Parituksista ja niihin perustuvista protokollista

Tomas Stenman

Pro gradu -tutkielma
Heinäkuu 2023

Tarkastajat:
Prof. Jarkko Kari
FT Arto Lepistö

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Tomas Stenman: Parituksista ja niihin perustuvista protokollista
Pro gradu -tutkielma, 34 s.
Matematiikka
Heinäkuu 2023

Tutkielmassa esitetään paritukset ja niihin tarvittavat elliptiset käyrät sekä käsitellään parituksia käyttäviä kryptografisia protokollia.

Tutkielma alkaa esittelemällä parituksiin tarvittavien elliptisten käyrien perusasioita ja ominaisuuksia, sekä esitetään parituksissa tärkeiden jakajien ja torsiopisteiden määritelmät. Toisessa luvussa käsitellään parituksia, joista esitellään Weilin ja Taten paritukset, sekä näissä käytettävien funktioiden laskemiseen käytettävä Millerin algoritmi. Tutkielman kolmannessa luvussa käsitellään kolmea parituksia käyttävää kryptografista protokollaa, eli kolmen osapuolen Diffie–Hellmanin avaimenvaihtoprotokollaa, lyhyiden allekirjoitusten järjestelmää ja identiteettiin perustuvaa salausta.

Asiasanat: elliptiset käyrät, paritukset, protokollat, kryptografia

Sisällys

1 Johdanto

Julkisen avaimen kryptosysteemit toimivat yksisuuntaisten funktioiden ja takaporttifunktioiden (eng. trapdoor function) avulla. Yksisuuntaisten funktioiden toimintaperiaate on se, että ne ovat helposti laskettavia injektiivisiä funktioita $f : A \to B$, mutta niiden käänteisfunktio f^{-1} taas on erittäin vaikeasti laskettava. Takaporttifunktio on yksisuuntaisten funktioiden erityistapaus, jossa funktio on muuten samanlainen kuin tavalliset yksisuuntaiset funktiot, mutta ratkaisu toiseen suuntaan on mahdollista käyttämällä jotakin ratkaisuun tarvittavaa lukua k, eli nk. takaporttia.

Tämänkaltaisten yksisuuntaisten funktioiden olemassaolo on avoin ongelma, ja yksisuuntaisten funktioiden olemassaolon todistaminen todistaisikin samalla tunnetun $P = NP$ -ongelman. Julkisen avaimen kryptografian voikin siis todeta pohjautuvan vahvasti konjektuureihin, sillä yksisuuntaisten funktioiden olemassaolon todistaminen vääräksi, sekä tämän kaltaisten ongelmien ratkaisuun tarvittavien algoritmien löytäminen rikkoisi olemassaolevat julkisen avaimen kryptosysteemit. Yksisuuntaisia funktioita pidetään yleisesti kuitenkin tarpeeksi turvallisena kryptografisiin sovelluksiin, ja monet uskovatkin, ettei näitä avoimia ongelmia tulla koskaan ratkaisemaan.

Julkisen avaimen kryptografia perustuu siihen, että takaporttifunktioita käyttäen viestinnän osapuolet pystyvät keskustelemaan julkisia kanavia pitkin salausta käyttämällä, koska vain heidän tiedossaan olevalla avaimella salatun tekstin kääntäminen selkokielelle onnistuu helposti. Koska keskustelut käydään julkisia kanavia pitkin, niin kanavalla olevalla mahdolliselle salakuuntelijalle näiden viestien murtaminen on lähes mahdotonta salaisen avaimen puutteen takia. Avaimen luontiin ja sen turvalliseen siirtämiseen julkisia kanavia pitkin keskustelun salaamiseksi on kehitetty monia protokollia, joista ensimmäisiä on Diffie–Hellmanin avaimenvaihtoprotokolla.

Tilanteessa, jossa kaksi keskustelun osapuolta tarvitsevat käyttöönsä salatun kanavan keskustelua varten, mutta käytössä on kuitenkin vain kanava, joka ei ole turvallinen, niin Diffie–Hellmanin avaimenvaihtoprotokollaa käyttämällä osapuolet saavat sovittua käyttöönsä salaisen avaimen. Tämän avaimen kanssa osapuolet pystyvät pitämään keskustelunsa kyseisellä julkisella kanavalla ilman pelkoa siitä, että mahdollinen salakuuntelija saisi selvitettyä viestejen sijainnit. Protokolla menee seuraavasti:

1. Alice ja Bob sopivat yhdessä alkuluvun p ja ryhmän Z_p^* generaattorin g.

2. Alice valitsee jonkin luvun a ja Bob valitsee jonkin luvun b, niin että $1 < a, b < p - 2$

3. Alice lähettää Bobille luvun $t_a = g^a \pmod{p}$, ja Bob lähettää Alicelle luvun $t_b = g^b \pmod{p}$.

4. Alice laskee luvun $k = t_b^a \pmod{p}$, ja Bob laskee luvun $k = t_a^b \pmod{p}$.

Koska $t_b^a = (g^b)^a = (g^a)^b = t_a^b$, niin molemmat osapuolet saavat saman tuloksen (eli avaimen k). Vaikka keskustelu on käyty julkista kanavaa käyttämällä, niin mahdollinen ulkopuolinen salakuuntelija ei ainakaan nykytiedon mukaan pysty tehokkaasti laskemaan lukua k, vaikka hänellä olisikin tiedossaan luvut p, g, t_a ja t_b. Tätä ongelmaa kutsutaan Diffie–Hellman-ongelmaksi (DHP).

Diffie-Hellmanin avaimenvaihtoprotokollaa voidaan käyttää myös useamman kuin kahden osapuolen välillä. Useammalla osapuolella algoritmi vaatii useampia kierroksia, kun taas kahden osapuolen tapauksessa vaaditaan vain yksi kierros. Kolmen osapuolen kohdalla algoritmi menee seuraavasti:

1. Alice, Bob ja Carol sopivat yhdessä alkuluvun p ja ryhmän Z_p^* generaattorin g.

2. Alice valitsee jonkin luvun a, Bob valitsee jonkin luvun b ja Carol valitsee jonkin luvun c, niin että $1 < a, b, c < p - 2$.

3. Alice laskee ja lähettää Bobille luvun $g^a \pmod p$.

4. Bob laskee Alicelta saatua lukua g^a käyttäen luvun $(g^a)^b \pmod p = g^{ab}$ ja lähettää saadun luvun Carolille.

5. Carol laskee Bobilta saatua lukua g^{ab} käyttäen luvun $k = (g^{ab})^c \pmod p = g^{abc}$.

Saatu luku $k = g^{abc}$ on nyt Carolin avain. Samaa avainta tulevat tietenkin tarvitsemaan myös Alice ja Bob, joten avaimenvaihtoprotokollan algoritmia tulee vielä jatkaa kaikkien osapuolten kesken.

6. Bob laskee ja lähettää Carolille luvun $g^b \pmod p$.

7. Carol laskee Bobilta saatua lukua g^b käyttäen luvun $(g^b)^c \pmod p = g^{bc}$, ja lähettää saadun luvun Alicelle

8. Alice laskee Carolilta saatua lukua g^{bc} käyttäen luvun $k = (g^{bc})^a \pmod p = g^{abc}$.

Alicelle on nyt myös saatu sama avain $k = g^{abc}$. Algoritmia tulee jatkaa vielä edelleen, että avain saadaan jaettua myös Bobille.

9. Carol laskee ja lähettää Alicelle luvun $g^c \pmod p$.

10. Alice laskee Carolilta saatua lukua g^c käyttäen luvun $(g^c)^a \pmod p = g^{ac}$, ja lähettää saadun luvun Bobille.

11. Bob laskee Alicelta saatua lukua g^{ac} käyttäen luvun $k = (g^{ac})^b \pmod p = g^{abc}$.

Nyt kaikilla osapuolilla on tiedossaan sama salainen avain k. Kuten myös ylempänä kahden osapuolen tapauksessa, kaikki tuloksien lähetykset on tehty julkisia kanavia pitkin. Mahdollisella salakuuntelijalla on siis tiedossaan kaikki välitulokset, eli luvut $g^a, g^b, g^c, g^{ab}, g^{ac}$ ja g^{bc}, mutta kuten ylempänä näitä käyttämällä ei lopullisen avaimen g^{abc} laskeminen tehokkaasti onnistu.

Samaa algoritmia käyttäen pystytään julkisten kanavien kautta laskemaan yhteinen salausavain rajattomalle määrälle osapuolia. Tätä kyseistä algoritmia käyttäessä ongelmaksi kuitenkin muodostuu selvästi algoritmin aikakompleksisuus. Jokainen n osapuolta joutuu algoritmin aikana tekemään n kappaletta protokollassa tarvittavia modulaarisia potenssilaskuja. Toisena ongelmana on, ettei algoritmissa ole sisäänrakennettuna minkäänlaista vastapuolien identiteetin tarkistukseen tarvittavia varmenteita, joten algoritmi on erityisen haavoittuvainen väliintulohyökkäyksille.

Näitä ongelmia pystytään korjaamaan käyttämällä bilineaarisia parituksia. Yläpuolella esitetyn avaimenvaihtoprotokollan aikakompleksisuuden ongelmaan liittyen tutkielmassa esitetään kolmen osapuolen Diffie–Hellmanin avaimenvaihtoprotokolla, joka paritusten avulla voidaan suorittaa vain yhden kierroksen aikana. Identiteetin tarkistukseen liittyvien ongelmien välttämiseksi esitetään esimerkki parituksiin pohjautuvasta identiteettiin perustuvasta salausjärjestelmästä.

Tutkielman luvussa 2 käsitellään parituksiin tarvittavia elliptisiä käyriä ja niiden ominaisuuksia, sekä esitellään paritusten teoriassa tarvittavat jakajien ja torsiopisteiden määritelmät. Luku siis antaa tarvittavat pohjatiedot parituksien teorian ymmärtämiselle. Kolmannessa luvussa siirrytään tarkastelemaan näitä bilineaarisia parituksia, joista konkreettisina esimerkkeinä annetaan Weilin ja Taten paritukset. Luvun lopussa esitellään vielä Millerin algoritmi, jota käytetään parituksissa tarvittavien funktioiden laskemiseen. Tutkielman neljännessä luvussa esitellään näitä parituksia käyttäviä kryptografisia protokollia.

2 Elliptiset käyrät

Tässä luvussa esitetään myöhemmin parituksiin tarvittavia elliptisten käyrien perusmääritelmiä ja -lauseita. Luvussa käsitellään ensin Weierstrassin yhtälöt ja elliptiset käyrät, jonka jälkeen tarkastelu siirtyy jakajien ja torsiopisteiden teoriaan.

2.1 Elliptiset käyrät

Aloitetaan esittämällä elliptisten käyrien kannalta tärkeät affiinin avaruuden ja projektiivisen avaruuden määritelmät. Määritelmissä käytetään merkintää $\overline{K}$ esittämään kunnan K algebrallista sulkeumaa.

Määritelmä 2.1.1. Affiini n-avaruus yli kunnan K on joukko, johon kuuluu kaikki n-tuplat

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{P = (x_1, ..., x_n) : x_i \in \overline{K}\}.$$

Affiinista 2-avaruudesta käytetään nimitystä *affiini taso.*

Affiinin avaruuden avulla voidaan määritellä projektiivinen avaruus, jonka määritelmässä ja myöhemminkin tutkielmassa on käytetty merkintää K^* kunnan nollasta eroaville alkioille.

Määritelmä 2.1.2. Projektiivinen n-avaruus $\mathbf{P}^n$ yli kunnan K on joukko ekvivalenssiluokkia avaruudessa $\mathbb{A}^{n+1}\backslash\{(0, 0, \cdots, 0)\}$, jotka on määritelty ekvivalenssirelaation $\sim$ avulla. Projektiivisesta 2-avaruudesta käytetään nimitystä *projektiivinen taso.* Tutkielmassa käsitellään vain projektiivista tasoa, joten esitetään relaatio $\sim$ projektiivisen tason kohdalla. Relaatio $\sim$ toteutuu, eli

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$$

jos ja vain jos on olemassa kerroin $\gamma \in \overline{K}^*$, jolla $(\gamma x_1, \gamma y_1, \gamma z_1) = (x_2, y_2, z_2)$. Eri pisteet, jotka toteuttavat relaation $\sim$ jonkin toisen pisteen kanssa muodostavat ekvivalenssiluokkia, jotka ovat projektiivisen tason $\mathbf{P}^2$ origon läpi kulkevia suoria. Pisteen (x, y, z) sisältävää ekvivalenssiluokkaa merkitään $(x : y : z)$.

Koska mikä tahansa piste (x, y, z), jossa $z \neq 0$ on ekvivalentti pisteen

$$(x/z, y/z, z/z) = (x/z, y/z, 1)$$

kanssa, nämä ekvivalenssiluokat voidaan jaotella kahteen ryhmään, muotoa $(x : y : 1)$ ja muotoa $(x : y : 0)$ oleviin ekvivalenssiluokkiin. Edeltävään ryhmään kuuluvat ekvivalenssiluokat muodostavat affiinin tason $\mathbb{A}^2$, kun taas jälkimmäiseen ryhmään kuuluvat ekvivalenssiluokat eivät kuulu affiiniin tasoon, ja muodostavat projektiivisen tason äärettömyyspisteet.

Weierstrassin yhtälö voidaan määritellä kunnan K algebrallisessa sulkeumassa $\overline{K}$ olevien pisteiden avulla.

