Tellija

RIIGI INFOSÜSTEEMI AMET

Postkvant-krüptograafia ülevaade

UURING

2018

CYBERNETICA

Postkvant-krüptograafia ülevaade

Tehniline dokument

Versioon 1.0

28. jaanuar 2019. a.

22 lk

Dok A-101-10

Projektijuhid:	Tõnis Reimo (Riigi Infosüstemi Amet)
	Mari Seeba (Cybernetica)
Autorid:	Alisa Pankova, PhD (Cybernetica)
	Jan Willemson, PhD (Cybernetica)
	Ahto Buldas, PhD (Cybernetica)

Riigi Infosüsteemi Amet, Pärnu maantee 139a, 15169 Tallinn, Eesti.
Email: ria@ria.ee, Web: `https://www.ria.ee`, Telefon: +372 663 0200.

Cybernetica AS, Mäealuse 2/1, 12618 Tallinn, Eesti.
E-mail: info@cyber.ee, Web: `https://www.cyber.ee`, Telefon: +372 639 7991.

Sisukord

1 Sissejuhatus

Viimasel viiel aastal räägitakse palju kvantarvutitest ja nende ilmumisega kaasnevast ohust täna kasutusel olevale krüptograafiale. Võib jääda mulje, et peatselt luuaksegi võimsad kvantarvutid ja kogu traditsiooniline krüptograafia muutub kasutuks.

Kui tõsine on see oht tegelikkuses, ei ole aga päris selge. Praktiliselt teostatud ja avalikkusele teadaolevad kvantarvutid on veel väga kaugel praktilise krüptograafia murdmisest.

Samuti on teada palju krüptograafilisi algoritme, mida ei osata kvantarvutiga murda ja ka selliseid, mille kohta arvatakse, et kvantarvutid neid kunagi murda ei suudagi. Selliste krüptoalgoritmide uurimise ja konstrueerimisega tegeleb *postkvant-krüptograafia*.

Postkvant-krüptograafiat aetakse sageli segi *kvantkrüptograafiaga*. Kui post-kvant krüptograafia algoritmid on mõeldud kasutamiseks tavalistes arvutites, siis kvantkrüptograafia tähendab kvantefektide krüptograafilist kasutamist kas kvantarvutis või mingis lihtsamas kvantseadmes. Ka kvantkrüptograafia pakub krüpteerimisviise, mis ei ole kvantarvutitele murtavad, kuid kvantkrüptograafia praktiline kasutamine eeldab eriaparatuuri, mille kiire ja massiline kasutuselevõtt ei ole täna veel võimalik ega otstarbekas.

Postkvant-krüptograafia võimaldab kvantarvutitest tulenevale ohule praktilist lahendust, jäädes olemasoleva arvutitehnoloogia raamesse. Sellest hoolimata oleks kõikide krüptoteekide vahetus äärmiselt keerukas ja kallis projekt, mida ei saa teostada üleöö. Tänast olukorda iseloomustavad kõige paremini kaks asjaolu:

- Kasutuses olevad krüptoteegid postkvant-krüptograafiat sisuliselt ei toeta.
- Postkvant-krüptograafia standardimine on alles algjärgus.

Kui lähiajal peaks ehitatama tänapäevaseid krüptoalgoritme ohustav kvantarvuti, tähendaks see suure tõenäosusega kaost, sest isegi kui suudetaks kiiruga täiendada krüptolahendusi, satuks standardite puudumise tõttu ohtu lahenduste koostöövõime.

Hetkel jääb üle vaid loota, et kasutusel olevat krüptot reaalselt ohustavat kvantarvutit lähima viie aasta jooksul ei looda, mis annaks aega krüptoteekide täiendamiseks postkvant-krüptograafia primitiividega ja samuti postkvant-krüptograafia standardimiseks. Teekide õigeaegne järk-järguline täiendamine kvant-immuunsete krüptoalgoritmidega võimaldab kvantohuga kaasnevaid riske oluliselt vähendada, tekitades valmisoleku kiireks reageerimiseks, juhul kui ilmnevad tõendid kvantarvutitest tuleneva ohu suurenemisest.

Selles dokumendis antakse lühiülevaade kvantarvutitest, võrreldes neid klassikaliste (traditsiooniliste) arvutitega ning selgitatakse, miks on elliptkõveratel põhinevad krüptoalgoritmid ja RSA kvantarvutiga murtavad. Samuti antakse ülevaade postkvant-krüptograafia hetkeseisust.

2 Klassikaline ja kvantmehaanika

Klassikalises mehaanikas on isoleeritud süsteemi käitumine tulevikus üheselt määratud kui on teada iga komponendi:

- asukoht x_i
- impulss p_i (massi ja kiiruse korrutis)

Et muutused on pidevad, siis ennustamiseks piisab tuletistest:

$$\begin{aligned} \frac{dx_i}{dt} &= X(x_i, p_i) &&= \frac{\partial H}{\partial p_i} \\ \frac{dp_i}{dt} &= P(x_i, p_i) &&= -\frac{\partial H}{\partial x_i} \end{aligned}$$

kus H on süsteemi koguenergiat iseloomustav Hamiltoni funktsioon ning X ja P mingid kahe muutuja funktsioonid. Näitena võib tuua vedruostsillaatori (Joonis 1), mille Hamiltoni funktsioon on $H = \frac{p^2}{2m} + \frac{kx^2}{2}$, kus m on ostsilleeruva keha mass ja k on konstant, mis sõltub vedru elastsusest ja pinna hõõrdeomadustest. Et $\frac{\partial H}{\partial p} = \frac{p}{m}$ ja $-\frac{\partial H}{\partial x} = -kx$, saame Joonise 1 paremal ülanurgas kujutatud evolutsioonivõrrandid.

