Essee on valminud Arenguseire Keskuse tellimusel kogumikus “Pikksilm” avaldamiseks.

Kolmas kvantrevolutsioon: kvantarvutite tulekuga kaasnevad probleemid ja võimalused

Võib väita, et praegu on maailmas käimas kolmas kvantrevolutsioon ehk kvantarvutite reaalne kasutuselevõtt. Maailma suurriigid on algatanud hiigelprogrammid ja juhtivad tehnoloogiafirmad raporteerivad lausa igakuiselt uutest rekordtulemustest tehnoloogiliste takistuste ületamise teel. Kõigele lisaks muudab IT-valdkonna arengu topeltmurranguliseks see, et paralleelselt on toimumas plahvatuslik hüpe tehisintellekti vallas. Kui need kaks revolutsiooni liituvad, on oodata ühiskonda ja majandust ümberkorraldavaid suuri muutusi. Seejuures ei ole välistatud tehnoloogilise raskuskeskme nihkumine Aasia riikidesse, kes panustavad praegu tohutult nii tehisintellekti kui ka kvanttehnoloogiate arendamisse. Kui tõdeda, et Eesti panus tehnoloogiateadustesse ja tehnoloogiaõppesse on võtnud kursi langusele, võib täheldada märgatavaid ohumärke.

Kvanttehnoloogiate liigitusest

Teemast aitab paremini aru saada kvanttehnoloogiate üldine klassifitseerimine:

- **kvantmetroloogia –** kogu teaduse, tehnika ja majanduse üha täpsemad standardid;
- **kvantsensoorika –** parim näide on MRI-tomograafia kasutamine meditsiinis;
- **kvantkrüptograafia –** pealtkuulamiskindlad optilised sideliinid;
- **kvantsimulaatorid –** spetsialiseeritud kvantarvutid teatud (optimiseerimis)ülesannete lahendamiseks;
- **universaalsed kvantarvutid –** eelmiste laiendus; on võimelised kõikide praeguste tavaarvutite arvutusvõimsust ületama ja piisavalt suure kvantbittide arvu korral tänapäevaseid üldkasutatavaid krüptoalgoritme murdma.

Ülikeerukad ülesanded – pigem reegel kui erand

Lugejal võib pähe tulla küsimus, kust tekivad suure keerukusastmega ülesanded ning miks tänapäevased ülikiired ja paljutuumalised arvutiprotsessorid siin raskustesse satuvad. Vaatame näiteks optimiseerimisülesannet, kus meil on vaja läbi arvutada 10 väärtust 16 muutuja jaoks, seega kokku 10^{16} kombinatsiooni. See number võrdub ligikaudu 2^{53}. Kui tavaarvuti teeks ühe arvutuse 1 mikrosekundiga, kuluks kõikide kombinatsioonide läbiarvutamiseks ligikaudu 3000 aastat. Google'i poolt 23. oktoobril 2019 avalikustatud 53-kvantbitine kvantarvuti on võimeline oma protsessoris korraga võrdlema kõiki (2^{53}) vastusevariante. Kvantarvuti ei anna tulemust ühe käivitusega, vaid vajab tulemuse statistiliseks väljatoomiseks palju korduskatseid. Kui eeldada, et lahenduse nägemiseks on vaja teha miljon katset ja et üks katse võtab aega 100 mikrosekundit, oleks optimiseerimise tulemus ikkagi kõigest 100 sekundiga käes.

Ülesannete dimensiooni kasvades (näiteks ravimitööstuses uute ravimite molekulide disain) suureneb kvantarvutite eelis tavaarvutite ees väga kiiresti.

Paradokse täis kvantteooriate keerukusest

Kvantnähtused sisaldavad palju paradokse, milles orienteerumine nõuab pikaajalist tutvumist nii protsesside füüsikalise kui ka matemaatilise poolega.

Suur metodoloogiline paradoks on see, et kuigi arvutusreeglid töötavad ja annavad häid tulemusi, on siiamaani kokku leppimata tõlgendusküsimused, näiteks kuhu jääb kvantobjekti iseloomustav tõenäosuslaine pärast mõõtmisprotseduuri (kontakti välismaailmaga), millega valitakse tõenäosuslikult välja üks võimalik baasolek[1].

Igasuguste analüüside ja arenduste jaoks on täpselt kvanditud baasolekutest tihti palju olulisem erinevate olekute vahel ning ruumis ja ajas “laiali määrdunud” tõenäosuslaine (olekufunktsioon). Selle kvantarvuti protsessoris manipuleeritava n-osakese läbipõimunud komplekslaine “mõõtmisega” iga katse lõpus peavad kvantbitid tõenäosuslikult valima baasoleku “0” või “1”.