Määritelmä 2.1.3. Weierstrassin yhtälö on kolmannen asteen homogeenininen yhtälö, joka on muotoa

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1}$$

jossa $a_i \in K$. Yhtälö voidaan kirjottaa muodossa $F(X, Y, Z) = 0$, ja käyrän tangentti pisteessä $P = (X_0, Y_0, Z_0)$ määritellään suorana

$$\frac{\partial F}{\partial X}X + \frac{\partial F}{\partial Y}Y + \frac{\partial F}{\partial Z}Z = 0,$$

missä osittaisdifferentiaalien arvot on laskettu pisteen P suhteen. Yhtälö on *epäsingulaarinen*, jos yhtälön $F(X, Y, Z)$ osaderivaatat eivät katoa samanaikaisesti missään käyrän pisteessä, eli toisin sanoen tangentti on määritelty kaikkialla.

Yhtälöstä (1) voidaan korvaamalla $x = X/Z$ ja $y = Y/Z$ johtaa epäsingulaarinen Weierstrassin yhtälö

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2}$$

Jokainen piste (x, y), joka toteuttaa yhtälön (2) vastaa yhtälön (1) pisteiden toteuttamaa ekvivalenssiluokkaa $(x : y : 1)$. Yläpuolella mainitun epäsingulaarisen Weierstrassin yhtälön johtamiseen käytetyn muuttujien vaihdon myötä ne yhtälön (1) pisteet, joissa $Z = 0$ jäävät käsittelemättä. Tällöin ainoa yhtälön (1) toteuttava ekvivalenssiluokka, jossa $Z = 0$, on $(0 : 1 : 0)$. Tätä vastaavaa projektiivisen tason pistettä merkitään $\mathcal{O}$, ja sitä kutsutaan *pisteeksi äärettömässä.*

Määritelmä 2.1.4. Käyrän *K-rationaalisiksi pisteiksi* kutsutaan joukkoa $E(K)$, johon kuuluu piste äärettömässä $\mathcal{O}$ ja pisteet $(x, y) \in K \times K$, jotka toteuttavat yhtälön (2).

Elliptinen käyrä on pari $(E, \mathcal{O})$, jossa E on joukko, johon kuuluu kaikki projektiivisen tason $\mathbf{P}^2$ pisteet, jotka toteuttavat epäsingulaarisen Weierstrassin yhtälön, ja $\mathcal{O} \in E$. Tutkielmassa käytetään elliptisestä käyrästä pääosin merkintää E, jolloin siihen sisältyy myös piste $\mathcal{O}$. Elliptinen käyrä E on määritelty yli kunnan K, jos käyrän yhtälössä kertoimet $a_i \in K$. Tällöin käyrästä voidaan käyttää myös merkintää E/K.

Jos kunnan $\overline{K}$ karakteristika $\mathrm{ch}(\overline{K}) \neq 2$, niin korvauksen

$$y \mapsto \frac{1}{2}(y - a_1x - a_3)$$

tekemällä yhtälö (2) saadaan yksinkertaistettua muotoon

$$y^2 = 4x^3 + b_2x^2 + 2b_4 + b_6, \tag{3}$$

jossa

$$b_2 = a_1^2 + 4a_2,$$
$$b_4 = 2a_4 + a_1a_3 \text{ ja}$$
$$b_6 = a_3^2 + 4a_6.$$

Lisäksi voimme määritellä arvot

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4,$$
$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$
$$j = c_4^3/\Delta \text{ ja}$$
$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y},$$

joissa Δ on Weierstrassin yhtälön diskriminantti, j on elliptisen käyrän j-invariantti, ja ω on Weierstrassin yhtälön differentiaalinen invariantti. Yläpuolella määritellyt arvot toteuttavat yhtälöt $4b_8 = b_2b_6 - b_4^2$ ja $1728\Delta = c_4^3 - c_6^2$.

Näiden arvojen avulla yhtälöä voidaan yksinkertaistaa vielä pidemmälle, jos kunnan $\overline{K}$ karakteristika $\mathrm{ch}(\overline{K}) \neq 2, 3$. Tällöin korvauksella

$$(x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$$

saadaan eliminoitua yhtälöstä (3) termi x^2, jolloin yhtälö saadaan vielä helpompaan muotoon

$$y^2 = x^3 - 27c_4x - 54c_6. \tag{4}$$

Elliptinen käyrä, joka on määritelty käyttämällä yhtälöä (3) tai (4) on symmetrinen x-akselin suhteen, toisin kuin yhtälön (2) määrittelemä käyrä.

Lause 2.1.5. *E on elliptinen käyrä, eli Weierstrassin yhtälö* (2) *on epäsingulaarinen jos ja vain jos $\Delta \neq 0$.*

Todistus. Todistus on esitetty kirjan [1] sivuilla 45-47 ja 409-412. □

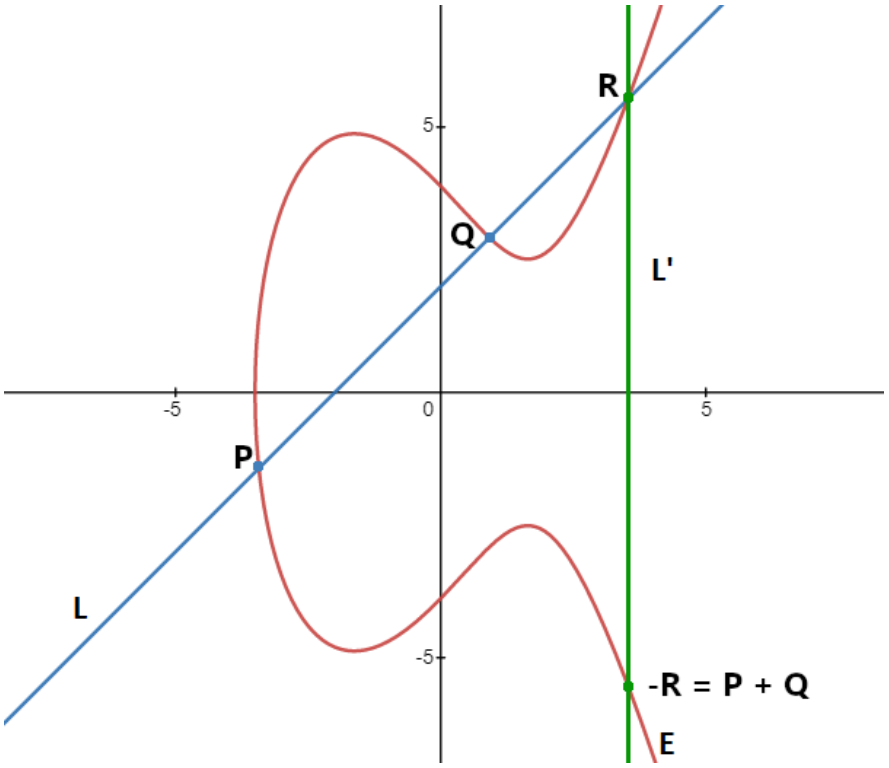
2.2 Ryhmälaki

Käyrän E pisteet muodostavat Abelin ryhmän käyrälle E piirrettyjen jänteiden ja tangenttien avulla. Aloitetaan ryhmän laskulakien tarkastelu ensin geometrisesti reaaliluvuilla, ja siirrytään myöhemmin kappaleessa 2.5 äärellisiin kuntiin joissa käytetään myös samaa laskulakia. Laskulakien esittäminen geometrisesti käyrille piirrettyjen jänteiden ja tangenttien avulla ei kuitenkaan ole äärellisten kuntien tapauksessa

enää mielekästä, joten äärellisten kuntien tapauksessa käytetään samaa, ei geometrista vaan aritmeettista laskulakia myöhemmin tämän kappaleen aikana esitettyjen laskusääntöjen avulla.

Ryhmän neutraalialkio on $\mathcal{O}$. Elliptiseltä käyrältä voidaan minkä tahansa pisteen $P \in E$ valitsemalla valita myös piste $-P \in E$, jolla on sama x-koordinaatti kuin pisteellä P, eli jos $P = (x_1, y_1)$, niin $-P = (x_1, y_2)$, jossa y_1 ja y_2 ovat käyrän E kaksi juurta sijoituksella $x = x_1$.

Jos pisteet P ja Q ovat käyrällä E, niin kolmas piste $P + Q$ voidaan määritellä piirtämällä suora L, joka kulkee valittujen pisteiden läpi. Koska käyrän yhtälö on kolmatta astetta, niin L leikkaa yleensä käyrän myös kolmannessa pisteessä R. Piirtämällä nyt suoran L', joka kulkee pisteiden R ja $\mathcal{O}$ lävitse saadaan suoralle L' ja käyrälle E toinen leikkauspiste $-R$, joka on siis vastapäätä pistettä R, eli toisin sanoen neutraalialkion $\mathcal{O}$ kautta kulkeva suora on pystysuora. Piste $-R$ on nyt summan $P + Q$ tulos, ts. $P + Q = -R$. Sama pätee myös, jos pisteet $P = Q$, ja käyrälle E piirretty tangentti leikkaa käyrän jossakin toisessa pisteessä R. Käyrän E ja jonkin sille piirretyn tangentin tai jänteen L leikkauspisteiden summa ryhmässä on aina $\mathcal{O}$.



Kuva 1: *Punaisella elliptinen käyrä E, jonka yhtälönä $y^2 = x^3 - 8x + 15$. Sinisellä pisteiden P ja Q läpi piirretty suora L, joka leikkaa käyrän E pisteessä R. Vihreä suora L' näyttää, miten summa $P + Q = -R$ on määritelty.*

Yläpuolella esitetyllä tavalla suoritetulle pisteiden väliselle yhteenlaskulle voidaan todistaa vielä lisää laskusääntöjä. Nämä laskusäännöt todistavat sen, että el-

liptisen käyrän pisteet muodostavat Abelin ryhmän. Lause ja sen todistus seuraavat kirjassa [1] sivuilla 51-52 esitettyä todistusta:

Lause 2.2.1. *Pisteiden välisellä yhteenlaskulla on seuraavat ominaisuudet:*

1. *Jos suora L leikkaa elliptisen käyrän E pisteissä P, Q ja R, niin $(P+Q)+R = \mathcal{O}$.*

2. *$P + \mathcal{O} = P$ kaikilla $P \in E$*

3. *$P + Q = Q + P$ kaikilla $P, Q \in E$*

4. *Olkoon P piste käyrällä E. Käyrällä E on myös piste $-P$, jolla $P+(-P) = \mathcal{O}$*

5. *Olkoon P, Q ja R pisteitä käyrällä E. Pisteet toteuttavat yhtälön $(P + Q) + R = P + (Q + R)$ kaikilla $P, Q, R \in E$, ts. pisteiden välinen yhteenlasku on assosiatiivinen.*

6. *Oletetaan, että E on määritelty yli kunnan K. Tällöin $E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$ on käyrän E aliryhmä.*

Todistus. Esitetään jokaiselle lauseen kohdalle oma todistuksensa:

1. Ennen lauseen esitystä näytettiin, miten pisteiden välinen yhteenlasku on määritelty. Todistus seuraa suoraan tästä, jonka näkee myös kuvasta 1.

2. Ylempänä esitetyllä tavalla valitessa pisteiksi pisteet P ja $\mathcal{O}$ nähdään, että näiden kautta kulkeva suora L leikkaa käyrän E pisteissä $P, \mathcal{O}$ ja R. Suora L' taas leikkaa käyrän pisteissä $R, \mathcal{O}$ ja $P + \mathcal{O}$. Toisin sanoen, $P + \mathcal{O} = P$

3. Tapa, jolla yhteenlasku on määritelty on selvästi symmetrinen, koska sen määrää käyrän E ja pisteiden P ja Q kautta piirretty suora.

4. Olkoon $P \in E$. Koska elliptisen käyrän ja sen pisteiden läpi kulkevan suoran leikkauspisteiden summa on $\mathcal{O}$, niin jokin pisteen P kautta piirretty pystysuora viiva joko leikkaa käyrän toisessa pisteessä R, jolloin $P + R + \mathcal{O} = P + R = \mathcal{O}$, tai pystysuora viiva on tangentti jolloin $R = P$ ja $P + P + \mathcal{O} = P + P = \mathcal{O}$.

5. Assosiatiivisuus voidaan todistaa tapauskohtaisesti alla esitettyjen tarkkojen kaavojen avulla. Tämä monisivuinen todistus löytyy lähteestä [2].

6. Jos pisteet P ja Q kuuluvat kuntaan K, niin näiden kautta piirretyn suoran L yhtälön vakiokertoimet kuuluvat myös kuntaan K. Jos elliptinen käyrä E on määritelty yli kunnan K, niin käyrän E yhtälön vakiokertoimet kuuluvat kuntaan K. Suoran L ja käyrän E kolmannen leikkauspisteen R koordinaatit määritellään suoran L ja käyrän E kuntaan K kuuluvien vakiokertoimien avulla, joten piste R kuuluu myös kuntaan K.

