardą eurų kvantinei kompiuterijai Europos sąjungoje vystyti. .

Europos didelio našumo skaičiavimų bendroji iniciatyva (*angl. The European High Performance Computing Joint Undertaking – EuroHPC JU)* yra 2018 metais susikūrusi Europos sąjungos (atstovaujamos Europos komisijos), iniciatyvoje dalyvaujančių valstybių narių ir privataus sektoriaus

iniciatyva bendrai koordinuoti veiksmus ir pastangas, kad Europa taptų pasaulio super kompiuterių lydere.

Šiai dienai iniciatyvoje dalyvauja 32 Europos valstybės tame tarpe ir Lietuva. Pati programa 2021 – 2027 metams turi numatytą, net 7 milijardų bendrą biudžetą.

Iki šių metų EuroHPC JU vystė klasikinius super kompiuterius, kurių šiai dienai turi aštuonis, skirtinguose Europos valstybėse: Portugalijoje, Bulgarijoje, Čekijoje, Slovenijoje, Liuksemburge, Suomijoje, Ispanijoje ir Italijoje.

EuroHPC puikiai supranta ir kvantinių kompiuterių būsimą reikšmingumą, todėl vis daugiau iniciatyvos lėšų investuoja ir į kvantinės kompiuterijos vystymą bei yra parengusi atskirą kvantinių kompiuterių vystymo programą HPCQS.

2022 metų kovo mėnesį EuroHPC paskelbė kvietimą valstybės nariams kurti kvantinius kompiuterius, o jau spalio mėnesį komisija pranešė, kad pirmieji HPCQS iniciatyvos kvantiniai kompiuteriai tikimasi jau 2023 metų pabaigoje atsiras šešiuose Europos valstybėse: Čekijoje, Vokietijoje, Ispanijoje, Prancūzijoje, Italijoje ir Lenkijoje.

Kvantinės kompiuterijos Europoje vystymą remia Europos sąjunga ir 17 HPCQS programoje dalyvaujančių valstybių. Deja Lietuva šioje iniciatyvoje nedalyvauja, tačiau mūsų kaimynai tiek Lenkija, tiek Latvija yra prisijungusios prie minėtos iniciatyvos ir investuoja į kvantinės kompiuterijos vystymą skirdamos ne tik savo investicijas, tačiau sėkmingai pritraukdamos ir Europos sąjungos ar privataus sektoriaus lėšas. Pavyzdžiui, Lenkijoje pirmas kvantinis kompiuteris turėtų atsirasti Poznanės superkompiuterių ir tinklo centre, prie Bioorganinės chemijos instituto (*angl. Poznan Supercomputin and Network Center affiliated to the Institute of Biorganic Chemistry -PSNS*) į kuri bus investuojama ne tik HPCQS iniciatyvos lėšų, bet ir iš Lenkijos vyriausybės, o taip pat ir privataus sektoriaus lėšų. Viena didžiausių Lenkijos moderniųjų technologijų įmonių Creotech, kuri pasirinkta, kaip kvantinio kompiuterio gamintojas žada irgi investuoti į kvantinio kompiuterio kūrimą.

Pasak PSNC vadovo de. Cezary Mazurek pagrindinis faktorius kuris lėmė, kad kvantiniai kompiuteriai atsiras Poznanėje, lėmė PSNS bendradarbiavimas su vietinės rinkos gamintoju t.y. Creotech kuris buvo pasiryžęs prisidėti ir investuoti. Dr. Cezary Mazurek pristatydamas pirmojo Lenkijos kvantinio kompiuterio projektą akcentavo, kad projektui tai pat yra svarbi partnerystė su Lenkijos teorinės fizikos centru bei taip pat ir su Latvijos universitetu, kuris pasak dr. Cezary Mazurek yra atlikęs labai reikšmingų darbų kvantinės kompiuterijos srityje. Tikimasi, kad Latvijos universiteto mokslininkai prisidėdami prie projekto padės sukurti hibridinius (klasikinius – kvantinius) algoritmus ir mechanizmus, kad kvantinis kompiuteris būtų pasiekiamas tyrėjams ir kitoms suinteresuotoms šalims iš visos Europos (Mazurek, 2022).

PSNC kvantinės kompiuterijos programos vadovas dr. Krzysztof Kurowski sako, kad tikisi jog prie pirmojo kvantinio kompiuterio vystymo rytų ir centrinėje Europoje prisidės ir kitos valstybės tokios kaip Latvija, Lietuva, Slovėnija, Vengrija ar Austrija (Kurowski, 2022).

Iš pačios kvantinės kompiuterijos programos plėtros Europoje pasak EuroHPC vadovo Anders Dam Jensen tikimasi galimybės greičiau išspęsti problemas susijusias su sveikata, „daug greitesnis ir efektyvesnis naujų vaistų kūrimas, „skaitmeninio žmogaus dvynio“ sukūrimas, ant kurio bus galima išbandyti naujus vaistus“ taip pat , klimato kaita, logistika „galimybė įmonėms sutaupyti laiko ir kurą bei sumažinti CO2 pėdsaką“ ir energijos naudojimu (Jensen, 2022).

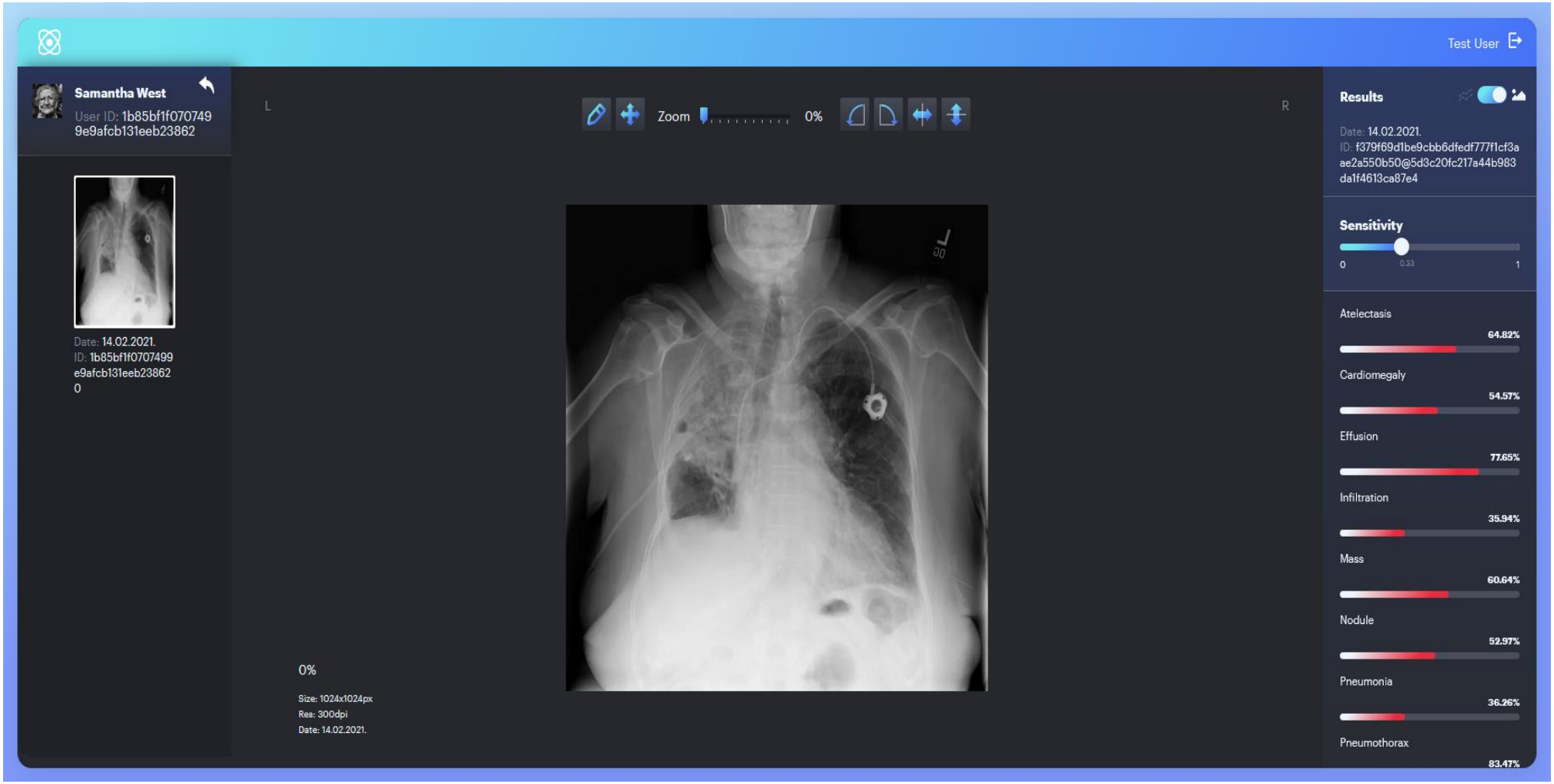
2.5. *Accenture Baltics* ir Latvijos universiteto bendradarbiavimo atvejis

Rentgeno, kompiuterinės tomografijos (KT) ar magnetinio rezonanso (MR) technologijos šiai dienai yra neatsiejamos pacientų gydimo kurso dalis, kuriomis naudojasi medikai visame pasaulyje ir nors šios technologijos ir yra labai ištobulintos, vis dėl to jos yra paremtos žmogiškuoju faktoriumi, t.y. medicinos personalas vizualiai pats identifikuoja galimas anomalijas technologijų sugeneruotuose vaizduose. Tačiau, deja pasaulinė praktika rodo, kad bent penki iš šimto specialistų analizuotų vaizdų yra neteisingai identifikuojami, o labai retais susirgimų atvejais specialistai iš nuotraukų sugeba identifikuoti tik du iš trijų ir nors tokie rezultatai yra priimtini medikų bendruomenėje, tačiau paprastam žmogui jie gali pakeisti ir visą gyvenimą.

Šiai dienai jau yra pristatomi įvairūs kompiuteriniai sprendimai iš kurių dauguma yra paremti dirbtiniu intelektu ir mašinų mokymuisi, tačiau kaip jau buvo paminėta anksčiau, dirbtinis intelektas irgi turi ribas, kurias pasiekia naudojant klasikinius kompiuterius, todėl norint pasiekti labai tikslių rezultatų dirbtiniam intelektui reikia labai didelės skaičiavimo galios ir labai daug laiko, arba tik kvantinio kompiuterio galimybių.

Pasaulinė aukštųjų technologijų įmonė Accenture, jau kelis metus aktyviai dirba kvantinės kompiuterijos srityje. Visame pasaulyje Accenture turi daugiau kaip 15 kvantinės kompiuterijos komandų ir 100 ekspertų dirbančių su ja. Accenture įmonė bendradarbiaudama su Latvijos Universiteto kvantinės kompiuterijos skyriumi bei ten dirbančiais mokslininkais, o taip pat su kvantinės sistemas kuriančia įmone D-WAWE, šiais metais pristatė demo (prototipą) aplikaciją, pavadinimu QuRay (žr. 12 pav.), kuri naudodama kvantini mašinų mokymosi metodą Quantum Restricted Boltzmann Machine - QRBM ir analizuoja įkeltas rentgenogramas, bei ieško patologinių pakitimų juose.

Tyrimo eiga: iš viešai prieinamos duomenų bazės su krūtinės ląstos rentgenogramomis, kuriuose yra identifikuota 14 skirtingų patologijų, aplikacijai mokytis ir veikti buvo atrinktos aštuonios, tokios kaip: atelektazė, kardiomegalija, plaučių lėtinė obstrukcija, plaučių uždegimas ir k.t.

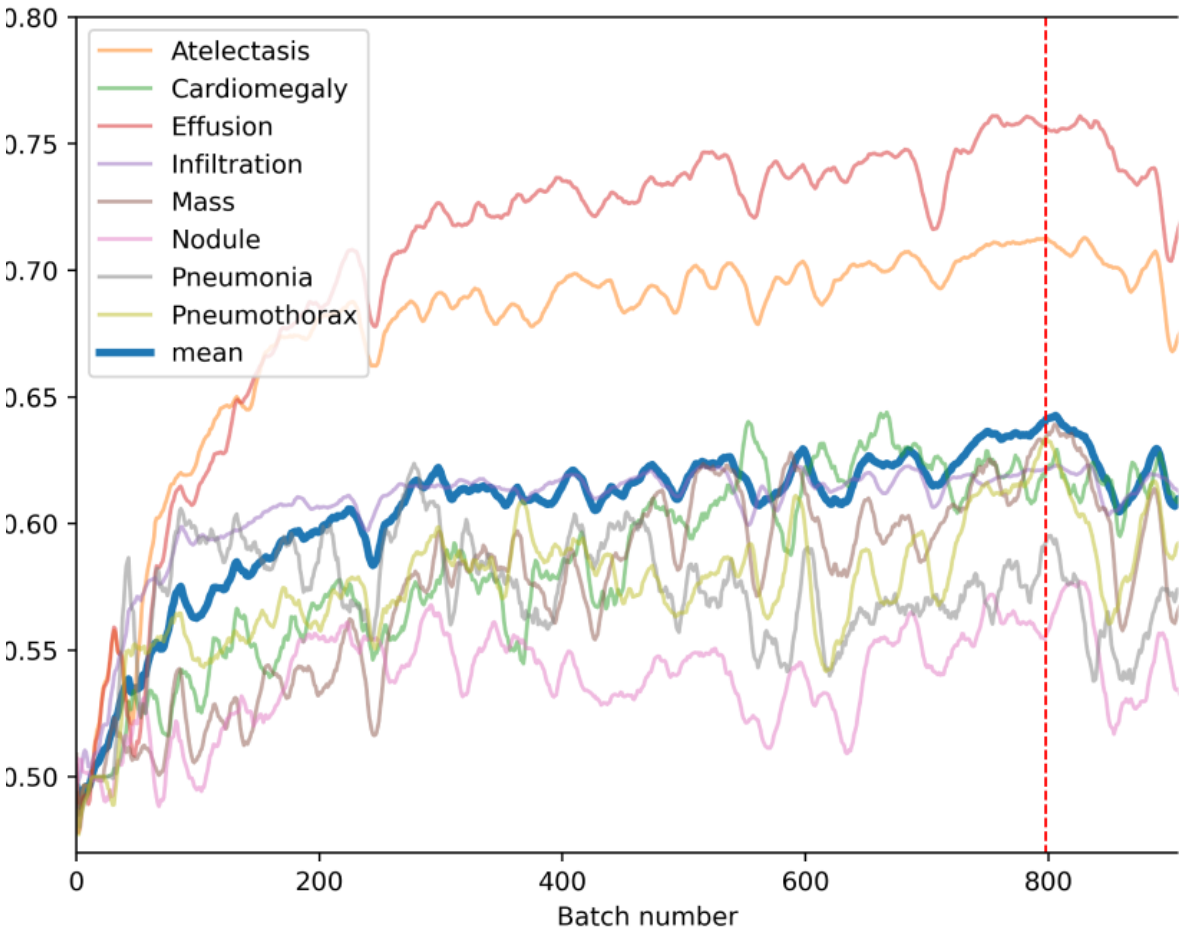


12 pav. QuRay aplikacija

Esminis atlikto tyrimo tikslas buvo naudojantis panaudoti kvantinį mašinų mokymosi metodą - QRBM, kuris pats turėjo apsimokyti ir atpažinti pateiktas anomalijas, bet taip pat apsimokyti identifikuoti ir tas kurios nebuvo pateiktos.

