Tartu Ülikool
Loodus- ja täppisteaduste valdkond
Matemaatika ja statistika instituut

Calvin Pärn

Supersingulaarsete elliptkõverate isogeensed teisendused ning rakendused signatuuriskeemi CSI-FiSh näitel

Matemaatika

Bakalaureusetöö (9 EAP)

Juhendajad: PhD Jan Villemson, prof. Valdis Laan

Tartu 2021

SUPERSINGULAARSETE ELLIPTKÕVERATE ISOGEENSED TEISENDUSED NING RAKENDUSED SIGNATUURISKEEMI CSI-FISH NÄITEL

Bakalaureusetöö

Calvin Pärn

Lühikokkuvõte Aastal 2019 avaldasid W. Beullens, T. Kleinjung ja F. Vercauteren artikli, kus tutvustasid allkirjastusskeemi CSI-FiSh, mida usutakse praegu olevat kvantturvaline. Käesoleva bakalaureusetöö eesmärk on esitada elliptkõverate ning nende isogeensete teisenduste baasteooria eesmärgiga seletada lahti signatuuriskeemi CSI-FiSh toimimine. Töös anname edasi elliptkõverate ja nende isogeensete teisenduste põhiteooria, anname edasi CSI-FiSh-ist arusaamiseks vajaminevad ringiteooria definitsioonid ja tulemused ning selgitame miks ja kuidas CSI-FiSh töötab.

CERCS teaduseriala: P120 Arvuteooria, väljateooria, algebraline geomeetria, algebra, rühmateooria
Märksõnad: Elliptilised jooned, rühmad (mat.), teisendused

ISOGENIES OF SUPERSINGULAR ELLIPTIC CURVES AND APPLICATIONS AT THE EXAMPLE OF THE SIGNATURE SCHEME CSI-FISH

Bachelor thesis

Calvin Pärn

Abstract In the year 2019 W. Beullens, T. Kleinjung and F. Vercauteren published an article introducing the signature scheme CSI-FiSh, which as of today is believed to be quantum-secure. The aim of this bachelor's thesis is to introduce the basic theory of elliptic curves and isogenies of elliptic curves in order to understand how CSI-FiSh works. In the thesis we will convey the basics of elliptic curves and isogenies between elliptic curves, we shall introduce necessary definitions and results from ring theory for understanding CSI-FiSh and we will explain in detail how and why CSI-FiSh works.

CERCS research specialisation: P120 Number theory, field theory, algebraic geometry, algebra, group theory
Key Words: Elliptic curves, groups, transformations

Sisukord

Sissejuhatus **3**

1 Matemaatiline taust **4**

1.1 Elliptkõver üle korpuse $\mathbb{K}$ 4

1.2 Elliptkõver kui rühm 5

1.3 Supersingulaarsed elliptkõverad 7

1.4 j-invariant 9

1.5 Endomorfismid 10

1.6 Isogeensed teisendused 13

2 Eelteadmised CSI-FiSh-ile **17**

2.1 Kompleksne korrutamine 17

2.2 Kompleksne korrutamine elliptkõveratel üle lõplike korpuste 17

2.3 Ideaalid 21

3 CSI-FiSh **24**

3.1 Miks supersingulaarsed kõverad? 24

3.2 Baasprobleemid 24

3.3 Baasskeem 25

3.4 Allkirjastusskeem 26

Kasutatud allikad **28**

Sissejuhatus

CSI-FiSh (lüh. *Commutative Supersingular Isogeny Fiat-Shamir*) on supersingulaarsete elliptkõverate isogeensetel teisendustel põhinev allkirjastusskeem, mis põhineb probleemil, mille murdmiseks ei leidu praeguse seisuga piisavalt efektiivset algoritmi nii tavalisel arvutil kui ka kvantarvutil. Aastal 2019 teatasid W. Beullens, T. Kleinjung ning F. Vercauteren oma artiklis, et on läbi viinud suuremahulised teadusarvutused, mille abil on nüüd võimalik CSI-FiSh-i baasskeemil, CSIDH-il saavutada piisav turvalisustase, et olla tõsiseltvõetav kandidaat rakendatavale kvantturvalisele allkirjastusskeemile – CSI-FiSh-i kasuks räägivad ka väikesemahulised allkirjad. Antud töö näol on tegemist referatiivse tööga, mille eesmärk on kirjeldada skeemi matemaatilist tausta ning ka skeemi ennast.

Töö esimeses ning mahukaimas peatükis esitame elliptkõverate krüptograafia mõistmiseks vajaliku taustmaterjali elliptkõverate kohta. Näitame, kuidas saab defineerida elliptkõveral üle korpuse rühmatehte, defineerime supersingulaarsed elliptkõverad ning kirjeldame elliptkõverate vaheliste isogeensete teisenduste omadusi. Enamus peatükist põhineb raamatul [1].

Töö teises peatükis anname edasi teadmised, mis on vajalikud CSI-FiSh-i ülesehituse mõistmiseks. Kuna elliptkõvera endomorfismid moodustavad ringi, siis keskendub see peatükk endomorfismide ringi uurimisele ringiteoreetiliselt vaatepunktist. Peatükk on võrdlemisi ülevaatlik, kuid annab piisava, et vaadeldavat skeemi mõista.

Töö kolmandas ning viimases peatükis kirjeldame CSI-FiSh-i ennast, räägime, miks on skeemi kasutamiseks mõistlik valida just supersingulaarsed kõverad ning tutvustame erinevaid parendusi, mis algsele skeemile rakendati, et saada praegusel kujul välja pakutud CSI-FiSh.

1 Matemaatiline taust

1.1 Elliptkõver üle korpuse $\mathbb{K}$

Antud töös vaatleme elliptkõveraid vaid üle korpuste. Elliptkõverat on võimalik defineerida kahte tüüpi võrrandite abil, millest lihtsama ülesehitusega nõuab, et korpus, üle mille me teda defineerime, ei oleks karakteristikaga 2 või 3. Esitame definitsiooni algul üle suvalise korpuse.

Definitsioon 1.1. ([1, lk. 10, valem 2.1]) *Elliptkõver* üle korpuse $\mathbb{K}$ on võrrandit

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$$

rahuldavate paaride $(x, y) \in \mathbb{K} \times \mathbb{K}$ hulk, kus $a_1, \ldots, a_5 \in \mathbb{K}$. Selliseid paare (x, y) kutsutakse elliptkõvera *punktideks* ning neid punkte defineerivat võrrandit nimetatakse *üldistatud Weierstrassi võrrandiks*.

Kui korpuse karakteristika pole 2, on meil võimalik jagada kahega ning saame seeläbi moodustada võrrandi vasakule poolele täisruudu

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_5\right),$$

mida on võimalik muutuja vahetuse $y_1 = y + \frac{a_1x}{2} + \frac{a_3}{2}$ ning uute konstantide a_2', a_4', a_5' abil viia kujule

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_5'.$$

Kui korpuse karakteristika pole ka 3, on võimalik jagada kolmega ning muutuja vahetusega $x = x_1 - \frac{a_2'}{3}$ saame võrrandi kujul

$$y_1^2 = x_1^3 + Ax_1 + B, \tag{1}$$

kus $A, B \in \mathbb{K}$. Antud kujul võrrandit nimetatakse *Weierstrassi võrrandiks* ning kui pole öeldud teisiti, kasutame edaspidi elliptkõverast rääkides seda kuju [1, lk. 10].

Et defineerida mõistlikul viisil liitmine elliptkõveral, peame lisama tema punktide hulka ka n-ö *lõpmatuspunkti* (∞, ∞), mida tähistame lihtsalt märgiga ∞. Meil on võimalus vaadelda elliptkõveraid ka üle $\mathbb{K}$ alamkorpuste või üle mõne teda sisaldava korpuse. Kui tahame vaadelda elliptkõvera punkte, mille koordinaadid on korpusest $\mathbb{K}$, siis tähistame seda kirjutisega $E(\mathbb{K})$ ning mõistame selle all punktihulka, kuhu on lisatud ka lõpmatuspunkt ehk

$$E(\mathbb{K}) = \{\infty\} \cup \{(x, y) \in \mathbb{K} \times \mathbb{K} \mid y^2 = x^3 + Ax + B\}.$$

Näide 1. [1, lk. 95] Leiame kõik elliptkõvera E punktid üle korpuse $\mathbb{Z}_5$, kus E on antud võrrandiga $y^2 = x^3 + x + 1$. Selleks leiame kõik avaldise $x^3 + x + 1$ võimalikud väärtused ning võtame neist ruutjuured.

x	$x^3 + x + 1$	Punktid
0	1	$(0,1), (0,4)$
1	3	$--$
2	1	$(2,1), (2,4)$
3	1	$(3,1), (3,4)$
4	4	$(4,2), (4,3)$
∞	∞	∞

Näeme, et hulgas $E(\mathbb{Z}_5)$ on 9 elementi. Tähistame seda ka kui $\#E(\mathbb{Z}_5) = 9$.

Peatüki lõpetuseks toome ühe tähtsa tulemuse elliptkõvera punktide arvu kohta üle lõplike korpuste.

Teoreem 1 (Hasse teoreem)**.** [1, lk. 97, 4.2] *Olgu E elliptkõver üle lõpliku korpuse $\mathbb{F}_q$. Siis kehtib järgmine võrratus:*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Ehk teisisõnu, igal elliptkõveral üle lõpliku korpuse $\mathbb{K}$ on enam-vähem sama palju $\mathbb{K}$-ratsionaalseid punkte, kui korpuses endas elemente.

1.2 Elliptkõver kui rühm

Kui vaatleme elliptkõverat üle reaalarvude, siis on võimalik defineerida liitmistehe, kus kahe punkti summa saadakse, kui joonestatakse sirge läbi antud punktide, võetakse punkt, kus sirge lõikab kõverat kolmandat korda, ning peegeldatakse seda punkti x-telje suhtes. Selle summapunkti koordinaate on võimalik kirjeldada mugavalt ratsionaalfunktsioonide abil [1, lk. 14].