□

Lauseen 2.2.1 kuudes kohta on helpompi ymmärtää, kun esitetään käyrän E laskuoperaatioille tarkat kaavat. Olkoon elliptinen käyrä E käyrä, joka toteuttaa Weierstrassin yhtälön

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

ja olkoon piste $P_0 = (x_0, y_0) \in E$. Lauseen 2.2.1 kohdassa 4 esitetyn pisteen $-P_0$ koordinaatit voidaan laskea suoraan pisteen P_0 koordinaateista. Pisteiden P_0 ja $\mathcal{O}$ kautta piirretty suora L leikkaa siis käyrän E myös kolmannessa pisteessä. Suoran L yhtälö on $L : x - x_0 = 0$. Suoran yhtälöstä saadaan siis koordinaatti $x = x_0$. Tämän koordinaatin sijoittamalla Weierstrassin yhtälöön, jolla käyrä E on määritelty, saadaan yhtälöksi

$$f(x_0, y) = y^2 + a_1x_0y + a_3y - x_0^3 - a_2x_0^2 - a_4x_0 - a_6 = 0.$$

Yhtälöstä $f(x_0, y)$ tulee siis toisen asteen yhtälö

$$f(x_0, y) = y^2 + (a_1x_0 + a_3)y - (x_0^3 + a_2x_0^2 + a_4x_0 + a_6) = 0,$$

jolla on nollakohdat y_0 ja y_0', joten yhtälö voidaan kirjoittaa muodossa $f(x_0, y) = b(y-y_0)(y-y_0')$, jossa $b = 1$ on yhtälön toisen asteen termin kerroin. Yhtälö saadaan siis muotoon $f(x_0, y) = (y - y_0)(y - y_0')$.

Yhtälön ensimmäisen asteen termin kertoimista saadaan yhtälön nollakohta $y_0' = -y_0 - a_1x_0 - a_3$. Piste $-P_0$ voidaan siis esittää muodossa

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

Pisteen x-koordinaatti on siis sama kuin pisteellä P_0, koska muodossa (3) elliptinen käyrä on symmetrinen x-akselin suhteen ja muunnos yhtälöiden (2) ja (3) välillä ei muuta pisteiden x-koordinaatteja..

Pisteiden summaan voidaan esittää samantapainen kaava kuin negatiiviselle pisteelle. Olkoon $P_1 = (x_1, y_1)$ ja $P_2 = (x_2, y_2)$ pisteitä käyrällä E. Jos pisteiden x-koordinaatit x_1 ja x_2 ovat samat ja $y_1 + y_2 + a_1x_2 + a_3 = 0$, lauseen 2.2.1 kohdan 4 sekä yläpuolella johdetun negatiivisen pisteen määritelmän nojalla $P_1 = -P_2$ jolloin $P_1 + P_2 = \mathcal{O}$. Muussa tapauksessa pisteiden P_1 ja P_2 läpi kulkevalla suoralla L on yhtälö, joka on muotoa

$$L : y = \lambda x + v,$$

jossa λ on suoran L kulmakerroin ja v vakiotermi.

Kuten ylempänä esitetyssä negatiivisen pisteen määritelmässä, sijoittaessa suoran L yhtälön elliptisen käyrän yhtälöön

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

saadaan yhtälöksi

$$\begin{aligned} f(x, \lambda x + v) =& (\lambda x + v)^2 + a_1 x(\lambda x + v) + a_3(\lambda x + v) - x^3 - a_2 x^2 - a_4 x - a_6 \\ =& a_1 vx + a_3 v + a_1 x^2 \lambda - a_2 x^2 + a_3 x\lambda - a_4 x - a_6 \\ & + v^2 + 2vx\lambda - x^3 + x^2\lambda^2 \\ =& - x^3 + (a_1\lambda - a_2 + \lambda^2)x^2 + (a_1 v + a_3\lambda - a_4 + 2v\lambda)x \\ & + (a_3 v - a_6 + v^2) \\ =& 0. \end{aligned}$$

Yhtälö on kolmatta astetta, joten sillä on kolme nollakohtaa x_1, x_2 ja x_3. Tämä kolmas juuri x_3 onkin suoran L ja käyrän E kolmannen leikkauspisteen $P_3 = (x_3, y_3)$ x-koordinaatti. Lauseen 2.2.1 kohdan 1 nojalla

$$P_1 + P_2 + P_3 = \mathcal{O}.$$

Käyrän E yhtälö voidaan taas esittää tekijämuodossa

$$f(x, \lambda x + v) = b(x - x_1)(x - x_2)(x - x_3),$$

jolloin kolmannen asteen termin kertoimesta saadaan $b = 1$ ja yhtälö saadaan muotoon

$$f(x, \lambda x + v) = (x - x_1)(x - x_2)(x - x_3).$$

Toisen asteen termin kertoimella $a_1\lambda - a_2 + \lambda^2$ saadaan pisteiden x-koordinaattien yhtälö $x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$, josta voidaan laskea suoralla L sijaitsevan pisteen P_3 x-koordinaatti. Tämän jälkeen pisteen y-koordinaatti voidaan laskea suoran L yhtälöstä sijoituksen $(x, y) \mapsto (x_3, y_3)$ tekemällä. Tällä saadaankin pisteen $P_3 = (x_3, y_3)$ koordinaatit.

Kuten kappaleen alussa todettiin, summa $P_1 + P_2 = -P_3$, kun $P_1, P_2, P_3 \in L$. Summan tulos $-P_3$ saadaankin, kun käytetään negatiivisen pisteen laskusääntöä saatuun pisteeseen P_3.

Laskusäännöt voidaan tiivistää helpommin esitettävään algoritmiseen muotoon.

Määritelmä 2.2.2. *(Summausalgoritmi.)* Olkoon E elliptinen käyrä

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

- Olkoon piste $P_0 = (x_0, y_0)$. Tällöin piste $-P_0 = (x_0, -y_0 - a_1 x_0 - a_3)$.
- Olkoon $P_1 + P_2 = P_3$, ja $P_i = (x_i, y_i) \in E$.
  - Jos $x_1 = x_2$ ja $y_1 + y_2 + a_1 x_2 + a_3 = 0$, niin $P_1 + P_2 = \mathcal{O}$.
  - Jos $x_1 = x_2$ ja $y_1 + y_2 + a_1 x_2 + a_3 \neq 0$, niin

$$\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} \quad \text{ja} \quad v = \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}.$$

– Jos $x_1 \neq x_2$, niin

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{ja} \quad v = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

Tällöin λ ja v ovat pisteiden P_1 ja P_2 kautta piirretyn suoran $L : y = \lambda x + v$ yhtälössä olevia vakioita.

- Pisteellä $P_3 = P_1 + P_2$ on koordinaatit

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - v - a_3,$$

jossa λ ja v ovat yläpuolella esitettyä muotoa.

2.3 Jakajat

Seuraavaksi esitellään myöhemmin tutkielmassa käsiteltäviin parituksiin tarvittava jakajan käsite. Tämä voidaan aloittaa käsittelemällä rationaalifunktioiden nollakohtia ja napoja. Rationaalifunktio voidaan esittää yleisessä muodossa

$$f(x) = \frac{a_0 + a_1 x + \cdots + a_n x^n}{b_0 + b_1 x + \cdots + b_m x^m}.$$

Rationaalifunktio on siis kahden polynomifunktion osamäärä. Nämä polynomifunktiot voidaan jakaa tekijöihin, jolloin funktio f saa muodon

$$f(x) = \frac{a(x-\alpha_1)^{d_1}(x-\alpha_2)^{d_2}\dots(x-\alpha_r)^{d_r}}{b(x-\beta_1)^{e_1}(x-\beta_2)^{e_2}\dots(x-\beta_s)^{e_s}},$$

jossa $\alpha_i, \beta_i \in \mathbb{C}$ kaikilla $i \in \mathbb{N}$, ja voidaan olettaa että $\alpha_i \neq \beta_j$ kaikilla $i, j \in \mathbb{N}$.

Funktion f nollakohtia ovat tällöin ne muuttujan x arvot, joilla osoittajan arvo on 0, ja funktion napoja ovat ne muuttujan x arvot, joilla nimittäjän arvo on 0. Tällöin voidaan sanoa, että funktiolla f on nollakohdat pisteissä $\alpha_1, \alpha_2 \dots \alpha_r$ ja navat pisteissä $\beta_1, \beta_2, \dots \beta_s$. Jokaisella nollalla α_i on kertalukuna d_i, ja jokaisella navalla β_j on kertalukuna e_j. Tällöin funktion f jakaja $\operatorname{div}(f)$ määritellään formaalina summana

$$\operatorname{div}(f) = d_1(\alpha_1) + d_2(\alpha_2) + \cdots + d_r(\alpha_r) - e_1(\beta_1) - e_2(\beta_2) - \cdots - e_s(\beta_s),$$

jossa (α_i) ja (β_i) ovat kommutatiivisen ryhmän vapaita generaattoreita. Formaalina summana määritelty jakaja on siis formaalinen esitysmuoto alkioiden (α_i) ja (β_i) generoimalle kommutatiivisen ryhmän alkiolle.

Kuten yläpuolella yhden muuttujan tapauksessa, voidaan funktioille määrittää jakajat myös useamman muuttujan tapauksessa. Seuraavaksi esitellään käyrän jakajan määritelmä yleisessä muodossa.

Määritelmä 2.3.1. Olkoon E elliptinen käyrä, joka on määritelty yli kunnan K.

Käyrän E jakajien ryhmä $\mathrm{Div}(E)$ koostuu käyrän E *jakajista* $D \in \mathrm{Div}(E)$. Jakaja D on formaalina summana

$$D = \sum_{P \in E} n_P(P)$$

esitetty käyrän E pisteiden vapaasti generoiman kommutatiivisen ryhmän alkio, jossa $n_P \in \mathbb{Z}$ ja $n_P \neq 0$ äärellisellä määrällä alkioita $P \in E$.

Määritelmä 2.3.2. Jakajan D aste

$$\deg D = \sum_{P \in E} n_P.$$

Jakajaa D, jonka aste $\deg D = 0$ kutsutaan *nolla-asteisiksi jakajiksi.* Nolla-asteiset jakajat muodostavat ryhmän $\mathrm{Div}(E)$ aliryhmän $\mathrm{Div}^0(E)$.

Määritelmä 2.3.3. Jakajan D *kantaja* on niiden pisteiden $P \in E$ joukko, joilla $n_P \neq 0$.

Rationaalifunktion f jakaja $\mathrm{div}(f) = \sum_{P \in E} m_P(P)$, jossa m_P merkitsee, kuinka monta kertaa piste P esiintyy funktion f juurena tai napana. Kyseisen formaalin summan lausekkeessa funktion nollakohdat esitetään positiivisilla ja navat negatiivisilla kertoimilla m_P. Jakajaa D kutsutaan *pääjakajaksi,* jos se on muotoa $D = \mathrm{div}(f)$ jollakin funktiolla f. Kaksi jakajaa $D_1, D_2 \in \mathrm{Div}(E)$ ovat *lineaarisesti ekvivalentteja*, ts. $D_1 \sim D_2$, jos $D_1 = D_2 + \mathrm{div}(f)$ jollakin funktiolla f.

Lause 2.3.4. *Olkoon E elliptinen käyrä.*

a) Funktion f jakaja $\mathrm{div}(f) = 0$ *jos ja vain jos f on nollasta eroava vakiofunktio.*

b) Funktioiden f ja g jakajat $\mathrm{div}(f) = \mathrm{div}(g)$ *jos ja vain jos $f = ng$ jollain $n \neq 0$.*

Todistus. Kohdan a) todistus on esitetty kirjassa [1] sivulla 28, ja kohdan b) todistus on esitetty tutkielman [5] sivulla 24. □

Seuraavaksi esitettävää lausetta varten ja myöhemminkin tutkielmassa tarvitaan määritelmä sille, miten funktion arvo määräytyy kun sen argumenttina on jakaja D.

Määritelmä 2.3.5. Olkoon f funktio, ja $D = n_1(P_1) + \cdots + n_k(P_k)$ jakaja. Merkinnällä $f(D)$ tarkoitetaan tuloa

$$f(P_1)^{n_1} \cdots f(P_k)^{n_k}.$$

Esitetään vielä myöhempien lauseiden todistuksiin tärkeä Weilin vastavuoroisuuslause, jonka nojalla $f(\mathrm{div}(g)) = g(\mathrm{div}(f))$.

Lause 2.3.6. *Olkoon f ja g nollasta eroavia rationaalisia funktioita elliptisellä käyrällä E/K. Oletetaan, että funktioiden jakajien* $\mathrm{div}(f)$ *ja* $\mathrm{div}(g)$ *kantajat eivät jaa samoja pisteitä. Tällöin*

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f)).$$

Todistus. Todistus on esitetty kirjassa [3] sivuilla 212-213. □

2.4 Torsiopisteet ja -aliryhmät

Myöhemmin tutkielmassa esitettävät Weilin ja Taten paritukset tarvitsevat pisteen monistamisen, pisteiden kertaluvun sekä torsiopisteiden ja -aliryhmien määrittelyä.

Määritelmä 2.4.1. Ryhmän alkiota P monistettaessa, ts. lisättäessä useamman kerran itseensä käytetään notaatiota $[n]P$. Erityisesti elliptisten käyrien ryhmässä E, kun $n \in \mathbb{Z}$ ja $P \in E$, kirjoitetaan

$$[n]P = \overbrace{P + \cdots + P}^{n \text{ kpl, kun n>0}}, \qquad [n]P = \overbrace{-P - \cdots - P}^{n \text{ kpl, kun n<0}}, \qquad [0]P = \mathcal{O}$$

Toimintaperiaate on siis sama, kuin luonnollisten lukujen kertolaskussa.

Torsiopisteet vastaavat kysymykseen siitä, kuinka monta kertaa tiettyä pistettä P voidaan lisätä itseensä, kunnes summan tulokseksi tulee $\mathcal{O}$.