Selgub, et mikromaailma objekte st molekule, aatomeid, elementaarosakesi ei saa adekvaatselt kirjeldada klassikalise mehhaanika abil. Tuleb kasutada kvantmehhaanikat, kus süsteemi olek ei ole esitatav sõltumatute komponentide olekute summana. Süsteemi kui terviku olekut kirjeldab ühikpikkusega vektor Ψ kompleksarvuliste koordinaatidega vektorruumis – nn. *Hilberti ruumis*, kus iga kahe vektori Ψ ja Φ korral on määratud nende skalaarkorrutis $\langle \Psi, \Phi \rangle$.

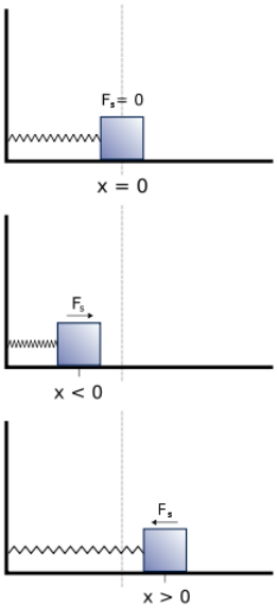
Isoleeritud süsteemi käitumine tulevikus on samuti üheselt määratud kui on teada süsteemi olekuvektor Ψ. Süsteemi evolutsiooni määrab Schrödingeri võrrand:

$$\frac{\partial}{\partial t}\Psi = \frac{1}{i\hbar} \cdot \mathrm{H}\Psi \ ,$$

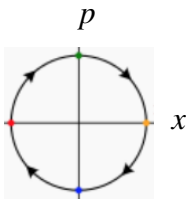
kus H on koguenergiat esitav lineaarne[1] (Hamiltoni) operaator, $\hbar$ on Plancki konstant ($6.62607015 \cdot 10^{-34}$ J $\cdot$ s) ja i imaginaarühik ($i^2 = -1$).

Üks kvantmehhaanika olulisi iseärasusi on, et süsteemi ei saa vaadelda ilma sellesse sekkumata ja seetõttu ei ole vaadeldav süsteem enam isoleeritud ega allu Schrödingeri võrrandile. Vaatlusi tuleb kvantmehhaanikas käsitleda eraldi.

[1] Operaator H on lineaarne, kui $H(\lambda\Phi + \xi\Psi) = \lambda H(\Phi) + \xi H(\Psi)$ mis tahes kahe vektori Φ, Ψ ja skalaari λ, ξ korral



$$\frac{dx}{dt} = \frac{1}{m} \cdot p$$
$$\frac{dp}{dt} = -k \cdot x$$



Joonis 1. Vedruostsillaator, tema evolutsioonivõrrandid ja evolutsioonitrajektoor faasiruumis, st ruumis koordinaatidega x ja p. (pildid Wikipediast)

Igale vaadeldavale suurusele vastab lineaarne operaator L, millel leidub süsteemi olekuruumis omavektoritest [2] koosnev ortogonaalne baas $\{\Psi_1, \Psi_2, \ldots\}$, st

$$\langle \Psi_i, \Psi_j \rangle = \begin{cases} 1 & \text{kui } i = j \\ 0 & \text{kui } i \neq j \end{cases}$$

ja iga olekuvektorit Ψ saab üheselt esitada summana:

$$\Psi = z_1\Psi_1 + z_2\Psi_2 + \ldots \ ,$$

kus $L\Psi_i = \lambda_i\Psi_i$, kus λ_i on mingid reaalarvud. Arvud λ_i on mõõdetava suuruse kõikvõimalikud väärtused. Mõõtmise tulemus näib juhusliku protsessina, kus tõenäosusega $|z_i|^2$:

- Süsteemi olekut kirjeldav vektor Ψ muutub vektoriks Ψ_i.
- Mõõtmistulemus on λ_i.

Seega sõltub süsteemi käitumine kvantmehhaanikas sellest, kas süsteemi vaadeldakse või mitte.

[2] Operaatori L omavektor on selline vektor Ψ, mille korral leidub skalaar $\lambda \in \mathbb{C}$, nii et $L\Psi = \lambda\Psi$. Skalaari λ nimetatakse operaatori *omaväärtuseks*. Et mõõdetavad suurused on harjumuspäraselt reaalsed, siis vaadeldavale suurusele vastava operaatori omaväärtused peavad olema reaalarvud. Selleks piisab kui nõuda, et vaadeldavatele suurustele vastavad operaatorid on nn. *Hermite'i operaatorid*. Hermite'i operaator on defineeritud võrdusega $H^\dagger = H$, kus $H^\dagger$ on selline lineaarne operaator, et $\langle H^\dagger\Phi, \Psi\rangle = \langle \Phi, H\Psi\rangle$ Hilberti ruumi mis tahes vektorite Φ ja Ψ korral. Sellise operaatori olemasolu tõestatakse elementaarses lineaaralgebras.

3 Kvantarvutid

Kvantarvutite kirjeldamisel on sobilik alustada kvantbitist (ingl. *qubit*), mis on vaadeldav suurus kahe võimalikku väärtusega: näiteks 0 ja 1. Kvantbitti kirjeldav Hilberti ruum on kahemõõtmeline ja kvantbiti oleku kirjeldamiseks kasutatakse kahte baasivektorit, mida tähistame Ψ_0 ja Ψ_1. Kvantbitt ise võib olla mis tahes olekus kujul

$$\Psi = z_0\Psi_0 + z_1\Psi_1 \ ,$$

kus z_0 ja z_1 on kompleksarvud, nii et $|z_0|^2 + |z_1|^2 = 1$. See tuleneb nõudmisest, et süsteemi olekuvektor peab olema ühikvektor. Vaatlusel saadakse 0 tõenäosusega $|z_0|^2$ ja 1 tõenäosusega $|z_1|^2$.