Kui defineerida punkti liitmine iseendale kasutades sirge asemel, mis läbib kahte erinevat punkti, puutujat selles punktis, siis saab puutuja teist lõikepunkti kõveraga üle x-telje peegeldada ning defineerida niimoodi punkti liitmine enesele [1, lk. 14]. Selleks peame oleme kindlad, et polünoomil $x^3 + Ax + B$ poleks kordseid juuri ning see on samaväärne tingimusega $4A^3 + 27B^2 \neq 0$ [1, lk. 9].

Viimaks, kui defineerida sama x-koordinaadiga punktide summa kui ∞, saame, et punktide hulk moodustab Abeli rühma liitmise suhtes, kus ∞ on rühma ühikelement [1, lk. 14-15].

Antud operatsioonid on analüütiliselt väljendatud järgnevalt ning kehtivad üle suvaliste korpuste.

Teoreem 2. [1, lk. 14] *Olgu elliptkõver E kujul (1), kehtigu $4A^2 + 27B^2 \neq 0$ ning olgu $P_1 = (x_1, y_1)$ ja $P_2 = (x_2, y_2)$ punktid sellel kõveral, kusjuures $P_1, P_2 \neq \infty$. Defineerime punkti $P_1 + P_2 = P_3 = (x_3, y_3)$ järgmiselt:*

1. *Kui $x_1 \neq x_2$, siis*

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{kus } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

2. *Kui $x_1 = x_2$, aga $y_1 \neq y_2$, siis $P_1 + P_2 = \infty$.*

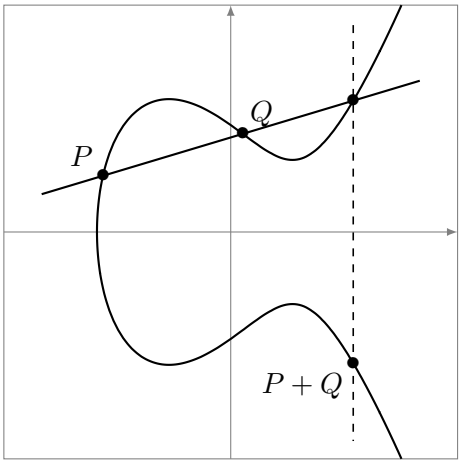
3. *Kui $P_1 = P_2$ ja $y_1 \neq 0$, siis*

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{kus } m = \frac{3x_1^2 + A}{2y_1}.$$

4. *Kui $P_1 = P_2$ ja $y_1 = 0$, siis $P_1 + P_2 = \infty$.*

5. *Iga $P \in E$ korral $P + \infty = P$.*

Hulk $E(K)$ on Abeli rühm selliselt defineeritud liitmistehte suhtes. Selle rühma ühikelement on ∞ ning elemendi $P = (x, y)$ vastandelement on $-P = (x, -y)$.



Joonis 1: Punktide P ja Q liitmine elliptkõveral [2]

Märgime ka, et selleks, et punkti liitmine iseendale oleks alati defineeritav, peab elliptkõvera igas punktis leiduma üheselt määratud puutuja. Kui punktis ei leidu elliptkõverale üheselt määratud puutujat, siis kutsutakse seda punkti *singulaarseks* ning kõverat, millel leidub singulaarseid punkte nimetatakse analoogiliselt

singulaarseks kõveraks. Punkti singulaarsus on samaväärne sellega, et funktsiooni $F(x, y) = y^2 - x^3 - Ax - B$ osatuletised mõlema muutuja järgi antud punktis on korraga võrdsed nulliga st. punkt $P = (x_0, y_0)$ on singulaarne, kui

$$\frac{\partial F}{\partial y}(x_0, y_0) = 2y_0 = 0, \quad \frac{\partial F}{\partial x}(x_0, y_0) = -3x_0^2 - A = 0.$$

Oletame, et vaatluse all olev punkt $P = (x_0, y_0)$ on singulaarne. Siis saame, et $y_0 = 0$ ning kui defineerime $f(x) = x^3 + Ax + B$ kui Weierstrassi võrrandi parema poole, siis saame, et $f(x_0) = y_0^2 = 0$ ning $f'(x_0) = 3x_0^2 + A = 0$, sest $-f'(x_0) = \frac{\partial F}{\partial x}(x_0, y_0) = 0$. Seega näeme, et singulaarse punkti P $x-$koordinaat on polünoomi f kahekordne juur ning samuti, kui x_0 on f-i vähemalt kahekordne juur, siis on $(x_0, 0)$ elliptkõvera singulaarne punkt. Seega ei tohi rühmatehte defineerimiseks lubada polünoomile f kordseid juuri ehk samaväärselt $4A^2 + 27B^3 \neq 0$ [3, lk. 20-21].

1.3 Supersingulaarsed elliptkõverad

Olgu $n \in \mathbb{N}$ ning tähistagu $\overline{\mathbb{K}}$ korpuse $\mathbb{K}$ algebralist sulundit.

Definitsioon 1.2. [1, lk. 77] Elliptkõvera $E(\mathbb{K})$ *n-väänderühmaks* nimetame rühma $E(\overline{\mathbb{K}})$ alamrühma

$$E[n] = \{P \in E(\overline{\mathbb{K}}) \mid nP = \infty\},$$

kus nP tähistab summat

$$nP = \underbrace{P + P + \ldots + P}_{n \text{ liidetavat}}. \tag{2}$$

Täheldame, et summale (2) viitame töös veel hiljem mitu korda kuid seda täisarvude kontekstis. Selleks peame mainima, et kui $a \in \mathbb{Z}$ ja $a < 0$, siis liidame iseendale punkti P vastandelementi.

Näide 2. [1, lk. 47-49, 77–78] Leiame $3-$väänderühma $E[3]$ elliptkõverale üle korpuse, mille karakteristika pole 2 ega 3. Seega saame esitada elliptkõvera kujul $y^2 = x^3 + Ax + B$. Peame leidma kõik punktid $P \in \overline{\mathbb{K}} \times \overline{\mathbb{K}}$ nii, et $3P = \infty$. See on samaväärne tingimusega $2P = -P$, mis omakorda tähendab, et $2P$ ja P $x-$koordinaadid on samad ning $y-$koordinaadid erinevad vaid märgi poolest (kui $y-$koordinaadid ühtiksid, saaksime, et $2P = P$, millest järeldub, et $P = \infty$).

Kasutades elliptkõvera rühmatehte koordinaatvalemeid saame, et

$$m^2 - 2x = x, \quad \text{kus } m = \frac{3x^2 + A}{2y}.$$

Kasutades teadmist, et $y^2 = x^3 + Ax + B$ saame, et

$$\begin{aligned}
\left(\frac{3x^2 + A}{2y}\right)^2 &= 3x, \\
\frac{(3x^2 + A)^2}{4y^2} &= 3x, \\
(3x^2 + A)^2 &= 12xy^2, \\
(3x^2 + A)^2 &= 12x(x^3 + Ax + B), \\
9x^4 + 6Ax^2 + A^2 &= 12x^4 + 12Ax^2 + 12Bx, \\
3x^4 + 6Ax^2 + 12Bx - A^2 &= 0.
\end{aligned}$$

On võimalik näidata, et võrrandi vasakul poolel asuval polünoomil pole kordseid juuri. Seega leidub 4 erinevat x väärtust korpuses $\overline{\mathbb{K}}$, mis seda võrdust rahuldavad. Kuna iga x-i kohta on elliptkõveral 2 punkti, siis saame, et rühmas $E[3]$ on koos lõpmatuspunktiga 9 erinevat elliptkõvera punkti ning seega saame, et

$$E[3] \cong \mathbb{Z}_3 \times \mathbb{Z}_3.$$

Järgnev teoreem on selle näite üldistus.

Teoreem 3. [1, lk. 79, teoreem 3.2] *Olgu $E(\mathbb{K})$ elliptkõver üle korpuse $\mathbb{K}$ ning olgu $n \in \mathbb{N}$. Kui korpuse $\mathbb{K}$ karakteristika ei jaga arvu n või on 0, siis*

$$E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n.$$

Kui korpuse karakteristika on $p > 0$, kus p on algarv ja $p \mid n$, siis võttes $n = p^r n'$, kus $p \nmid n'$ saame, et

$$E[n] \cong \mathbb{Z}_{n'} \times \mathbb{Z}_{n'} \qquad \text{või} \qquad E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_{n'}.$$

Definitsioon 1.3. [1, lk. 79] Kui korpuse $\mathbb{K}$ karakteristika on p, siis elliptkõverat $E(\mathbb{K})$ nimetatakse *harilikuks*, kui $E[p] \cong \mathbb{Z}_p$ ning elliptkõverat nimetatakse *supersingulaarseks*, kui $E[p] \cong 0$ st. ainus kõvera punkt järguga p on ∞.

Tuleb ka märkida ära, et supersingulaarsed kõverad ja singulaarsed kõverad (need, mis omavad singulaarseid punkte) ei ole omavahel tähenduslikult seotud mõisted.

Peatüki lõpetuseks toome kaks samaväärset tingimust elliptkõvera supersingulaarsusega üle lõplike korpuste.

Lause 1. [1, lk.130, 4.31] *Olgu E elliptkõver üle lõpliku korpuse $\mathbb{F}_q$, kus $q = p^r$, $r \in \mathbb{N}$ ja p on algarv. Olgu $a = q + 1 - \#E(\mathbb{F}_q)$. Kõver E on supersingulaarne siis ja ainult siis, kui $a \equiv 0 \pmod{p}$, mis juhtub parajasti siis, kui $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$.*

Järeldus 3.1. [1, lk 131, 4.32] *Olgu $p \geq 5$ algarv ning olgu elliptkõver E defineeritud üle lõpliku korpuse $\mathbb{F}_p$. E on supersingulaarne siis ja ainult siis, kui $a = 0$, mis juhtub parajasti siis, kui $\#E(\mathbb{F}_p) = p + 1$.*

Tõestus. Kui $a = 0$, siis E on supersingulaarne tänu eelnevale lausele. Oletame, et E on supersingulaarne, aga $a \neq 0$. Seetõttu, kui $a \equiv 0 \pmod{p}$, siis $|a| \geq p$. Hasse teoreemist teame, et $|a| \leq 2\sqrt{p}$ ehk $p \leq 2\sqrt{p}$. Sellest järeldame, et $p \leq 4$, mis on vastuolu. □

1.4 j-invariant

Olgu elliptkõver E kujul (1). Viime läbi muutujavahetuse

$$x = \frac{x_1}{\mu^2}, \quad y = \frac{y_1}{\mu^3}, \tag{3}$$

milles $\mu \in \overline{\mathbb{K}}^\times$, kus $\overline{\mathbb{K}}^\times$ on korpuse $\mathbb{K}$ algebralise sulundi nullist erinevate elementide multiplikatiivne rühm.