QRMB algoritmas yra dar 1986 metais sukurto mašinų mokymosi algoritmo Restricted Boltzmann machine – RBM pritaikymas kvantiniams kompiuteriams. Nors pats RBM algoritmas praktikoje veikia, tačiau naudojant jį klasikiniuose kompiuteriuose reikia labai daug resursų ir laiko.

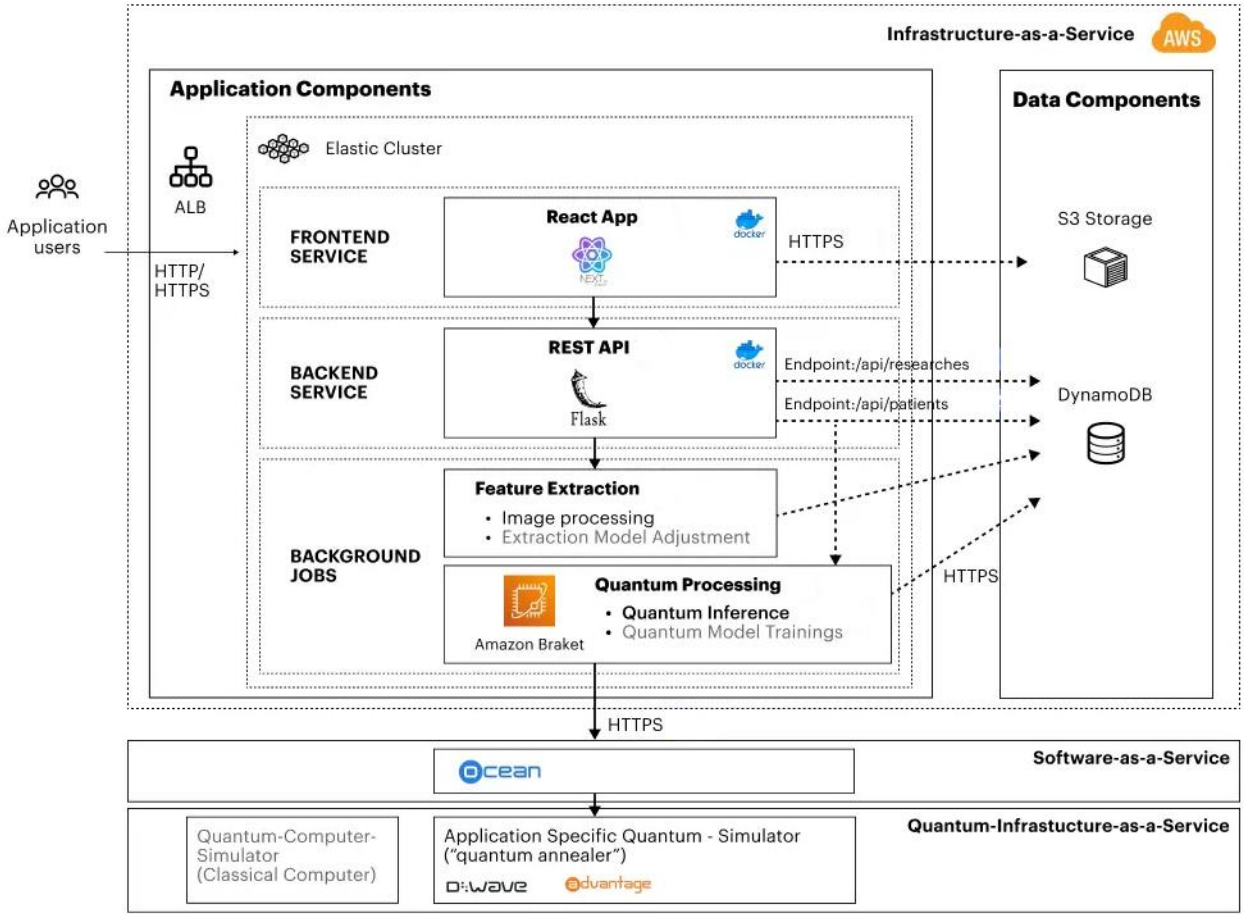
Tuo tarpu naudojant kvantinį kompiuterį ir QRMB algoritmą, pavyko apmokyti aplikaciją per milisekundės dalį. (žr. 13 pav.) Pasitelkus AUC metrikas (viena iš mašinų mokymosi metrikų) į QuRay aplikaciją buvo įkeliamos nuotraukos grupėmis, ir kas 10 grupių buvo suteikiamas laikas atkaitinimui, kuris atsispindi diagramoje, tačiau taip pat atsispindi kaip greit aplikacija sugebėjo apsimokyti identifikuoti patologijas iš vaizdų.



13 pav. Mašinų mokymosi pavyzdys iš QuRay aplikacijos, pasitelkiant AUC metrikas

Taigi nors praktiškai šiai dienai šią aplikaciją medicininiai diagnostikai naudoti būtų dar neįmanoma, dėl prieš tai aprašytų kvantinių kompiuterių, tiek galios trūkumo, tiek ir dėl didelių reikalavimų specifinei aplinkai, vis dėl to Accenture pavyko įrodyti pasitelkus AUC metrikas, kad naudojant kvantinius kompiuterius mašinų mokymasis vyksta keliasdešimt kartų greičiau.

Taip pat šis kvantinio kompiuterio panaudojimo eksperimentas patvirtina prieš tai išsakytą hipotezę, kad kvantiniai kompiuteriai nepakeis klasikinių kompiuterių, bet juos papildys. Jeigu pažvelgtume į visos aplikacijos architektūrą (žr. 14 pav.) matome, kad aplikacija visų pirma yra pasiekiama per naršyklę, o pati yra patalpinta AWS debesų kompiuterijoje. Pati aplikacija turi nešyklės aplikaciją (*angl. fornt-end*) ir serverio aplikaciją (*angl. back-end*). Taip pat aplikacija naudoja AWS paslaugą, pavadinimu Amazon Braket, kuri suteikia galimybę iš klasikinio kompiuterio aplinkos kurti kvantinius algoritmus, pasiekti kvantinius kompiuterius esančius kitų įmonių infrastruktūroje, taip ir čia per Amazon Braket yra pasiekiama D:WAWE OCEAN SDK aplinka. OCEAN yra Python programavimo kalbos interpretatorius, kuris Python programinį kodą išverčia į D:WAWE, kvantiniam kompiuteriui suprantamą kalbą.



14 pav. QuRay aplikacijos architektūra

Taip pat prie šios kvantinės kompiuterijos panaudojimo praktikos reikėtų paminėti, kad Lietuvoje turime plėtojama panašios koncepcijos spartuolį pavadinimu Oxipit. (www.oxipit.ai). Nors Oxipit ir naudojasi mašinų mokymosi ir dirbtinio intelekto sistemomis, tačiau visas duomenų apdorojimas yra atliekamas naudojant klasikinius kompiuterius. Tokiu atveju, tokioms įmonėms rekomenduotume investuoti ir į kvantinę kompiuteriją, kadangi nors iš šiai dienai jie negalėtų tiesiogiai pritaikyti kvantinės

kompiuterijos verslo vystymui, tačiau jeigu nebus pradėta investuoti jau dabar, po kokių 10-15 metų tikėtina, kad bus išstumti iš rinkos tų įmonių, kurios investavo į kvantinę kompiuteriją.

Prie QuRay aplikacijos dirbo iš Acenture pusės Dr. Hassan Naseri, Evrim T. Ozmemer, Zame Klanina ir k.t. iš Latvijos Universiteto pusės prie projekto dirbo prof. rr. Andris Ambainis, dr. Karlis Freivalds, dr. Kaspars Balodis ir k.t.

2.6. Kvantinės kompiuterijos ir kvantinio šifravimo panaudojimo galimybės Lietuvoje

Prieš tai magistro baigiamajame darbe išsiaiškinome, kad kvantinės kompiuterijos teikiamas galimybes galima panaudoti:

- kibernetiniame saugume;
- naujų vaistų paieškoje;
- finansinėse institucijose;
- kuriant naujas baterijas elektromobiliams;
- eismo optimizavimui;
- oro prognozėms;
- dirbtiniam intelektui ir t.t

Iš nebaigtinio sąrašo galime matyti, kad iš esmės kvantinės kompiuterijos galimybes galime pritaikyti ir Lietuvos ūkyje, kadangi Lietuvoje turime ir biotechnologijų pramonės sektorių ir finansinių technologijų įmonių, taip pat didelę dalį Lietuvos ekonomikoje užimančiame transporto sektoriuje ar besivystančiame kibernetinio saugumo sektoriuje.

Kalbant apie kibernetinį saugumą, kvantinė kompiuterija turėtų būti aktuali valstybiniam sektoriui, ypač už nacionalinį saugumą atsakingoms įstaigoms. Pvz. jau dabar Lietuvos ginkluotosios pajėgos naudoja įvairias šifravimo sistemas, pavyzdžiui TCE 671 (viešųjų pirkimų informacija). Iš viešai prieinamos informacijos galime matyti, kad toks įrenginys naudoja du šifravimo algoritmus, pirmas yra NATO slaptas algoritmas kodiniu pavadinimu EINRIDE, o kitas jau prieš tai aptartas AES algoritmas. Kadangi informacijos apie EINRIDE yra labai mažai ir ji visa užslaptinta, tačiau atsižvelgus į tai, kad šalia yra naudojamas ir AES algoritmas, kurio didžiausias rakto ilgis yra tik 256 bitų galima teigti, kad EINRIDE gali būti simetrinis krypavimo algoritmas, nes AES dažniausiai yra naudojamas privatiems raktams saugiai perduoti.

Vėlgi, kaip prieš tai buvo aptarta nors šiai dienai ir greičiausiai kelis metus ar dešimtmečius AES kaip po simetrinio šifravimo algoritmas yra saugus, tačiau mokslininkai nėra šimtu procentu tuo garantuoti, todėl jau dabar už nacionalinį saugumą atsakingos įstaigos turėtų aktyviai domėtis kvantinės kompiuterijos ir post-kvantinio šifravimo algoritmais bei galimybėmis pradėti juos taikyti.

Lietuvoje taip pat yra vystoma viena iš populiariausių pasaulyje virtualaus privataus tinklo paslaugų (*angl. Virtual private network*) NordVPN. NordVPV, kaip ir bet kuris VPN naudoja dvi plačiai

paplitusias technologijas tai OpenVPN standartą ir IpSec protokolą kurios nėra atsparios post kvantiniam šifravimui, tačiau jau dabar yra kuriamas ir jau yra sukurtos VPN technologijos, kurios bus atsparios post kvantiniam šifravimui, pavyzdžiui, OpenQuantumSafe projektas ir WireGuard projektas. Atsižvelgiant į post kvantinio šifravimo grėsmes, tokios įmonės kaip NordVPN norėdamos likti konkurencingos informacijos konfidencialumo produktų rinkoje, jau dabar turėtų pradėti kurti, jei ne post-kvantinio šifravimo sprendimus, tai bent jau nusimatyti strategijas.

Lietuvos biotechnologijų sektorius taip pat yra reikšminga Lietuvos ūkio dalis ir pasak Lietuvos mokslo, inovacijų ir technologijų agentūros sudaranti apie 2.5 prc. Lietuvos BVP. Tai yra vienas iš sparčiausiai augančių Lietuvos pramonės sektorių.

Kaip kvantinė kompiuterija galėtų prisidėti prie biotechnologijų mokslo vystymosi Lietuvoje? Pirmiausiai tai kvantinės kompiuterijos galimybės gali prisidėti biotechnologijų tyrimuose, naujų vaistų paieškose, juo labiau, kad tokie dalykai kaip naujų proteino struktūrų sinteze yra paremti kvantinės mechanikos principais ir šiuolaikiniai, net patys galingiausi kompiuteriai su tokiomis užduotimis nesusitvarko, todėl kaip išganymo yra laukiami kvantiniai kompiuteriai, kurie tikėtina kartu su dirbtiniu intelektu galėtų vėlgi sukurti vaistus nuo šiai dienai nepagydomų ligų.

Finansų sektorius Lietuvoje taip pat užima reikšmingą ekonomikos dalį. Šalyje turime įsikūrusius didžiausius Skandinavijos bankus, taip pat pasak Fintech Lithuania šiai dienai Lietuvoje jau turime daugiau kaip 200, taip vadinamų finansinių technologijų (*angl. Fintech)* įmonių, kurioms taip pat aktualu išlikti konkurencingoms globaliame finansiniame pasaulyje, kuriame tokios pasaulinio garso finansinės įstaigos kaip J.P. Morgan, Wells Fargo, Barclays, Mitsubishi Finansial Group, Citigroup, Goldman Sachs ir Caixa Bankai jau šiandien yra vieni didžiausiu investuotojų į kvantinės kompiuterijos technologijas. Tačiau daug kam kyla klausimas: „Ar kvantinės technologijos finansų sektoriui yra potencialas ar grėsmė?„ Visų pirma, finansinis sektorius yra paremtas sudėtingais matematiniais skaičiavimais: kredito reitingai, palūkanų normos, ateities įžvalgos, bankinės operacijos. Jau dabar bankai joms naudoja taip vadinamus superkompiuterius. Lietuvoje 2010 – 2019 metais veikęs Barclays bankas čia taip pat buvo įkūręs ir *Mainframe* kompiuterių centrą, kuris atlikdavo sudėtingus skaičiavimus.