Kõige paradoksaalsem on siiski mitteklooni tavuse teoreem, teisiti väljendudes vahevaatluse keeld või infotehnoloogia keeles COPY-protseduuri võimatus. Kui mingi kvantobjekt või -objektide süsteem on paljude võimalustega superpositsioonilises olekus, ei tohi me proovida hankida informatsiooni selle vaheoleku kohta – vastasel korral superpositsiooniline olek kaob. COPY- protseduuri võimatus annab võimaluse füüsikaliselt krüpteeritud sideliinide loomiseks, teiselt poolt tekib aga väga suur takistus kvantarvuti arendamisel.

Esimene kvantrevolutsioon

Alates Max Plancki energiakvantide hüpoteesist 1900. a kuni John von Neumanni raamatuni („Mathematische Grundlagen der Quantenmechanik“) 1932. a. Formuleeriti teoreetilised põhiprintsiibid ja „mõõtmise“ teooria (protseduur valib tõenäosuslikult ühe baasoleku).

Teine kvantrevolutsioon

1980-ndad kuni 21. saj algus. Selle tunnuseks võiks pidada üksikute kvantobjektide manipuleerimise võimekust, kvantpõimunud objektide kaugmõju tõestamist, suurte molekulide lainelise oleku katseid, footonite teleportatsioone, samuti kvantarvutite ja ka kvantkrüpteeritud sideliinide ideed ning esimesi katsetusi.

Universaalse kvantarvuti põhimõtted, mis oma n-kvantbitises registris

suudaks korraga võrrelda 2^n lahendusvarianti, formuleeris 1985. aastal Inglise teadlane David Deutsch. Tavaarvuti peab kõiki neid lahendusvariante hindama ükshaaval, ning piisavalt suure n korral ulatub arvutusaeg miljarditesse aastatesse isegi ülisuurte serveriparkide jaoks.

Pärast Deutschi põhimõtete täpset sõnastamist oli võimalik alustada formaliseeritud matemaatilise kvantinformaatika arendamisega. Kõige olulisem tähis sellel suunal on ameeriklase Peter Shori 1994. a avastatud algoritm, mis võimaldab piisavalt suure kvantarvuti abil kiiresti murda praeguse krüptotehnoloogia aluseks olevad põhialgoritmid (RSA ja elliptkõveratel põhinevad[2]).

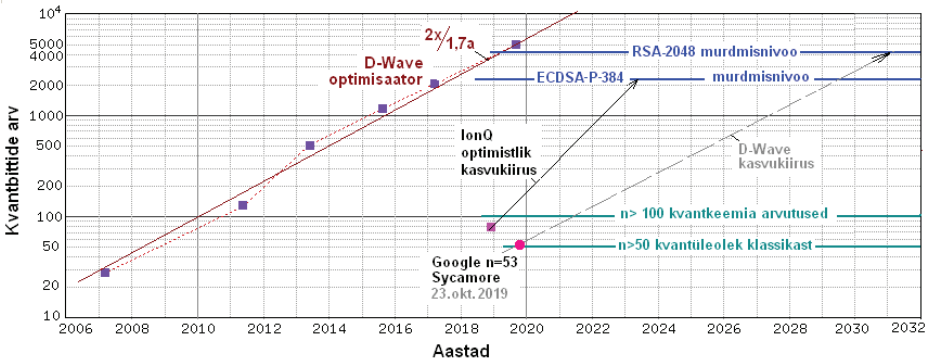
Kolmas kvantrevolutsioon ja kvantarvutite tulek

Kolmas kvantrevolutsioon on siinkohal välja pakutud termin iseloomustamaks viimase tosina aasta jooksul toimunud tormilisi arenguid kvantsimulaatorite ja kvantarvutite alal.

Otsustav läbimurre saabus 2007. aastal, kui Kanada firma D-Wave andis teada 28-kvantbitise optimiseerimisülesannetele spetsialiseeritud kvantarvuti (*quantum annealer*) loomisest. Seda võikski lugeda kolmanda kvantrevolutsiooni alguseks. D-Wave tõi sisse kaks läbimurdelist uuendust:

1. Makroskoopiliste mõõtmetega (0,2 mm) kvantbitid ülijuhtivate vooluringide baasil ülimadalatel temperatuuridel (0,015 K).
2. Kvantbittide arvu kasvatamise töötav tehnoloogia ja D-Wave'i kvantoptimisaatorite muljetavaldav eksponentsiaalne areng, mis on esitatud Joonisel 1. Kasvukiirus on olnud 12 aasta jooksul sarnane pooljuhtkiipide Moore'i seadusega.

Joonis 1. Kvantarvutite tehnoloogia eksponentsiaalne areng ja prognoosid. Näidatud on praegu üldkehtiva krüptoalgoritmi RSA-2048 ja Eesti ID-kaartide krüptoalgoritmi ECDSA-P-384 dekodeerimiseks vajalik kvantbittide arv.