Saame, et

$$y_1^2 = x_1^3 + A_1 x_1 + B_1,$$

kus $A_1 = \mu^4 A$ ja $B_1 = \mu^6 B$ [1, lk. 45-46].

Definitsioon 1.4. [1, lk. 46] Elliptkõvera E *j-invariandiks* nimetame korpuse $\mathbb{K}$ elementi

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Märgime ära, et kuna vaatleme kordsete juurteta kõveraid, siis murru nimetajas asuv avaldis erineb nullist. Järgnev teoreem väidab, et kui elliptkõveral viia läbi muutujavahetus (3), siis uue kõvera ning algse kõvera j-invariandid on samad. Samuti, kui kahe kõvera j-invariandid on võrdsed, siis on võimalik sobiva μ korral muuta antud muutujavahetusega üks kõver teiseks. Kuna (3) on pööratav protsess tänu μ pööratavusele, siis on sama $j-$invariandiga kõverad isomorfsed üle $\overline{\mathbb{K}}$ st kui kõveratel E_1 ja E_2 on ühine j-invariant, siis leidub rühmade isomorfism $\alpha\colon E_1(\overline{\mathbb{K}}) \to E_2(\overline{\mathbb{K}})$.

Teoreem 4. [1, lk. 46, 2.19] *Olgu $y_1^2 = x_1^3 + A_1 x_1 + B_1$ ja $y_2^2 = x_2^3 + A_2 x_2 + B_2$ elliptkõverad, mille $j-$invariandid on vastavalt j_1 ning j_2. Kui $j_1 = j_2$, siis leidub $\mu \in \overline{\mathbb{K}}^\times$ nii, et*

$$A_2 = \mu^4 A_1 \quad ja \quad B_2 = \mu^6 B_1.$$

Muutuja vahetus

$$x_2 = \mu^2 x_1, \quad y_2 = \mu^3 y_1$$

muudab esimese kõvera teiseks kõveraks.

Tõestus. Oletame, et $A_1 \neq 0$. See on samaväärne sellega, et $j_1 \neq 0$, mistõttu $j_2 \neq 0$ ning $A_2 \neq 0$. Valides $\mu \in \overline{\mathbb{K}}^\times$ nii, et $A_2 = \mu^4 A_1$ (selline μ leidub, sest oleme algebraliselt kinnises korpuses) saame

$$\frac{4A_2^3}{4A_2^3 + 27B_2^2} = \frac{4A_1^3}{4A_1^3 + 27B_1^2} = \frac{4\mu^{-12}A_2^3}{4\mu^{-12}A_2^3 + 27B_1^2} = \frac{4A_2^3}{4A_2^3 + 27\mu^{12}B_1^2},$$

millest järeldub, et

$$B_2^2 = (\mu^6 B_1)^2.$$

Seetõttu $B_2 = \pm\mu^6 B_1$. Kui $B_2 = \mu^6 B_1$, on teoreem tõestatud. Kui $B_2 = -\mu^6 B_1$, siis võttes avaldises μ asemele $i\mu$, kus $i^2 = -1$, saame, et kehtivad korraga $A_2 = \mu^4 A_1$ ning $B_2 = \mu^6$.

Kui $A_1 = 0$, siis ka $A_2 = 0$. Kuna eelduse kohaselt $4A_i^3 + 27B_i^2 \neq 0$, kus $i = 1, 2$, siis $B_1, B_2 \neq 0$. Seetõttu piisab vaid valida $\mu \in \overline{\mathbb{K}}^\times$ nii, et $B_2 = \mu^6 B_1$. □

Paneme tähele, et kuna $\mu \in \overline{\mathbb{K}}^\times$, siis on muutuja vahetus (3) pööratav ning seetõttu on vastavad elliptkõverad isomorfsed üle $\overline{\mathbb{K}}$. Seetõttu omab sügavamat tähendust järgmine definitsioon.

Definitsioon 1.5. [1, lk. 47] Kui kaks elliptkõverat üle korpuse $\mathbb{K}$ on sama $j-$invariandiga, siis öeldakse, et vastavad elliptkõverad on teineteise *väänded*.

1.5 Endomorfismid

Definitsioon 1.6. [1, lk.50] Elliptkõvera E *endomorfismi* all mõistame rühmade homomorfismi $\alpha\colon E(\overline{\mathbb{K}}) \to E(\overline{\mathbb{K}})$, mis on väljendatud ratsionaalfunktsioonide abil. See tähendab, et $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$ ning leiduvad ratsionaalfunktsioonid $R_1(x, y)$,$R_2(x, y)$, mille kordajad on korpusest $\overline{\mathbb{K}}$, nii et

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)).$$

Kui $\alpha(x, y) = \infty$ iga $(x, y) \in E(\overline{\mathbb{K}})$ korral, tähistame $\alpha = 0$. Selline kujutus on endomorfism ning kutsume teda *nullendomorfismiks*.

Paneme tähele, et igal elliptkõveral leiduvad endomorfismid

$$a : E(\overline{\mathbb{K}}) \to E(\overline{\mathbb{K}}), \quad P \to aP,$$

kus $a \in \mathbb{Z}$ ning aP on defineeritud võrdusega (2) [1, lk. 311]. Siin ja edaspidi kuritarvitame sümboolikat ning tähistame täisarvu ja täisarvule vastavat endomorfismi sama tähisega. Samuti märkame, et antud ratsionaalfunktsioonide nimetajad peavad erinema nullist iga punktipaari $(x, y) \in E(\overline{\mathbb{K}})$ korral, et endomorfism saaks olla defineeritud. Et sellele probleemile sobivalt läheneda, leiame ratsionaalfunktsioonidele mugavad üldkujud.

Olgu meil suvaline ratsionaalfunktsioon $R(x, y)$ ning täheldame, et alati kehtib võrdus $y^2 = x^3+Ax+B$. Seetõttu saame $R(x, y)$-s asendada iga y paarisarvulise astme mingi teatud polünoomiga $p(x)$ ning iga paarituarvulise y astme saame asendada mingi polünoomiga $p(x)$, mis on korrutatud läbi y-ga. Seetõttu saame funktsiooni $R(x, y)$ esitada kujul

$$R(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}.$$

Kui korrutame murru lugejat ja nimetajat avaldisega $p_3(x) - p_4(x)y$ ja asendades tekkiva liikme y^2 avaldisega $x^3 + Ax + B$, saame viia murru kujule

$$R(x, y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{4}$$

Vaadeldes nüüd suvalist endomorfismi $\alpha(x, y) = (R_1(x, y), R_2(x, y))$ näeme, et kuna ta on homomorfism, siis

$$\alpha(x, -y) = \alpha(-(x, y)) = -\alpha(x, y),$$

mistõttu $R_1(x, -y) = R_1(x, y)$ ning $R_2(x, y) = -R_2(x, y)$. Seetõttu näeme, et kui ratsionaalfunktsioonid on antud kujul (4), siis R_1 puhul $q_2(x) = 0$ ja R_2 puhul $q_1(x) = 0$. Seetõttu saame eeldada, et meie endomorfism α on kujul

$$\alpha(x, y) = (r_1(x), r_2(x)y),$$

kus $r_1(x), r_2(x)$ on ratsionaalfunktsioonid [1, lk. 50-51].

Vaatleme nüüd juhtu, kus üks ratsionaalfunktsioonidest pole mõnes punktis defineeritud. Kirjutame r_1 kujul

$$r_1(x) = p(x)/q(x),$$

kus polünoomidel $p(x)$ ja $q(x)$ pole ühiseid tegureid. Kui $q(x) = 0$ mingi teatud punkti (x, y) korral, siis defineerime $\alpha(x, y) = \infty$. Näitame, et kui $q(x) \neq 0$, siis on korrektselt defineeritud ka r_2.

Olgu

$$\alpha(x, y) = (p(x)/q(x), y \cdot s(x)/t(x))$$

elliptkõvera E endomorfism, kus E on kujul (1) ning p, q, s, t on sellised polünoomid, kus p ja q ei oma ühiseid juuri ning s ja t ei oma ühiseid juuri. Näitame, et leidub polünoom $u(x)$ nii, et q ja u ei oma ühiseid juuri ning

$$\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3}.$$

Selleks fikseerime punktid $(x,y),(x_0,y_0) \in E(\overline{\mathbb{K}})$ nii, et $\alpha(x,y)=(x_0,y_0)$. Saame, et

$$\frac{(x^3+Ax+B)s(x)^2}{t(x)^2} = \frac{y^2 s(x)^2}{t(x)^2} = y_0^2 = x_0^3 + Ax_0 + B = \\ = \frac{p(x)^3}{q(x)^3} + \frac{Ap(x)}{q(x)} + B = \frac{p(x)^3 + Ap(x)q(x)^2 + Bq(x)^3}{q(x)^3}.$$

Oletame nüüd, et leidub $a \in \overline{\mathbb{K}}$ nii, et $q(a)=0$ ning $p(a)^3+Ap(a)q(a)^2+Bq(a)^3=0$. Sellest järeldub, et $p(a)^3=0$. Siis $p(a)=0$, sest korpuses pole nullitegureid. See on vastuolus eeldusega, et p ja q ei oma ühiseid juuri. Seega sobib valida $u(x)=p(x)^3+Ap(x)q(x)^2+Bq(x)^3$.