Määritelmä 2.4.2. Olkoon E/K elliptinen käyrä, ja $n > 0 \in \mathbb{Z}$. Käyrän E n-torsioaliryhmä $E[n]$ on käyrän E kertalukua n olevien pisteiden (nk. torsiopisteiden) joukko

$$E[n] = \{P \in E : [n]P = \mathcal{O}\}.$$

Jos tällaista kokonaislukua n ei ole olemassa, pisteen P kertaluku on ääretön.

Käyrän E torsioaliryhmä E_{tors} on kaikkien n-torsioaliryhmien unioni, ts. kaikkien äärellistä kertalukua olevien pisteiden joukko

$$E_{tors} = \bigcup_{n=1}^{\infty} E[n].$$

Jos käyrä E on määritelty yli kunnan K, niin $E_{tors}(K)$ on äärellistä kertalukua olevien pisteiden joukko käyrällä E/K.

Lause 2.4.3. *Äärellistä kertalukua oleva piste P kuuluu äärettömän moneen n-torsioaliryhmään $E[n]$.*

Todistus. Tarkastellaan ensin pistettä $\mathcal{O}$. Koska $[1]\mathcal{O} = \mathcal{O}$, niin piste $\mathcal{O}$ kuuluu 1-torsioaliryhmään $E[1]$. Lauseen 2.2.1 nojalla $[2]\mathcal{O} = \mathcal{O} + \mathcal{O} = \mathcal{O}$, ja $[3]\mathcal{O} = \mathcal{O} + [2]\mathcal{O} = \mathcal{O}$. Induktiolla seuraa, että $\mathcal{O} \in E[n]$ kaikilla positiivisilla kokonaisluvuilla n.

Jokaiselle äärellistä kertalukua olevalle pisteelle $P \neq \mathcal{O}$ on olemassa jokin kokonaisluku n, jolla $[n]P = \mathcal{O}$. Kuten myös pisteen $\mathcal{O}$ tapauksessa, muillakin äärellistä kertalukua olevilla pisteillä voidaan induktiolla todeta, että ne kuuluvat äärettömän moneen n-torsioaliryhmään. Koska $[2n]P = [n]P + [n]P = \mathcal{O} + \mathcal{O} = \mathcal{O}$ ja $[3n]P = [2n]P + [n]P = \mathcal{O} + \mathcal{O} = \mathcal{O}$, induktiolla seuraa että $P \in E[kn]$ kaikilla positiivisilla kokonaisluvuilla k. □

Kuten mainittu, kryptografian sovelluksissa tarvitaan sekä elliptisten käyrien pisteiden $[n]P$ koordinaatteja että kertalukujen löytämistä. Kuten sovelluksissa yleensäkin, tulee käytettyjen lukujen kuitenkin olla tarpeeksi suuria sovellusten laskennallisen turvallisuuden varmistamiseksi. Pienillä kertoimilla n pisteen $[n]P$ koordinaatit voidaan löytää kohtuullisen pienellä vaivalla määritelmän 2.2.2 laskusääntöjä

käyttämällä. Ongelmia näiden laskusääntöjen käyttämisessä tuleekin vasta siinä vaiheessa, kun halutaan löytää pisteiden monikertoja tätä huomattavasti suuremmilla kertoimilla. Pisteen $[1000]P$ laskeminen vaatisi summausalgoritmin käyttöä erikseen tuhat kertaa.

Suurten kokonaislukukertoimien laskemista varten onkin kehitetty nk. double-and-add-algoritmi [4], jonka toiminta perustuu kokonaislukukertoimen n esittämiseen sen binäärimuodossa

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 2^2 + \cdots + n_r \cdot 2^r,$$

jossa $n_i \in \{0, 1\}$ ja $n_r = 1$. Tämän kokonaislukukertoimen binäärimuodon lisäksi algorimissa tarvitaan myös pisteet

$$Q_0 = P,\ Q_1 = [2]Q_0,\ Q_2 = [2]Q_1,\ \cdots,\ Q_r = [2]Q_{r-1}.$$

Jokainen piste Q_i on siis edellinen piste Q_{i-1} tuplattuna, joten

$$Q_i = [2^i]P.$$

Näillä pisteillä ja binäärimuodolla voidaan laskea pisteen P monikerran koordinaatit käyttämällä enintään r kappaletta yhteenlaskuja,

$$[n]P = [n_0]Q_0 + [n_1]Q_1 + [n_2]Q_2 + \cdots + [n_r]Q_r.$$

2.5 Elliptiset käyrät yli äärellisten kuntien

Tähän mennessä tutkielmassa ollaan puhuttu elliptisistä käyristä vain yleisesti yli jonkin kunnan K. Tarkastelu siirtyy tässä kappaleessa äärellisiin kuntiin, joissa on $q \in \mathbb{P}$ alkiota. Koska aikaisemmin esitetyt lauseet ja määritelmät on esitelty yleisesti jossain kunnassa K, ne toimivat kuitenkin myös äärellisten kuntien tapauksessa.

Kuvassa 1 pisteiden välinen yhteenlasku on esitelty geometrisesti käyrällä $E/\mathbb{R}$. Kuten aikaisemmin kappaleessa 2.2 mainittiin, tämän esittäminen käyrille piirrettyjen tangenttien ja leikkauspisteiden avulla ei kuitenkaan enää ole mielekästä, mutta lauseessa 2.2.1 ja määritelmässä 2.2.2 esitetyt ominaisuudet ja laskusäännöt toimivat myös äärellisten kuntien tapauksessa, käytettäessä äärellisen kunnan $\mathbb{F}_p$ laskusääntöjä.

Esimerkki 2.5.1. Tarkastellaan seuraavaksi elliptistä käyrää

$$E : y^2 = x^3 + 2x + 4 \text{ yli kunnan } \mathbb{F}_7.$$

Kuntaan $\mathbb{F}_7$ kuuluu seitsemän alkiota, eli $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Piste $(x, y) \in \mathbb{F}_7 \times \mathbb{F}_7$ kuuluu käyrän $\mathbb{F}_q$-rationaalisiin pisteisiin $E(\mathbb{F}_q)$, jos piste toteuttaa kongruenssiyhtälön $y^2 \equiv x^3 + 2x + 4 \bmod 7$. Toisin sanoen, piste (x, y) on käyrällä jos $y^2 \bmod 7$ ja $x^3 + 2x + 4 \bmod 7$ saavat samat arvot.

Valitaan pisteeksi $(2, 3)$. Tällöin käyrän yhtälössä vasemman puolen arvoksi saadaan $y^2 \bmod 7 = 3^2 \bmod 7 = 9 \bmod 7 = 2$, ja oikean puolen arvoksi saadaan

$x^3 + 2x + 4 \bmod 7 = 2^3 + 2 \cdot 2 + 4 \bmod 7 = 16 \bmod 7 = 2$. Piste $(2, 3)$ on siis käyrällä E. Samaan tapaan voidaan tarkistaa kaikki mahdolliset pisteet, jolloin saadaan käyrän $\mathbb{F}_q$-rationaalisten pisteiden joukko

$$E(\mathbb{F}_q) = \{(0,2), (0,5), (1,0), (2,3), (2,4), (3,3), (3,4), (6,1), (6,6), \mathcal{O}\}.$$

Kuten kappaleen alussa mainittiin, pisteiden välinen yhteenlasku toimii äärellisissä kunnissa samalla tavalla kuin kunnassa $\mathbb{R}$. Valitaan pisteet $P = (1, 0)$ ja $Q = (3, 4)$. Määritelmässä 2.2.2 annettuja kaavoja käyttämällä voidaan laskea $P+Q$:

$$\begin{aligned}
\lambda &= \frac{y_2 - y_1}{x_2 - x_1} \bmod 7 = \frac{4 - 0}{3 - 1} \bmod 7 = 2, \\
v &= \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \bmod 7 = \frac{0 \cdot 3 - 4 \cdot 1}{3 - 1} \bmod 7 = -2 \bmod 7 = 5, \\
x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \bmod 7 = 2^2 + 0\lambda - 0 - 1 - 3 \bmod 7 = 0, \\
y_3 &= -(\lambda + a_1)x_3 - v - a_3 \bmod 7 = -(2 + 0)0 - 5 - 0 \bmod 7 = -5 \bmod 7 = 2.
\end{aligned}$$

Laskusääntöjä käyttämällä saatiin siis yhteenlaskun tulokseksi $P+Q = (x_3, y_3) = (0, 2) \in E(\mathbb{F})$. Kaikille pisteille $P, Q \in E(\mathbb{F})$ voidaan laskea samalla tavalla summat, näiden kaikkien pisteparien summat löytyvät kuvasta 2.

+	$\mathcal{O}$	(0,2)	(0,5)	(1,0)	(2,3)	(2,4)	(3,3)	(3,4)	(6,1)	(6,6)
$\mathcal{O}$	$\mathcal{O}$	(0,2)	(0,5)	(1,0)	(2,3)	(2,4)	(3,3)	(3,4)	(6,1)	(6,6)
(0,2)	(0,2)	(2,4)	$\mathcal{O}$	(3,4)	(0,5)	(6,6)	(1,0)	(6,1)	(2,3)	(3,3)
(0,5)	(0,5)	$\mathcal{O}$	(2,3)	(3,3)	(6,1)	(0,2)	(6,6)	(1,0)	(3,4)	(2,4)
(1,0)	(1,0)	(3,4)	(3,3)	$\mathcal{O}$	(6,6)	(6,1)	(0,5)	(0,2)	(2,4)	(2,3)
(2,3)	(2,3)	(0,5)	(6,1)	(6,6)	(3,4)	$\mathcal{O}$	(2,4)	(3,3)	(1,0)	(0,2)
(2,4)	(2,4)	(6,6)	(0,2)	(6,1)	$\mathcal{O}$	(3,3)	(3,4)	(2,3)	(0,5)	(1,0)
(3,3)	(3,3)	(1,0)	(6,6)	(0,5)	(2,4)	(3,4)	(2,3)	$\mathcal{O}$	(0,2)	(6,1)
(3,4)	(3,4)	(6,1)	(1,0)	(0,2)	(3,3)	(2,3)	$\mathcal{O}$	(2,4)	(6,6)	(0,5)
(6,1)	(6,1)	(2,3)	(3,4)	(2,4)	(1,0)	(0,5)	(0,2)	(6,6)	(3,3)	$\mathcal{O}$
(6,6)	(6,6)	(3,3)	(2,4)	(2,3)	(0,2)	(1,0)	(6,1)	(0,5)	$\mathcal{O}$	(3,4)

Kuva 2: *Pisteiden väliset summat elliptisellä käyrällä* $E : y^2 = x^3 + 2x + 4$ *yli kunnan* $\mathbb{F}_7$. *Saatu ryhmä on kymmenen alkion syklinen ryhmä.*

Pisteen kertaluku voidaan määrittää esimerkin 2.5.1 tapaan yhteenlaskun avulla. Näin löydetään määritelmässä 2.4.2 esitettyjen torsioaliryhmien alkiot.

Esimerkki 2.5.2. Valitaan elliptiseltä käyrältä $E/\mathbb{F}_7 : y^2 = x^3 + 2x + 4$ piste $P = (2, 3)$. Tällöin pisteen monikerrat voidaan laskea esimerkissä 2.5.1 esitetyllä tavalla, tai kuvaa 2 seuraamalla:

$$
\begin{aligned}
&[1]P = (2,3)\\
&[2]P = (2,3) + (2,3) = (3,4)\\
&[3]P = (2,3) + (2,3) + (2,3) = (3,4) + (2,3) = (3,3)\\
&[4]P = (2,3) + (2,3) + (2,3) + (2,3) = (3,3) + (2,3) = (2,4)\\
&[5]P = (2,3) + (2,3) + (2,3) + (2,3) + (2,3) = (2,4) + (2,3) = \mathcal{O}.
\end{aligned}
$$

Pisteen P kertaluku $n = 5$. Tällöin piste kuuluu käyrän E kertalukua 5 olevien pisteiden muodostamaan 5-torsioaliryhmään $E[5]$.

Pisteiden monikertojen laskeminen tällä tavoin manuaalisesti on selvästi etenkin suuremmilla vakion n arvoilla varsin työläs prosessi. Edellisessä kappaleessa käsiteltiinkin tätä prosessia huomattavasti nopeuttavan double-and-add -algoritmin toimintaperiaatetta. Esitetään tässä vielä esimerkki algoritmin toiminnasta.

Esimerkki 2.5.3. Tarkastellaan elliptistä käyrää

$$E : y^2 = x^3 + 2x + 4 \text{ yli kunnan } \mathbb{F}_7.$$

Kuvassa 2 ja esimerkissä 2.5.1 on annettuina joukkoon $E(\mathbb{F}_q)$ kuuluvat pisteet sekä kaikkien kyseisen pistejoukon välisten pisteparien summat. Valitaan piste $P = (0, 5)$, ja lasketaan algoritmin avulla $[7]P$.

Algoritmin käyttöön tarvitaan kokonaislukukertoimen $n = 7$ binääriesitystä

$$7 = 1 + 1 \cdot 2 + 1 \cdot 2^2.$$

Lisäksi tarvitaan pisteet

$$
\begin{aligned}
&Q_0 = P = (0,5),\\
&Q_1 = [2]Q_0 = (0,5) + (0,5) = (2,3) \text{ ja}\\
&Q_2 = [2]Q_1 = (2,3) + (2,3) = (3,4).
\end{aligned}
$$

Pisteen $[n]P$ koordinaateille saadaan nyt yhtälö

$$[n]P = [n_0]Q_0 + [n_1]Q_1 + [n_2]Q_2 = (0,5) + (2,3) + (3,4) = (6,1) + (3,4) = (6,6),$$

joka voidaan varmistaa oikeaksi myös kuvasta 2.