Vienas pagrindinių privalumų kuriuos tikimasi suteiks kvantinė kompiuterija finansų sektoriui, tai galimybę apskaičiuoti taip vadinamą *MonteCarlo* simuliaciją. *MonteCarlo* simuliacija gali labai tiksliai nuspėti ateities rinkų tendencijas, nustatyti rizikas ir nežinomuosius finansų rinkose. Kol kas net ir galingiausi kompiuteriai *MonteCarlo* algoritmo negali apskaičiuoti.

Vis dėl to, kaip buvo aptarta anksčiau, kvantinė kompiuterija kelia labai didelę grėsmę šifravimui, o finansų sektoriuje kur yra labai aukštas duomenų ir informacijos apsaugos lygis, taip pat jam taikomi ir labai aukšti priežiūros įstaigų reikalavimai, todėl daugelis mokslininkų ir kvantinės kompiuterijos specialistų didžiausią grėsmę būtent įžvelgia finansų sektoriuje. 2021 metais Niujorke vykusioje

kasmetinėje kvantinės kompiuterijos konferencijoje *Inside Quantum Technology* Accenture, kvantinės kompiuterijos programos vadovas Dan Garrison savo pranešime paminėjo, kad didžiausią grėsmę kvantinei kompiuterijai kelia būtent finansų sektoriui (Garisson, 2021). Pasak Dan Garisson visų pirma vis daugiau žmonių atlieka įvairius atsiskaitymus elektroninėje erdvėje, taip pat atliekami įvairūs piniginiai pervedimai, ir viskas tai atliekama pasitelkus įvairius šifravimo metodus, pavyzdžiui, naudojant jau prieš tai aptartus TLS. Klientų informacija irgi dažnu atveju yra apsaugota ir šifruota laikoma saugiai finansinių institucijų duomenų bazėse, tad teoriškai netgi jeigu ir bus nutekintos tokios duomenų bazės, jeigu jos yra tinkamai apsaugotos (panaudoti moderniausi šių laikų šifravimo algoritmai). Tačiau jos yra saugios tik šiai dienai, nes piktavaliai kurie gavo prieigą prie tokių duomenų bazių gali jas laikyti saugiai pasidėję kelis metus ar dešimtmetį, ir laukti kuomet atsiras pilnai funkcionuojantis ir viešai visiems prieinami kvantiniai kompiuteriai, ir tuos duomenis tada dešifruoti. Galbūt daugelis tokių duomenų ir neturės jokios reikšmės, bet pagalvokime apie situaciją, kuomet atsiradus kvantiniam kompiuteriui tokia informacija taps prieinama. Pavyzdžiui duomenys apie 2016 metų JAV prezidentinės kompanijos finansavimą, apie kuriuos buvo labai plačiai diskutuota visame pasaulyje, todėl finansinės institucijos jau dabar turėtų domėtis ir esant galimybei įdiegti įvairias apsaugos priemones, kurios būtų atsparios post-kvantiniam šifravimui, pavyzdžiui, pradėti naudoti prieš tai aptartus kvantiniams kompiuteriams atsparius šifravimo algoritmus.

Labai dažnai plačiai aptariamas kvantinės kompiuterijos panaudojimo atvejis yra elektromobilių baterijų gamyba. Šiai dienai elektromobilių baterijos yra išimtinai gaminamos iš ličio ir jos yra brangiausia automobilio dalis. Taip pat tiek Europoje, tiek likusiam vakarų pasaulyje yra plačiai deklaruojamas elektromobilių naudojimo skatinimas, tiek finansinėmis, tiek kitomis priemonėmis. Lietuvos Respublikos vyriausybė taip pat yra numačiusi strategiją, kad iki 2030 metų šalyje įrengti 60000 viešų įkrovos vietų, o tuo tarpu Europos Komisija yra pareiškusi, kad 2035 metais visi bendrijoje parduodami automobiliai turės būti elektriniai. Taigi kur čia gali būti kvantinės kompiuterijos pranašumas ir galimybė Lietuvai? 2.1 poskyryje buvo pateiktas IBM su Daimler korporacijos bendradarbiavimo pavyzdys , kad išrasti naujas automobilių baterijas su greitesniu pasikrovimo greičiu. Iš esmės čia vėl yra kalbama apie kvantinės mechanikos, fizikos ir chemijos procesus detaliai aprašytus nagrinėjant biotechnologijų ir kvantinės kompiuterijos panaudojimo atvejį. Kadangi kaip išsiaiškinome Lietuvoje turime tikrai stiprų biotechnologijų sektorių, o ir Lietuvos Vyriausybės užmojai tikrai yra nemaži, prisiminkime Lietuvos Respublikos kvietimą Tesla įmonei, įkurti baterijų gamyklą Lietuvoje, tačiau Tesla vis dėl to savo baterijų gamyklai pasirinko Vokietiją, (prieš tai Europoje Tesla baterijų gamykla jau buvo įsikūrusi Nyderlanduose), tai įdomų ar Vokietijos vyriausybei reikėjo įdėti kažkokių papildomų pastangų siekiant pritraukti Teslą statyti gamyklą prie Berlyno, greičiausiai ne, nes visam pasauliui yra puikiai žinoma, kad Vokietija ne tik pasižymi puikia verslo aplinka, tačiau taip pat ir stipriu aukštųjų technologijų ir mokslo sektoriumi. Vokietija taip pat labai daug investuoja į mokslą, vien per

ateinančius penkis metus ji yra numačiusi investuoti 2 milijardus eurų į kvantines technologijas (neapeinant kvantinės kompiuterijos). Atsižvelgiant į pateiktus skaičius tikrai negalime atmesti fakto, kad Tesla Vokietiją pasirinko būtent dėl jų. Todėl tiek Lietuvos verslui, tiek Lietuvos valstybei norint pritraukti milijonines investicijas, kurti naujas darbo vietas, būtina investuoti į mokslą ir tyrimus ir dalyvauti įvairiuose aukštųjų technologijų vystymo iniciatyvose, pavyzdžiui tokiuose kaip prieš tai aptarta HPCQS iniciatyva.

Sekančios sritys, kur Lietuva galėtų parodyti savo kvantinės kompiuterijos potencialą, tai sukuriant ar bent prisidedant prie sukūrimo programinės įrangos veikiančios kvantinės kompiuterijos pagrindų, tai yra eismo organizavimas ir meteorologija. Kalbant apie eismo organizavimą, mes kalbame apie bet kokį maršrutizavimą (*angl. routing*) ar tai būtų logistikos įmonės, siuntų pristatymo įmonės, ar tie patys kamščiai Vilniaus mieste.

Nuo 1930 metų yra žinoma, kaip po keliaujančio pardavėjo problema (*angl. Traveling salesman problem – TSP*).

Problemos esmė yra rasti optimaliausią maršrutą tarp skirtingų taškų (originalioje problemoje miestų) ir grįžti į pradinį tašką. Atrodytų argi sunku apskaičiuoti optimaliausią maršrutą, tačiau atlikus skaičiavimus matome, kad iš 10 skirtingų taškų galima sudaryti 300000 skirtingų maršrutų, tuo tarpu iš 15 jau būtų 87 milijonai. Taigi kaip ir buvo paminėta prieš tai, kuo skaičiai didesni tuo sunkiau klasikiniams kompiuteriams susidoroti su jais ir atlikti reikiamus skaičiavimus.

Todėl manome, kad atsižvelgiant į pateiktus skaičius, maršrutų organizavimas - optimizavimas pasitelkiant kvantinės kompiuterijos galimybes Lietuvoje susilauktų tikrai daug dėmesio iš verslo, nes nuo pat nepriklausomybės atgavimo Lietuva tapo vienu pagrindiniu transporto sektoriaus dalyvių Europos rinkoje. Lietuviški sunkvežimiai raižo Europos kelius nuo Gibraltaro iki Permes, nuo Tromso iki Stambulo. Traukiniai krovinius veža iš Pekino, o atidarius RailBaltica tikimasi, kad Lietuvos Geležinkeliai sėkmingai įsilies ir į Europos geležinkelių logistikos tinklą.

Sekanti problema, kurią gali išspręsti kvantinė kompiuterija, tai meteorologija. Šiandien orai nuspėjami pasitelkiant kompiuterius, tačiau net ir galingiausi super kompiuteriai tiksliai orus nuspėti gali apie penkias dienas į priekį ir tai tikslumas būtų tik apie 90 %, septynių dienų prognozė apie 80 % ir su kiekviena diena prognozės tikslumas mažėja.

Paskutinis šiame magistro baigiamajame darbe nagrinėjamas kvantinės kompiuterijos panaudojimo galimybių atvejis (bet tikrai ne paskutinis, apskritai) manome turėtų būti dirbtinis intelektas. 2018 metai Lietuvos ekonomikos ir inovacijų ministerija kartu su akademiniais ir verslo partneriais paskelbė Lietuvos dirbtinio intelekto strategiją, kurioje nurodomos Lietuvos strategiją vystant dirbtinio intelekto tyrimus, mokslą, verslą ir pritaikymą Lietuvoje. Tačiau strategijoje visiškai nėra užsimenama apie dirbtinio intelekto ir kvantinės kompiuterijos sąryšį, nors daugelis tiek pasaulio dirbtinio intelekto ir kvantinės kompiuterijos mokslininkų ir advokatų apie dirbtinio intelekto ateityje

kalba kaip po neatsiejamą nuo kvantinės kompiuterijos, pavyzdžiui su dirbtiniu intelektu paremtų sprendimų kuriančios kompanijos AiMultiple vadovas Cem Dilmegani savo studijoje kalba apie tai, kad dirbtinis intelektas ir kvantinė kompiuterija jau dabar turėtų eiti koja į koją, o ateityje tapti apskritai neatsiejami (Dilmegani, 2022).

Todėl keista matyti, kad tiek Lietuvos dirbtinio intelekto sektoriaus atstovai, tiek valdžios institucijos advokataudamos dirbtinio intelekto sektorių visiškai nekalba apie kvantinę kompiuteriją. Čia vėlgi galime įžvelgti, kad nors siekiai ir yra pagirtini tačiau dažnu atveju labai atsiliekame nuo vakarų, o šiai dienai drįstume sakyti, kad ir nuo tolimųjų rytų technologinių požiūrių, todėl vėlgi pasikartosime, kad norint išlikti konkurencingai ir kurti konkurencingus produktus valstybė ir šalies įmonės, mokslo įstaigos turėtų pačios investuoti į tyrimus, pritaikomumo atvejų studijas ir pan. Puikus dirbtinio intelekto ir kvantinės kompiuterijos panaudojimo pavyzdys buvo pateiktas 2.5 poskyryje.

Apibendrint šį poskyri galima būtų panaudoti Jonathan Rune išsakyti minti, kad vis dar yra atotrūkis tarp kvantinės kompiuterijos supratimo ir visų galimybių išnaudojimo. Mokslininkai jau dešimtmečius dirba ties kvantinė kompiuterija ir jį vis evoliucionuoja ir ar evoliucijos pikas bus pasiektas 2022 nėra aišku tik tai, kad pažanga bus pasiekta ir verslas turi tam pasiruošti (Rune 2021).

3. KVANTINĖS KOMPIUTERIJOS PANAUDOJIMO IR KVANTINĖS KOMPIUTERIJOS GRĖSMIŲ TYRIMAS

3.1. Tyrimo metodologija

Tyrimui atlikti buvo pasirinktas kokybinis tyrimo metodas – ekspertų apklausa (kokybinis interviu). Kokybinio interviu tikslas apklausti kibernetinio saugumo, IT ir kitų susijusių su tyrimo tema profesijų ekspertus ir gauti atsakymus bei jų nuomonę į tyrime išsikeltus klausimus.

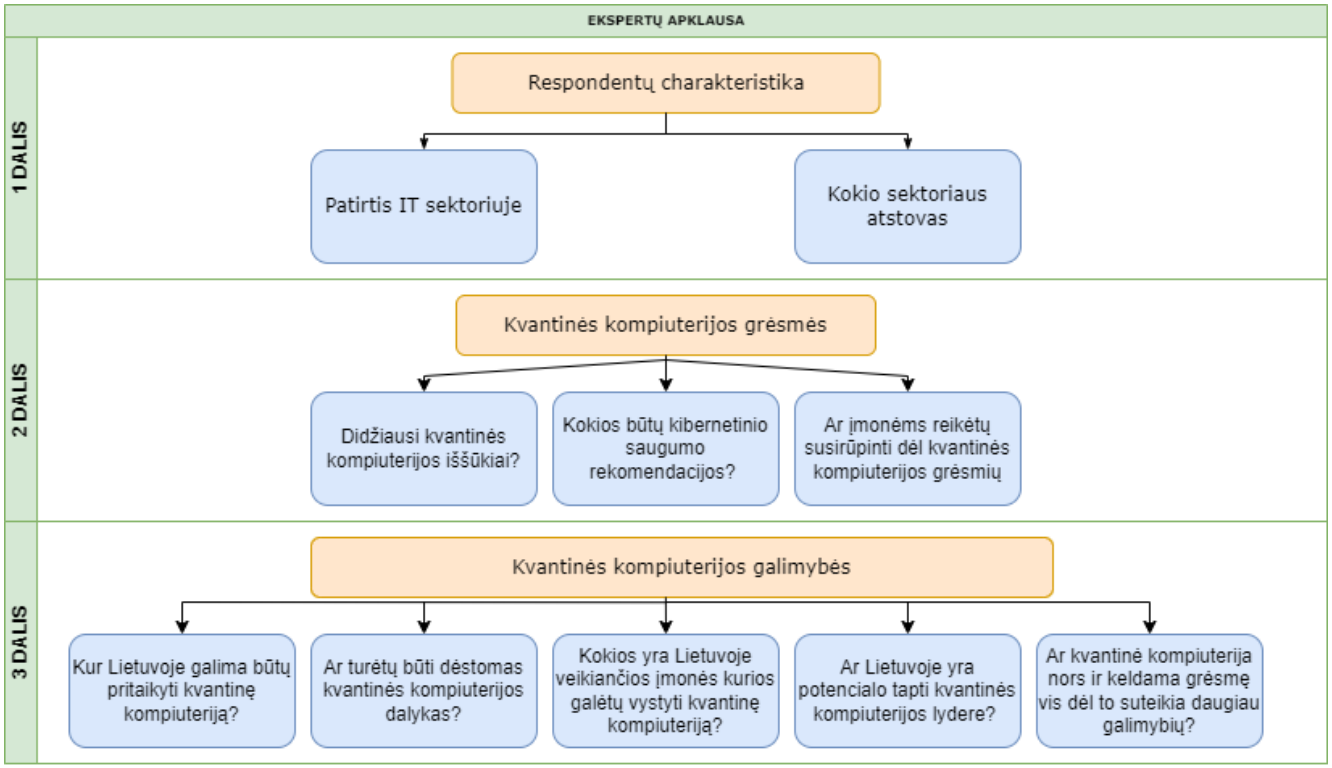
Pasak I. Gaižauskienės ir N. Valavičienės „*Interviu metu gilinamasi į nuomones, nuostatas, patirtis, motyvus, jausmus ir pan. Kitaip tariant, interviu atliekamas tada, kai iš žmonių norime sužinoti tai, ko negalime matyti tiesiogiai – mes negalime matyti (stebėti) jausmų ir minčių; negalime atkartoti elgesio ar sąveikų, kurios įvyko prieš tam tikrą laiką; negalime apčiuopti prasmių, kurias žmonės suteikia juos supančiam pasauliui, ir daugelio kitų 3 Apmąstantis ir įsisąmoninantis savo veiklą. 16 1.1. dalykų (Patton, 2002). Kai tiriame tai, ko negalime matyti, tenka užduoti klausimus. Interviu leidžia įžengti į kito žmogaus perspektyvą, o kokybinis interviu remiasi prielaida, kad kitų žmonių perspektyva yra prasminga, pažintina ir gali būti aiškiai išsakyta. Interviu imami siekiant įsigilinti, kas yra kitų žmonių mintyse, kaupiamos jų istorijos“* (Gaižauskiene ir Valevičienė, 2016 m.)