Nüüd tõestame, et $t(x_0)=0 \Rightarrow q(x_0)=0$ ehk samaväärselt $q(x_0)\neq 0 \Rightarrow t(x_0)\neq 0$. Eeldame, et $t(x_0)=0$. Eelnevast teame, et

$$t(x)^2 u(x) = (x^3+Ax+B)s(x)^2 q(x)^3.$$

Võrduse vasakus pooles esineb eelduse kohaselt tegur $(x-x_0)$ vähemalt kaks korda. Kuna kehtib võrdus ning asume algebraliselt kinnises korpuses, siis peab ta esinema ka paremas pooles vähemalt kaks korda. Oleme eeldanud ning eeldame praegugi, et polünoomil x^3+Ax+B pole kordseid juuri, seega saab vaid üks teguritest $(x-x_0)$ esineda tema lineaarliikmeteks lahutuses. Kuna polünoomidel s ja t eelduse kohaselt ühiseid juuri ei esine, siis peab teine tegur esinema polünoomi $q(x)^3$ lahutuses. Kuna polünoomide ring $\overline{\mathbb{K}}[x]$ on faktoriaalne, siis esineb tegur $(x-x_0)$ polünoomi $q(x)$ lahutuses ehk samaväärselt $q(x_0)=0$.

Sellega oleme näidanud, et r_1 defineeritusest punktis piisab ka r_2 defineerituseks. Seetõttu on õigustatud järgmistes definitsioonides vaid r_1 vaatlus. Märgime veel, et endomorfismid moodustavad ringi, kus liitmistehe on defineeritud võrdusega $(f+g)(x,y)=f(x,y)+g(x,y)$ ning korrutamine on endomorfismide komponeerimine.

Definitsioon 1.7. [1, lk. 51] Kui $\alpha \neq 0$, siis nimetame α *astmeks* naturaalarvu

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\}.$$

Kui $\alpha=0$, siis määrame $\deg(\alpha)=0$. Endomorfismi $\alpha\neq 0$ nimetame *eralduvaks*, kui tuletis $r_1'(x)$ pole samaselt null. On võimalik näidata, et see on samaväärne sellega, et vähemalt üks tuletistest $p'(x)$ või $q'(x)$ pole samaselt null.

Näide 3. [1, lk. 50, 52] Olgu E elliptkõver kujul (1) ning olgu $\alpha(P)=2P$ iga $P\in E(\overline{\mathbb{K}})$ korral. Paneme tähele, et α on rühmade homomorfism ning

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)),$$

kus

$$R_1(x,y) = \left(\frac{3x^2+A}{2y}\right)^2 - 2x,$$

$$R_2(x,y) = \left(\frac{3x^2+A}{2y}\right)\left(3x - \left(\frac{3x^2+A}{2y}\right)^2\right) - y.$$

Näeme, et tegemist on endomorfismiga. Viime nüüd R_1 kujule, kus ta sõltub ainult muutujast x ning uurime α astet ning eralduvust. Niisiis

$$\begin{aligned} R_1(x,y) &= \left(\frac{3x^2+A}{2y}\right)^2 - 2x = \frac{9x^4+6Ax^2+A^2-8xy^2}{4y^2} = \\ &= \frac{9x^4+6Ax^2+A^2-8x(x^3+Ax+B)}{4(x^3+Ax+B)} = \frac{x^4-2Ax^2-8Bx+A^2}{4(x^3+Ax+B)} \\ &=: r_1(x). \end{aligned}$$

Näeme, et $\deg(\alpha) = 4$ ning et α on eralduv, sest nii lugeja kui ka nimetaja tuletis ei ole samaselt nullid (korpuse karakteristika ei ole 2 ega 3).

1.6 Isogeensed teisendused

Definitsioon 1.8. [1, lk. 386-387] Olgu meil kaks elliptkõverat

$$E_1 \colon y_1^2 = x_1^3 + A_1x_1 + B_1 \quad \text{ja} \quad E_2 \colon y_2^2 = x_2^3 + A_2x_2 + B_2$$

üle korpuse $\mathbb{K}$. *Isogeenseks teisenduseks* kõverate E_1 ja E_2 vahel on mittekonstantne homomorfism $\alpha \colon E_1(\overline{\mathbb{K}}) \to E_2(\overline{\mathbb{K}})$, mis on väljendatud ratsionaalfunktsioonide kaudu.

See tähendab, et elliptkõvera nullist erinevad endomorfismid on isogeensed teisendused rühmast $E_1(\overline{\mathbb{K}})$ iseendasse. Analoogiliselt endomorfismidega defineeritakse isogeensete teisenduste *aste* ning *eralduvus*.

Lause 2. [1, lk. 387, 12.8] *Olgu $\alpha \colon E_1 \to E_2$ isogeenne teisendus. Märgime ära, et isogeense teisenduse tuum on rühma $E_1(\overline{\mathbb{K}})$ lõplik alamrühm. Kui α on eralduv, siis*

$$\deg \alpha = \# \ker(\alpha).$$

Kui α pole eralduv, siis

$$\deg \alpha > \# \ker(\alpha).$$

Tõestus. Olgu

$$\alpha(x,y) = (r_1(x), yr_2(x)),$$

kus $r_1(x) = p(x)/q(x)$, kus p ja q ei oma ühiseid tegureid. Eeldame, et α on eralduv. Seega $r_1' \neq 0$, mistõttu $pq' - p'q$ pole nullpolünoom.

Defineerime hulga

$$S = \{x \in \overline{\mathbb{K}} \mid (pq' - p'q)(x)q(x) = 0\}.$$

Näitame, et leidub punkt $(a,b) \in E_2(\overline{\mathbb{K}})$, mis rahuldab järgnevaid tingimusi:

- $a \neq 0$, $b \neq 0$, $(a, b) \neq \infty$,
- $\deg(p(x) - aq(x)) = \max\{\deg(p), \deg(q)\} = \deg(\alpha)$,
- $a \notin r_1(S)$,
- $(a, b) \in \alpha(E_1(\overline{\mathbb{K}}))$.

Kuna $pq' + p'q$ pole nullpolünoom, siis S on lõplik hulk ning seega on selle hulga kujutis funktsiooni r_1 korral lõplik. Hulga $\overline{\mathbb{K}}$ kujutis sama funktsiooni korral on aga lõpmatu. Kuna hulgas $E_1(\overline{\mathbb{K}})$ leidub iga x korral punkt (x, y), siis on hulk $\alpha(E_1(\overline{\mathbb{K}}))$ lõpmatu hulk. Seetõttu leidub selline punkt (a, b), mis ülaltoodud tingimusi rahuldab.

Soovime tõestada, et leidub täpselt $\deg(\alpha)$ punkti $(x_1, y_1) \in E_1(\overline{\mathbb{K}})$ nii, et kehtib $\alpha(x_1, y_1) = (a, b)$. α definitsiooni kohaselt kehtib sellise võrduse korral

$$\frac{p(x_1)}{q(x_1)} = a, \quad y_1 r_2(x_1) = b.$$

Kuna $(a, b) \neq \infty$, siis $q(x_1) \neq 0$. Teame eelnevast, et sel juhul on defineeritud ka $r_2(x_1)$, st. r_2-e nimetajas ei teki nulli. Kuna $b \neq 0$ ja $y_1 r_2(x_1) = b$, siis $y_1 = b/r_2(x_1)$. Näeme, et y_1 väärtus oleneb üheselt x_1 väärtusest ning seega peame otsitavate punktide arvu leidmiseks lugema vaid võimalikke x_1 väärtuseid.

Teise tingimuse põhjal, mis me punktile (a, b) seadsime, saame väita, et polünoomil $p(x) - aq(x)$ on täpselt $\deg(\alpha)$ juurt, kuid mõned neist võivad olla kordsed. Näitame, et tema kõik juured on siiski ühekordsed. Oletame, et x_0 on antud polünoomi kordne juur. Sel juhul teame algebrast, et

$$p(x_0) - aq(x_0) = 0 \quad \text{ja} \quad p'(x_0) - aq'(x_0) = 0.$$

Korrutades omavahel võrdused $p(x_0) = aq(x_0)$ ja $aq'(x_0) = p'(x_0)$ saame, et

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0).$$

Kuna $a \neq 0$, siis saame, et x_0 on polünoomi $pq' - p'q$ juur ning seega $x_0 \in S$. Seetõttu $a = r_1(x_0) \in r_1(S)$, mis on vastuolus meie eeldusega punkti (a, b) kohta. Seetõttu pole polünoomil $p - aq$ kordseid juuri ning seega on tal $\deg(\alpha)$ erinevat juurt. Seetõttu on täpselt $\deg(\alpha)$ sellist punkti (x_1, y_1), mille korral $\alpha(x_1, y_1) = (a, b)$ ning kuna α on homomorfism, siis piisab seda leida vaid ühe punkti (a, b) korral, et väita, et α tuumas on $\deg(\alpha)$ elementi.

Kui α poleks eralduv, siis jääks kehtima kõik ülaltoodu, kuid $p' - aq'$ on alati nullpolünoom, mistõttu on polünoomil $p - aq$ alati kordseid juuri ehk erinevate juurte koguarv on väiksem arvust $\deg(\alpha)$. □

Lause 3. [1, lk. 387, 12.9] *Isogeenne teisendus* $\alpha\colon E_1(\overline{\mathbb{K}}) \to E_2(\overline{\mathbb{K}})$ *on sürjektiivne.*

Tõestus. Olgu $(a,b) \in E_2(\overline{\mathbb{K}})$. Kuna $\alpha(\infty) = \infty$, siis piisab vaadelda juhtu, kus $(a,b) \neq \infty$. Samuti olgu $r_1(x) = p(x)/q(x)$, kus p ja q ei oma ühiseid juuri. Teame, et kui $p(x) - aq(x)$ pole konstantne polünoom, siis tal leidub juur x_0. Kuna p ja q ei oma ühiseid juuri, siis $q(x_0) \neq 0$. Olgu $y_0 \in \overline{\mathbb{K}}$ üks lahenditest võrrandile $y_0^2 = x_0^2 + Ax_0 + B$. Kuna teame, et $q(x_0) \neq 0$, siis on defineeritud ka $\alpha(x_0, y_0)$ ning $\alpha(x_0, y_0) = (a, b')$, kus $b' \in \overline{\mathbb{K}}$. Kuna b' rahuldab võrdust $b' = a^3 + Aa + B = b^2$, siis kehtib $b = \pm b'$. Juhul kui $b' = b$, siis $\alpha(x_0, y_0) = (a, b)$. Kui $-b' = b$, siis $\alpha(x_0, -y_0) = -\alpha(x_0, y_0) = -(a, b') = (a, -b') = (a, b)$.