Kuigi D-Wave'i kvantoptimisaatorid ei oma universaalse kvantarvuti kõiki omadusi, ostsid need endale paljud olulised USA firmad ja uurimisasutused, näiteks Lockheed Martin, NASA, Google ja Los Alamos National Lab. Viimane omandas ka tuliuue, 2019. a septembris välja lastud 5000-kvantbitise D-Wave'i uusversiooni. See, et tehnoloogiagigant Google ostis 2013. aastal 512-kvantbitise kvantoptimisaatori ja teatas nüüd, 23.10.2019 sarnase tehnoloogiaga universaalse 53-kvantbitise arvuti loomisest, lubab järgmistel aastatel oodata isegi kiiremat kasvu, kui on prognoositud Joonisel 1. Kohe pärast Google'it teatas sama suure, 53-kvantbitise arvuti käikulaskmisest ja lisaks avalikku kasutusse andmisest ka IBM.

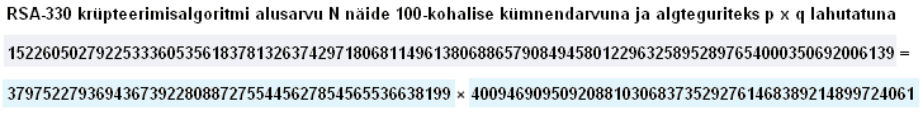
Firma IonQ, kes vastupidiselt teistele (Google, IBM, Intel ja Rigetti) on valinud ioonlõksude (*Trapped Ions*) tehnoloogia, väidab end olevat välja töötanud madala vigade nivooga kergesti laiendatava ning vähem jahutust vajava tehnoloogia ning on lubanud kvantbittide arvu kahekordistumist igal järgmisel aastal (optimistlik kasvustsenaarium Joonisel 1).

Seda, et just praegu on käimas revolutsiooniline areng, kinnitab maailma suurvõimude panus sellesse. Oktoobris 2018 alustas tööd EL-i *Quantum Flagship* koondprogramm mahuga 1 miljard eurot. 21. detsembril 2018 kirjutas USA president alla Rahvusliku Kvantinitsiatiivi seadusele; programmi maht on 1,2 miljardit USA dollarit. Hiina on alates 2017. aastast finantseerimas 10 miljardit USA dollarit kvanttehnoloogiate keskussse, eesmärgiga saada enda kätte lisaks maailma pikima kvantkrüpteeritud sidekanali rekordile (1203 km) ka kvantarvuti realiseerimise rekord ja tehnoloogialiidri positsioon.

Universaalne kvantarvuti kui praeguse e-krüptograafia ohustaja

Juba kvantarvutite matemaatiliste teooriate arendamise alguses 1994. aastal esitas Peter Shor algoritmi, millega on võimalik üldkasutatava RSA (Rivest-Shamir-Adleman, 1977) krüptomeetodi dekrüptimine, kui kvantarvuti registri kvantbittide arv ületab 2n+1, kus n on RSA võtmepikkus bittides. RSA puhul seisneb dekrüptimise kaitse pika avaliku võtme algtegurite leidmise töömahukuses. Joonisel 2 on toodud illustreeriv näide kuus korda lühema võtme kohta.

Joonis 2. Üldkasutatava RSA krüptoalgoritmi selgitus. Dekrüptimise kaitse põhineb pika täisarvu algteguriteks lahutamise töömahukusel. Näide on esitatud üle kuue korra lühendatud juhtumi kohta, võrreldes praegu üldkasutatava RSA-2048 algoritmiga.



Teine, samuti Shori algoritmiga murtav üldkasutatav krüptoalgoritmide klass on "elliptkõveratel ja digitaalsel logaritmil" põhinevad krüptometoodikad[2], näiteks ECDSA. Tavaarvutite vastu vajab ECDSA sama kaitse kindlustamiseks umbes kaheksa korda lühemat võtit RSA-ga võrreldes, aga dekrüptimisvõimelise kvantarvuti registripikkuse kriteerium on 6n. Pärast RSA-2048 tehnoloogilise vea avastamist on Eesti ID-kaardi puhul kasutusel krüptoalgoritm ECDSA-P-384.

Kokkuvõttes on olukord selline, et mõlema krüptoalgoritmi murdmise vastu universaalse kvantarvuti poolt kaitseb ainult vajalike kvantbittide suur arv, mis on vastavalt 4097 ja 2304 (vt Joonis 1). Teiseks kaitseb selle eest ka reaalsete kvantbitt-operatsioonide märgatav vigade protsent, mis aga väheneb pidevalt ja on juba lähenemas 0,1%-le. Viimase viie aastaga on vigade protsent vähenenud ligikaudu kümme korda; see tendents näitab tehnoloogia küpsust. Joonisel 1 esitatud prognooside järgi võivad universaalsed kvantarvutid hakata praegust krüptometoodikat ohustama nelja kuni üheteistkümne aasta pärast.