Kokybinis tyrimo (interviu) atlikimo metodas pasirinktas, nes teorinėje dalyje buvo nustatyta, kad pasirinkta nagrinėti tema yra labai nauja ir nenagrinėta Lietuvoje, dauguma hipotezių, dar yra tik teoretinės, todėl pasak kokybinių tyrimų atlikėjų, toks metodas leidžia apklausti mažesnę, tačiau tikslesnę auditoriją. Taip pat kokybinio tyrimo metu gauta informacija atspindi tik specifinį atvejį ir išvados yra hipotetinės (Gaižauskienė ir Valavičienė, 2016 m.).

Tyrimui atlikti buvo sukurta anketa - klausimynas (1 priedas) su 10 klausimų susijusių su nagrinėjama tema. Pateikta anketa atitinka bendruosius anketos sudarymo reikalavimus (Didčkius, 2011):

1. Nustatyti, kokia informacija yra reikalinga;
2. Pasirinkti apklausos būdą;
3. Sumažinti respondento nenorą ar nesugebėjimą atsakyti;
4. Įvertinti klausimo esmę;
5. Pasirinkti klausimo struktūrą;
6. Pasirinkti tinkamus žodžius;
7. Išdėstyti klausimus anketoje;
8. Nustatyti anketos formą;
9. Patikrinti anketą.

Anketos klausimus galima suskirstyti į 3 pagrindinės dalis (žr. 15 pav.)



15 pav. Klausimyno struktūros loginė schema

Tyrimo organizavimas

Tyrimas buvo atliekamas 2022 kovo 15-30 dienomis. Tyrimo klausimynas dalyviams buvo išsiųstas elektroniniu paštu ir per socialinio tinklo LinkedIn susirašinėjimo funkcionalumą.

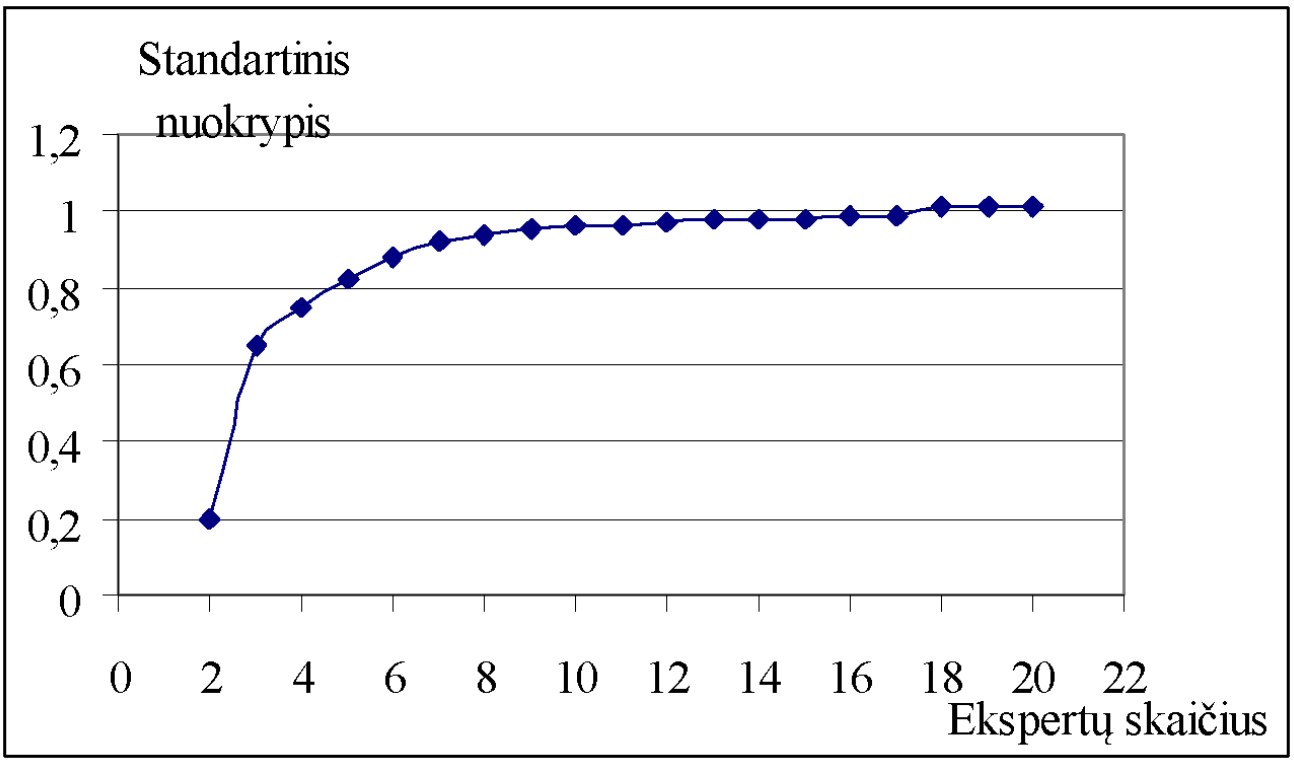
Tyrimas buvo atliekamas apklausiant įvairius kibernetinio saugumo ekspertus. Tyrimo metu buvo apklausti šie 7 ekspertai:

- ESET Lietuva kibernetinio saugumo ekspertas;
- Baltic Amadeus informacijos saugumo architektas;
- Critical Security kibernetinio saugumo ekspertas;
- Kauno technologijų universiteto profesorius;
- Įmonės kibernetinio saugumo vadovas;
- Laisvai samdomas kibernetinio saugumo specialistas;
- Accenture Baltics OT/IoT security expert.

Pasirinkta ekspertų imtis visų pirma buvo nulemta to, kad Lietuvoje turime labai mažai specialistų galinčių ir norinčių pasidalinti savo nuomone nagrinėjama tema. Tyrimo pradžioje iš viso buvo kreiptasi į 20 informacinių technologijų, fizikos, kibernetinio saugumo ekspertų, tačiau tyrime sutiko dalyvauti tik septyni vis dėl to, pasak I. Gaižauskienės ir N. Valavičienės *„...kokybiniams tyrimams būdingos mažos imtys (tai gali būti vos keli ar netgi vienas atvejis)... Imties „mažumas“ labiau susijęs su tuo, kad*

kiekvienas atvejis tiriamas išsamiai, todėl mažesnis atvejų skaičius gali duoti pakankamą kiekį duomenų tyrimo tikslui pasiekti. Be to, kokybinių interviu metu surenkami dideli tekstinių duomenų masyvai, kurių analizei reikia daug darbo ir laiko.“ Atsižvelgiant į tai, kad tyrimo metu dauguma respondentų turėjo daugiau kaip 10 metų patirtį ir sutiko pasidalinti savo žiniomis ir nuomone apie kvantinę kompiuteriją ir kvantinį šifravimą, galima teigti, kad tyrimo metu surinkta informacija yra aukšto patikimumo.

Tą patį paliudija Baležentis ir Žalimaitė (2011 m.) pateikdami Ekspertų vertinimų standartinio nuokrypio priklausomybės nuo ekspertų skaičiaus kreivę (žr. 16 pav.)



16 pav. Ekspertų vertinimų standartinio nuokrypio priklausomybė nuo ekspertų skaičius

Tyrimo tikslas – ekspertų apklausos metu išsiaiškinti ekspertų nuomonę ir gauti atsakymus į magistrinio darbo metu išsikeltus uždavinius: išanalizuoti kvantinės kompiuterijos ir kvantinio šifravimo teoriją, nustatyti kvantinės kompiuterijos ir kvantinio šifravimo grėsmes, įvertinti kvantinės kompiuterijos ir kvantinio šifravimo panaudojimo galimybes Lietuvoje.

Tyrimo uždaviniai:

- Išsiaiškinti ekspertų nuomonę apie kvantinės kompiuterijos panaudojimo galimybes Lietuvoje. Kuriuose verslo ar viešojo sektoriuose Lietuvoje būtų galima pritaikyti kvantinę kompiuteriją;
- Nustatyti ekspertų nuomonę apie keliamas kvantines kompiuterijos grėsmes. Ar įmonėms ir organizacijoms jau reikėtų sunerimti, dėl kvantinės kompiuterijos keliamų grėsmių?;
- Išsiaiškinti kvantinės kompiuterijos dalyko aktualumą Lietuvoje;
- Gauti ekspertų rekomendacijas, kaip Lietuvai išlaikyti aukštas kibernetinio saugumo pozicijas;
- Nustatyti ar Lietuvos verslas yra pasirengęs dirbti su kvantine kompiuterija;

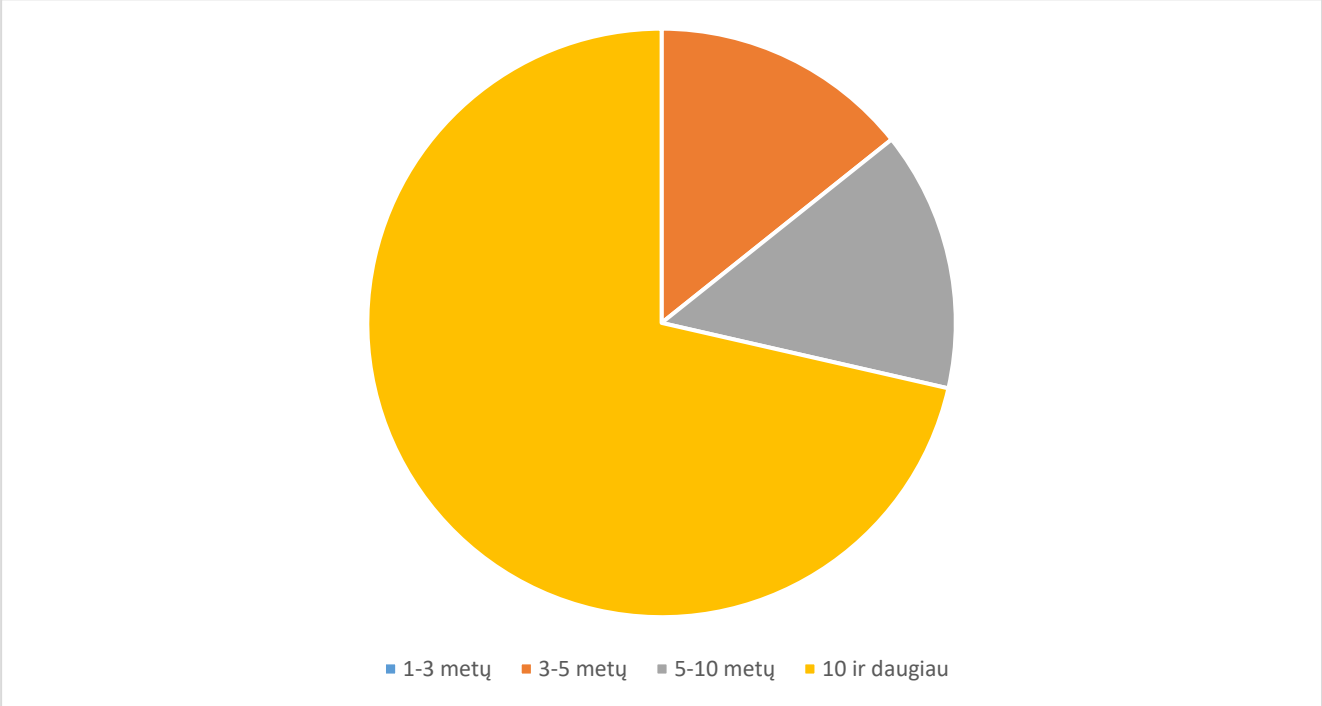
- Išsiaiškinti ekspertų nuomonę ar žengiant į kvantinės kompiuterijos amžių nereikėtų pradėti dėstyti kvantinės kompiuterijos dalyko aukštojoje mokykloje;
- Išsiaiškinti kokia ekspertų nuomonė yra dėl to ar įmonėms reikėtų sunerimti jau dabar, dėl kvantinės kompiuterijos keliamų grėsmių;
- Išsiaiškinti atsižvelgiant į ekspertų nuomonę, kokie yra didžiausi iššūkiai Lietuvoje susiję su kvantine kompiuterija;
- Surinkti ekspertų atsakymus į išsikelta probleminį klausimą: ar kvantinė kompiuterija suteiks daugiau galimybių nei grėsmių?

Tyrimo objektas – kvantinės kompiuterijos panaudojimo galimybės Lietuvoje ir kvantinės kompiuterijos keliamos grėsmės.