Nüüd vaatame juhtu, kus $p - aq$ on konstantne polünoom. Kuna $E_2(\overline{\mathbb{K}})$ on lõpmatu hulk ning $\ker \alpha$ on lõplik, siis on vaid lõplik arv punkte hulgas $E_1(\overline{\mathbb{K}})$, mis saavad kujutuda mingile fikseeritud punktile $(x, y) \in E_2(\overline{\mathbb{K}})$. Seetõttu peab olema kas p või q mittekonstantne.

Kui p ja q on mõlemad mittekonstantsed polünoomid, siis leidub täpselt üks konstant $a \in \overline{\mathbb{K}}$ nii, et $p - aq$ on konstantne. Tõepoolest, kui a' oleks teine selline konstant, siis saame, et

$$(a' - a)q = (p - aq) - (p - a'q)$$

on konstantne ning et

$$(a' - a)p = a'(p - aq) - a(p - a'q)$$

on konstantne ning seega p ja q oleks korraga konstantsed polünoomid, mis on vastuolu. Seega leidub ülimalt kaks sellist punkti, (a, b) ning $(a, -b)$, kus $b \in \overline{\mathbb{K}}$, mis ei kuulu α kujutisse. Olgu $(a_1, b_1) \in \alpha(E_1(\overline{\mathbb{K}}))$ ükskõik milline teine punkt. Sel juhul leidub $P_1 \in E_1(\overline{\mathbb{K}})$ nii, et $\alpha(P_1) = (a_1, b_1)$. Kuna meil on võimalik valida (a_1, b_1) nii, et $(a_1, b_1) + (a, b) \neq (a, \pm b)$, siis leidub $P_2 \in E_1(\overline{\mathbb{K}})$ nii, et $\alpha(P_2) = (a_1, b_1) + (a, b)$. Siis $\alpha(P_2 - P_1) = (a, b)$ ning $\alpha(P_1 - P_2) = (a, -b)$. Seega α on sürjektiivne. □

Rühmade homomorfismiteoreemist järeldub vahetult järgmine tulemus.

Järeldus 4.1. *Kui $\alpha\colon E_1(\overline{\mathbb{K}}) \to E_2(\overline{\mathbb{K}})$ on isogeenne teisendus kõverate E_1 ja E_2 vahel, mis on defineeritud üle korpuse $\mathbb{K}$, siis*

$$E_1(\overline{\mathbb{K}})/\ker \alpha \cong E_2(\overline{\mathbb{K}}).$$

Näide 4. [1, lk.388, 12.2] Olgu p paaritu algarv ning kuulugu A_1, B_1 korpusesse $\mathbb{K}$, mille karakteristika on p. Olgu $E_1\colon y_1^2 = x_1^3 + A_1x_1 + B_1$ ja $E_2\colon y_2^2 = x_2^3 + A_1^p x_2 + B_1^p$. Defineerime isogeense teisenduse järgnevalt

$$\phi_p(x_1, y_1) = (x_1^p, y_1^p) =: (x_2, y_2).$$

Oletame, et $x_1, y_1 \in \overline{\mathbb{K}}$ rahuldavad võrrandit $y_1^2 = x_1^3 + A_1x_1 + B_1$. Kui astendame mõlemaid võrrandi pooli p-ga, siis korpuses karakteristikaga p kehtib järgnev võrdus:

$$(y_1^p)^2 = (x_1^p)^3 + A_1^p x_1^p + B_1^p.$$

Kuna $x_2 = x_1^p$ ja $y_2 = y_1^p$, siis on ϕ_p korrektselt defineeritud st. tegemist on kujutusega $E_1(\overline{\mathbb{K}}) \to E_2(\overline{\mathbb{K}})$. Kasutades karakteristikaga astendamise omadust, saab kontrollida, et ϕ_p on rühmade homomorfism.

Teame, et

$$r_1(x) = x^p \quad \text{ja} \quad r_2(x) = (y^2)^{(p-1)/2} = (x^3 + A_1 x + B_1)^{(p-1)/2}.$$

Seega $\deg(\phi) = \deg r_1 = p$. On kerge näha, et $\ker \phi = \{\infty\}$, sest korpuses pole nullitegureid. Näeme, et teisenduse aste on seetõttu suurem kui tema tuuma võimsus ning see on kooskõlas ka faktiga, et ϕ pole eralduv. Näites kasutatud endomorfismi kutsutakse ka *Frobeniuse endomorfismiks*.

Kui soovida kontrollida, kas kaks elliptkõverat on isomorfsed rühmadena üle korpuse, tuleb välja arvutada nende j-invariant, kuid ilmneb, et on võimalik defineerida ka tugevamat sorti isomorfsus, mis on seotud isogeensete teisendustega.

Definitsioon 1.9. [1, lk. 389] Öeldakse, et elliptkõverad E_1 ja E_2 on *isomorfsed*, kui leiduvad rühmade homomorfismid $\beta\colon E_1(\overline{\mathbb{K}}) \to E_2(\overline{\mathbb{K}})$ ja $\gamma\colon E_2(\overline{\mathbb{K}}) \to E_1(\overline{\mathbb{K}})$ nii, et β ja γ on väljendatud ratsionaalfunktsioonidena ning $\gamma \circ \beta = \mathbf{1}_{E_1}$ ja $\beta \circ \gamma = \mathbf{1}_{E_2}$.

Järgnev tähtis tulemus näitab, et igal isogeensel teisendusel leidub sisuliselt pöördelement.

Teoreem 5. [1, lk. 391, 12.14] *Olgu $\alpha\colon E_1 \to E_2$ isogeenne teisendus. Leidub duaalne isogeenne teisendus $\widehat{\alpha}\colon E_2 \to E_1$, mille korral $\widehat{\alpha} \circ \alpha = \deg \alpha$, kus*

$$\deg \alpha\colon E_1 \to E_1, \quad P \to (\deg \alpha)P,$$

kus $(\deg \alpha)P$ on defineeritud võrdusega (2).

2 Eelteadmised CSI-FiSh-ile

2.1 Kompleksne korrutamine

Vaatleme nüüd lähemalt elliptkõverate endomorfismide ringi läbi kompleksse korrutamise mõiste.

Definitsioon 2.1. [1, lk. 311] Öeldakse, et elliptkõver E on *kompleksse korrutamisega*, kui tema endomorfismide ring $End(E)$ on rangelt suurem kui $\mathbb{Z}$, st $\mathbb{Z} \subset End(E)$.

Et vaadelda hulka $\mathbb{Z}$ endomorfismide teooria suhtes, siis peame seda mõistma nii, et iga $a \in \mathbb{Z}$ puhul on kujutus

$$a\colon E(\overline{\mathbb{K}}) \to E(\overline{\mathbb{K}}), \quad P \to aP$$

kõvera E endomorfism ning seda tüüpi teisendused moodustavad $End(E)$ alamringi, mis on isomorfne $\mathbb{Z}$-ga, mistõttu kirjutame $\mathbb{Z} \subseteq End(E)$. Sisalduvus $\mathbb{Z} \subset End(E)$ tähendab seda, et kõveral leidub rohkem endomorfisme kui ainult täisarvukordne punkti liitmine iseendale.

Ilmneb, et kõik elliptkõverad üle lõplike korpuste on kompleksse korrutamisega, kuid enne selle näitamist toome sisse paar mõistet algebralisest arvuteooriast.

Definitsioon 2.2. [1, lk. 314] Olgu $d > 0$ täisarv, mille standardkujus ei ole ühegi algarvu aste suurem ühest, ning olgu

$$K = \mathbb{Q}(\sqrt{-d}) = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Q}\}.$$

Sellist korpust K kutsutakse *imaginaar-ruutkorpuseks*. Paneme tähele, et K on kompleksarvude korpuse $\mathbb{C}$ alamkorpus [1, lk. 314].

Igasuguse lõplikumõõtmelise vektorruumi K puhul üle $\mathbb{Q}$ ehk samaväärselt iga korpuse $\mathbb{Q}$ laiendkorpuse K puhul, (see tähendab, et ka imaginaar-ruutkorpuse korral) saame defineerida K *järguringi* kui K alamringi $\mathcal{O}$, mis on samaaegselt ka samamõõtmeline moodul üle $\mathbb{Z}$-i [4, lk. 15, definitsioon 27].

Järguringe on iga vektorruumi puhul erinevaid, kuid hiljem märgime ära, et on võimalik leida neist maksimaalne.

2.2 Kompleksne korrutamine elliptkõveratel üle lõplike korpuste

Võtame teadmiseks, et kehtib järgnev väide.

Lause 4. [1, lk. 101, 4.10] *Olgu elliptkõver E defineeritud üle lõpliku korpuse $\mathbb{F}_q$ ning vaatleme Frobeniuse endomorfismi*

$$\phi_q \colon E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q}), \quad (x, y) \to (x^q, y^q).$$

Näites 4 näitasime, et tegemist on endomorfismiga. Kui $a = q + 1 - \#E(\mathbb{F}_q)$, siis

$$\phi_q^2 - a\phi_q + q = 0$$

elliptkõvera E endomorfismide ringis ehk kui $(x, y) \in E(\overline{\mathbb{F}}_q)$, siis

$$(x^{q^2}, y^{q^2}) - a(x^q, y^q) + q(x, y) = \infty.$$

Näitame, et elliptkõver E üle lõpliku korpuse $\mathbb{F}_q$ on alati kompleksse korrutamisega. Teame nüüd, et Frobeniuse endomorfism ϕ_q on polünoomi

$$X^2 - aX + q$$

juur, kus $a = q+1-\#E(\mathbb{F}_q)$, q on korpuse $\mathbb{F}_q$ võimsus ning nad mõlemad tähistavad endomorfisme kujul (2). Seetõttu saame Hasse teoreemi tõttu väita, et $|a| \leq 2\sqrt{q}$. Kui $|a| < 2\sqrt{q}$, siis näeme ruutvõrrandi lahendivalemis diskriminanti uurides, et sellel polünoomil on ainult komplekssed juured ning seega $\phi_q \notin \mathbb{Z}$. Seega

$$\mathbb{Z} \neq \mathbb{Z}[\phi_q] \subseteq End(E),$$

kus $\mathbb{Z}[\phi_q] = \{a + b\phi_q \mid a, b \in \mathbb{Z}\}$. On võimalik näidata, et kui $a = \pm 2\sqrt{q}$, siis on endomorfismide ring endiselt rangelt suurem kui $\mathbb{Z}$, mistõttu on ka siis kõveral kompleksne korrutamine [1][lk. 318].