2.6 Elliptisten käyrien diskreetin logaritmin ongelma

Elliptisten käyrien käyttö kryptografisissa sovelluksissa perustuu elliptisten käyrien diskreetin logaritmin ongelmaan (eng. elliptic curve discrete logarithm problem, lyh. ECDLP), joka on johdannossa esitellystä diskreetin logaritmin ongelmasta johdettu vastaava ongelma, jossa joukkona on elliptisen käyrän pistejoukko.

Määritelmä 2.6.1. *(ECDLP.)* Olkoon P ja Q pisteitä, jotka ovat elliptisellä käyrällä $E/\mathbb{F}_q$. Elliptisten käyrien diskreetin logaritmin ongelmassa etsitään kokonaislukua n, joka toteuttaa yhtälön $[n]P = Q$.

Koska johdannossa esitetty Diffie-Hellmanin avaimenvaihtoprotokolla voidaan toteuttaa tarvittavien muutosten jälkeen missä tahansa kommutatiivisessa ryhmässä, niin se voidaan toteuttaa myös elliptisten käyrien avulla. Avaimenvaihtoprotokollan suoritus tapahtuu tällöin seuraavalla tavalla:

1. Alice ja Bob sopivat yhdessä äärellisen kunnan $\mathbb{F}_q$, elliptisen käyrän $E/\mathbb{F}_q$, ja pisteen $P \in E(\mathbb{F}_q)$.

2. Alice valitsee jonkin salaisen kokonaisluvun a, ja laskee pisteen $P_A = [a]P \in E(\mathbb{F}_q)$.

3. Bob valitsee jonkin salaisen kokonaisluvun b, ja laskee pisteen $P_B = [b]P \in E(\mathbb{F}_q)$.

4. Alice ja Bob lähettävät toisilleen pisteet P_A ja P_B.

5. Alice laskee luvun $[ab]P = [a]P_B$, ja Bob laskee luvun $[ab]P = [b]P_A$.

Molemmilla osapuolilla on nyt yhteinen avain $k = [ab]P$. Jos avaimenvaihto tapahtuu suojaamatonta kanavaa pitkin, niin mahdollinen salakuuntelija saa tietoonsa pisteet $P, [a]P, [b]P \in E(\mathbb{F}_q)$. Kuitenkin protokollan avulla tuotetun avaimen selvittämiseen salakuuntelijan tarvitsee joko ratkaista elliptisten käyrien diskreetin logaritmin ongelma ja saada tätä kautta tietoonsa kokonaisluvut a ja b tai vaihtoehtoisesti ratkaista elliptisten käyrien Diffie-Hellman-ongelma, jossa pisteitä $P, [a]P, [b]P \in E(\mathbb{F}_q)$ käyttäen pitäisi laskea piste $[ab]P$. Jos protokollan parametrit on valittu oikein, niin ainoa tunnettu metodi elliptisten käyrien Diffie–Hellman-ongelman ratkaisemiseksi on kuitenkin ratkaista ensin elliptisten käyrien diskreetin logaritmin ongelma, joten protokollaa voidaan pitää varsin turvallisena.

3 Paritukset

Tutkielman johdannossa on esitetty Diffie–Hellmanin avaimenvaihtoprotokolla sekä kahden että kolmen osapuolen tapauksessa. Kuten jo aikaisemmin todettiin, ei protokolla esitetyssä muodossa ole kovin mielekästä käyttää useammalla kuin kahdella osapuolella, sillä algoritmiin tarvittavien kierrosten ja laskutoimitusten määrä kasvaa liian nopeasti. Kolmen osapuolen avaimenvaihdon järjestäminen tehokkaasti yhdellä kierroksella olikin pitkään ongelma, jota ei oltu ratkaistu. Lopulta ongelmaan löydettiin ratkaisuksi paritukset. Tässä kappaleessa esitetäänkin parituksiin tarvittavat perusasiat, Weilin ja Taten paritukset sekä paritusten toimintaan tarvittavien funktioiden generoimiseen tarvittava Millerin algoritmi.

3.1 Paritusten perusteet

Olkoot G_1 ja G_2 ryhmiä, joiden neutraalialkio on 0, ja joiden kaikkien alkioiden n :s moninkerta on neutraalialkio (eli $[n]P = 0$ kaikilla $P \in G_1, G_2$). Olkoon G_T syklinen ryhmä, jonka kertalukuna on kokonaisluku n ja neutraalialkio on 1. Ryhmissä G_1 ja G_2 ryhmäoperaatiolle käytetään additiivista merkintää $+$, ja ryhmässä G_T käytetään multiplikatiivista merkintää $\cdot$. Bilineaarinen paritus on kuvaus $e : G_1 \times G_2 \to G_T$, joka toteuttaa seuraavat ehdot:

- Bilineaarisuus: $e(A_1 + B_1, A_2) = e(A_1, A_2)e(B_1, A_2)$ kaikilla $A_1, B_1 \in G_1$ ja kaikilla $A_2 \in G_2$, ja $e(A_1, A_2 + B_2) = e(A_1, A_2)e(A_1, B_2)$ kaikilla $A_1 \in G_1$ ja kaikilla $A_2, B_2 \in G_2$.
- Epädegeneratiivisuus: Kaikilla neutraalialkiosta eroavilla alkioilla $P \in G_1$ on olemassa $Q \in G_2$, jolla $e(P, Q) \neq 1$, ja kaikilla neutraalialkiosta eroavilla alkioilla $Q \in G_2$ on olemassa $P \in G_1$, jolla $e(P, Q) \neq 1$.
- e on tehokkaasti laskettavissa.

Paritus on symmetrinen, jos $G_1 = G_2$.

Lause 3.1.1. *$e(a_1A_1, a_2A_2) = e(A_1, A_2)^{a_1a_2}$ kaikilla $(A_1, A_2) \in G_1 \times G_2$ ja kaikilla $a_1, a_2 \in \mathbf{Z}$*

Todistus. Esitetään todistus bilineaarisuusominaisuutta useamman kerran käyttäen:

$$\begin{aligned} e(A_1, A_2)^{a_1a_2} &= (e(A_1, A_2)^{a_1})^{a_2} \\ &= e([a_1]A_1, A_2)^{a_2} \\ &= e([a_1]A_1, [a_2]A_2). \end{aligned}$$

□

Sekä parituksien että parituksiin pohjautuvien protokollien laskennallinen turvallisuus liittyy vahvasti bilineaarisen Diffie–Hellman-ongelman (eng. bilinear Diffie-Hellman problem, lyhennettynä BDHP) laskennalliseen vaikeuteen. BDHP on aikaisemmin mainitusta Diffie-Hellman-ongelmasta johdettu ongelma, jota ainakaan nykytiedoilla ei pystytä ratkaisemaan tehokkaasti elliptisten käyrien Weilin tai Taten parituksia käytettäessä.

Määritelmä 3.1.2. *(Bilineaarinen Diffie–Hellman-ongelma.)* Annetuilla pisteillä $P, Q, P_1 = [a]P$ ja $P_2 = [b]P$, joilla $e(P, Q) \neq 1$ tulee laskea

$$e([ab]P, Q).$$

BDHP on selvästi korkeintaan yhtä vaikeasti ratkaistavissa oleva ongelma kuin elliptisten käyrien Diffie–Hellman-ongelma, sillä jos on mahdollista löytää $[ab]P$ millä tahansa tunnetuilla muuttujilla $P, [a]P$ ja $[b]P$, niin saadaan laskettua myös $e([ab]P, Q)$ annetuille $P, Q, [a]P$ ja $[b]P$. Yleisesti BDHP:ta pidetään kuitenkin tarpeeksi vaikeana kryptografisiin sovelluksiin.

3.2 Weilin paritus

Määritelmä 3.2.1. Olkoon E elliptinen käyrä ja m kokonaisluku. Olkoon $P, Q \in E[m]$ ja f_P, f_Q rationaalisia funktioita elliptisellä käyrällä E, joilla

$$\mathrm{div}(f_P) = m(P) - m(\mathcal{O}) \text{ ja } \mathrm{div}(f_Q) = m(Q) - m(\mathcal{O}).$$

Tällöin *Weilin paritus* on määritelty seuraavasti:

$$e_m(P, Q) = \frac{f_P(Q+S)}{f_P(S)} / \frac{f_Q(P-S)}{f_Q(-S)},$$

jossa käyrällä E oleva piste $S \notin \{\mathcal{O}, P, -Q, P-Q\}$. Tässä funktion jakajan $\mathrm{div}(f_P)$ lausekkeessa esiintyvä $m(P)$ tarkoittaa, että funktiolla f_P on astetta m oleva nolla pisteessä P, ja $m(\mathcal{O})$ sitä, että funktiolla on astetta m oleva napa pisteessä $\mathcal{O}$.

Edellä mainitut rajoitukset pisteelle S varmistavat, että paritus on määritelty. Seuraavaksi esitetään Weilin paritukselle tärkeitä ominaisuuksia. Lauseen todistus seuraa tutkielman [5] todistusta.

Lause 3.2.2. *Weilin parituksella on seuraavat ominaisuudet:*

a) $e_m(P, Q)$ *on riippumaton funktioiden* f_P *ja* f_Q *valinnasta sekä pisteestä* S*.*

b) $e_m(P, Q)^m = 1$ *kaikilla* $P, Q \in E[m]$*. Toisin sanoen Weilin parituksen arvo on* m*:s ykkösenjuuri.*

c) Weilin paritus on bilineaarinen, eli

$$e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q), \text{ kaikilla } P_1, P_2, Q \in E[m]$$

ja

$$e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2), \text{ kaikilla } P, Q_1, Q_2 \in E[m].$$

d) $e_m(P, P) = 1$ *kaikilla* $P \in E[m]$*. Tästä seuraa, että* $e_m(P, Q) = e_m(Q, P)^{-1}$ *kaikilla* $P, Q \in E[m]$*.*

e) Weilin paritus on epädegeneroitunut, eli

$$\text{jos } e_m(P, Q) = 1 \text{ kaikilla } Q \in E[m], \text{ niin } P = \mathcal{O}.$$

Todistus. a) Tarkastellaan ensin funktion f_P valintaa. Määritelmän 3.2.1 mukaan kyseisen funktion jakaja $\mathrm{div}(f_P) = m(P) - m(\mathcal{O})$. Valitaan funktion f_P tilalle siis jokin muu funktio g_P, jolla $\mathrm{div}(f_p) = \mathrm{div}(g_P)$. Lauseen 2.3.4 kohdan (b) nojalla

funktio g_P tulee valita niin, että $g_P = nf_P$ jollain $n \neq 0$. Sijoittamalla Weilin paritukseen $e_m(P,Q)$ funktion g_P saadaan paritus

$$\begin{aligned} e'_m(P,Q) &= \frac{g_P(Q+S)}{g_P(S)} / \frac{f_Q(P-S)}{f_Q(-S)} \\ &= \frac{nf_P(Q+S)}{nf_P(S)} / \frac{f_Q(P-S)}{f_Q(-S)} \\ &= \frac{f_P(Q+S)}{f_P(S)} / \frac{f_Q(P-S)}{f_Q(-S)} \\ &= e_m(P,Q). \end{aligned}$$

Todistus pätee samalla tapaa myös funktion f_Q valinnan kohdalla. Weilin paritus on siis riippumaton funktioiden f_P ja f_Q valinnasta.

Tarkastellaan seuraavaksi pisteen S valintaa. Aloitetaan tämä tarkastelemalla Weilin paritusta $e_m(P,Q)$ funktiona $F(S) : E(K) \to K$, jossa

$$F(S) = \frac{f_P(Q+S)}{f_P(S)} / \frac{f_Q(P-S)}{f_Q(-S)}.$$

Parituksen riippumattomuus pisteen S valinnasta voidaan todeta osoittamalla, ettei funktiolla $F(S)$ ole nollakohtia eikä napoja. Lauseen 2.3.4 a)-kohdan nojalla tämä tarkoittaa, että funktio on nollasta eroava vakiofunktio. Funktioiden f_P ja f_Q jakajien nojalla näitä nollakohtia ja napoja voi muodostua vain, kun

1. $Q + S = P$,
2. $-S = Q$,
3. $S = \mathcal{O}$,
4. $P - S = \mathcal{O}$.