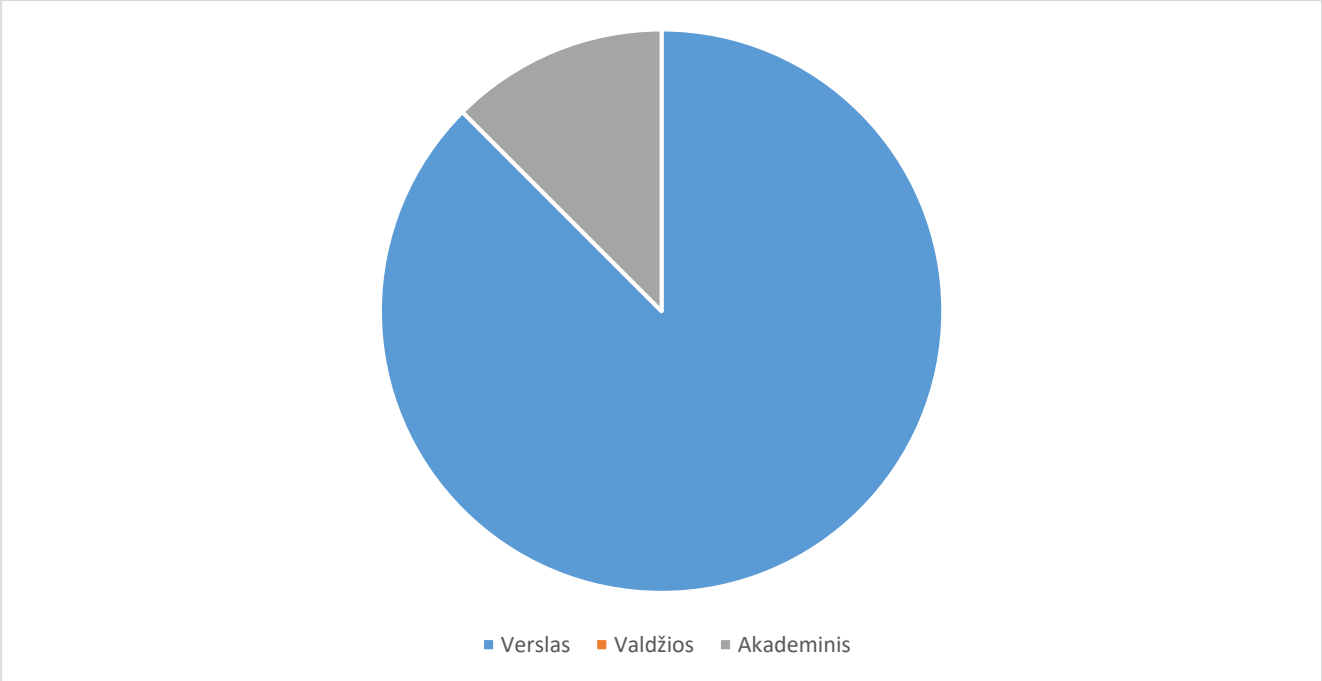
3.2. Tyrimo duomenų analizė

Tyrimo duomenys buvo apdorojami Microsoft Exel programa.

Tyrimo pradžioje pirmiausiai buvo siekiama išsiaiškinti kokio sektoriaus (verslo, valdžios, akademinio) atstovas yra respondentas bei kokia yra respondento patirtis kibernetinio saugumo ar informacinių technologijų sektoriuje.



17 Pav. Ekspertų patirtis



18 pav. Ekspertų darbo sektorius

Kaip matome dauguma apklausoje dalyvavusių ekspertų turi daugiau kaip 10 metų patirtį kibernetinio saugumo srityje. Su tokia sukaupta ekspertų patirtimi galime teigti, kad tyrimo rezultatai bus labai aukšto ekspertinio lygmens.

Pagal sektorius matome, kad beveik visi apklausos dalyviai yra iš verslo sektoriaus ir vienas tyrimo dalyvis yra iš akademinės bendruomenės. Gaila tačiau atliekant tyrimą nepavyko apklausti ir gauti nei vienos nuomonės iš valstybinio sektoriaus, nors atliekant tyrimą buvo kreiptasi ir į juos.

Atliekant tyrimą pirmiausiai buvo siekiama išsiaiškinti ekspertų nuomonė ar kvantinės kompiuterijos tema jau šiandien turėtų būti aktuali Lietuvoje, jiems buvo užduotas vienas atviras klausimas: „*Jūsų nuomone ar kvantinė kompiuterija jau šiandien turėtų būti aktuali tema Lietuvoje ir kodėl*?“ .

Apibendrinus ekspertų atsakymus visi atsakė panašiai tai yra, kad kvantinė kompiuterija kol kas verslui ar valstybiniam sektoriui yra sunkiai pasiekiamas dalykas, tačiau visi sutartinai atsakė, kad kvantinė kompiuterija pirmiausiai turėtų būti plėtojama akademinėje plotmėje:

„Kvantinė kompiuterija turėtų būti aktuali kaip mokslo bei apskritai žinių disciplina. Besiruošiant praktiniam taikymui ateityje, galbūt kaip vienas dalykas dėstomas universitete…“ – pasisakė vienas iš respondentų.

Toliau tyrimo metu norėjome išsiaiškinti respondentų požiūrį į dabartinę Lietuvos kibernetinio saugumo situaciją, kadangi Lietuva pagal nacionalini kibernetinio saugumo reitingą patenka į kibernetiškai atspariausių šalių antrą vietą (*National Cyber Security Index 2022*), respondentų klausėme jų nuomonės apie galimybes išlaikyti tokius pačius aukštus reitingus post-kvantiniam pasaulyje.

Vėlgi ties vienu dalyku visi ekspertai priėjo konsensuso, kad **būtina didinti kibernetinio saugumo švietimą ir kultūros vystymą**. Taip pat buvo paminėta, kad reikia platesnio verslo ir valdžios bendradarbiavimo, kibernetinės erdvės stebėjimo ir incidentų tyrimą naudojant inovacijas.

Kaip matome ekspertai užsiminė apie inovacijas ir greičiausiai buvo turima omenyje tokias technologijas, kaip dirbtinis intelektas ir mašinų mokymasis, apie kurias kalbėjome teorinėje dalyje, kai aiškinomės kvantinės kompiuterijos panaudojimo galimybes, šios tendencingos technologijos yra neatsiejamos nuo kibernetinių incidentų tyrimų ir užkardimo.

Apklausos metu buvo siekiama išsiaiškinti ekspertų nuomones, kuriose verslo ar valdžios sektoriuose galima būtų pritaikyti kvantinę kompiuteriją.

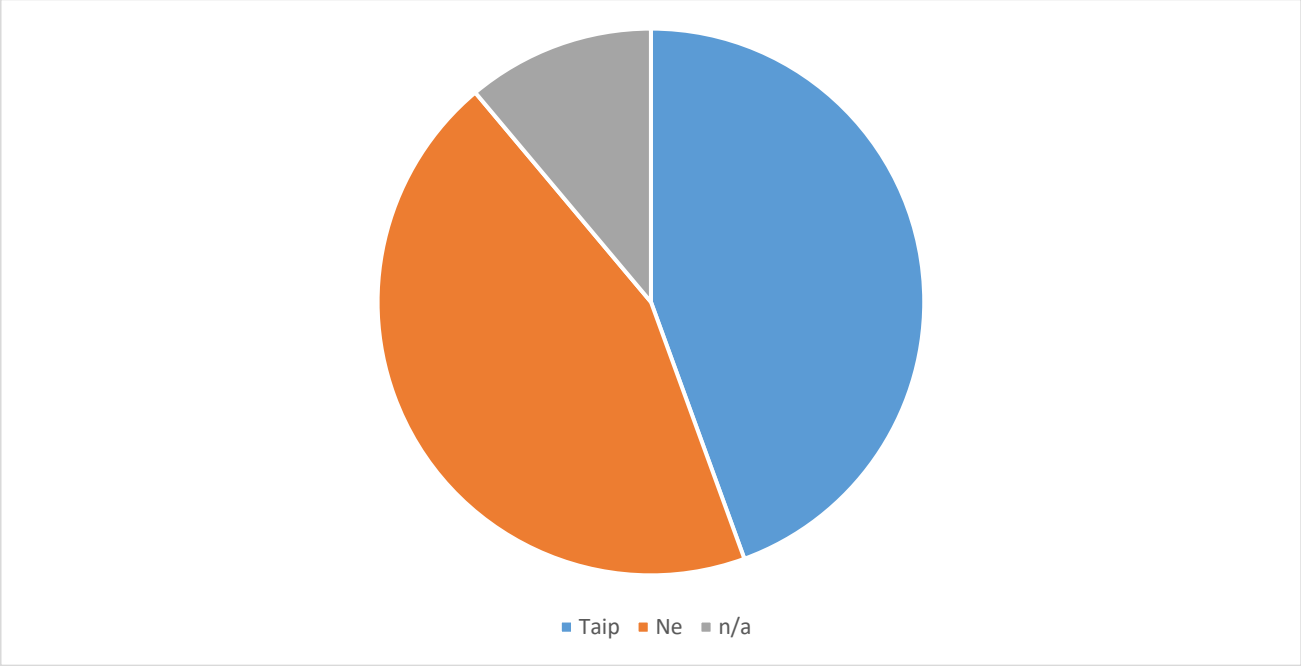
Atstovas iš akademinio pasaulio atsakė, kad jau dabar akademinė bendruomenė naudoja superkompiuterius, todėl tikrai rastų kur pritaikyti ir kvantinius kompiuterius, tuo tarpu verslo atstovai atsakė, kad pirmiausiai reikėtų verslui atlikti kaštų ir naudos analizę, tačiau visi sutartinai pritarė, kad kvantinė kompiuterija daugiausiai naudos atneštų jau teorinėje dalyje aptartoms tokioms verslo sritims, kaip chemijos, biologijos, sveikatos priežiūros, medžiagų mokslo, finansų ir dirbtinio intelekto.

Vienas iš ekspertų pateikė pastebėjimą, kad į „traukinį“ valdžios sektorius greičiausiai įšoktų paskutinis. Su šiuo eksperto pastebėjimu negalima ne sutikti, kadangi kaip jau buvo išsiaiškinta nagrinėjant tiek kvantinės kompiuterijos teoriją, tiek praktiką, Lietuva nėra prisijungusi prie jokių kvantinės kompiuterijos iniciatyvų, taip pat nėra vystomi jokie moksliniai projektai šioje srityje.

Kadangi magistriniame darbe vienas iš nagrinėjamų klausimų yra kvantinės kompiuterijos panaudojimo galimybės Lietuvoje, respondentams buvo užduotas klausimas „*ar Lietuvoje yra įmonių kurios galėtų pradėti teikti kvantinės kompiuterijos (kvantinio programavimo, apsaugos nuo kvantinių grėsmių ir k.t.) paslaugas*“. Deja, didžioji respondentų dalis negalėjo atsakyti į šį klausimą. ESET atstovas atsakė, kad jų įmonei kvantiniai kompiuteriai pagelbėtų greičiau aptikti klientų saugumo pažeidžiamumus, surasti dešifravimo raktus ir nors šiuo metu jų įmonėje kvantiniai kompiuteriai nėra naudojami pasak eksperto tai tik laiko klausimas, kada jie atkeliaus.

Tuo tarpu pasaulinės IT paslaugų įmonės Accenture ekspertas paminėjo, kad Accenture nors ir pati negamina kvantinių kompiuterių ir to nežada daryti, kadangi yra konsultacijų įmonė, tačiau šiai dienai Accenture teikia konsultacines paslaugas susijusias su kvantine kompiuterija, taip pat dirba ir konsultuoja kvantinius kompiuterius gaminančias įmones. Vienas ryškiausių projektų ties kuriuo dirba su partneriu IonQ tai hibridinės kvantinės – debesų technologijos kūrimas. Baltijos valstybėse Accenture veikia jau 20 metų ir nuo praeitų metų pradėjo bendradarbiavimą su Latvijos Universiteto kvantinės kompiuterijos centru. Šiai dienai Accenture Baltijos šalyse įskaitant ir Lietuvą, kur savo tiesioginę veiklą pradėjo tik 2021 metais turi apie 12-os entuziastų komandą dirbančią kvantinės kompiuterijos srityje.

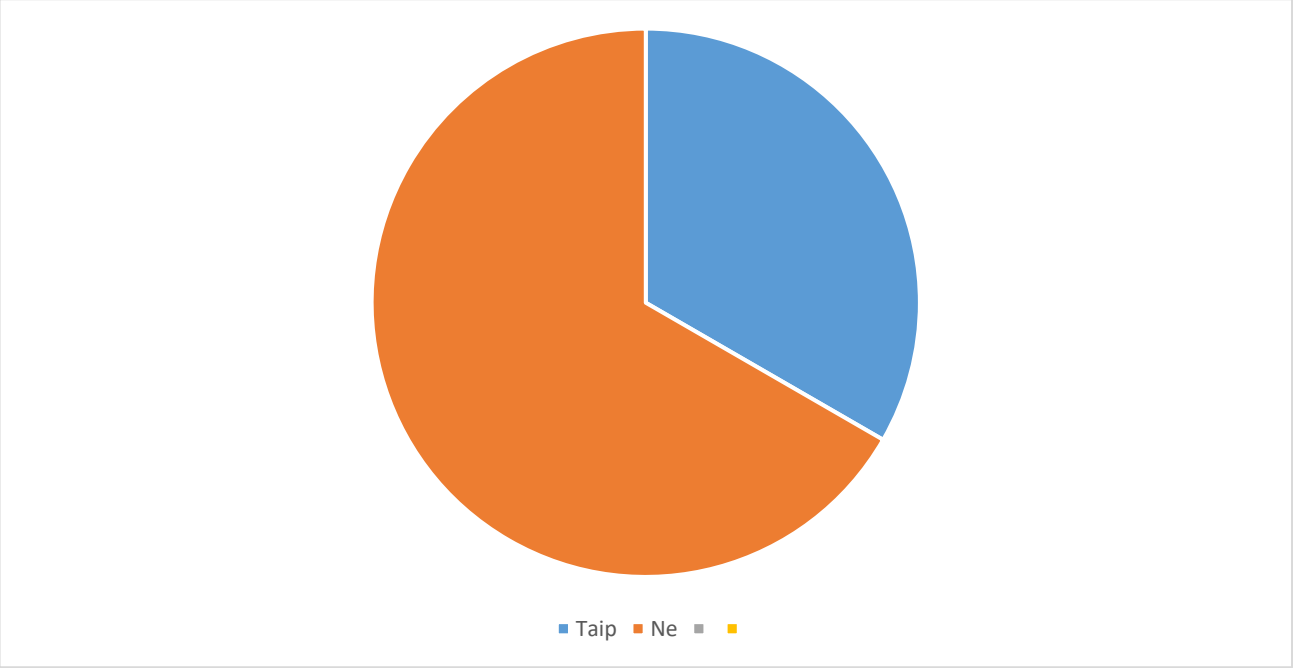
Kaip jau buvo išsiaiškinta teorinėje dalyje pasaulyje yra pastebima, kad vienas iš pagrindinių kvantinės kompiuterijos taikymo iššūkių, tai specialistų trukumas, neabejotina, kad su šiais iššūkiais susidurs ir Lietuvos įmonės kurios pasiriš plėtoti kvantinę kompiuteriją, todėl apklausos metu ekspertų buvo klausiama „*ar sutinka su teiginiu, kad kvantinės kompiuterijos modulis turėtų būti jau dabar pradėtas dėstyti IT studentams aukštosiose mokyklose“*.