Näitame järgnevalt, et kui vaatleme elliptkõverat, mis on defineeritud üle lõpliku korpuse, siis tema endomorfismide ring on järguring kvaternioonide algebras, mistõttu on see suurem kui järguring imaginaar-ruutkorpuses.

Definitsioon 2.3 (lk. 318)**.** [1] *Kvaternioonide algebra* on ring

$$\mathcal{Q} = \{a + b\alpha + c\beta + d\alpha\beta \mid a, b, c, d \in \mathbb{Q}\},$$

kus

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \quad \beta^2 < 0, \quad \beta\alpha = -\alpha\beta.$$

Kvaternioonide algebra on mittekommutatiivne ring, kus igal nullist erineval elemendil leidub pöördelement korrutamise suhtes ning selleks, et tuua hiljem konkreetne näide selle teooria rakendustest, defineerime ka ühe erijuhu kvaternioonidest.

Definitsioon 2.4 (lk. 318)**.** [1] *Hamiltoni kvaternioonid* on ring kujul

$$\mathbf{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{Q}\},$$

kus $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ ning $\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$.

Definitsioon 2.5. [1, lk. 319] Ütleme, et kvaternioonide algebra $\mathcal{Q}$ alamring $\mathcal{O}$ on *maksimaalne järguring*, kui ta on lõpliku baasiga Abeli rühm liitmise suhtes ning kui iga ringi $\mathcal{R}$ korral, kus $\mathcal{O} \subseteq \mathcal{R} \subseteq \mathcal{Q}$ ning kus $\mathcal{R}$ on lõpliku baasiga Abeli rühm liitmise suhtes, $\mathcal{O} = \mathcal{R}$.

Näide 5. [1][lk. 319] Vaatleme näiteks Hamiltoni kvaternioone $\mathbf{H}$. Alamring

$$\mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\mathbf{k}$$

on lõpliku baasiga Abeli rühm liitmise suhtes, kuid ta pole maksimaalne järguring kvaternioonide algebras, sest ta on ringi

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\frac{1 + \mathbf{i} + \mathbf{j} + \mathbf{k}}{2} \subset \mathbf{H}$$

alamring. On võimalik näidata, et hoopis $\mathcal{O}$ on Hamiltoni kvaternioonide maksimaalne järguring.

Järgnevalt sõnastame olulise tulemuse, mis annab ühe põhjustest, miks eelistatakse krüptograafilistes rakendustes supersingulaarseid kõveraid – nende endomorfismide ringid on suuremad kui tavalistel kõveratel.

Teoreem 6. [1][lk. 319, 10.6] *Olgu E elliptkõver defineeritud üle lõpliku korpuse, mille karakteristika on p. Siis*

1. *Kui E on harilik elliptkõver, siis $End(E)$ on isomorfne mingi järguringiga imaginaar-ruutkorpuses.*
2. *Kui E on supersingulaarne elliptkõver, siis $End(E)$ on isomorfne mingi maksimaalse järguringiga kvaternioonide algebras.*

Näide 6. [1, lk. 321] Vaatleme elliptkõverat E, mis on defineeritud üle korpuse $\mathbb{F}_2$ ning on antud võrrandiga

$$y^2 + y = x^3.$$

On kerge kontrollida, et

$$E(\mathbb{F}_2) = \{(0,0), (1,0), \infty\}$$

ning seetõttu lause 1 abil saame, et

$$a = 2 + 1 - \#E(\mathbb{F}_2) = 2 + 1 - 3 = 0.$$

Seega on vaadeldav kõver supersingulaarne ning lause 4 põhjal

$$\phi_2^2 + 2 = 0.$$

Kui $(x, y) \in E(\overline{\mathbb{F}}_2)$, siis

$$2(x, y) = -\phi_2^2(x, y) = -(x^4, y^4) = (x^4, y^4 + 1),$$

sest kõveral E

$$-(x, y) = (x, y + 1).$$

Teoreemi 6 põhjal on $End(E)$ maksimaalne järguring kvaterniioonide algebras. Üks selline maksimaalne järguring oleks eelnevalt vaadeldud

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\frac{1 + \mathbf{i} + \mathbf{j} + \mathbf{k}}{2}.$$

Leiame järgnevalt endomorfismid $\mathbf{i}, \mathbf{j}, \mathbf{k}$. Rahuldagu $\omega \in \mathbf{F}_4$ võrdust

$$\omega^2 + \omega + 1 = 0.$$

Defineerime endomorfismid järgnevalt:

$$\begin{aligned}
\mathbf{i}(x, y) &= (x + 1, y + x + \omega), \\
\mathbf{j}(x, y) &= (x + \omega, y + \omega^2 x + \omega), \\
\mathbf{k}(x, y) &= (x + \omega^2, y + \omega x + \omega).
\end{aligned}$$

Täheldame, et antud kujutused on endomorfismid, sest korpuse $\mathbb{F}_2$ algebraline sulund on $\overline{\mathbb{F}_2} = \bigcup_{n \geq 1} \mathbb{F}_{2^n}$ [1, lk. 482].

Kerge kontrolli tulemusel on võimalik näha, et

$$\mathbf{i}(\mathbf{j}(x, y)) = \mathbf{k}(x, y), \quad \mathbf{j}(\mathbf{i}(x, y)) = -\mathbf{k}(x, y)$$

ning

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1.$$

Elliptkõvera arvutusvalemeid kasutades on võimalik näidata, et

$$(1 + \mathbf{i} + \mathbf{j} + \mathbf{k})(x, y) = (\omega x^4, y^4) = \phi_2^2(\omega x, y) = -2(\omega(x, y)),$$

kus viimases võrduses tähistab $\omega(x, y)$ endomorfismi $(x, y) \to (\omega x, y)$.

Seega

$$\frac{1 + \mathbf{i} + \mathbf{j} + \mathbf{k}}{2} = -\omega \in End(E)$$

ning saame, et

$$\mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\frac{1 + \mathbf{i} + \mathbf{j} + \mathbf{k}}{2} \subseteq End(E).$$

Eelnevast teoreemist saame, et leitud maksimaalne järguring ongi terve endomorfismide ring

2.3 Ideaalid

Definitsioon 2.6. [4, lk. 28, definitsioon 50] Olgu $\mathcal{O}$ järguring korpuses $\mathbf{K}$, mis on samuti lõplikumõõtmeline vektorruum üle $\mathbb{Q}$. *Murruline ideaal* ringis $\mathcal{O}$ on mittetriviaalne alamrühm liitmise suhtes $\mathbf{I} \subset \mathbf{K}$, mis rahuldab järgmisi tingimusi:

1. $x\mathbf{I} \subseteq \mathbf{I}$ iga $x \in \mathcal{O}$ korral
2. leidub nullist erinev element $x \in \mathcal{O}$ nii, et $x\mathbf{I} \subseteq \mathcal{O}$.

Murrulist ideaali $\mathbf{I}$ nimetatakse *peaideaaliks*, kui leidub $x \in \mathbf{K}$ nii, et $I = x\mathcal{O}$ ning murrulist ideaali $\mathbf{I}$ kutsutakse *pööratavaks*, kui leidub teine murruline ideaal $\mathbf{J}$ nii, et

$$\mathbf{IJ} = \{ij \mid i \in \mathbf{I}, j \in \mathbf{J}\} = \mathcal{O}.$$

Näide 7. Murruliseks ideaaliks ringis $\mathbb{Z}$ on näiteks ideaal

$$\frac{2}{3}\mathbb{Z} = \left\{\frac{2}{3}a \mid a \in \mathbb{Z}\right\}.$$

Ilmselt on $\mathbb{Z}$ järguring ratsionaalarvude korpuses $\mathbb{Q}$ ning valides $x = 3$ saame, et $\frac{2x}{3}\mathbb{Z} \subset \mathbb{Z}$. Näeme samuti, et $\frac{2}{3}\mathbb{Z}$ on peaideaal ning ta on ka pööratav, kusjuures ta pöördelemendiks on ideaal $\frac{3}{2}\mathbb{Z}$.

Paneme tähele, et pööratavate murruliste ideaalide korrutamine on assotsiatiivne ning kommutatiivne, sest $\mathbf{I}, \mathbf{J} \subset \mathbf{K}$. Samuti on kerge tähele panna, et peaideaalide korrutis on peaideaal. Nende tähelepanekute tõttu saab väita, et pööratavad murrulised ideaalid moodustavad korrutamise suhtes Abeli rühma, kus $\mathcal{O}$ on ühikelement ning pööratavad murrulised peaideaalid moodustavad selle rühma alamrühma. Seetõttu on võimalik läbi viia järgnev konstruktsioon.

Definitsioon 2.7. [4, lk. 29, lause 51] Olgu $\mathcal{O}$ järguring lõplikuastmelises ratsionaalarvude laiendkorpuses $\mathbf{K}$. Olgu $\mathcal{I}(\mathcal{O})$ järguringi pööratavate murruliste ideaalide rühm ning olgu $\mathcal{P}(\mathcal{O})$ järguringi pööratavate murruliste peaideaalide rühm. Järguringi $\mathcal{O}$ *ideaaliklassirühmaks* kutsume faktorrühma

$$Cl(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O}).$$

Märgime ära olulise fakti, et $Cl(\mathcal{O})$ on lõplik Abeli rühm st. alati on võimalik leida $N = \#Cl(\mathcal{O})$ [4, lk.29, lause 51].