Todistetaan väite kohdassa 1. Muut kohdat menevät vastaavasti. Kohdassa 1 annetusta pisteestä $P = Q + S$ saadaan piste S muotoon $S = P - Q$. Tällöin

$$F(S) = \frac{f_P(P)}{f_P(P-Q)} / \frac{f_Q(Q)}{f_Q(Q-P)}.$$

Funktioiden f_P ja f_Q jakajien nojalla $f_P(P) = f_Q(Q) = 0$, joten funktion F arvoa pisteessä S ei ole määritelty. Kyseinen singulariteetti on kuitenkin poistuva, joten koska sekä $f_P(P-Q)$ ja $f_Q(Q-P)$ ovat nollasta eroavia, niin $F(P-Q) \neq 0$.

b) Tarkastellaan ensin Weilin parituksen osoittajaa korotettuna potenssiin m, jolloin

$$\frac{f_P(Q+S)^m}{f_P(S)^m} = f_P(Q+S)^m f_P(S)^{-m}.$$

Saatu tulo voidaan esittää vielä funktion f_P saamana arvona, kun muuttujana on jakaja $m(Q+S)-m(S)$, ts.

$$f_P(Q+S)^m f_P(S)^{-m} = f_P(m(Q+S)-m(S)).$$

Funktion $f_Q(X-S)$ jakaja $\mathrm{div}(f_Q(X-S)) = m(Q+S)-m(S)$. Jos funktiot f_P ja f_Q rajoitetaan näiden jakajien mukaisiin lähtöjoukkoihin, saadaan lauseen 2.3.6 nojalla

$$f_P\big|_{\mathrm{div}(f_Q(X-S))} = f_Q(X-S)\big|_{\mathrm{div}(f_P)}.$$

Koska funktion f_P jakaja $\mathrm{div}(f_P) = m(P)-m(\mathcal{O})$,

$$\begin{aligned}\frac{f_P(Q+S)^m}{f_P(S)^m} &= f_Q(m(P-S)-m(-S)) \\ &= \frac{f_Q(P-S)^m}{f_Q(-S)^m}.\end{aligned}$$

Weilin parituksen osoittaja ja nimittäjä ovat siis yhtäsuuret korotettuna potenssiin m, joten $e_m(P,Q)^m = 1$.

c) Todistetaan bilineaarisuusominaisuudesta vain ensimmäinen kohta, koska toisen kohdan todistus on identtinen ensimmäisen kanssa. Ensimmäisestä yhtälöstä

$$e_m(P_1+P_2,Q) = e_m(P_1,Q)e_m(P_2,Q)$$

saadaan Weilin parituksen yhtälöt sijoittamalla

$$\begin{aligned}\frac{f_{P_1+P_2}(Q+S)}{f_{P_1+P_2}(S)}\Big/\frac{f_Q(P_1+P_2-S)}{f_Q(-S)} &= \left(\frac{f_{P_1}(Q+S)}{f_{P_1}(S)}\Big/\frac{f_Q(P_1-S)}{f_Q(-S)}\right) \\ &\quad\cdot\left(\frac{f_{P_2}(Q+S)}{f_{P_2}(S)}\Big/\frac{f_Q(P_2-S)}{f_Q(-S)}\right) \\ &= \frac{f_{P_1}(Q+S)f_{P_2}(Q+S)}{f_{P_1}(S)f_{P_2}(S)}\Big/\frac{f_Q(P_1-S)f_Q(P_2-S)}{f_Q(-S)f_Q(-S)}.\end{aligned}$$

Näitä yhtälöitä uudelleenjärjestelemällä saadaan todistettavaksi väitteeksi

$$\frac{f_{P_1+P_2}(Q+S)}{f_{P_1}(Q+S)f_{P_2}(Q+S)}\Big/\frac{f_{P_1+P_2}(S)}{f_{P_1}(S)f_{P_2}(S)} = \frac{f_Q(P_1+P_2-S)f_Q(-S)}{f_Q(P_1-S)f_Q(P_2-S)}. \tag{5}$$

Todistuksen loppuun tarvitaan vielä kaksi uutta funktiota, F_{P_1,P_2} ja G_{P_1,P_2}. Määritellään ensin funktio

$$F_{P_1,P_2}(X) = \frac{f_{P_1+P_2}(X)}{f_{P_1}(X)f_{P_2}(X)}.$$

Tämän funktion F_{P_1,P_2} jakaja

$$\begin{aligned}\mathrm{div}(F_{P_1,P_2}) &= m(P_1+P_2)-m(\mathcal{O})-(m(P_1)-m(\mathcal{O}))-(m(P_2)-m(\mathcal{O})) \\ &= m((P_1+P_2)-(P_1)-(P_2)+(\mathcal{O})) \\ &= m\cdot\mathrm{div}(G_{P_1,P_2})\end{aligned}$$

on siis jonkin funktion G_{P_1,P_2} jakajan monikerta, ts. $\mathrm{div}(G_{P_1,P_2}) = (P_1+P_2)-(P_1)-(P_2)+(\mathcal{O})$, joten $F_{P_1,P_2}(X) = (G_{P_1,P_2}(X))^m$. Tämän nojalla yhtälön (5) vasemmasta puolesta saadaan

$$\begin{aligned}\frac{f_{P_1+P_2}(Q+S)}{f_{P_1}(Q+S)f_{P_2}(Q+S)} \Big/ \frac{f_{P_1+P_2}(S)}{f_{P_1}(S)f_{P_2}(S)} &= \frac{F_{P_1,P_2}(Q+S)}{F_{P_1,P_2}(S)} \\ &= \frac{G_{P_1,P_2}(Q+S)^m}{G_{P_1,P_2}(S)^m} \\ &= G_{P_1,P_2}(Q+S)^m G_{P_1,P_2}(S)^{-m}.\end{aligned}$$

Kuten kohdan b) todistuksessa mainittiin, saatu tulo voidaan esittää funktion G_{P_1,P_2} saamana arvona, kun muuttujana on funktion $f_Q(X-S)$ jakaja $m(Q+S)-m(S)$

$$\begin{aligned}G_{P_1,P_2}(Q+S)^m G_{P_1,P_2}(S)^{-m} &= G_{P_1,P_2}(m(Q+S)-m(S)) \\ &= G_{P_1,P_2}(\mathrm{div}(f_Q(X-S))).\end{aligned}$$

Lausetta 2.3.6 käyttämällä saadaan

$$\begin{aligned}G_{P_1,P_2}(\mathrm{div}(f_Q(X-S))) &= f_Q(\mathrm{div}(G_{P_1,P_2}) - S) \\ &= f_Q(((P_1+P_2)-(P_1)-(P_2)+(\mathcal{O}))-S) \\ &= \frac{f_Q(P_1+P_2-S)f_Q(-S)}{f_Q(P_1-S)f_Q(P_2-S)}\end{aligned}$$

Saatu osamäärä on yhtälön (5) oikea puoli, joten $e_m(P_1+P_2,Q) = e_m(P_1,Q)e_m(P_2,Q)$.

d) Tarkastellaan nyt funktiota

$$e_m(P,P) = \frac{f_P(P+S)}{f_P(S)} \Big/ \frac{f_P(P-S)}{f_P(-S)}.$$

Lauseen kohdan a) nojalla paritus on riippumaton pisteen S valinnasta, joten valitaan $S = \mathcal{O}$, jolloin

$$e_m(P,P) = \frac{f_P(P)}{f_P(\mathcal{O})} \Big/ \frac{f_P(P)}{f_P(\mathcal{O})} = 1.$$

Lauseen kohdan c) bilineaarisuusominaisuutta käyttämällä saadaan

$$\begin{aligned}e_m(P+Q,P+Q) &= e_m(P,P)e_m(P,Q)e_m(Q,P)e_m(Q,Q) \\ &= e_m(P,Q)e_m(Q,P) \\ &= 1.\end{aligned}$$

e) Valitaan piste $P \in E[m]$ niin, että $e_m(P,Q) = 1$ kaikilla $Q \in E[m]$. Weilin paritus voidaan esittää kahden jakajan $D_P = (P-S)-(-S)$ ja $D_Q = (Q+S)-(S)$ avulla. Tällöin

$$e_m(P,Q) = f_P(D_Q)/f_Q(D_P).$$

Nyt, jos $e_m(P,Q) = 1$, aikaisemmin saatuja arvoja sijoittamalla saadaan

$$\begin{aligned} e_m(P,Q) &= \frac{f_P(D_Q)}{f_Q(D_P)}, \\ f_P(D_Q) &= f_Q(D_P), \\ \frac{f_P(Q+S)}{f_P(S)} &= f_Q(D_P), \\ f_P(Q+S) &= f_Q(D_P) f_P(S). \end{aligned}$$

Koska Weilin paritus on riippumaton pisteen S valinnasta, voidaan piste S korvata pisteellä $Q+S$ ja tämän jälkeen sijoittaa yhtälöön aikaisemmin saatu arvo $f_P(Q+S)$. Tällöin

$$\begin{aligned} f_P([2]Q+S) &= f_Q(D_P) f_P(Q+S) \\ &= f_Q(D_P)^2 f_P(S). \end{aligned}$$

Kun tätä prosessia toistetaan m kertaa, saadaan

$$f_P([m]Q+S) = f_Q(D_P)^m f_P(S).$$

Alkuperäisen oletuksen mukaan $Q \in E[m]$, joten $[m]Q = \mathcal{O}$. Näin ollen

$$f_P(S) = f_Q(D_P)^m f_P(S).$$

Aikaisemmin saatu yhtälö $f_P(Q+S) = f_Q(D_P) f_P(S)$ voidaan nyt korottaa potenssiin m. Tällöin saadaan yhtälö

$$f_P(Q+S)^m = f_Q(D_P)^m f_P(S)^m,$$

ja koska $f_P(S) = f_Q(D_P)^m f_P(S)$, saadaan yhtälön oikeaksi puoleksi $f_P(S)^m$. Näin saadaan uusi yhtälö

$$f_P(Q+S)^m = f_P(S)^m, \tag{6}$$

kaikilla $S \in E[m]$ ja $Q \in E[m]$.

Weilin parituksen määritelmässä on annettu funktion f_P jakaja $\operatorname{div}(f_P) = m(P) - m(\mathcal{O})$. Näin ollen $\operatorname{div}(f_P^m) = m^2(P) - m^2(\mathcal{O})$, eli jos $P \neq \mathcal{O}$, niin funktion f_P^m nollakohta on piste P. Toisin sanoen, $f_P^m(P) = 0$.

Edellä todistetun kaavan (6) mukaan $f_P(Q+P)^m = 0$ kaikilla $Q \in E[m]$, joten funktiolla f_P^m on nollakohtina kaikki ryhmän $E[m]$ pisteet. Tämä on ristiriidassa funktion jakajan $\operatorname{div}(f_P^m) = m^2(P) - m^2(\mathcal{O})$ kanssa, jonka mukaan funktiolla on vain yksi nollakohta pisteessä P. □

3.3 Taten paritus

Tässä kappaleessa esitellään Taten paritus. Kappaleen todistukset mukailevat kirjan [3] todistuksia. Esitetään Taten parituksen määritelmää varten vielä tarvittavat

ykkösenjuurten joukon ja kunnan K_0 määritelmät. Parituksen määritelmässä elliptinen käyrä E on määritelty yli kunnan K_0. Olkoon n kokonaisluku, joka ei jaa kunnan K_0 karakteristikaa $\mathrm{ch}(K_0)$. Tällöin kunta $K = K_0(\mu_n)$ on kunnan K_0 laajennus, jossa $\mu_n = \{u \in \overline{K_0} : u^n = 1\}$, eli toisin sanoen joukkoon μ_n kuuluu n:nnet ykkösenjuuret kunnasta $\overline{K_0}$.

Määritelmä 3.3.1. Olkoon E elliptinen käyrä, joka on määritelty yli kunnan K_0, pisteet $P \in E(K)[n]$ ja $Q \in E(K)$, ja f_P funktio, jolla $\mathrm{div}(f_P) = n(P) - n(\mathcal{O})$. Olkoon jakaja $D \sim (Q) - (\mathcal{O})$ jokin nolla-asteinen jakaja, joka on määritelty yli kunnan K, ja jolla jakajan D ja funktion f_P jakajan $\mathrm{div}(f_P)$ kantajat ovat erilliset.

Tällainen jakaja D voidaan konstruoida valitsemalla jokin piste $S \in E(K)$, ja määrittelemällä $D = (Q + S) - (S)$. Tällöin Taten paritus on kuvaus

$$\tau : E(K)[n] \times E(K)/nE(K) \to K^*/(K^*)^n,$$

$$\tau(P, Q) = f_P(D) = \frac{f_P(Q + S)}{f_P(S)}.$$

Parituksen arvo $f_P(D)$ on kunnan K alkio, koska f_P ja D ovat määriteltyjä yli kunnan K. Piste $Q \in E(K)$ ajatellaan parituksessa ekvivalenssiluokan edustajana ryhmässä $E(K)/nE(K)$. Parituksen lähtöjoukon ryhmä $E(K)/nE(K)$ on tekijäryhmä, jossa ryhmä $nE(K) = \{[n]P : P \in E(K)\}$. Tekijäryhmä $E(K)/nE(K)$ voidaan ajatella ryhmän $E(K)$ pisteiden ekvivalenssiluokkien joukkona niin, että $P_1 \equiv P_2$ jos ja vain jos $(P_1 - P_2) \in nE(K)$. Maalijoukko on tekijäryhmä $K^*/(K^*)^n$ aliryhmän $(K^*)^n = \{u^n : u \in K^*\}$ suhteen.

Taten parituksen arvot eivät ole kunnan K^* hyvin määriteltyjä alkioita, koska arvot riippuvat jakajan D ja tekijäryhmän $E(K)/nE(K)$ ekvivalenssiluokan edustajan Q valinnasta. Tämän takia parituksen arvoja täytyy tarkastella ekvivalenssiluokkina ryhmässä $K^*/(K^*)^n$. Parituksen saama arvo on kuitenkin hyvin määritelty ryhmän $K^*/(K^*)^n$ alkiona, kuten kirjan [3] sivuilla 187-188 osoitetaan.

Esitetään nyt Taten parituksen tärkeimmille ominaisuuksille, eli bilineaarisuudelle ja epädegeneratiivisuudelle todistukset.