19 Pav. Ekspertų nuomonė apie kvantinės kompiuterijos modulio dėstymą aukštosiose mokyklose

Kaip matome iš pateikto atisakymų grafiko (žr. 19 pav.) vienas respondentas šiuo klausimu neturėjo nuomonės, tačiau kiti respondentų atsakymai pasiskirstė maždaug per puse. Tie respondentai kurie atsakė, kad toks modulis galėtų būti dėstomas papildomų argumentų nepateikė, tuo tarpu tie kurie pasisakė neigiamai akcentavo, kad šiuo metu trūksta daug ir programuotojų, ir inžinierių, todėl geriausia būtų galimas išlaidas su papildomu modulių kūrimų investuoti į minėtų IT specialistų rengimą. Ši ekspertų nuomonė atspindi ir pasaulio problemas. Kuomet MIT profesoriaus Ruane interviu metu buvo klausiama, kas yra jo nuomone didžiausia kliūtis kvantinės kompiuterijos vystymui, jis paminėjo būtent talentų trūkumą (Ruane 2022). Taip pat Ruane interviu metu paminėjo, kad MIT kvantinė kompiuterija yra dėstoma skirtingų disciplinų studentams, tokių kaip fizikos, informatikos mokslų ir verslo studentams.

Toliau ekspertų apklausos metu buvo siekiama išsiaiškinti ekspertų nuomonė, ar įmonėms ir organizacijos reikėtų sunerimti dėl kvantinės kompiuterijos keliamų grėsmių.



20 pav. Ekspertų nuomonė apie kvantinės kompiuterijos grėsmes

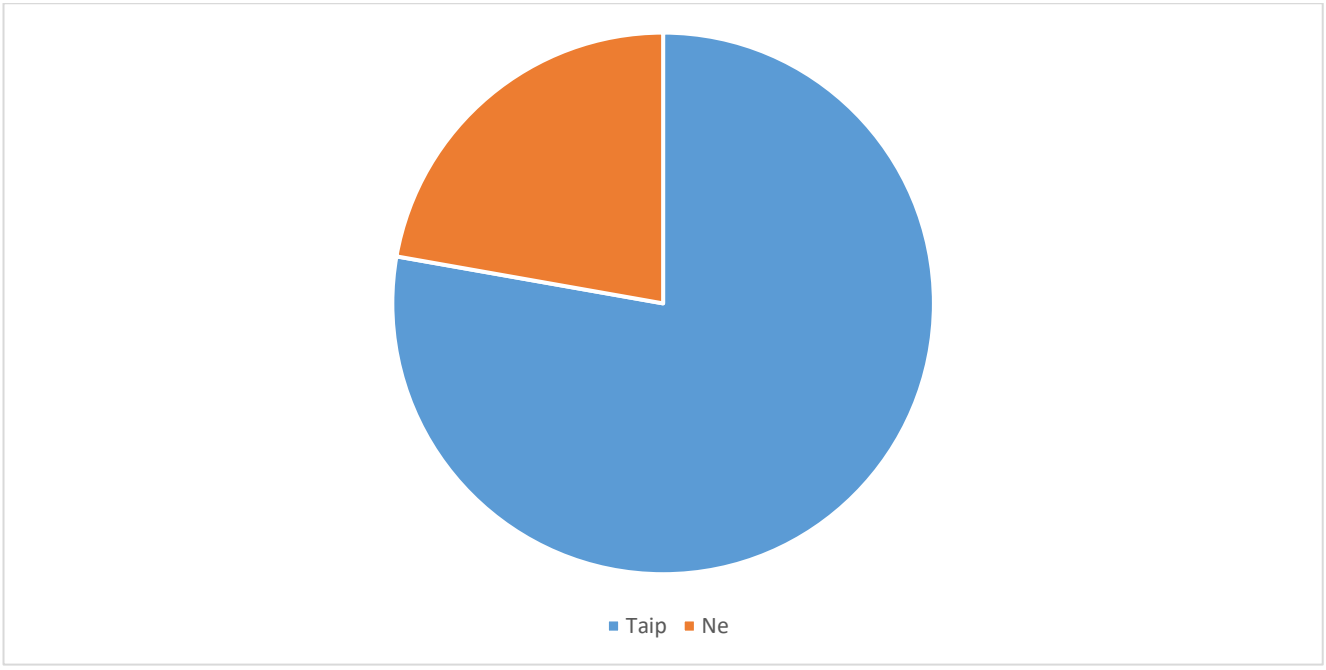
Kaip matome (žr. 20 pav.) didžioji dalis respondentų vis dėl to atsakė, kad ne. O ir tie kurie atsakė, kad taip, patikslino, kad - galbūt taip. Pagrindiniai argumentai tų ekspertų kurie pasisakė, kad ne – nereikėtų nerimauti buvo tokie: „*šiai dienai Lietuvoje susiduriama pagrinde su Phising tipo atakomis, todėl įmonėms ir organizacijoms jie labiausiai rekomenduotų užsiimti darbuotojų švetimu ir apsauga nuo Phising*“. Tačiau vienas iš ekspertų pabrėžė, kad „*atsiradus bent 1000 QBitu kvantiniam kompiuteriui situaciją iš esmės keistų, bet per artimiausius metus to greičiausiai nebus sulaukta*“.

Atsižvelgiant į ekspertų atsakymus galima daryti išvadas, kad Lietuvos ekspertai, taip kaip ir pasaulio vis dar tiksliai negali atsakyti su kokiais iššūkiais bus susiduriama kuomet turėsime pilnai veikiančius kvantinius kompiuterius, nes nors ir kai kurios kvantinių kompiuterių galimybės jau ir yra įgyvendinamos praktiškai, vis dėl to, kad kvantiniai kompiuteriai pradės kelti realias grėsmes dar turės praeiti nemažai laiko.

Siekiant išsiaiškinti kvantinės kompiuterijos panaudojimo galimybes Lietuvoje, respondentų buvo klausiama kokie jų nuomone galėtų būti didžiausi iššūkiai, kuriant, diegiant ir kitaip plėtojant kvantinę kompiuteriją.

Šiuo klausimu vėl gi tarp respondentų buvo pasiektas konsensusas. Visi respondentai vieningai atsakė, kad didžiausias iššūkis būtų specialistų trūkumas, pabrėžiant, kad kvantinė kompiuterija tai ne tik IT, bet kartu ir matematikos ir fizikos mokslas. Taip pat vienas iš ekspertų paminėjo, kad „*kliūtis galėtų būti infrastruktūros trūkumas, tiksliau jos nebuvimas*“.

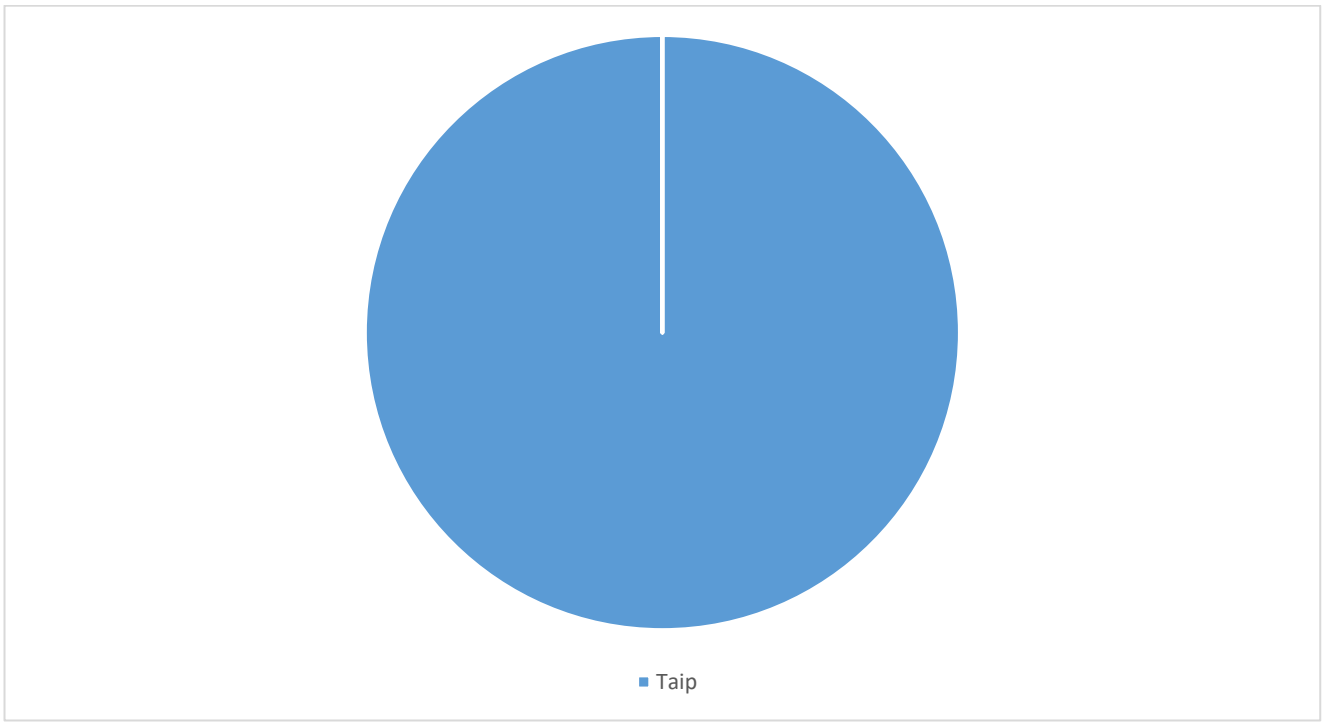
Atsižvelgiant į prieš tai atsakytus klausimus ir į teiginius, kad Lietuva yra viena iš lyderių lazerių (kvantinės mechanikos) ir kibernetinio saugumo lydere pasaulyje ekspertų buvo prašoma atsakyti ar jų nuomone Lietuva turi potencialo tapti ir kvantinės kompiuterijos lydere.



21 Pav. Ekspertų nuomonė apie Lietuvos galimybes tapti kvantinės kompiuterijos lydere.

Kaip matome iš grafiko (žr. 21 pav.) dauguma atsakė, kad taip. Tačiau vėl gi, kai kurie respondentai paminėjo, kad pirmiausiai tam koją kiša talentų trūkumas.

Galiausiai ekspertų paprašyta atsakyti į teiginį: Ar sutinkate su teiginiu, kad kvantinė kompiuterija nors ir keldama grėsmę informacijos konfidencialumui, vis dėl to pasauliui atveria daugiau galimybių ?



22 pav. Ar ekspertai sutinka su teiginiu: "Nors kvantinė kompiuterija ir kelia grėsmes, tačiau vis dėl to pasauliui atveria daugiau galimybių"

Šiuo klausimu visi apklausos dalyviai buvo vieningi ir atsakė – taip (žr. 22 pav.).

Tyrimo išvados:

- Ekspertai tyrimo metu tik patvirtinto teorinėje dalyje nustatytas galimas veiklos sritis kuriose Lietuvoje galima būtų išnaudoti įgyvendinant kvantinės kompiuterijos sprendimus, tai ta pati biotechnologijos, energetika, chemijos pramonė, finansų sektorius, tačiau daugumos nuomone šiai dienai kvantinės kompiuterijos panaudojimo galimybės Lietuvoje yra labai teorinės, pirmiausiai tiek dėl reikiamos infrastruktūros trūkumo, tiek dėl specialistų trūkumo.
- Ekspertų dauguma pasisakė, kad kvantinės kompiuterijos keliamų grėsmių Lietuvoje tikėtis artimiausiu metu neverta, o verčiau susikoncentruoti į esamas didžiausias kibernetinio saugumo grėsmes Lietuvoje, tokias kaip *Phising* ir jų užkardimą.
- Ekspertų dauguma sutaria, kad Lietuvoje kvantinė kompiuterija gali turėti aktualumo ir taip pat turi potencialo tapti kvantinės kompiuterijos lydere pasaulyje, tačiau iš kitos pusės kaip ir likęs pasaulis susiduria su specialistų trūkumu, todėl pasak ekspertų vargu ar artimiausiais metais Lietuvoje turėsime pakankama kiekį IT specialistų galinčių dirbti kvantinės kompiuterijos srityse.
- Ekspertai rekomendavo, kad Lietuvai norint išlaikyti aukštus kibernetinio saugumo reitingus labiausiai reikėtų susikoncentruoti į edukaciją;
- Atsižvelgiant į ekspertų nuomonę, Lietuvos verslas šiai dienai vystyti kvantinę kompiuteriją ar ją naudoti greičiausiai neturi jokio potencialo, o greičiausiai noro ir žinių. Tačiau neatmestina, kai pasaulyje atsiras daug daugiau kvantinių kompiuterių bei specialistų galinčių jais dirbti greičiausiai ir Lietuvos verslas pradės kažkuria linkme judėti link kvantinės kompiuterijos;
- Dauguma ekspertų sutiko su tuo, kad galbūt kvantinę kompiuteriją jau kaip vieną iš modulių reikėtų pradėti dėstyti informatikos ar gimininguų sričių studijų studentams, tačiau buvo ir oponuojančių, sakančių, kad reikėtų daugiau skirti dėmesio bendrajam kibernetinio saugumo edukavimui;
- Pasak ekspertų didžiausi iššūkiai su kuriais galima susidurti plėtojant kvantinę kompiuteriją Lietuvoje, tai reikiamos infrastruktūros ir specialistų trūkumas;
- Ekspertų dauguma sutaria, kad Lietuva turi potencialo tapti kvantinės kompiuterijos lydere pasaulyje, tačiau iš kitos pusės kaip ir likęs pasaulis susiduria su specialistų trūkumu, todėl pasak ekspertų vargu ar artimiausiais metais Lietuvoje turėsime pakankama kiekį IT specialistų galinčių dirbti kvantinės kompiuterijos srityse.
- Visi apklausiami ekspertai sutiko, kad kvantinė kompiuterija nors ir kelia grėsmes kibernetiniam saugumui, tačiau tikėtina pasaulyje suteiks daugiau naudos.