Kahebitine kvantregister on süsteem koos vaadeldava suurusega, mille väärtused on 00, 01, 10, 11, n-bitine kvantregister võib olla mis tahes olekus (superpositsioonis):

$$\Psi = \sum_x z_x\Psi_x \ ,$$

kus summeerimine toimub üle kõigi 2^n võimaliku x väärtuse.

Kvant-paralleelsus: Mis tahes funktsioonile $f(x)$ saab konstrueerida kvantarvuti, st süsteemi, mille evolutsioon Schrödingeri võrrandi järgi viib kvantregistri olekusse:

$$\Psi = \sum_x z_x\Psi_{x,f(x)} \tag{1}$$

Klassikalises arvutis vastaks sellele paralleelarvutus, kus korraga töötab 2^n lõime (*thread*).

Kõik lõimed aga ei ole korraga kättesaadavad. Väljundi vaatlemisel saame üheainsa väärtuse $y = f(x)$. See oleks aga samaväärne $f(x)$ arvutamisega juhuslikult valitud argumendist x, mis on efektiivselt teostatav ka klassikalise arvutiga.

Klassikalises paralleelarvutuses on kõikide lõimede tulemid korraga kättesaadavad ja lõimed võivad infot vahetada suvalisel viisil. Ka kvantarvutis saavad lõimed infot vahetada, kuid äärmiselt piiratult.

Kui kõik lõimed arvutavad ühe-bitilist suurust (predikaati), siis ei osata kvantarvutiga leida kõigi lõimede väljundbittide korrutist. Kui see oleks võimalik, saaks kvantarvutiga lahendada **NP**-täielikke ülesandeid polünomiaalses ajas. See aga ei tundu vähemasti praegu keerukusteooria spetsialistidele tõenäoline.

Kvantarvutuse idee seisneb superpositsiooni (1) mõjutamises sellisel viisil, mis suurendab "huvitavate" komponentide $z_x\Psi_{x,f(x)}$ väljatuleku tõenäosust $|z_x|^2$ "ebahuvitavate" arvelt. Huvitavate komponentidega seotud mõõtmistulemus $(x, f(x))$ annab olulist informatsiooni krüptosüsteemi murdmisega seotud kombinatoorikaülesande lahendamiseks.

4 RSA murdmine kvantarvutiga

RSA krüptosüsteemi privaatvõtme moodustavad kaks algarvu p, q ja privaatastendaja d. Avalik võti koosneb avalikust moodulist $n = pq$ ja avalikust astendajast e, mis on konstantne ja standardiga fikseeritud. Võtme genereerimisel leitakse juhuslikud algarvud p ja q, arvutatakse Euleri funktsioon $\varphi(n) = (p-1)(q-1)$ ja leitakse $d = \frac{1}{e} \bmod \varphi(n)$ kasutades nn. Eukleidese algoritmi.

Sõnumi $m \in \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ krüptogramm on $c = E(m) = m^e \bmod n$, millele vastav avatekst arvutatakse privaatvõtme abil järgmiselt: $m = D(c) = c^d \bmod n$.

Üks ülesanne, mida kvantarvutiga efektiivselt lahendada saab, on funktsiooni *perioodi* leidmine. Täisarvulise argumendi ja väärtusega funktsiooni f *perioodiks* nimetatakse vähimat rangelt positiivset täisarvu λ, nii et $f(x + \lambda) = f(x)$ iga x korral.

Funktsiooni perioodi leidmine kvantarvutiga toimub Peter Shori poolt aastal 1994 esitatud kvantalgoritmi [27] abil, milles kasutatakse kaheosalist kvantregistrit sisend- ja väljundosaga, ja mis koosneb järgmistest sammudest:

1. Luuakse superpositsioon $\Psi = \frac{1}{\sqrt{N}} \sum_x \Psi_{x,f(x)}$, kus N on registri kõikvõimalike sisendosa bitikombinatsioonide arv.
2. Registri sisendosale rakendatakse nn. *Fourier' kvant-teisendust* [17], mis teisendab superpositsioonis Ψ kordajad $z_x = \frac{1}{\sqrt{N}}$ kordajateks z'_x, mille absoluutväärtused on ühelähedased ($|z'_x| \approx 1$) kui $x = \lambda \frac{N}{r}$, kus $\lambda \in \{0, 1, \ldots, r-1\}$.
3. Mõõdetakse esimest registrit ja suure tõenäosusega saadakse tulemus $x \approx \lambda \frac{N}{r}$.
4. Leitakse r kasutades algebrast tuntud *ahelmurdude* meetodit.

RSA avaliku võtmega krüpteerimisfunktsioon $E(m) = m^e \bmod n$ murtav seetõttu, et kui on teada funktsiooni $f(x) = a^x \bmod n$ periood r mingi vahemikust $(0...n)$ juhuslikult valitud a korral, siis tõenäosusega vähemalt $\frac{1}{2}$ on r paarisarv ja arv $u = a^{r/2} \bmod n$ on $\sqrt{1}$ mittetriviaalne väärtus, st $u \not\equiv \pm 1 \pmod{n}$ ja $u^2 \equiv 1 \pmod{n}$. Lihtne on näidata, et suurimad ühistegurid $\gcd(u+1, n)$ ja $\gcd(u-1, n)$, mida saab efektiivselt arvutada *Eukleidese algoritmi* abil, on mooduli n algarvulised tegurid p ja q, mis aga omakorda võimaldavad leida RSA salajase astendaja $d = \frac{1}{e} \bmod (p-1)(q-1)$.

Seetõttu on RSA krüpteerimisalgoritm ja sarnastel põhjustel ka elliptkõveratel põhinevad krüpteerimisalgoritmid kvantarvuti abil tõhusalt murtavad.

5 Postkvant-krüptograafia

Postkvant-krüptograafia on kvantarvutitele vastupidavate krüptosüsteemide koondnimetus. Need liigitatakse järgnevalt:

- võrepõhised,
- mitmemuutujalised,
- räsipõhised,
- koodipõhised,
- isogeensuspõhised.