Lause 3.3.2. *Taten parituksella on seuraavat ominaisuudet:*

a) Taten paritus on bilineaarinen, eli

$\tau(P_1+P_2, Q) = \tau(P_1, Q)\tau(P_2, Q)$, *kaikilla* $P_1, P_2 \in E(K)[n]$ *ja* $Q \in E(K)/nE(K)$

ja

$\tau(P, Q_1+Q_2) = \tau(P, Q_1)\tau(P, Q_2)$, *kaikilla* $P \in E(K)[n]$ *ja* $Q_1, Q_2 \in E(K)/nE(K)$.

b) Oletetaan, että K on äärellinen kunta. Taten paritus on epädegeneroitunut, eli kaikilla $P \in E(K)[n], P \neq \mathcal{O}$ on olemassa $Q \in E(K)/nE(K)$ jolla $\tau(P, Q) \neq 1$, ja kaikilla $Q \in E(K)/nE(K)$, $Q \neq nE(K)$ on olemassa $P \in E(K)[n]$, jolla $\tau(P, Q) \neq 1$.

Todistus. Bilineaarisuuden todistus on esitetty kirjan [3] sivuilla 188-189 ja parituksen epädegeneratiivisuuden todistus löytyy artikkelista [6]. □

Tutkitaan nyt Taten paritusta kunnassa $K_0 = \mathbb{F}_q$. Olkoon E elliptinen käyrä, joka on määritelty yli kunnan $\mathbb{F}_q$. Oletetaan, että elliptisen käyrän E kardinaliteetti $\#E(\mathbb{F}_q) = hn$, jossa n on kokonaisluku, jolla $\text{syt}(n, q) = 1$. Olkoon k pienin positiivinen kokonaisluku toteuttaen ehdon $n|(q^k - 1)$. Tällöin kunta $K = K_0(\mu_n)$ on äärellinen laajennus $\mathbb{F}_{q^k}$.

Kuten määritelmässä 3.3.1 esitettiin, Taten parituksen maalijoukkona on ryhmä $K^*/(K^*)^n = \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$, ja parituksen arvot ovat tällöin ekvivalenssiluokkia ryhmässä $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$. Kryptografisia käytännön sovelluksia varten näillä ekvivalenssiluokilla tulisi olla yksiselitteinen edustaja. Ongelmaksi äärellisissä kunnissa muodostuvat siis lukujen n:nnet ykkösenjuuret. Näistä päästään helposti eroon, kun korotetaan parituksen saama arvo potenssiin $(q^k - 1)/n$. Potenssiin korotuksen ansiosta parituksen maalijoukosta tulee ryhmän $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$ sijasta ryhmä μ_n. Taten parituksen pohjalta saadaan kryptografisiin sovelluksiin huomattavasti paremmin soveltuva *redusoitu Taten paritus*.

Määritelmä 3.3.3. Olkoon E elliptinen käyrä, joka on määritelty yli kunnan $\mathbb{F}_q$. Redusoitu Taten paritus on alla määritelty kuvaus

$$\hat{\tau} : E[n] \times E[n] \to \mu_n.$$

Olkoon $P, Q, R \in E[n]$. Olkoon f_P funktio, jolla $\text{div}(f_P) = n(P) - n(\mathcal{O})$ ja olkoon jakaja $D = (Q + R) - (R)$. Piste R valitaan niin, että se toteuttaa ehdon $R \notin \{\mathcal{O}, P, -Q, P - Q\}$. Tällä pisteen R valinnalla varmistetaan, että jakajilla D ja $\text{div}(f_P)$ on toisistaan eroavat kantajat. Tällöin redusoitu Taten paritus on

$$\hat{\tau}(P, Q) = f_P(D)^{(q^k-1)/n} = \left(\frac{f_P(Q + R)}{f_P(R)}\right)^{(q^k-1)/n}.$$

Paritus on bilineaarinen ja epädegeneroitunut.

Taten parituksen mahdollisesti tärkein ero kryptografisten sovellusten kannalta verrattuna Weilin parituksen on se, että Taten parituksessa funktioita f tarvitaan kaksi kappaletta, kun taas Weilin parituksessa niitä tarvitaan neljä. Seuraavassa kappaleessa esitettävä Millerin algoritmi laskee näitä tarvittavia funktioita lineaarisessa ajassa. Taten paritus on siis kyseisten funktioiden laskemisen suorittamiseen vaadittavan ajan myötä kaksi kertaa tehokkaampi käyttää, kuin Weilin paritus, jonka takia Taten paritusta käytetään Weilin parituksen sijasta monissa kryptografian sovelluksissa. [1]

3.4 Millerin algoritmi

Sekä Weilin, että Taten parituksissa on määritelty tarkasti minkälaiset jakajat tarvitaan niissä käytetyille funktioille. Tässä kappaleessa esitetään yhdysvaltalaisen

matemaatikon Victor Millerin kehittämä algoritmi, jolla pystytään laskemaan lineaarisessa ajassa tarvittavia funktioita. Algoritmi on erittäin tärkeässä roolissa parituksiin perustuvan kryptografian sovelluksissa. Algoritmissa asetetaan ensin nollasta eroava käyrän E piste $T = P$ sekä valitaan positiivinen kokonaisluku m, jolla on binääriesitys

$$m = \varepsilon_0 + \varepsilon_1 \cdot 2^1 + \varepsilon_2 \cdot 2^2 + ... + \varepsilon_t \cdot 2^t,$$

missä $\varepsilon_i \in \{0, 1\}$ ja $\varepsilon_t \neq 0$. Algoritmia varten määritellään myös funktio $f = 1$, jonka jälkeen funktiota f iteroidaan käyttämällä apuna funktiota

$$h_{P,Q}(x, y) = \begin{cases} \dfrac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2 - a_1\lambda + a_2}, & \text{jos } \lambda \neq \infty, \\ x - x_P, & \text{jos } \lambda = \infty, \end{cases}$$

missä λ on pisteiden P ja Q läpi kulkevan suoran kulmakerroin, tai jos suora on pystysuora, $\lambda = \infty$. Algoritmin lopussa saavutetaan funktio f, joka täyttää parituksiin tarvittavat ehdot. Algoritmin iteraatiokierrokset menevät seuraavasti:

1) Aseta $T = P$ ja $f = 1$
2) Toista $i = t - 1 \text{ -> } 0$
3) Aseta $f = f^2 \cdot h_{T,T}$
4) Aseta $T = [2]T$
5) Jos $\varepsilon_i = 1$, niin
6) Aseta $f = f \cdot h_{T,P}$
7) Aseta $T = T + P$
8) Palauta funktio f

Algoritmi 1: *Millerin algoritmi.*

Esitetään seuraavaksi kaksiosainen lause, jonka kohdassa (a) näytetään miten Millerin algoritmin käyttämät funktiot määritellään, ja kohdassa (b) esitetään Millerin algoritmi. Lauseen todistus seuraa kirjan [1] todistusta.

Lause 3.4.1. *Olkoon E elliptinen käyrä, joka esitetään Weierstrassin yhtälöllä (2), ja olkoon $P = (x_P, y_P)$ ja $Q = (x_Q, y_Q)$ nollasta eroavia pisteitä käyrällä E.*

(a) Algoritmissa käytetyn funktion $h_{P,Q}$ jakaja on muotoa

$$div(h_{P,Q}) = (P) + (Q) - (P + Q) - (\mathcal{O}).$$

(b) ***Millerin algoritmi.*** *Ylempänä esitetty algoritmi 1 palauttaa funktion f_P, jonka jakaja täyttää ehdon*

$$div(f_P) = m(P) - ([m]P) - (m - 1)(\mathcal{O}).$$

Jos piste $P \in E[m]$, niin $div(f_P) = m(P) - m(\mathcal{O})$.

Todistus. (a) Aloitetaan lauseen kohdan (a) todistaminen tapauksesta, jossa $\lambda \neq \infty$. Olkoon $y = \lambda x + v$ suora, joka kulkee pisteiden P ja Q lävitse, tai käyrän tangentti pisteessä P, jos $P = Q$. Suora leikkaa käyrän E pisteissä P, Q ja $-P - Q$, joten

$$\operatorname{div}(y - \lambda x - v) = (P) + (Q) + (-P - Q) - 3(\mathcal{O}).$$

Saatu jakaja on nyt funktion $h_{P,Q}$ osoittajan jakaja.

Funktion $h_{P,Q}$ nimittäjälle voidaan määritellä jakaja samalla tavalla. Määritelmästä 2.2.2 nähdään, että $x_{P+Q} = \lambda^2 + a_1\lambda - a_2 - x_P - x_Q$. Funktion $h_{P,Q}$ nimittäjä on siis

$$x - x_{P+Q} = x - \lambda^2 - a_1\lambda + a_2 + x_P + x_Q.$$

Tämä on pystysuora suora, joka leikkaa käyrän E pisteissä $P + Q$ ja $-P - Q$, joten sen jakaja

$$\operatorname{div}(x - x_{P+Q}) = (P + Q) + (-P - Q) - 2(\mathcal{O}).$$

Funktion $h_{P,Q}$ jakaja on siis

$$\begin{aligned}\operatorname{div}(h_{P,Q}) &= \operatorname{div}(y - \lambda x - v) - \operatorname{div}(x - x_{P+Q}) \\ &= (P) + (Q) + (-P - Q) - 3(\mathcal{O}) - ((P + Q) + (-P - Q) - 2(\mathcal{O})) \\ &= (P) + (Q) - (P + Q) - (\mathcal{O}).\end{aligned}$$

Jos $\lambda = \infty$, niin suora on pystysuora ja $P + Q = \mathcal{O}$. Funktion $h_{P,Q}$ jakaja on muotoa

$$\operatorname{div}(h_{P,Q}) = (P) + (Q) - (P + Q) - (\mathcal{O}) = (P) + (-P) - 2(\mathcal{O}),$$

joka on siis funktion $x - x_P$ jakaja.

(b) Lauseen kohdasta (a) huomataan, että algoritmin 3. ja 6. vaiheen funktioiden $h_{T,T}$ ja $h_{T,P}$ jakajat ovat

$$\begin{aligned}\operatorname{div}(h_{T,T}) &= 2(T) - ([2]T) - (\mathcal{O}), \\ \operatorname{div}(h_{T,P}) &= (T) + (P) - (T + P) - (\mathcal{O}).\end{aligned}$$

Algoritmin iteraatiokierroksia, eli vaiheita 2-7 suorittaessa annettua arvoa i kohden jokaisen kierroksen alussa pisteellä T ja funktiolla f on alkuarvot T_i^a ja f_i^a. Jokaisen kierroksen lopussa kyseiset muuttujat ovat saaneet arvot T_i^l ja f_i^l.

Aloitetaan algoritmin analysointi käsittelemällä, mitä pisteelle T tapahtuu yhden iteraatiokierroksen aikana. Yhden kierroksen aikana muuttujan T arvo tuplataan algoritmin vaiheessa 4, ja tämän jälkeen, jos $\varepsilon_i = 1$ siihen lisätään arvo P algoritmin vaiheessa 7. Tämä muuttuja T_i^l saadaan siis yhden kierroksen aikana relaatiolla

$$T_i^l = [2]T_i^a + [\varepsilon_i]P.$$

Kuten pisteen T myös funktion f muutos yhden kierroksen avulla voidaan esittää relaation muodossa. Algoritmin vaiheessa 3 funktio korotetaan toiseen potenssiin ja

kerrotaan funktiolla $h_{T,T}$. Jos $\varepsilon_i = 1$, niin algoritmin vaiheessa 6 funktio f kerrotaan vielä funktiolla $h_{2T,P}$ (koska algoritmin vaiheessa 4 pisteen T arvo on tuplattu ennen vaihetta 6). Näin ollen funktio f_i^l saadaan esitettyä relaatiolla

$$f_i^l = (f_i^a)^2 \cdot h_{T_1^a,T_1^a} \cdot h_{2T_i^a,P}^{\varepsilon_i}.$$

Funktion f_i^l jakaja saadaan siten esitettyä funktion f_i^a jakajan avulla:

$$\begin{aligned}
\operatorname{div}(f_i^l) &= 2\ \operatorname{div}(f_i^a) + \operatorname{div}(h_{T_i^a,T_i^a}) + \varepsilon_i\ \operatorname{div}(h_{2T_i^a,P}) \\
&= 2\ \operatorname{div}(f_i^a) + (2(T_i^a) - ([2]T_i^a) - (\mathcal{O})) + \varepsilon_i(([2]T_i^a) + (P) - ([2]T_i^a + P) - (\mathcal{O})) \\
&= 2\ \operatorname{div}(f_i^a) + 2(T_i^a) - ([2]T_i^a + [\varepsilon_i]P) + \varepsilon_i(P) - (1+\varepsilon_i)(\mathcal{O}) \\
&= 2\ \operatorname{div}(f_i^a) + 2(T_i^a) - (T_i^l) + \varepsilon_i(P) - (1+\varepsilon_i)(\mathcal{O}).
\end{aligned}$$