IŠVADOS IR PASIŪLYMAI

1. Kvantinė kompiuterija per ateinančius 10 metų bus greičiausiai auganti ir daugiausiai susidomėjimo sulauksianti aukštųjų technologijų sritis. Tačiau kvantiniai kompiuteriai nepakeis dabartinių namų ar super kompiuterių, o juos tik papildys, kadangi kvantiniai kompiuteriai gali veikti tik tam tikromis laboratorijos lygmens sąlygomis, nes skirtingai nei mums jau puikiai žinomi klasikiniai kompiuteriai veikiantys elektros principais, kvantiniai kompiuteriai veikia kvantinės mechanikos ir kvantinės fizikos paremtais principais, tai yra veikdami mažiausias mums žinomas daleles protonus, atomus ir elektronus. Kvantinė kompiuterija iš kvantinės mechanikos pasiėmė ir pritaikė du esminius principus: superpozicijos ir kvantinio susiejimo.

Super pozicijos principas suteikia neribotas skaičiavimo galimybes, kadangi dėl šio principo visi skaičiavimai yra atliekami vienu metu, tuo tarpu kvantinio susiejimo esmė yra ta, kad visos mažosios dalelytės yra kvantiškai susietos viena su kita, net gi per labai didelius atstumus ir vienos jų būvio negalima pakeisti nepakeitus kito. Pvz. perduodant šifruotą informaciją naudojant kvantinį tinklą sudarytą iš šviesolaidinių kabelių, jeigu kas nors pabandytų tokią informaciją perimti jis pakeistų kitos susietos kvantinės dalelytės būvį, todėl tiek informacijos siuntėjas, tiek gavėjas iš karto tokį bandymą pastebėtų. Teoriškai tarp mokslininkų yra kalbama, kad kvantinis šifravimas yra nenulaužiamas, tačiau vis dėl to, kad pradėti plačiai vystyti kvantinį šifravimą, reikėtų labai didelių investicijų infrastruktūrai, kadangi būtų reikalingas atskiras kvantinis tinklas susidedantis iš specialių šviesolaidžių kabelių, kvantinių tranzistorių, palydovų ir t.t.

Šiai dienai kvantinį tinklą vysto Kinija, kuri jau yra sujungusi savo didžiuosius miestus. Taip pat Europos sąjunga yra numačiusi savo strategijoje vystyti tokį tinklą saugiam informacijos perdavimui, tačiau jis nebus prieinamas plačiai visuomenei, o tik institucijoms saugiai dalintis informacija.

2. Europos sąjungoje dar 2016 metais buvo išleistas Kvantinis manifestas kviečiantis ES nares ir kitas suinteresuotas valstybės bei privatų verslą Europoje prisijungti prie kvantinės iniciatyvos kurti ir vystyti kvantinius kompiuterius, dėl to Europoje atsirado HPCQS kvantinė iniciatyva, o Europos sąjunga jai skyrė 6 mlrd. eurų, kad vystyti kvantinę kompiuteriją ir kvantinį tinklą. Ilgai laukti šios iniciatyvos rezultatų nereikėjo, nes jau šiais metais buvo paskelbta, kad iki 2023 metų pabaigos Europoje turėtume turėti 6 kvantinius kompiuterius, iš kurių vienas atsiras kaimyninėje Lenkijoje. Deja Lietuva dėl nežinomų priežasčių, nėra prisijungusi prie šios iniciatyvos.

Kvantinė kompiuterija taip pat yra vystoma kaimyninėje Latvijoje, kur Latvijos Universiteto mokslininkai, kartu su privataus sektoriaus partneriais kuria programas, gebančias atpažinti pakitimus rentgenogramose pasitelkiant kvantinius kompiuterius.

Deja Lietuvoje susidomėjimas kvantine kompiuterija nėra didelis, tačiau išnagrinėjus galimus panaudojimo atvejus matome, kad Lietuvoje tikrai yra sektorių kuriems būtų aktuali kvantinė kompiuterija: biotechnologijos, finansinės technologijos, logistika, kibernetinis saugumas.

Visgi, net per daug ir nesidomint Lietuvoje kvantine kompiuterija visiems teks su ja susidurti, ypač su kvantinės kompiuterijos keliamomis grėsmėmis ir įgyvendinti post – kvantinės atsparumo priemones, pavyzdžiui pradėti naudoti kvantiniams kompiuteriams atsparius algoritmus reikėtu jau šiandien.

3. Remiantis kokybinio ekspertų nuomonės tyrimo duomenų analize buvo išsiaiškinta, kad kvantinė kompiuterija, nors ir keldama grėsmę vis dėl to pasauliui suteiks daugiau galimybių. Deja ekspertai nebuvo pozityvus, dėl kvantinės kompiuterijos plėtojimo galimybių Lietuvoje, dažniausiai buvo paminėta, kad tam gali pakišti koją specialistų trūkumas, valstybės požiūris bei koncentravimasis į kitus IT sektorius. Tačiau pasak ekspertų, kvantinę kompiuteriją į Lietuvą gali atnešti didžios tarptautinės korporacijos, kaip pavyzdį, vienas iš apklaustų ekspertų pateikė teorinėje dalyje aprašytą Accenture, jau 20 metų veikiančios Latvijoje bendradarbiavimo pavyzdį kvantinėje srityje su Latvijos universitetu.

Pasiūlymai:

- . Pasak Lietuvos skaitmeninių technologijų asociacijos „Infobalt“, vien tik šiandien galima būtų įdarbinti 14000 IT specialistų, tačiau per vienerius metus Lietuvos aukštosios mokyklos paruošia tik apie 4 tūkst. IT srities absolventų, todėl siekiant ne tik toliau sėkmingai plėtoti IT sektorių, bet ir kvantines technologijas Lietuvoje, valstybė turėtų taikyti sekančias priemones:

1. Dar daugiau investuoti į IT specialistų ruošimą;
2. Palengvinti sąlygas asmenų atvykimui iš trečiųjų šalių;
3. Investuoti į dėstytojų ir mokytojų rengimą;
4. Peržiūrėti kai kurias IT krypties programas, pritaikant jas šių dienų rinkos poreikiams;

- Rekomenduojama įmonėms ir organizacijoms jau šiandien susirūpinti kvantinių kompiuterių keliamomis grėsmėmis ir įraukti galimas rizikas į savo rizikų valdymo planus. Pagrindinės priemonės kurias jau šiandien galima būti taikyti:

1. Užtikrinti, kad archyvuojami elektroniniai duomenys yra tinkamai saugomi ir naikinami;
2. Inventorizuoti sistemas kurios naudoja viešojo ir privataus rakto sistemas ir pradėti naudoti kvantiniams kompiuteriams atsparius šifravimo algoritmus, tokius kaip MDB minimus *CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON ir SPHINCS+*.

- Į įvairias valstybes vystymosi ir skaitmenizavimo strategijas įtraukti ir pažangių technologijų (dirbtinis intelektas, kvantiniai kompiuteriai, robotai) vystymo programų gaires;

- Tiek valstybei, tiek privačiam verslui domėtis galimybėmis pritraukti ES, tiek kitų valstybių ar organizacijų finansavimą aukštųjų technologijų vystymui. ES kvantinės kompiuterijos vystymui jau yra skyrusi 8 mlrd. eurų
- Kai kvantiniai kompiuteriai taps prieinami visiems, nepasiruošusiam verslui gali būti per sunku ar net vėlu adaptuotis, todėl rekomenduojama verslui jau dabar ruoštis ir rengti verslo ir IT strategijas atsižvelgiant į tai, kad netolimoje ateityje kvantiniai kompiuteriai bus prieinami plačiai visuomenei:

1. Išsiaiškinti ką kvantiniai kompiuteriai gali ir ar tai pritaikoma jūsų versle;
2. Pasiruošti kvantinės inovacijos planą;
3. Įvertinti kvantinių kompiuterių ir kvantinės programinės įrangos pritaikomumą ir pradėti eksperimentuoti;
4. Investuoti į talentus galėsiančius dirbti su kvantiniais kompiuteriais.

LITERATŪRA

1. Aumasson, J.P. (2018). *Serious Cryptography* No streach press
2. Aaronson, S. (2013). *Quantum Computing Since Democritus.* Cembridge University Press
3. Hoffstein, J., Pipher, J., Silverman, H. J. (2014). *An Introduction to Mathematical Cryptography*. Springer
4. Krishnakumar, A. (2022). *Quantum Computing and Blockchain in Business*, Packt.
5. Agbaje, M. (2019). A review of quantum computing and its architecture. *Caribbean Journal of Science* 53(1), 314-329.
6. Arute, F., Arya, K., & Martinis, M. J. (2019). Quantum supremacy using a programmable superconducting processor. *Nature* 574, 505-510.
7. Ball, H., Biercuk, M., Hush, M. (2021). Quantum firmware and quantum computing stack. *Physics Today* (74), 28p.
8. Bennett, C.H. & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems and Signal Processing* 175, 8.
9. Biamonte, J. Wittek, P. ir k.t. Quntum machine learning *Nature* 549, 195 – 202.
10. Christ P.S & Slowak P.A. Why Blu-ray vs HD-DVD Is Not VHS vs BETAMAX: The Evolution of Standard-Setting Consortia *Universitat Hohenheim: Discussion paper-05* 2009.
11. Curty, M., Azuma, K., & Lo, K.W. (2021) A quantum leap in security *Physics today.* (74) p.36.
12. Crosson, E.J. & Lidar, D.A. (2021). Prospects for quantum enhancement with diabatic quantum annealing. *Nature reviews physics* 3, 466-489.
13. Denning, E. D. (2019). Is quantum computing a cybersecurity threat? *American Scientist*, 107, 83
14. Diffie, W. & Hellman M.E. (1976). New Directions in Cryptography *IEEE Transactions on information theory.* 22, 644 – 654.
15. Kelley, B.K. (2022). Charting the Cource for Quantum Computing *Isaca Journal* (4) p.11-13.
16. Khader, D. & Siddiqi H. (2022). Making and Breaking Data Security With Quantum Machines *Isaca Journal* (4) p.22-26.
17. Lewandowski, H.J., Zwickl, Zwickl, B.M. & Fox, M.F.J. (2020) Preparing for the quantum revolution: What is the role of higher education? *Physical Review Physics Education Research* (16).
18. Liu, J., Shen M.Z., & Jiang H. (2022). Quantum Computing Methods for Supply Chain Managment. *ACM/IEEE Workshop on Quantum Computing.*
19. Madsen, L.S., Laudenbach. F., Falamarzi, M. & others. (2022) Quantum computational advantage with a programmable photonic processor *Nature* 606, 75-81.

20. Menard, A., Ostojic, I., & Volz, D. (2020). A game plan for quantum computing *McKinsey Quarterly* Prieiga per internetą: URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/a-game-plan-for-quantum-computing

21. Mone, G. (2020). The Quantum threat *Communications of the ACM* 63. 12-14.

22. Feyman, R.P. (1982). Symulating physics with computers. *International Journal of Theretical Physics,* 21. 467-488

23. Ruanne, J. (2022). The Business Case for Quantum Computing *MIT Iniatiative on the Digital Economy* Prieiga per internetą: URL: https://ide.mit.edu/insights/the-business-case-for-quantum-computing/

24. Ruane, J., McAfee, A. & Oliver, D.W. (2022). Quantum Computing for Bussiness Leaders. *Harvard Business Review*. 2022 January – February.

25. Shrodinger, E. (1935). Die gegenwartige Situation in der Quantenmechanik *Naturwissenchaften,* 23. 807-812, 823-828, 844-849.

26. Shor, W. P. (1995). Polynormial-Time Algorithms for Prime Factorization and Discrate Logarithms on a Quantum Computer *A preliminary version of this paper appeared in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science,* Santa Fe, NM, Nov. 20–22, 1994, IEEE Computer Society Press, pp. 124–134.

27. Carminati, F. (2019). Quantum Computing: CERN, *IBM collaborate on quantum computing*. Prieiga per internetą: URL: https://www.ibm.com/blogs/research/2019/03/cern-ibm-quantum

28. Dennning, E.D, Is Quantum Computing a Cybersecurity Threat? *American Scientist.* Prieiga per internetą URL: https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat

29. Dilmegani, C. (2021). In-Depth Guide to Quantum Artificial Intelligence *Ai Multiple*.
Prieiga per internetą: URL: https://research.aimultiple.com/quantum-ai/

30. Kee, L. (2021). RSA Is Dead – We Just Haven`t Accepted It Yet. *Forbes.* Prieiga per internetą URL: https://www.forbes.com/sites/forbestechcouncil/2021/05/06/rsa-is-dead---we-just-haventaccepted-ityet/?sh=39281e7e5d22

31. Marchenkova, A. What`s the difference between quantum annealing and universal gate quantum computers? Personal blog. Prieiga per internetą URL:
https://www.amarchenkova.com/posts/quantum-annealing-vs-universal-gate-quantum-computer

32. Martinis, J., & Boixo, S. (2019). Quantum Supremacy Using a Programmable Superconducting Processor. *Google Research*. Prieiga per internetą
URL: https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html

33. Middleton, C. (2021). What`s under the hood of a quantum computer? *Phisics today* (74) p. 64.

34. Mishima, Hiroaki (2018). Non-Abelian strategies in quantum penny flip game. *Progress of Theoretical and Experimental Physics.* Prieiga per internetą:

URL: https://academic.oup.com/ptep/article/2018/1/013A04/4823607

35. Pakin, S., Coles, P. (2019). The Problem with Quantum Computers. *Scientific American* Prieiga per internetą: URL: https://blogs.scientificamerican.com/observations/the-problem-with-quantum-computers/

36. Rammamurthy, V. (2020). Quantum Computing. *GavsTech* Prieiga per internetą: https://www.gavstech.com/quantum-computing-2/

37. Sparleanu, C. (2021). Quantum Computing in banking and finnace – threat of opportunity? *Supertrends* Prieiga per internetą: URL: *https://www.supertrends.com/quantum-computing-in-banking-and-finance-threat-or-opportunity/*

38. Witner, S. (2020). Delta partners with IBM to explore quantum computing – an airline industry first. *Delta News Hub.* Prieiga per internetą: URL: https://news.delta.com/delta-partners-ibm-explore-quantum-computing-airline-industry-first

39. Poznan Supercomputing and Networking Center. Spaudos pranešimas. *One of the first quantum computers produced in Europe to be launched in Poland*.