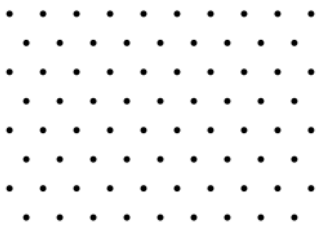
Ka tavalised plokkšifrid (näiteks AES) on tänase seisuga kvant-immuunsed. Plokkšifrite uurimist ja konstrueerimist ei loeta aga postkvant-krüptograafia valdkonda kuuluvaks.

5.1 Võrepõhine krüptograafia

Võresid uurisid juba Joseph Louis Lagrange ja Carl Friedrich Gauss. Krüptograafias on võresid kasutatud näiteks arvkongruentsidel põhinevate pseudojuhuarvugeneraatorite krüptoanalüüsis. Miklós Ajtai [1] näitas 1996. aastal esmakordselt, et võresid saab kasutada ka uute krüptosüsteemide loomisel. Craig Gentry [13] kasutas 2009. aastal võresid esimese täishomomorfse krüptosüsteemi loomisel.

Võreks nimetatakse eukleidilise ruumi $\mathbb{R}^n$ vektorite (punktide) diskreetset alamhulka, mis on kinnine vektorite liitmise ja lahutamise suhtes. Öeldakse, et võre dimensioon on n kui võre ei sisaldu ruumi $\mathbb{R}^n$ üheski pärisalamruumis (st madalama dimensiooniga alamruumis).

Visuaalselt kujutatuna on võre kogu ruumi ulatuses *korrapäraselt paiknevate punktide kogum* (Joonis 2). Algebralise süsteemina on võre lõplikult genereeritud *vaba Abeli rühm*.



Joonis 2. Võre tasandil.

Võre L baasiks nimetatakse vektorite hulka B, nii et võre L iga punkt (vektor) avaldub ühesel viisil hulga B elementide täisarvulise lineaarkombinatsioonina. Kui võre dimensioon on vähemalt 2, siis on võres alati lõpmatu arv baase.

Krüptograafias on aga vaja, et avatekst, krüptogramm ja võti oleksid lõplikud bitijadad. Seetõttu kasutatakse krüptograafias võresid, mis on mitte ruumis $\mathbb{R}^n$ vaid K^n, kus K on mingi lõplik korpus.

Võrepõhine krüptograafia toetub järgmiste kombinatoorikaprobleemide oletatavale raskusele.

- *Lühim vektor*: Leida baasiga B esitatud võre L lühim vektor v Eukleidilise pikkuse $\sqrt{\langle v, v\rangle}$ mõttes, kus $\langle\cdot,\cdot\rangle$ tähistab skalaarkorrutist.
- *Lähim vektor*: Baasiga B esitatud võre L ja vektori $v \notin L$ korral leida võre vektor $v' \in L$, mis on lähim vektorile v Eukleidilise kauguse $d(v', v) = \sqrt{\langle v' - v, v' - v\rangle}$ mõttes, kus $\langle\cdot,\cdot\rangle$ tähistab skalaarkorrutist.

Need probleemid usutakse olevat üldjuhul (enamiku baaside B korral) raskesti lahenduvad. Kui aga baasivektorid on lühikesed ja peaaegu ortogonaalsed, muutuvad mõlemad probleemid kergesti lahenduvaks. Sellise baasi koostamist nimetatakse võre baasitaanduseks (*lattice basis reduction*) ja tuntuim algoritm taanduse teostamiseks on Lenstra–Lenstra–Lovászi (LLL) algoritm [21] aastast 1982 .

Turvalisust arvestades jagunevad võrepõhised krüptosüsteemid kahte klassi.

- Turvatõestuseta, kuid väga tõhusad ja konkureerivad parimate teadaolevate algoritmidega, näiteks NTRU algoritmide perekond.
- Turvatõestusega, kuid enamasti vähetõhusad ja ebapraktilised. Näiteks vigadega õppimisel (*Learning with Errors, LWE*) põhinevad algoritmid.

Ringidel põhinev vigadega õppimine (Ring-LWE) aga lubab konstrueerida krüptosüsteeme, mis on enam-vähem tõhusalt arvutatavad ja samas ka formaalse turvatõestusega.

5.2 Mitmemuutujaline krüptograafia

Mitmemuutujaliste algebraliste võrrandite lahendamine on **NP**-raske ja kvantarvutid ei suuda arvatavasti **NP**-raskeid ülesandeid tõhusalt lahendada.

On teada vaid mitmemuutujalistel võrranditel põhinevaid *signeerimisskeeme* nagu *Unbalanced Oil and Vinegar (UOV)* [19] aastast 1999, *Hidden Field Equations (HFE)*, *Hidden Field Equation Vinegar (HFEv)* [25] aastast 1996 ja Rainbow [12] aastast 2005. Need on vähese arvutusmahuga ja sobivad riistvarasse. Nõuavad aga suhteliselt pikka võtit (paar tuhat baiti).

Pea kõik mitmemuutujalised (avaliku võtmega) *krüpteerimisskeemid* on aga osutunud ebaturvalisteks. Näiteks Imai-Matsumoto krüptosüsteemi aastast 1988 murdis Patarin aastal 1995. Patarini enda skeemi Little Dragon [24] aastast 1995 murdsid Coppersmith ja Patarin ise aastal 1996 [20].

Mitmemuutujaline krüptograafia toetub algebraliste võrrandisüsteemide lõplikes korpustes lahendamise oletatavale raskusele. Näiteks kui korpusena kasutatakse kahe-elemendilist

korpust $\mathbb{Z}_2 = \{0, 1\}$, on lahendatav võrrandisüsteem järgmine:

$$\begin{aligned} P_1(x_1, x_2, \ldots, x_{2n}) &= y_1 \\ P_2(x_1, x_2, \ldots, x_{2n}) &= y_2 \\ &\ldots \\ P_n(x_1, x_2, \ldots, x_{2n}) &= y_n \ , \end{aligned} \tag{2}$$

kus $P_1, \ldots, P_n \in \mathbb{Z}[x_1, \ldots, x_{2n}]$ on polünoomid astmega ülimalt kaks.