Olgu E elliptkõver üle korpuse $\mathbb{F}_q$. Teoreemist 6 teame, et $End(E) \cong \mathcal{O}$, kus $\mathcal{O}$ on teatud järguring $\mathbf{K}$-s, kus $\mathbf{K}$ on kas imaginaar-ruutkorpus või kvaternioonide algebra – sõltuvalt sellest, kas E on harilik või supersingulaarne kõver. CSI-FiSh-is kasutatakse aga supersingulaarse elliptkõvera E endomorfisme, mis on defineeritud üle $\mathbb{F}_q$ ehk milles ratsionaalfunktsioonide lugeja ja nimetaja on polünoomid üle $\mathbb{F}_q$

ning tähistame neid endomorfisme $End_{\mathbb{F}_q}(E)$. Need endomorfismid moodustavad $End(E)$ alamringi, kusjuures supersingulaarse kõvera puhul kehtib range sisalduvus $End_{\mathbb{F}_q}(E) \subset End(E)$, ning on teada, et $End_{\mathbb{F}_q}(E) \cong \mathcal{O}$, kus $\mathcal{O}$ on järguring imaginaar-ruutkorpuses $\mathbb{Q}(\sqrt{-q})$ [5, lk. 4]. Järgnevalt kasutame ainult neid endomorfisme ning seega kirjutame $End_{\mathbb{F}_q}(E)$ asemel lihtsalt $End(E)$ ning fikseerime järguringi $\mathcal{O} \subset \mathbb{Q}(\sqrt{-q})$, kus $\mathcal{O} \cong End(E)$.

Vaatleme nüüd elliptkõvera E endomorfismide ringi ideaaliklassidest moodustatud rühma

$$Cl(End(E)) = \mathcal{I}(End(E))/\mathcal{P}(End(E)),$$

kus $\mathcal{I}(End(E))$ on E endomorfismide ringi pööratavate murruliste ideaalide rühm ning $\mathcal{P}(End(E))$ on selle rühma pööratavate peaideaalide alamrühm. Rühmateooriast teame, et $Cl(End(E))$ koosneb kõrvalklassidest $\overline{\mathfrak{a}} := \mathfrak{a}\mathcal{P}(End(E)) \subseteq \mathcal{I}(End(E))$, kus $\mathfrak{a} \in \mathcal{I}(End(E))$.

Valides nüüd ideaaliklassi $\overline{\mathfrak{a}} \in Cl(End(E))$, saame vaadata $E(\overline{\mathbb{F}_q})$ alamrühma

$$S_{\overline{\mathfrak{a}}} = \bigcap_{\alpha \in \mathfrak{a}} \ker \alpha,$$

kus $\mathfrak{a}$ on klassi $\overline{\mathfrak{a}}$ esindaja ning kus $\alpha \in \mathfrak{a}$ on rühma $E(\mathbb{F}_q)$ endomorfism. Rühm $S_{\overline{\mathfrak{a}}}$ on rühma $E(\mathbb{F}_q)$ alamrühm, sest ta on rühma $E(\mathbb{F}_q)$ endomorfismide tuumade ühisosa. Märgime ära, et alamrühma $S_{\overline{\mathfrak{a}}}$ ülesehitus ei sõltu esindaja $\mathfrak{a} \in \overline{\mathfrak{a}}$ valikust [5, lk.4].

Kuna $S_{\overline{\mathfrak{a}}}$ on rühma $E(\mathbb{F}_q)$ alamrühm, saame moodustada faktorrühma $E_{\overline{\mathfrak{a}}} := E/S_{\overline{\mathfrak{a}}}$ ning tähistame

$$\overline{\mathfrak{a}} * E := E/S_{\overline{\mathfrak{a}}}.$$

On teada, et iga alamrühm $S \subseteq E(\mathbb{F}_q)$ defineerib ühe isogeense teisenduse $\phi\colon E \to E/S$, kus $S = \ker \phi$. See tähendab, et iga pööratava murrulise ideaali $\mathfrak{a} \subseteq End(E)$ korral on võimalik defineerida isogeenne teisendus $\phi_{\mathfrak{a}}\colon E \to E_{\overline{\mathfrak{a}}}$, kus $\overline{\mathfrak{a}}$ on ideaali $\mathfrak{a}$ sisaldav kõrvalklass [5, lk. 4].

On teada, et $End(E) \cong End(E_{\overline{\mathfrak{a}}}) \cong \mathcal{O}$, kus $\mathcal{O}$ on ülalpool defineeritud järguring ning seetõttu defineerib kujutus $(\overline{\mathfrak{a}}, E) \to E_{\overline{\mathfrak{a}}}$ *rühma* $Cl(\mathcal{O})$ *toime* hulgal $Ell_q(\mathcal{O})$, mis tähistab kõiki elliptkõveraid üle korpuse $\mathbb{F}_q$, mille endomorfismide ring on isomorfne ringiga $\mathcal{O}$.

Teoreem 7. [4, lk. 29, teoreem 53] *Olgu $\mathbb{F}_q$ lõplik korpus ning olgu $\mathcal{O} \subset \mathbb{Q}(\sqrt{-q})$ järguring imaginaar-ruutkorpuses. Kui $Ell_q(\mathcal{O})$ on mittetühi, saame defineerida rühma $Cl(\mathcal{O})$ toime hulgal $Ell_q(\mathcal{O})$ järgnevalt:*

$$\begin{aligned} Cl(\mathcal{O}) \times Ell_q(\mathcal{O}) &\to Ell_q(\mathcal{O}) \\ (\overline{\mathfrak{a}}, E) &\to \overline{\mathfrak{a}} * E, \end{aligned}$$

kusjuures iga $\overline{\mathfrak{a}}, \overline{\mathfrak{b}} \in Cl(\mathcal{O})$ *ning* $E \in Ell_q(\mathcal{O})$ *korral* $\overline{\mathfrak{a}} * (\overline{\mathfrak{b}} * E) = (\overline{\mathfrak{a}}\overline{\mathfrak{b}}) * E$ *ja iga* $E, E' \in Ell_q(\mathcal{O})$ *korral leidub üheselt määratud* $\overline{\mathfrak{a}} \in Cl(\mathcal{O})$ *nii, et* $E' = \overline{\mathfrak{a}} * E$.

Sellel rühma toimel põhinebki järgnevalt vaatluse alla tulev signatuuriskeem – CSI-FiSh.

3 CSI-FiSh

3.1 Miks supersingulaarsed kõverad?

CSI-FiSh baseerub võtmevahetusskeemil CSIDH (Commutative Supersingular Isogeny Diffie-Hellman), mis omakorda baseerub tugevalt eelmise peatüki lõpus toodud rühma toimel. CSIDH-i puhul kasutatakse kõvera $E(\mathbb{F}_p)$ terve endomorfismide ringi asemel alamringi, mis koosneb kõigist endomorfismidest, mis on defineeritud üle lõpliku korpuse $\mathbb{F}_p$. Nagu eelnevalt mainitud, siis selline alamring on järguring imaginaar-ruutkorpuses $\mathbb{Q}(\sqrt{-p})$, mitte enam kvaternioonide algebras [5, lk.4].

Selleks, et leida isogeenset teisendust kõverast E kõverasse E/S, kus S on mingi lõplik $E(\mathbb{F}_p)$ alamrühm, ning et leida ka kõver E/S ise, on olemas Vélu valemid, mille arvutuslik keerukus sõltub alamrühma S võimsusest. Seega on vaja rühma toime $\mathfrak{a} * E$ kiireks arvutamiseks, et vaadeldav $E(\mathbb{F}_p)$ alamrühm oleks väike. [5, lk.4].

Selleks valitakse CSIDH-i konstruktsioonis $p = 4l_1l_2 \dots l_n - 1$, kus $l_1, \dots, l_n$ on algarvud. Kui $p > 5$, siis supersingulaarse kõvera puhul $\#E(\mathbb{F}_p) = p + 1$, mistõttu $\#E(\mathbb{F}_p) = 4l_1 \dots l_n$ ning Cauchy teoreemi [6, lk.84] tõttu teame, et siis leiduvad rühmal $E(\mathbb{F}_p)$ kindlasti alamrühmad võimsusega $l_1, \dots, l_n$. Kui valida $l_1, \dots, l_n$ kõik väikesed algarvud, siis leidub meil garanteeritult väikeseid alamrühmi ning saame faktoriseerimist läbi viia efektiivselt [5, lk.5].

3.2 Baasprobleemid

Valime algul supersingulaarse baaskõvera E_0, mille korral tähistame $End(E_0) = \mathcal{O}$. Seejärel tähistame kõikide elliptkõverate üle $\mathbb{F}_p$ hulga, mille endomorfismide ring on isomorfne $\mathcal{O}$-ga, $Ell_p(\mathcal{O})$-ga. Järgnevas eeldame, et ideaaliklassirühm $Cl(\mathcal{O})$ on tsükliline. Olgu $N = \#Cl(\mathcal{O})$ ning olgu rühma moodustaja kõrvalklass $\mathfrak{g}$. See tähendab, et

$$Cl(\mathcal{O}) = \{\mathfrak{g}, \mathfrak{g}^2, \dots, \mathfrak{g}^N = \mathcal{O}\} \cong \mathbb{Z}_N.$$

Selle eelduse tõttu saame defineerida kujutuse

$$[\cdot] \colon \mathbb{Z}_N \times Ell(\mathcal{O}) \to Ell(\mathcal{O}), \quad (a, E_1) \mapsto [a]E_1 = \mathfrak{g}^a * E_1.$$

Näeme, et tegemist on eelnevalt sisse toodud rühma toimega juhul, kui $Cl(\mathcal{O})$ on tsükliline. Seetõttu saame teoreemi 7 tõttu väita, et iga $a, b \in \mathbb{Z}_N$ ning kõvera $E \in Ell_p(\mathcal{O})$ korral

$$[a]([b]E) = \mathfrak{g}^a * (\mathfrak{g}^b * E) = (\mathfrak{g}^a \cdot \mathfrak{g}^b) * E = \mathfrak{g}^{a+b} * E = [a + b]E.$$

Vaatleme järgnevalt rasket ülesannet, millel CSI-FiSh põhineb. Olgu E_0 eelnevalt fikseeritud "baaskõver", mille korral $End(E_0) = \mathcal{O}$.

Definitsioon 3.1. [5, lk. 5] **Group Action Inverse Problem (GAIP)** Olgu meil antud elliptkõver E, mille korral $End(E) = \mathcal{O}$. Leia ideaal $\mathfrak{a} \subset \mathcal{O}$ nii, et $E = \mathfrak{a} * E_0$.