Kvantarvutikindlad krüptoalgoritmid

Kuna on olemas võimalus, et RSA ja ECDSA tüüpi üldkasutatavad krüptoalgoritmid võivad järgmise 5–10 aasta jooksul kvantarvutitest ohustatud saada, on hakatud tõsisemalt uurima ka kvantkindlate krüptoalgoritmide kasutuselevõtu võimalusi. Põhimõtteliselt on siin palju valikuid. USA Rahvuslik Standardite Instituut NIST algatas 2017. a lõpus konkursi, kus sõelale jäi tervelt 60 ettepanekut[2]. Uute metoodikate probleem on see, et nende standardimine ja kasutuselevõtt võib võtta vähemalt viis aastat.

Teine, võib-olla isegi suurem probleem on see, et kvantarvutid suudavad avada juurdepääsu varem välja antud salajastele dokumentidele. Olukorda komplitseerib asjaolu, et dokumendid võivad olla laialdaselt kopeeritud.

Kokkuvõte ja soovitused

- Infotehnoloogiate valdkonnas on praegu käimas väga suured muutused kogu maailmas. Varem välja kuulutatud küberfüüsikaliste süsteemide (Tööstus 4.0) prioriteedile ning tekkinud tehisintellektibuumile on nüüd lisandunud suurriikide ja juhtivate tehnoloogiafirmade võidujooks kvanttehnoloogiate vallas.
- Kuna kahe viimase aasta jooksul on kogu maailmas kvanttehnoloogia programmidesse investeeritud miljardeid ja kvantarvuti on suurriikidele prestiiži küsimus, pole võimalust, et tulemusi ei saavutata. Võib püstitada prognoosi, et D-Wave'i kvantoptimisaatorite eksponentsiaalse kasvu järel näeme me praegu 10-aastase nihkega universaalsete kvantarvutite eksponentsiaalse kasvu algust.
- 2019. a sügis oli üks murdepunkte, kui Google teatas, et saavutatud on kvantarvutite ülemvõimu esimene tinglik piir (50 kvantbitti). Kohe teatas sama ka IBM ja pakkus oma arvutit avalikku kasutusse. Ilmselt on kohe tulemas kahe võtmetehnoloogia sümbioos ja järgmine arenguhüpe (tehisintellekt kvantarvutitel). Eesti ettevõtlus ja kõrgharidus ei ole selleks valmis.
- On raske prognoosida, millal murravad universaalsed kvantarvutid praeguse krüptotehnoloogia, aga ei ole välistatud, et see toimub juba 5–10 aasta jooksul. Igal juhul peab maailm kohe alustama uute krüptotehnoloogia standardite väljavalimise ja kehtestamisega. Selles mõttes on murdmine juba toimunud. Eestil on siin mõningane valmidus olemas[2].
- Eesti kõrgkoolides on kvanttehnoloogiate oskusteabe olukord ebarahuldav. Kui näiteks tehisintellekt on seotud olemasoleva infotehnoloogiaga ja ka ettevõtted oskavad nõudmisi esitada, on kvanttehnoloogiad palju spetsiifilisem uus ala. Siin on kiiresti tarvis täiendavaid stimuleerivaid programme mitte niivõrd tippteaduses, kuivõrd just uusi tehnoloogiaid tutvustavates õppeainetes ja projektides, näiteks HITSA sihtasutuse suunalt.
- Tehnoloogiaga tegelevad Eesti kõrgkoolid ei vaja kitsast spetsiifiliste küsimustega ametis olevat tippteadust, vaid kõrgkooliõppega seotud vahendavat teadust, mis suudab jälgida maailma erinevaid arengusuundi. Seda eriti ajal, mil maailmas ja Euroopas on käivitatud *Quantum Flagship* tüüpi läbimurdelised programmid, mis muudavad tehnoloogia arengut.

Andres Udal
TTÜ tarkvarateaduse instituudi vanemteadur

Kasutatud allikad

[1] Wikipedia koduleht “Interpretations of quantum mechanics” (Kvantmehaanika interpretatsioonid) https://en.wikipedia.org/wiki/Interpretations_of_quantum_mechanics.

[2] A. Pankova, J. Willemson, A. Buldas (2018). Postkvant-krüptograafia ülevaade. Tehniline dokument. Riigi Infosüsteemide Amet ja AS Cybernetica. 22 lk. https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/postkvant-kruptograafia-ulevaade-2018.pdf