Mitememuutujalise signatuuriskeemi avalik võti on polünoomide $P_1, \ldots, P_n$ kirjeldus.

Sõnumi M signatuur on $3n$-bitine ning koosneb $2n$ bitist $x_1, \ldots, x_{2n}$ ja lisaks veel n-bitisest juhuarvust r, nii et

$$H(r, M) = P_1(x_1, \ldots, x_{2n}) || \ldots || P_n(x_1, \ldots, x_{2n}) \ ,$$

kus H on mis tahes n-bitise väljundjadaga räsifunktsioon ja $||$ tähistab bitijadade konkatenatsiooni.

Sõnumi M signeerimiseks tuleb esmalt arvutada räsi $H(r, M) = y_1 y_2 \ldots y_n$ kasutades juhuarvu r ja seejärel lahendada võrrandisüsteem (2).

Polünoomid P_i on valitud erilisel viisil, nii et teades nende salajast struktuuri – nn. HFE (*Hidden Field Equation*) struktuuri – on võrrandisüsteemi lihtne lahendada. Selle salajase struktuuri avastamiseks (kas avalikust võtmest või juba moodustatud signatuuridest) ei ole teada tõhusaid algoritme. Sellise signeerimisalgoritmi esitas Patarin [25] aastal 1996 ja tänini ei ole teada efektiivseid ründemeetodeid.

5.3 Räsipõhine krüptograafia

Räsifunktsioonidel põhinevad ühed vanimaist signeerimisskeemidest – Lamporti ja Merkle'i signatuuriskeemid, mis loodi juba eelmise sajandi 70-ndate aastate lõpul.

Räsipõhiseid signeerimisskeeme on uuritud juba kaua ja neid loetakse turvaliseks eeldusel, et kasutatav räsifunktsioon on turvaline (kollisioonrünnete vastu).

Räsipõhiste signatuuriskeemide põhipuudus on võimalike signatuuride piiratud arv.

Lamporti signatuuriskeem ühe biti b signeerimiseks:

- Privaatvõti: kaks n-bitist (pseudo)juhuarvu k_0 ja k_1
- Avalik võti: paar $f(k_0), f(k_1)$, kus f on ühesuunaline funktsioon
- Biti $b \in \{0, 1\}$ signeerimiseks avalikustab signeerija poole oma privaatvõtmest, nimelt k_b, ja kustutab (unustab) teise poole k_{1-b}.

Pikema sõnumi M signeerimiseks on vaja n (näiteks $n = 256$) privaatvõtit $(k_0^1, k_1^1), \ldots, (k_0^n, k_1^n)$. Sõnum räsitakse ja selle räsi $y = y_1 y_2 \ldots y_n = H(M)$ iga bitt y_i signeeritakse eraldi.

Signatuuri suurus $n = 256$ korral: $n^2 = 256 \cdot 256 = 65536$ bitti ehk 8 kilobaiti. Avaliku võtme maht ühe sõnumi signeerimiseks on 16 kilobaiti.

Merkle'i signatuuriskeem on Lamporti skeemi edasiarendus, kus avaliku võtme mahu vähendamiseks kasutatakse räsipuud, mille juurräsi on avalik võti. Merkle'i signatuuriskeemis

saab ühe avaliku ja privaatvõtmega signeerida palju sõnumeid, ehkki nende arv on piiratud. Kuni m signeerimist võimaldava võtme korral on signatuuri suurus $n^2 + n \log_2 m$ bitti, st mitte oluliselt suurem kui ühekordset signeerimist võimaldava skeemi korral. Näiteks $m = 1024$ ja $n = 256$ korral on signatuur $256 \cdot (256 + 10)$ bitti ehk umbes 8.5 kilobaiti.

Lamporti ja Merkli tüüpi signatuuriskeemidel on mitmeid modifikatsioone, näiteks:

- *XMSS* [5] aastast2011, mis $n = 256$ korral annab ühe sõnumi signeerimiseks vajaliku signatuuri suuruseks umbes 1.8 kilobaiti.
- *BLT* [8, 6, 7, 9] aastast 2014 võimaldab signeerida vaid koostöös serveriga ja vajab sünkroniseeritud kelli; signatuuri suurus on väiksem kui 1 kilobait.
- *SPHINCS* [3] aastast 2014 on esimene olekuvaba räsipõhine signatuuriskeem, kus ei ole vaja arvet pidada signeeritavate sõnumite arvu kohta (st muuta privaatvõtme olekut) ega suhelda serveriga. SPHINCS kasutab umbes 1 kilobaidist avalikku- ja 1 kilobaidist privaatvõtit, kuid signatuuri suurus on ligikaudu 42 kilobaiti.

5.4 Koodipõhine krüptograafia

Koodipõhine krüptograafia põhineb veaparanduskoodide omadustel. On olemas nii koodipõhiseid krüpteerimisskeeme nagu näiteks McEliece skeem aastast 1978 [22], kui ka signeerimisskeeme nagu näiteks Niederreiteri skeem aastast 1986 [23].

McEliece'i krüptosüsteem [22] on väga tõhus nii võtme genereerimise, krüpteerimise kui ka dekrüpteerimise kiiruse mõttes, kuid tema peamine puudus on väga suur avalik võti. Näiteks 2^{128}-turvalisuse saavutamiseks peaks võti olema enam kui 100 kilobaidine. Skeem põhineb lineaarkoodidel, st lineaarkombinatsioonide suhtes kinnistel vektorite hulkadel mingis n-mõõtmelises vektorruumis üle lõpliku korpuse $\mathbb{F}_q$, st lineaarkood on ruumi $\mathbb{F}_q^n$ mingi k-mõõtmeline alamruum.