40. Thankaraj, R. (2021). Quantum Computing with Future Business Model *Medium* Prieiga per internetą: URL https://regupathit.medium.com/quantum-computing-with-future-business-model-3d49f30c7290

41. ETP4HPC (2021). *European High-Performance Computing* Projects Handbook 2021

42. National cyber security index 2022 Prieiga per internerą: UR: https://ncsi.ega.ee/ncsi-index/?order=rank

43. The European High Performance Computing Joint Undertaking (EuroHPC JU) Spaudos pranešimas. *Selection of six sites to host the first European quantum computers*.

44. The Nobel Prize in Phyzics 2022. Press release. (2022) Preiga per internetą: URL: https://www.nobelprize.org/prizes/physics/2022/press-release/

Lavrenovas R. (2022). *Kvantinės kompiuterijos ir kvantinio šifravimo ypatumai ir panaudojimo galimybės Lietuvoje* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Magistro baigiamajame darbe susipažinus su kvantinės kompiuterijos ir kvantinio šifravimo teoriniais aspektais, kvantinio šifravimo ir kvantinės kompiuterijos panaudojimo galimybėmis, atlikus kokybinį tyrimą, buvo išskirtos galimos prioritetinės kvantinės kompiuterijos panaudojimo sritys Lietuvoje bei įvertintos kylančios kvantinės kompiuterijos grėsmės, bei galimas Lietuvos pasiruošimas joms. Pirmoje dalyje nagrinėjami kvantinės kompiuterijos ir kvantinio šifravimo teoriniai aspektai, nagrinėjama kvantinės kompiuterijos grėsmių praktika bei kvantinės kompiuterijos praktika Lietuvoje. Antroje dalyje yra analizuojama Europos sąjungos kvantinė iniciatyva bei kvantinės kompiuterijos taikymo Latvijoje atvejis. Analizuojamos galimos kvantinės kompiuterijos panaudojimo galimybės Lietuvoje. Trečioje dalyje nagrinėjamas atliktas tyrimas, kurio tikslas – pasitelkiant ekspertų žinias, išsiaiškinti kvantinės kompiuterijos ir kvantinio šifravimo panaudojimo galimybes Lietuvoje.

Pagrindiniai žodžiai: kvantinė kompiuterija, kvantinis šifravimas, post-kvantinis šifravimas, kvantinės grėsmės.

Lavrenovas R. (2022). *Features of Quantum Computing and Quantum Cryptography and Possible Use Cases in Lithuania* (Master thesis). Vilnius: Mykolo Romerio universitetas

ANNOTATION

In the master's final thesis after getting acquainted with the theoretical aspects of quantum computing and quantum encryption, the possible use cases for quantum encryption and quantum computing, and after conducting a qualitative study, possible priority sectors where quantum computing in Lithuania can be used were identified, also emerging quantum computing threats were assessed, as well as Lithuanian state preparation for them. In the first part of the thesis, the theoretical aspect of quantum computing and quantum cryptography studied, analyzed quantum computing threats, and current state of quantum computing in Lithuania. In the second part there was conducted analysis of possible use cases for quantum computing and quantum cryptography, European quantum initiative was studied, and the Latvian quantum computing usage case presented. Also, in the second part there was analyzed possible use cases for quantum computing in Lithuania. In the third part conducted research results is analyzed. Research goal was to interview experts and get the opinion about possible use cases of quantum computing and quantum cryptography in Lithuania.

Main keywords: Quantum computing, Quantum cryptography, post-quantum cryptography, quantum threats.

Lavrenovas R. (2022). *Kvantinės kompiuterijos ir kvantinio šifravimo ypatumai ir panaudojimo galimybės Lietuvoje* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

SANTRAUKA

Kvantinės kompiuterijos ir kvantinio šifravimo grėsmių ir panaudojimo galimybių magistro baigiamojo darbo tema yra kaip niekad aktuali pasaulyje. Pasaulyje mokslininkai išskiria labai daug galimų kvantinės kompiuterijos panaudojimo atvejų, taip pat yra paskelbta daug mokslinių tyrimų susijusių su kvantinėmis grėsmėmis ir apsisaugojimo nuo jų praktikomis, tačiau ši tema yra beveik neanalizuota Lietuvoje, dėl to ir buvo iškelta pagrindinė tyrimo problema – mokslo šaltiniuose nepakankamai plačiai išanalizuota ar Lietuvos verslas ir viešasis sektorius pasiruošęs kvantinių kompiuterių panaudojimui ir galimiems su tuo susijusiems iššūkiams? Tyrimo objektas – kvantinės kompiuterijos galimybės ir kvantinio šifravimo grėsmės. Šio tyrimo tikslas yra nustatyti bei apibrėžti kvantinės kompiuterijos ir kvantinio šifravimo panaudojimo galimybes bei kylančias grėsmes pasaulyje ir Lietuvoje, bei pateikti su tuo susijusias rekomendacijas. Taip pat buvo iškelti ir tyrimo uždaviniai: išanalizuoti kvantinės kompiuterijos ir kvantinio šifravimo teorinius aspektus, išnagrinėti kvantinės kompiuterijos ir kvantinio šifravimo praktiką, atlikti kvantinės kompiuterijos panaudojimo ir kvantinės kompiuterijos grėsmių tyrimą. Darbe taikyta mokslinės literatūros analizė siekiant išanalizuoti kvantinės kompiuterijos ir kvantinio šifravimo teorinius aspektus, atlikta Europos sąjungos kvantinės iniciatyvos analizė, taip pat išanalizuotas Latvijos universiteto kvantinės kompiuterijos praktinio pritaikymo pavyzdys. Taip pat darbe atliktas kokybinis ekspertų nuomonės tyrimas, kurio metu buvo apklausti 7 ekspertai. Tyrimu buvo siekiama išsiaiškinti, ekspertų nuomones apie galimas kvantinės kompiuterijos taikymo sritis Lietuvoje, Lietuvos pasiruošimą galimoms kvantinės kompiuterijos keliamoms grėsmėms.

Tyrimo metu buvo iškelta pagrindinė hipotezė: nors kvantinė kompiuterija ir kelia grėsmes, tačiau vis dėl to pasauliui atveria daugiau galimybių. Atlikus ekspertinį vertinimą buvo patvirtinta ši hipotezė, t.y., ekspertai vienbalsiai sutiko, kad nors kvantinė kompiuterija ir kelia grėsmes, vis dėl to pasauliui ji suteiks daugiau galimybių. Ekspertinio tyrimo metu taip pat buvo gauta nuomonė, kad pagrindinės kliūtys, galinčios trukdyti vystyti kvantinę kompiuteriją Lietuvoje yra specialistų trūkumas, taip pat, kad šiai dienai bendras kibernetinio saugumo raštingumas yra didesnis pavojus, nei galimos kvantinės kompiuterijos grėsmės ateityje. .

Magistro baigiamojo darbo pabaigoje pateikiamos išvados bei siūlymai dėl kvantinės kompiuterijos taikymo Lietuvoje, bei pasiruošimo rekomendacijos galimoms grėsmėms.

Lavrenovas R. (2022). *Features of Quantum Computing and Quantum Cryptography and Possible Use Cases in Lithuania* (Master thesis). Vilnius: Mykolo Romerio universitetas

SUMMARY

Quantum computing possible usage cases and quantum computing threats are very trending topics nowadays in the world. Researches all around the world have already identified a lot of possible use cases for quantum computing. Where are a lot of works published about quantum and quantum threats in the world, and how to prepare for them, however this topics wasn't studied or analyzed in Lithuania a lot, this is why we have raised the scientific problem – There is not enough researches done about Lithuanian business and public sector preparation for use of quantum computing and possible quantum threats. The object is – possible use cases of quantum computing and quantum threats. The main aim of this study is to determine and define quantum computing and quantum cryptography possible use cases and raising threats in the world and Lithuania, also provide relevant to topic recommendations. The main tasks of the study are: To analyze quantum computing and quantum cryptography theoretical aspects, to analyze quantum computing usage practices, conduct quantum computing and quantum threats research. The methodology of master thesis: analysis of scientific literature to analyze the theoretical aspects of quantum computing and quantum encryption, the analysis of the quantum initiative of the European Union was carried out, as well as the example of the practical application of quantum computing at the University of Latvia was analyzed. Also, a qualitative study of expert's opinion was conducted in the work, during which 7 experts were interviewed. The aim of the research was to find out the opinions of experts about the possible application areas of quantum computing in Lithuania and Lithuania's preparation for possible threats posed by quantum computing.

During the research, the main hypothesis was put forward: although quantum computing poses threats, it opens more opportunities for the world. The expert evaluation confirmed this hypothesis, i.e., the experts by consensus agreed that although quantum computing poses threats, it will give the world more opportunities. During the expert interview, the opinion was also received that the main obstacles that can hinder the development of quantum computing in Lithuania are the lack of specialists, as well as that today the general cyber security literacy is a greater danger than the possible threats of quantum computing in the future.

At the end of the master's thesis, conclusions and suggestions are presented regarding the application of quantum computing in Lithuania, as well as recommendations for preparation for possible threats.

PRIEDAI

1 Priedas. Tyrime panaudota anketa

Laba diena, gerbiamas (-oji) eksperte,

Aš Robertas Lavrenovas, Mykolo Romerio universiteto Kibernetinio saugumo valdymo magistrantūros studijų studentas, atlieku “Kvantinės kompiuterijos ir kvantinio šifravimo ypatumų ir panaudojimo galimybių Lietuvoje” tyrimą.

Kadangi kvantinė kompiuterija yra sąlyginai nauja, tačiau sparčiai besivystanti informatikos/fizikos mokslo sritis, pasaulyje vis dažniau yra kalbama apie kvantinės kompiuterijos suteikiamas galimybes - pavyzdžiui panaudojimą naujų vaistų atradimams. Tačiau šalia taip pat yra akcentuojamos kvantinės kompiuterijos keliamos grėsmės, pavyzdžiui visų mums žinomų šiuolaikinių šifravimo algoritmų neatsparumą kvantiniams kompiuteriams.

Taip pat pasaulyje jau dabar vyksta savotiškos “kvantinės lenktynės”. Kvantinius kompiuterius yra sukūrusios tokios valstybės, kaip Kinija, Vokietija, JAV, Kanada. O patys kompiuteriai ne tai, kad kiekvienais metais, bet net mėnesiais tampa vis galingesni. Pavyzdžiui, kinų startuolis SpinQ rinkai siūlo stalinius kvantinius kompiuterius už 5000 eurų[1].

Kadangi magistro baigiamajame darbe jau spėjome išsiaiškinti, kad kvantinė kompiuterija yra beveik nenagrinėta tema Lietuvoje, todėl šiuo tyrimu siekiame pasitelkiant ekspertų žinias išsiaiškinti, kvantinės kompiuterijos ir kvantinio šifravimo panaudojimo galimybes Lietuvoje ir jos keliamas grėsmes.

Tyrimo metu surinkta informacija bus naudojama tik magistro baigiamajame darbe, apibendrinta forma. Anketoje pateikti duomenys viešai skelbiami nebus. Prašome jūsų atsakyti į toliau pateiktus anketos klausimus.

1. Trumpai pristatykite, kokio sektoriaus (verslo, valdžios, akademinio ar k.t.) atstovas esate ir kelių metų jūsų patirtis yra šiame sektoriuje.

_____

_____

[1] https://futurism.com/the-byte/quantum-desktop-computer-5000

_____
_____
_____

2. Jūsų nuomone ar kvantinė kompiuterija jau šiandien turėtų būti aktuali tema Lietuvoje ir kodėl?

_____
_____
_____
_____
_____

3. Kokios būtų jūsų rekomendacijos, kad Lietuva išlaikytų aukštas kibernetinio saugumo pozicijas?

_____
_____
_____
_____
_____

4. Kaip manote kuriose verslo ar valdžios sektoriuose Lietuvoje galima būtų pritaikyti kvantinę kompiuteriją?

_____
_____
_____
_____
_____

5. Kaip manote ar Lietuvoje yra IT įmonių kurios galėtų pradėti teikti paslaugas susijusias su kvantine kompiuterija, pavyzdžiui, programuoti kvantinius kompiuterius, teikti kibernetinės apsaugos nuo kvantinių grėsmių paslaugas? Jeigu taip prašytume įvardinti ir galimas įmones (gali būti ir Lietuvoje veikiančios užsienio kapitalo)?

_____
_____
_____

6. Lietuvoje, kaip ir visame pasaulyje yra didelis iššūkis su IT specialistų trūkumu. Šiuo metu, kiek teko išsiaiškinti, kvantinės kompiuterijos modulis nėra dėstomas jokioje Lietuvos aukštojoje mokykloje. Kaip manote ar šis modulis turėtų būti dėstomas informatikos ir/ar su ją susijusių krypčių studijų programų studentams? Trumpai pakomentuokite.

7. Ar įmonėms ir organizacijoms reikėtų jau šiandien sunerimti dėl kvantinės kompiuterijos keliamų grėsmių, kalbame apie tai, kad kvantiniai kompiuteriai bus tokie galingi, kad galės "nulaužti" bet kokius šiuolaikinius šifravimo algoritmus pvz. RSA ?.

8. Kokius didžiausius iššūkius galimai galima įžvelgti Lietuvoje kuriant, diegiant, ir kitaip plėtojant kvantinę kompiuteriją?

9. Lietuva jau seniai yra įvardijama, kaip kvantinės fizikos (jeigu kalbame apie lazerius) viena iš lyderių pasaulyje[2]. Taip pat vertinant pagal skirtingus kibernetinio saugumo indeksus esame

[2] https://www.lrytas.lt/lietuvosdiena/svietimas/2021/06/23/news/lietuva-lydere-lazeriu-srityje-salyje-sukurti-lazeriai-keicia-zmonijos-gyvenima-19849463

pasauliniai lyderiai ir kibernetiniame saugumo srityje[3]. Kaip manote, ar Lietuva turi potencialo tapti ir kvantinės kompiuterijos lydere pasaulyje bei išlaikyti savo kibernetinio saugumo aukštus indeksavimo rezultatus įvertinus prieš tai užduotus klausimus ir jūsų atsakymus į juos?

_____

_____

_____

_____

_____

10. Ar sutinkate su teiginiu, kad kvantinė kompiuterija nors ir keldama grėsmę informacijos konfidencialumui, vis dėl to pasauliui atveria daugiau galimybių ?

a) taip

b) ne

Ačiū už atsakymus.

[3] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/