CSI-FiSh ise põhineb selle ülesande järgneval üldistusel, mille puhul on teada, et kui ideaaliklassirühma ülesehitus on teada, siis taandub üldistatud versioon algse probleemi lahendamisele. Ideaaliklassirühma ehituse teadmise all mõtleme, et iga ideaaliklassi on võimalik esitada mingisugusel kanoonilisel kujul ning suvalist ideaaliklassi on võimalik valida ühtlasest jaotusest, Märgime ära, et ideaaliklassirühma ülesehitus on teada "piisavalt suure" ideaaliklassirühma jaoks, et saavutada 128-bitiline turvalisus. Selleks viidi läbi suuremahulised teadusarvutused, mille käigus leiti, et uuritav ideaaliklassirühm on ka tsükliline ehk eeldus alapeatüki alguses on õigustatud [5, lk. 6]

Definitsioon 3.2. [5, lk. 6] **Multi-Target Group Action Inverse Problem (MT-GAIP)** Olgu antud k kõverat $E_1, \ldots, E_k$, mille korral $End(E_1) \cong \ldots \cong End(E_k) \cong \mathcal{O}$. Vali suvaliselt $i, j \in \{0, \ldots, k\}$ nii, et $i \neq j$ ning leia ideaal $\mathfrak{a} \subset \mathcal{O}$ nii, et $E_i = \mathfrak{a} * E_j$.

3.3 Baasskeem

CSI-FiSh põhineb järgneval skeemil, mille eesmärk on ühel osapoolel teisele tõestada, et ta teab jäägiklassi $a \in \mathbb{Z}_N$, andmata teisele osapoolele informatsiooni a enda kohta. Järgnevas skeemis ongi kaks osapoolt: tõestaja ja kinnitaja. Tõestaja genereerib alguses avaliku võtme

$$E_1 = \overline{\mathfrak{g}}^a * E_0 = [a]E_0.$$

Seejärel valib tõestaja suvalise jäägiklassi $b \in \mathbb{Z}_N$, genereerib kõvera

$$E = [b]E_0$$

ning saadab selle kinnitajale. Seejärel valib kinnitaja suvalise biti $c \in \{0, 1\}$ ning saadab selle tõestajale. Kui $c = 0$, saadab tõestaja kinnitajale täisarvu $r = b$ ning kinnitaja kinnitab, et $E = [r]E_0$. Kui $c = 1$, saadab tõestaja kinnitajale täisarvu $r = b - a \bmod N$ ning kinnitaja kinnitab, et $E = [r]E_1$. Viimane võrdus kehtib, sest

$$[r]E_1 = [b - a]([a]E_0) = [b - a + a]E_0 = [b]E_0 = E.$$

Paneme tähele veel seda, et täisarvu r jäägiga jagamine N-ga on vajalik selleks, et ei lekiks informatsiooni a kohta ning täheldame, et kinnitaja tehtav kontroll on väljendatav ka kujul $E = [r]E_c$ [5, lk. 11].

CSI-FiSh-is rakendatakse antud baasskeemile pärast allkirjastamiseks sobivaks tegemist veel kolme parendust, mis teevad skeemi efektiivsemaks. Esimene neist kasutab krüptograafilisi räsifunktsioone, mis aitavad vähendada allkirjade suurust.

Ülemises skeemis saadab tõestaja kinnitajale algul kõvera E asemel $\mathcal{H}(E)$, kus $\mathcal{H}$ on räsifunktsioon. Kinnitamisel peab kinnitaja siis võrduse $E = [r]E_c$ kontrollimise asemel vaatama, et kehtiks võrdus $\mathcal{H}(E) = \mathcal{H}([r]E_c)$. Ükski skeemi turvaomadus selle muutuse tõttu kannatada ei saa [5, lk. 13].

Teiseks kasutatakse baasprobleemina GAIP-i asemel MT-GAIP-i. Selleks kasutatakse avaliku võtmena ühe kõvera asemel $S-1$ kõverat, st avalik võti on järgnev järjend pikkusega S

$$(E_0, E_1 = [a_1]E_0, E_2 = [a_2]E_0, \ldots, E_{S-1} = [a_{S-1}]E_0)$$

ning tõestaja peab siis näitama, et suvaliselt valitud kõverate E_i ja E_j, kus $i, j \in \{0, \ldots, S-1\}$, $i \neq j$ korral ta teab jäägiklassi r nii, et $E_i = [r]E_j$. Selleks valib tõestaja endiselt suvalise jäägiklassi $b \in \mathbb{Z}_N$ ning saadab kinnitajale kõvera $E^{(i)} = [b]E_0$. Kinnitaja saadab nüüd tõestajale arvu $c \in \{0, \ldots, S-1\}$, mille peale saadab tõestaja talle vastu täisarvu $r = b - a_c \bmod N$. Seejärel kontrollib kinnitaja, kas $E^{(i)} = [r]E_c$. Antud muudatus vähendab tõenäosust, et kinnitaja kinnitab valeliku tõestaja saadetud päringu [5, lk. 13].

Viimane parendus kasutab fakti, et kõvera $E = [a]E_0$ vääne E^t on isomorfne kõveraga $[-a]E_0$ üle korpuse $\mathbb{F}_p$ [5, lk. 13]. See tähendab, et saame tasuta suurendada avalikus võtmes olevate kõverate arvu võttes avalikku võtmesse kõverad $E_{-S+1}, \ldots, E_0, \ldots, E_{S-1}$, kus $E_{-i} = E_i^t$. Sel juhul saadab kinnitaja tõestajale täisarvu $c \in \{-S+1, \ldots, S-1\}$ ning tõestaja saadab kinnitajale vastu täisarvu $r = b - \operatorname{sign}(c)a_{|c|}$. Kui $c \geq 0$, siis toimib kontrolli loogika samamoodi nagu eelmises lõigus, kuid kui $c < 0$, siis toimib kontroll samuti korrektselt, sest

$$[r]E_c = [r][-a_c]E_0 = [b + a_c][-a_c]E_0 = [b]E_0 = E^{(i)} \quad \text{[5, lk. 13]}.$$

3.4 Allkirjastusskeem

Ülaltoodud parendustega baasskeem muudetakse allkirjastusskeemiks kasutades Fiat-Shamiri transformatsiooni, mis põhimõtteliselt tähendab seda, et arve $c_i \in \{-S+1, \ldots, S-1\}$ ei saada kinnitaja tõestajale, vaid tõestaja genereerib need arvud ise, rakendades sõnele, mis kujutab endast kõverate teatud esituste ning allkirjastatava sõnumi konkatenatsiooni, krüptograafilist räsifunktsiooni. Tõestaja saadab seejärel kinnitajale allkirja, mis koosneb täisarvudest r_i ning c_i ning kinnitaja leiab kõverad $E^{(i)} = [r_i]E_{c_i}$ ning kontrollib, kas arvud c_i tulevad eelnevalt kirjeldatud konkatenatsioonile räsifunktsiooni rakendades samad. Kui nii juhtub, on allkiri kinnitatud.

Paneme tähele, et selleks, et taastada avalikust võtmest salajane võti, peab oskama lahendada MT-GAIP probleemi. Eelduse kohaselt on see raske ülesanne.

Järgnevad skeemi eri algoritmide kirjeldused. Järgnevas tähendab kirjutis $a \leftarrow_R A$, et hulgast A valitakse ühtlasega jaotusega suvaline element a.

Algoritm 1
Võtmete genereerimine

Antud: baaskõver E_0, täisarv $N = \#Cl(\mathcal{O})$
for $i \in \{1, \ldots, S-1\}$ **do**
    $a_i \leftarrow_R \mathbb{Z}_N$
    $E_i = [a_i]E_0$
end for
pk= $[E_1, \ldots, E_{S-1}]$
sk= $[a_1, \ldots, a_{S-1}]$
Tagasta: avalik võti **pk**, salajane võti **sk**

Algoritm 2
Allkirjastamine

Antud: sõnum m, salajane võti **sk**
$a_0 \leftarrow 0$
for $i = 1, \ldots, t$ **do**
    $b_1 \leftarrow_R \mathbb{Z}_N, E^{(i)} = [b_i]E_0$
end for
$(c_1, \ldots, c_t) = \mathcal{H}(E^{(1)} \| \ldots \| E^{(t)} \| m)$
for $i = 1, \ldots, t$ **do**
    $r_i = b_i - \text{sign}(c_1)a_{|c_i|} \bmod N$
end for
Tagasta: signatuur $\sigma = (r_1, \ldots, r_t, c_1, \ldots, c_t)$

Algoritm 3
Valideerimine

Antud: sõnum m, avalik võti **pk**, signatuur σ
$\sigma = (r_1, \ldots, r_t, c_1, \ldots, c_t)$
Defineeri $E_{-i} = E_i^t$, $i \in \{1, \ldots, S-1\}$.
for $i = 1, \ldots, t$ **do**
    $E^{(i)} = [r_i]E_{c_i}$
end for
$(c'_1, \ldots, c'_t) = \mathcal{H}(E^{(1)} \| \ldots \| E^{(t)} \| m)$
if $(c_1, \ldots, c_t) == (c'_1, \ldots, c'_t)$ **then**
    Kinnita allkiri.
else
    Lükka allkirja õigsus ümber.
end if

Kasutatud allikad

[1] L. C. Washington. *Elliptic curves. Number theory and cryptography*. 2. väljaanne. Boca Raton: Taylor & Francis Group, 2008.

[2] Jérémy Jean. *TikZ for Cryptographers*. https://www.iacr.org/authors/tikz/. 2016.

[3] J. T. Tate J. H. Silverman. *Rational Points on Elliptic Curves*. 2. väljaanne. Springer International Publishing Switzerland, 2015.

[4] Luca de Feo. *Mathematics of Isogeny Based Cryptography*. 2017. URL: %5Curl%7Bhttps://arxiv.org/pdf/1711.04062.pdf%7D.

[5] Ward Beullens, Thorsten Kleinjung ja Frederik Vercauteren. *CSI-FiSh: Efficient Isogeny based Signatures through Class Group Computations*. Cryptology ePrint Archive, Report 2019/498. https://eprint.iacr.org/2019/498. 2019.

[6] Valdis Laan. *Algebra II loengukonspekt. Kevad 2019*. https://courses.ms.ut.ee/2021/algebra2/spring/Main/Lectures.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Calvin Pärn,

1. Annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose "Supersingulaarsete elliptkõverate isogeensed teisendused ning rakendused signatuuriskeemi CSI-FiSh näitel", mille juhendajad on PhD Jan Villemson ning prof. Valdis Laan, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Calvin Pärn
18.05.2021