McEliece'i krüptosüsteemi ründekindlus põhineb *lähima koodsõna probleemil*, st valitud vektorile x Hammingi kauguse mõttes lähima koodsõna (alamruumi elemendi) leidmisel. On tõestatud, et selle ülesande kõige üldisem versioon on **NP**-raske.

McEliece'i krüptosüsteemi *privaatvõti* on juhuslikult valitud binaarne Goppa kood, mis on kergesti dekodeeritav ja parandab kuni t-bitiseid vigu.

Avalik võti saadakse järgmiselt. Valitud Goppa kood maskeeritakse üldise lineaarkoodiga. Kui G on koodi generaatormaatriks, mille reavektorid moodustavad koodi kui alamruumi baasi, siis avalik võti G' saadakse juhuslikult valitud pööratavate maatriksite S ja P abil järgmiselt:

$$G' = S \cdot G \cdot P \ ,$$

kus $\cdot$ tähendab maatriksite korrutamist. Seejuures on P permutatsioonimaatriks, mille igas reas ja veerus on täpselt üks 1.

Sõnumi m krüpteerimiseks kodeeritakse m esmalt t-bitise stringina, arvutatakse vektor $c' = mG'$, genereeritakse n-bitine juhuslik vektor z, mille koordinaatidest täpselt t on võrdsed ühega ja moodustatakse krüptogramm $c = c' + z$, st lisatud on t-bitine juhuslik viga.

Krüptogrammi dekrüpteerimine: pöördmaatriksi P^{-1} abil arvutatakse $\overline{c} = cP^{-1}$, dekodeeri-

takse $\overline{c}$ leides m' ning leitakse avatekst $m = m'S^{-1}$. Dekrüpteerimine on korrektne, sest

$$\overline{c} = cP^{-1} = mG'P^{-1} + zP^{-1} = mSG + zP^{-1} \ ,$$

mSG on koodsõna ja vektori zP^{-1} Hammingi norm ei ületa t (P on permutatsioonimaatriks).

5.5 Isogeensuskrüptograafia

Kahe elliptkõvera E_1 ja E_2 vaheline isogeensus on ratsionaalkujutus $E_1 \to E_2$ mis ühtlasi on rühmade homomorfism. Isogeensuskrüptograafia kasutab arvutusteks elliptkõveratevahelisi isogeensusi.

Isogeensuspõhise avaliku võtmega krüptograafia pakkusid esimesena välja Rostovtsev ja Stolbunov [26, 28]. Nende skeemi puudus oli aga väga pikk krüpteerimis- ja dekrüpteerimisaeg. Lisaks sellele leidsid Childs, Jao ja Soukharev [10] skeemile [26, 28] subeksponentsiaalse kvantründe.

Jao ja De Feo panid ette kasutada supersingulaarseid elliptkõveraid [18], mille eriline struktuur muudab artiklis [10] kirjeldatud ründe ebaefektiivseks. Lisaks sellele muutusid supersingulaarsete kõverate kasutusega oluliselt efektiivsemaks ka krüpteerimis- ja dekrüpteerimisaeg. Isogeensuspõhistel skeemidel on klassikaliste Diffie-Hellmani (DH) ja Elliptkõverate Diffie-Hellmani (ECDH) skeemidega väga sarnane struktuur ja seetõttu on isogeensuspõhised skeemid üheks parimatest Diffie-Hellmanni tüüpi skeemide postkvantasendajaks. Nende teostuste krüpteerimiskiirused ja sõnumi suurus on võrreldavad klassikaliste skeemidega [11].

Elliptkõverate teoorias on kesksel kohal *j-invariant* kui täisarvuliste väärtustega funktsioon järgmiste omadustega:

- $j(E)$ on lihtsasti arvutatav elliptkõvera E kirjeldusest (võrrandist)
- teatud klassi elliptkõverate korral $j(E) = j(E')$ parajasti siis kui E ja E' on isomorfsed.

Supersingular Isogeny Diffie-Hellman (SIDH) võtmekehtestusprotokoll [11] kasutab algarve kujul $p = \ell_A^{e_A} \cdot \ell_B^{e_B} \cdot f \pm 1$, kus ℓ_A and ℓ_B on väikesed algarvud, e_A ja e_B on (Alice'i ja Bobi) suured avalikud astendajad ja f on väike tegur.

Arvutusetes kasutatakse elliptkõverat E üle korpuse $\mathbb{F}_{p^2}$, nii et E-s leiduksid suured alamrühmad $E[\ell_A^{e_A}]$ ja $E[\ell_B^{e_B}]$, mis kuuluvad vastavalt Alice'le ja Bobile. Sellist elliptkõverat nimetatakse *supersingulaarseks*. Võtmekehtestus toimub järgmiste sammudega:

1. Alice valib juhusliku tsüklilise alamrühma $G_A \subset E[\ell_A^{e_A}]$ ja valib isogeensuse φ_A, mille tuum on G_A.
2. Alice avaldab oma isogeensuse sihtkõvera $\varphi_A(E)$ kirjelduse ja samuti $\varphi_A(E[\ell_B^{e_B}])$.
3. Bob teeb täpselt samamoodi
4. See info võimaldab Alice'l ja Bobil arvutada uue isogeensuse, mille tuuma moodustavad alamrühmad G_A ja G_B. Nendel kahel arvutatud isogeensustel on sama tuum ja sihtkõverad E_A ja E_B on seega isomorfsed.
5. Järelikult on neil sama j-invariant: $j(E_A) = j(E_B)$, mida saab kasutada kehtestatud ühisvõtmena.

