TEADLASE PILGUGA

Krüptograafia, mis paneb vastu ka kvantarvutile

Dan Bogdanov

Tänapäevased arvutusseadmed, meie nutitelefonid ja arvutid töötavad ränist tehtud kiipidel. Me tunneme neid hästi – näiteks on ränikiipidega tehtud kõik viimase aja läbimurded tehisintellekti alal. Insenerid on aga näinud ränist kiipide piire ning siht on seatud fotoonika ja kvantmehaanika suunas – ikka lootusega lahendada arvutiga veelgi keerulisemaid ülesandeid. Kõige ulmelisema maine on saanud kvantarvutid, millele omistatakse võimet lahendada keerukaid mõistatusi, proovides läbi paljud (või isegi kõik) lahendused ühekorraga. On tõde, et kvantarvutite programmeerimine vajab uut moodi mõtlemist ja teadlased tegelevad sellega nii Eestis kui ka välismaal.

Tänaseks on teada üks ülesanne, mille lahendamisel oleks piisavalt suurel kvantarvutil selge eelis ränikiipidel arvutite ees. Selleks on ühe arvu algarvuliste tegurite leidmine ehk tegurdamine. Kui keegi suudaks seda täna teha piisavalt suurte, üle 600 kümnendkohaga täisarvude jaoks, oleks ta võimeline murdma Eestis ja maailmas kasutatavaid krüptograafilisi algoritme (nagu näiteks RSA), saaks kuulata pealt salajast suhtlust ning võltsida digitaalseid allkirju. Tänaseks on ränikiipidega suudetud tegurdada kuni 250-kohalisi arve ja 600-kohaliste tegurdamist ei peeta inimkonna eluea jooksul ega meie planeedi eluea jooksul realistlikuks.

1994. aastal töötas Ameerika matemaatik Peter Shor välja algoritmi, mille abil saaks piisavalt suure kvantarvutiga tegurdada palju kiiremini kui tänaste arvutitega. Täna meil sellist kvantarvutit ei ole ja teadlaste konsensus on, et selle ehitamiseks kulub vähemalt 20 aastat. Siiski on teadlased hakanud uurima, millise krüptograafiaga kaitsta saladusi, mis peavad püsima varjatuna näiteks 25 aastat. Vastav teadusvaldkond on postkvant-krüptograafia.

Postkvant-krüptograafia toetub sellistele keerulistele matemaatilistele ülesannetele, mille lahendamiseks kvantarvutiga efektiivseid viise teada ei ole. Selliseid matemaatiliselt keerukaid ülesandeid on õnneks leitud ning loodud on esimesed efektiivsed postkvant-krüptograafilised digitaalse allkirjastamise ja turvalise side lahendused. Veelgi enam – mitmed neist on läbinud aastatepikkuse uurimise ja teadlaskonna kriitika ning jõudnud Ameerika Ühendriikide ja Euroopa Liidu standarditesse ja soovitustesse.

Iga tehnoloogiline uuendus töötab ainult siis, kui me seda ka rakendame. Seega peavad postkvant-krüptograafia jõudumööda kasutusele võtma ettevõtted, riigiasutused ning ka kõik meie erakätes olevad seadmed. Õnneks saab seda teha tarkvarauuendusega ja selleks ei pea uusi arvuteid välja mõtlema või ostma. Suured side- ja tehnoloogiaettevõtted, nagu Cloudflare ja Google, on enda võrkudes postkvant-krüptograafia ka kasutusele võtnud.

Eesti e-riik on maailmas hästi tuntud ja meie inimeste jaoks on e-teenused igapäevase elu osa. Seega peab ka Eesti oma postkvant-krüptograafiale

TEADLASE PILGUGA

ülemineku plaani valmis tegema. Selleks on samme juba tehtud – riigi infosüsteemi amet on tellinud ja avaldanud vastavaid uuringuid. Eesti teadlased on juba uurimas, millised peaksid olema postkvant-krüptograafilised X-tee, Smart-ID ja internetivalimised.

Kõike seda ei pea Eesti muidugi tegema üksi, sest samasuguses seisus on ka teised riigid, kus e-teenuseid kasutatakse. Näiteks toimub 13. mail Tallinnas teaduste akadeemias rahvusvaheline tulevikukrüptograafia konverents, mis keskendub just postkvant-krüptograafiale. Konverentsi korraldab akadeemia koostöös riigi infosüsteemi ameti, Cybernetica ASi ja Eesti-Tšehhi teadusprojektiga CHESS (Cyber-Security Excellence Hub In Estonia And South Moravia). Esinema tulevad Eesti ja Tšehhi teadlased, kes räägivad oma tööst kvantarvutikindlate IT-süsteemide ehitamise alal. Postkvant-krüptograafia suunas liikumisest tulevad rääkima ka Eesti ja Tšehhi riigiasutuste esindajad.

Teadmiste vahetamise tulemusena saavad Eesti ettevõtted, riik ja rahvusvahelised külalised teha julgemaid ühiseid plaane. Teadlaste eesmärk ongi, et kõigil osapooltel ei peaks olema palgal omaenda postkvant-krüptograafid. Piisab sellest, kui osata hinnata kirjanduses, internetikeskkondades ja meedias liikuva info tõepära.

Tuleb nentida, et kvantarvutite ehitajad on oma pressiteadetes jätnud mulje, nagu oleks taevas juba kukkumas ja kvantarvutid juba kõikvõimsad. Siiski, teadaoleva kontrollitud rekordi järgi on Peter Shori algoritmi käivitav kvantarvuti suutnud tegurdada arvu 21 teguriteks 3 ja 7. Ka koolilapsed suudavad paremini. Ometi, nagu mäletame arvutustehnika arengust, võivad suured hüpped tulla kiiresti ja üldsuse jaoks ka ootamatult. Seepärast ongi täna õige aeg postkvant-tuleviku jaoks plaane teha.

Ilmunud ajalehes Postimees 4. mail 2024