6 Funktsionaalsuspõhine ülevaade

Selles peatükis vaatleme lühidalt, mis seisus on kvantarvuti ilmumise korral krüptograafilised põhifunktsionaalsused:

- Räsifunktsioonid
- Plokkšifrid
- Digitaalsignatuurid
- Võtmekehtestusprotokollid
- Avaliku võtmega krüptosüsteemid

6.1 Räsifunktsioonid

Brassard jt on väitnud aastal 1998 [4], et Groveri algoritm [15] võimaldab kollisiooniotsingut ajas $O(2^{n/3})$, kus n on räsifunktsiooni väljundbittide arv. Hiljem on jõutud järeldusele, et see kiirendus (võrreldes klassikalise $O(2^{n/2})$) on praktilisi teostusi arvestades siiski illusoorne. Kiireim teadaolev kvantalgoritm kollisiooni leidmiseks on keerukusega $O(2^{2n/5})$.

Kvantarvuti saabudes tuleb kvant-eelse olukorraga sama turvataseme saavutamiseks suurendada kasutatavate räsifunktsioonide väljundbittide arvu umbes 25%.

6.2 Plokkšifrid

Ehkki plokkšifrite otseseks murdmiseks sobilikke kvantalgoritme ei teata, võimaldab Groveri algoritm [14] kiirendada kõigi võtmete läbivaatust (jõurünnet). Plokkšifrite n-bitist võtmeruumi saab läbi vaadata $2^{\frac{n}{2}}$ kvantoperatsiooniga.

128-bitine võti murtakse umbes 2^{64} sammuga, mis ei ole nüüdisajal piisav ründekindlus.

6.3 Digitaalsignatuurid

Ühed parimatest kandidaatidest digitaalsignatuuri skeemide postkvant asenduseks on:

- *Räsipõhised* signatuuriskeemid on neist usaldusväärseimad. Lühikesed 64–1056 baidised võtmed on lähedased klassikalistele RSA ja ECC skeemidele. Signatuuri suurus 2.5–41 KB on klassikaliste skeemidega võrreldes palju suurem. Näiteks olekuga XMSS skeemis [5] kasutatakse 64-baidist avalikku võtit ja signatuuri suurus on umbes 2.5–3.0 KB. Olekuta SPHINCS skeem [3] kasutab 1056-baidist avalikku võtit ja moodustab 41 KB suuruse signatuuri.

- *Mitmemuutujalised* signatuuriskeemid kasutavad avalikku võtit suurusega 500 kB kuni 1 MB, kuid signatuur ise on väike. Mitmemuutujalised signeerimisskeemid on aga räsipõhiste skeemidega võrreldes vähem usaldusväärsed, sest neid on tunduvalt vähem uuritud.

Tabelis 1 on toodud postkvant signeerimisskeemide parameetrite võrdlus klassikaliste signeerimisskeemide parameetritega.

Tabel 1. Signeerimisskeemide võrdlus võtme ja signatuuri suuruse järgi.

Skeem	**Tüüp**	**Avalik võti** (baitides)	**Signatuur** (baitides)
XMSS	räsipõhine	64	2500–3000
SPHINCS	räsipõhine	1056	41000
HFEv-	mitmemuutujaline	500000–1000000	25–32
RSA-4096	klassikaline	512	512
ECDSA-512	klassikaline	64	64

6.4 Võtmekehtestus

Ühed parimatest kandidaatidest võtmekehtestusskeemide postkvant asenduseks on:

- *Võrepõhised* võtmekehtestusskeemid. Näiteks NewHope skeemis [2] kasutatakse võtmekehtestussõnumeid suurusega 2 kB, mis on suur võrreldes klassikaliste skeemide 32–64 baidiga, nagu näiteks ECDH.
- *Isogeensuspõhised* võtmekehtestusskeemid. Näiteks SIDH skeemis [11] kasutatakse võtmekehtestussõnumeid suurusega 564 baiti. Samas ei saa SIDH skeemi lugeda täiesti usaldusväärseks, sest ühelt poolt ei ole teada taandusi ühelegi **NP**-raskele kombinatoorikaprobleemile ja teiselt poolt ei ole SIDH skeemi ründekindlust ka praktilise poole pealt piisavalt uuritud.

Võtmekehtestusskeeme saab koostada ka avaliku võtmega krüpteerimisskeemidest, nii et igas seansis valitakse uus juhuslik plokkšifri krüpteerimisvõti, mis edastatakse avaliku võtmega krüpteeritult teisele osapoolele.

Tabelis 2 on toodud postkvant võtmekehtestusskeemide parameetrite võrdlus klassikaliste võtmekehtestusskeemide parameetritega.

Tabel 2. Võtmekehtestusskeemide võrdlus andmete suuruse järgi.

Skeem	**Tüüp**	**Andmed** (baitides)
NewHope	võrepõhine	$\approx$ 2000
SIDH	isogeensuspõhine	564
DH	klassikaline	512
ECDH	klassikaline	64

6.5 Avaliku võtmega krüptosüsteemid

Ühed parimatest kandidaatidest avaliku võtmega krüpteerimisskeemide postkvant asenduseks on:

- *Koodipõhised* avaliku võtmega krüpteerimisskeemid. McEliece [22] ja Niederreiter's [23] skeeme, mis kasutavad Goppa koode, loetakse piisavalt usaldusväärseiks ja nende krüptogrammid on vaid 200 baidised, kuid avalikud võtmed on suurusjärgus 1 MB.
- *Võrepõhised* avaliku võtmega krüpteerimisskeemid. Võrepõhised skeemid kasutavad väiksemaid võtmeid ja krüptogramme, kuid ei ole vähemasti esialgu veel koodipõhiste skeemidega võrreldava usaldusväärsusega. Näiteks NTRUEncrpyt skeem [16] kasutab võtmeid ja krüptogramme suurusega 2 KB.

Tabelis 3 on toodud postkvant avaliku võtmega krüpteerimisskeemide parameetrite võrdlus klassikaliste avaliku võtmega krüpteerimisskeemide parameetritega.

Tabel 3. Avaliku võtmega krüpteerimisskeemide võrdlus võtme ja krüptogrammi suuruse järgi.

Skeem	**Tüüp**	**Avalik võti** (baitides)	**Krüptogramm** (baitides)
McEliece	koodipõhine	$\approx$ 1000000	$\approx$ 200
McBits	koodipõhine	$\approx$ 300000	$\approx$ 109 (lisainfo)
NTRU	võrepõhine	1500–2000	1500–2000
RSA-4096	klassikaline	512	512
ECC-512	klassikaline	64	64

7 Standardimine

NIST (National Institute of Standards) algatas *postkvant-krüptograafia standardimise* projekti. [3]

Uute algoritmide ettepanekud tuli esitada 2017. aasta lõpuks. Esitatigi 23 signatuuriskeemi ja 59 võtmekehtestus- ja avaliku võtmega krütograafilist algoritmi.

Hetkel on konkurentsis:

- 18 signatuuriskeemi (5 võrepõhist, 2 koodipõhist, 2 räsipõhist, 7 mitme-muutuja, 2 muud)
- 42 võtmekehtestus- ja avaliku võtmega krütograafilist algoritmi (20 võrepõhist, 17 koodipõhist, 2 mitme-muutuja, 1 isogeensuspõhine, 2 muud).

[3] https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

Kirjandus

[1] Miklós Ajtai. Generating Hard Instances of Lattice Problems (Extended Abstract). In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 99–108, New York, NY, USA, 1996. ACM.

[2] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange—a new hope. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 327–343, Austin, TX, 2016. USENIX Association.

[3] Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn. Sphincs: Practical stateless hash-based signatures. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015*, volume 9056 of *Lecture Notes in Computer Science*, pages 368–397, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[4] G. Brassard, P. Høyer, and A. Tapp. Quantum cryptanalysis of hash and claw-free functions. In C.L. Lucchesi and A.V. Moura, editors, *LATIN 1998*, volume 1380 of *Lecture Notes in Computer Science*, pages 163–169. Springer, Heidelberg, 1998.

[5] Johannes Buchmann, Erik Dahmen, and Andreas Hülsing. XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In B.-J. Yang, editor, *Post-Quantum Cryptography*, volume 7071 of *Lecture Notes in Computer Science*, pages 117–129. Springer Berlin Heidelberg, 2011.

[6] Ahto Buldas, Risto Laanoja, and Ahto Truu. Efficient Implementation of Keyless Signatures with Hash Sequence Authentication. Cryptology ePrint Archive, Report 2014/689, 2014. `http://eprint.iacr.org/`.

[7] Ahto Buldas, Risto Laanoja, and Ahto Truu. Efficient Quantum-Immune Keyless Signatures with Identity. Cryptology ePrint Archive, Report 2014/321, 2014. `http://eprint.iacr.org/`.

[8] Ahto Buldas, Risto Laanoja, and Ahto Truu. Security Proofs for the BLT Signature Scheme. Cryptology ePrint Archive, Report 2014/696, 2014. `http://eprint.iacr.org/`.

[9] Ahto Buldas, Risto Laanoja, and Ahto Truu. A server-assisted hash-based signature scheme. In Helger Lipmaa, Aikaterini Mitrokotsa, and Raimundas Matulevičius, editors, *Secure IT Systems*, pages 3–17, Cham, 2017. Springer International Publishing.

[10] Andrew M. Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Mathematical Cryptology*, 8:1–29, 2014.

[11] Craig Costello, Patrick Longa, and Michael Naehrig. Efficient algorithms for supersingular isogeny diffie-hellman. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016*, pages 572–601, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[12] Jintai Ding and Dieter Schmidt. Rainbow, a New Multivariable Polynomial Signature Scheme. In John Ioannidis, Angelos Keromytis, and Moti Yung, editors, *Applied Cryptography and Network Security*, volume 3531 of *Lecture Notes in Computer Science*, pages 164–175. Springer Berlin Heidelberg, 2005.

[13] Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009. `https://crypto.stanford.edu/craig`.

[14] M. Grassl, B. Langenberg, M. Roetteler, and R.Šteinwandt. Applying grover's algorithm to aes: quantum resource estimates. In T. Takagi, editor, *PQCrypto 2016*, volume 9606 of *Lecture Notes in Computer Science*, pages 29–43, 2016.

[15] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. ACM.

[16] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. Ntru: A ring-based public key cryptosystem. In Joe P. Buhler, editor, *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.

[17] Sandor Imre and Ferenc Balazs. *Quantum Computing and Communications: An Engineering Approach*. Wiley, 1st edition, 2013.

[18] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography*, pages 19–34, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[19] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced Oil and Vinegar Signature Schemes. In Jacques Stern, editor, *Advances in Cryptology – EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 206—222. Springer Berlin Heidelberg, 1999.

[20] Neal Koblitz. *Algebraic Aspects of Cryptography*. Number 3 in Algorithms and Computation in Mathematics. Springer, 1998.

[21] A.K. Lenstra, H.W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[22] R.J. McEliece. A public-key cryptosystem based on algebraic coding theory. The Deep Space Network Progress Report, DSN PR 42-44, pages 114–116, January and February 1978.

[23] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[24] Jacques Patarin. Asymmetric Cryptography with a Hidden Monomial. In Neal Koblitz, editor, *Advances in Cryptology – CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 45–60. Springer Berlin Heidelberg, 1996.

[25] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *Eurocrypt '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 1996.

[26] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on Isogenies. IACR Cryptology ePrint Archive, Report 2006/147, 2006. `http://eprint.iacr.org/`.

[27] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, SFCS '94, pages 124–134, Washington, DC, USA, 1994. IEEE Computer Society.

[28] Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Advances in Mathematics of Communications*, 4:215, 2010.