Jokaisen iteraatiokierroksen lopussa saadut arvot T_i^l ja f_i^l ovat seuraavan kierroksen aloitusarvot, eli $T_i^l = T_{i-1}^a$ ja $f_i^l = f_{i-1}^a$. Näin ollen saadaan pisteelle T annettua rekursioyhtälö

$$\begin{aligned}
T_{i-1}^a - [2]T_i^a &= T_i^l - [2]T_i^a \\
&= ([2]T_i^a + [\varepsilon_i]P) - [2]T_i^a \\
&= [\varepsilon_i]P,
\end{aligned}$$

ja funktion f jakajalle rekursioyhtälö

$$\begin{aligned}
\operatorname{div}(f_{i-1}^a) - 2\ \operatorname{div}(f_i^a) &= \operatorname{div}(f_i^l) - 2\ \operatorname{div}(f_i^a) \\
&= 2\ \operatorname{div}(f_i^a) + 2(T_i^a) - (T_i^l) + \varepsilon_i(P) - (1+\varepsilon_i)(\mathcal{O}) - 2\ \operatorname{div}(f_i^a) \\
&= 2(T_i^a) - (T_i^l) + \varepsilon_i(P) - (1+\varepsilon_i)(\mathcal{O}) \\
&= 2(T_i^a) - (T_{i-1}^a) + \varepsilon_i(P) - (1+\varepsilon_i)(\mathcal{O}).
\end{aligned}$$

Näiden rekursioyhtälöiden avulla voidaan laskea algoritmin viimeisen iteraatiokierroksen palauttaman funktion jakaja. Tähän tarvitaan kuitenkin ensin tietoa siitä, mikä pisteen T arvo on algoritmin päätyttyä. Tämä saadaan esitettyä todistuksessa aiemmin esitettyjen yhtälöiden avulla, sekä käyttämällä lauseessa annettua kokonaisluvun m binääriesitystä:

$$\begin{aligned}
T_0^l &= [\varepsilon_0]P + [2]T_0^a \\
&= [\varepsilon_0]P + \left(\sum_{i=1}^{t-1} 2^i (T_{i-1}^a - [2]T_i^a)\right) + [2^t]T_{t-1}^a \\
&= [\varepsilon_0]P + \sum_{i=1}^{t-1} [2^i\varepsilon_i]P + [2^t]T_{t-1}^a \\
&= \sum_{i=0}^{t} [2^i\varepsilon_i]P \\
&= [m]P.
\end{aligned}$$

Millerin algoritmin palauttama funktion f jakaja on

$$\begin{aligned}
\operatorname{div}(f_0^a) &= 2\ \operatorname{div}(f_0^a) + 2(T_0^a) - (T_0^l) + \varepsilon_0(P) - (1+\varepsilon_0)(\mathcal{O}) \\
&= \left(\sum_{i=1}^{t-1} 2^i(\operatorname{div}(f_{i-1}^a) - 2\ \operatorname{div}(f_i^a))\right) + 2(T_0^a) - ([m]P) + \varepsilon_0(P) - (1+\varepsilon_0)(\mathcal{O}) \\
&= \left(\sum_{i=1}^{t-1} 2^i(2(T_i^a) - (T_{i-1}^a) + \varepsilon_i(P) - (1+\varepsilon_i)(\mathcal{O}))\right) + 2(T_0^a) - ([m]P) \\
&+ \varepsilon_0(P) - (1+\varepsilon_0)(\mathcal{O}) \\
&= 2^t(T_{t-1}^a) + \sum_{i=0}^{t-1} 2^i\varepsilon_i(P) - \sum_{i=0}^{t-1} 2^i(1+\varepsilon_i)(\mathcal{O}) - ([m]P) \\
&= m(P) - (m-1)(\mathcal{O}) - ([m]P).
\end{aligned}$$

□

Lauseessa 3.4.1 ja algoritmissa 1 esitettyä Millerin algoritmia voidaan käyttää sekä funktion f_P löytämiseen että funktion arvon $f_P(R)$ laskemiseen, jos piste $R \in E$. Algoritmia käytetään molempiin tarkoituksiin samalla tavalla, mutta funktion arvon laskentaa varten algoritmin vaiheissa 3 ja 6 laskutoimitukset tehdään käyttämällä funktioiden $h_{T,T}$ ja $h_{T,P}$ saamia arvoja pisteessä R.

4 Protokollat

Tässä osassa esitellään parituksiin perustuvia protokollia eli siis kryptografisia sovelluksia, joiden laskennallinen turvallisuus perustuu paritusten ominaisuuksiin. Esitellään ensimmäisenä kolmen osapuolen Diffie–Hellmanin avaimenvaihtoprotokolla parituksia käyttämällä.

4.1 Kolmen osapuolen Diffie–Hellmanin avaimenvaihtoprotokolla

Johdannossa esitettiin kolmen osapuolen Diffie–Hellmanin avaimenvaihtoprotokolla ilman paritusten käyttöä. Antoine Joux esitteli parituksia käyttäen artikkelissaan [7] yhden kierroksen kolmen osapuolen Diffie–Hellmanin avaimenvaihtoprotokollan. Kuten johdannossa mainittiin, parituksia käyttämällä algoritmin tehokkuutta saadaan parannettua huomattavasti, sillä protokollan käyttö saadaan tiivistettyä vain yhteen iteraatiokierrokseen ja huomattavasti pienempään määrään laskutoimituksia.

Oletetaan, että Alice, Bob ja Carol haluavat määrittää yhteisen salaisen avaimen. Bilineaarista paritusta käyttämällä tämä pystytään suorittamaan yhden kierroksen aikana.

1. Osapuolet sopivat keskenään ryhmät G_1 ja G_T, alkion $P \in G_1$ ja bilineaarisen parituksen
$$e : G_1 \times G_1 \to G_T.$$

2. Alice lähettää muille osapuolille alkion $[a]P$, Bob lähettää alkion $[b]P$ ja Carol lähettää alkion $[c]P$.

3. Alice laskee $e([b]P, [c]P)^a$, Bob laskee $e([a]P, [c]P)^b$ ja Carol laskee $e([a]P, [b]P)^c$.

Koska lauseen 3.1.1 nojalla kaikilla osapuolilla on tämän jälkeen sama alkio

$$e(P, P)^{abc} = e([b]P, [c]P)^a = e([a]P, [c]P)^b = e([a]P, [b]P)^c,$$

niin tätä alkiota voidaan käyttää avaimena. Koska luvut a, b ja c ovat vain alkuperäisten lähettäjien tiedossa, niin mahdollinen hyökkääjä saa selville vain alkiot $P, [a]P, [b]P$ ja $[c]P$. Saadakseen selville alkion $e(P, P)^{abc}$, hyökkääjän täytyy ratkaista bilineaarisen Diffie–Hellman-ongelman erikoistapaus, jossa $P = Q$.

Protokolla ei ole käytännön näkökulmasta niinkään hyödyllinen, sillä se on resistantti vain passiivisia hyökkäyksiä kohtaan. Aktiivisten hyökkäysten torjuminen vaatisi vielä vähintään toisen kommunikointikierroksen osapuolten välillä. Protokolla toimiikin lähinnä esimerkkinä mahdollisesta parituksien käytöstä protokollien kehityksessä.

Tämä protokolla voidaan yleistää kolmen osapuolen sijasta myös useammalle osapuolelle. Näin saatu m:n osapuolen yhden kierroksen protokolla käyttää tehokkaasti laskettavaa multilineaarista kuvausta $g_n : G_1^{m-1} \to G_T$, josta saadaan taas BDHP:ta vastaava ongelma; annetuilla muuttujilla $P, [a_1]P, [a_2]P, ..., [a_n]P$ pitäisi laskea $g_n(P, P, ..., P)^{a_1 a_2 ... a_m}$. Tämänkaltaisen multilineaarisen kuvauksen olemassaolo kaikilla $m > 3$ on kuitenkin avoin ongelma, joten useammalle osapuolelle protokolla ei välttämättä toimi. [8]

Tarkastellaan protokollan toimintaa nyt määritelmässä 3.2.1 esiteltyä Weilin paritusta käyttämällä. Protokollan ongelmaksi tulee selvästi se, että lauseen 3.2.2 nojalla $e_m(P, P) = 1$ riippumatta pisteen P valinnasta. Weilin paritus ei kyseisen ominaisuuden vuoksi sovellu tällaisenaan kryptografisiin sovelluksiin, koska parituksia käyttävissä sovelluksissa yhtenä toimintaperiaatteena on yleensä yksittäisen pisteen P monikertojen, eli pisteiden $P_1 = [a]P$ ja $P_2 = [b]P$ käyttäminen parituksessa. Paritusta voidaan kuitenkin muuttaa niin, että uusi *muunnettu Weilin paritus* $\hat{e}$ toteuttaa kyseisen vaatimuksen $\hat{e}_m(P, P) \neq 1$.

Määritelmä 4.1.1. Muunnettu Weilin paritus $\hat{e}$, on paritus

$$\hat{e}_m(P, Q) = e_m(P, \phi(Q)),$$

jossa ϕ on vääristämiskuvaus käyrällä E.

Määritelmässä mainitun vääristämiskuvauksen avulla piste Q saa uuden arvon parituksen toiminnan varmistamiseksi. Kuvaus ϕ voidaan määritellä seuraavasti:

Määritelmä 4.1.2. Olkoon $m \geq 3$ alkuluku, E elliptinen käyrä ja $P \in E[m]$. Kuvaus $\phi : E \to E$ on m-vääristämiskuvaus, jos

1. $\phi([n]P) = [n]\phi(P)$ kaikilla kokonaisluvuilla $n \geq 1$.

2. $e_m(P, \phi(Q))$ on primitiivinen m:s ykkösenjuuri, eli $e_m(P, \phi(Q))^r = 1$ jos ja vain jos $m|r$.

Kuten aikaisemminkin on mainittu, muunnetun Weilin parituksen tärkeimmät ominaisuudet ovat sen epädegeneratiivisuus ja etenkin seuraavassa lauseessa esitetty ominaisuus, jonka mukaan $\hat{e}_m(P, P) \neq 1$.

Lause 4.1.3. *Olkoon E elliptinen käyrä, $P \in E[m]$, ϕ on $m-$vääristämiskuvaus pisteelle P, ja $\hat{e}_m$ muunnettu Weilin paritus. Olkoon pisteet Q ja R pisteen P monikertoja, ts. $Q = [s]P$ ja $R = [t]P$ jollain $s, t \in \mathbb{N}$. Tällöin*

$$\hat{e}_m(Q, R) = 1 \text{ jos ja vain jos } Q = \mathcal{O} \text{ tai } R = \mathcal{O}.$$

Todistus. Määritelmän 4.1.2, Weilin parituksen lineaarisuuden ja lauseen 3.1.1 nojalla

$$\hat{e}_m(Q, R) = \hat{e}_m([s]P, [t]P) = e_m([s]P, \phi([t]P)) = e_m([s]P, [t]\phi(P)) = e_m(P, \phi(P))^{st}.$$

Kuvauksen arvo $e_m(P, \phi(P))$ on primitiivinen m:s ykkösenjuuri, joten

$$\begin{aligned} \hat{e}_m(Q, R) = 1 &\iff m|st \\ &\iff m|s \text{ tai } m|t \\ &\iff Q = \mathcal{O} \text{ tai } R = \mathcal{O}. \end{aligned}$$

□

4.2 Lyhyiden allekirjoitusten järjestelmä

Parituksia voidaan käyttää avaimenvaihtoprotokollien lisäksi myös digitaalisten dokumenttien allekirjoittamiseen. Nyt esitettävän lyhyiden allekirjoitusten järjestelmän (BLS-järjestelmän) avulla voidaan allekirjoittaa dokumentteja erittäin lyhyillä allekirjoituksilla, kuten Dan Boneh, Ben Lynn ja Hovav Shacham ovat teoksessaan [9] esittäneet.

Järjestelmän nimessäkin mainittu yksi järjestelmän tärkeimmistä ominaisuuksista on nimenomaan juuri se, kuinka lyhyitä allekirjoitukset ovat niiden turvallisuuteen nähden. Allekirjoituksena toimii nimittäin yksittäinen piste (x, y) elliptiseltä käyrältä $E(\mathbb{F}_q)$. Tämä yksittäinen piste voidaan vielä pakata, jolloin piste voidaan esittää vain yhtenä lukuna $n \in \mathbb{F}_q$. Kyseinen pisteen pakkaaminen on mahdollista, koska elliptisellä käyrällä pisteen x-koordinaatti määrittää suoraan pisteen y-koordinaatin itseisarvon $|y|$. Pisteen x-koordinaatista vastaanottaja pystyy laskemaan arvon $\pm y$ laskemalla neliöjuuren kunnassa $\mathbb{F}_q$. Allekirjoituksen lähettäjä voi siis lähettää pelkästään pisteen x-koordinaatin ja yhden ylimääräisen bitin, josta vastaanottaja saa selville kumpi juurista tulee valita. [1]

Esimerkkinä BLS-järjestelmän allekirjoituksien lyhyydestä voidaan käyttää kahta yleisesti käytettyä allekirjoitusjärjestelmää RSA:ta ja DSA:ta. Käytettäessä RSA-järjestelmää 1024-bittisellä moduluksella allekirjoitukset ovat 1024 bittiä pitkiä, ja

DSA-järjestelmän allekirjoitukset ovat 1024-bittisellä moduluksella 320 bittiä pitkiä. BLS-järjestelmällä luodut allekirjoitukset taas ovat 160 bittiä pitkiä, ja vastaavat turvallisuudeltaan 320-bittistä DSA-allekirjoitusta. [9]

Esitetään seuraavaksi BLS-järjestelmän toiminta ja todistetaan allekirjoituksen oikeellisuus.

Lause 4.2.1. *Seuraavalla menettelyllä Alice voi allekirjoittaa digitaalisen dokumentin, ja Bob voi tarkistaa allekirjoituksen oikeellisuuden.*

1. Alice ja Bob sopivat keskenään kommutatiiviset ryhmät G_1, G_2 ja G_T, sekä alkion $P \in G_1$ niin, että on olemassa bilineaarinen paritus
$$e : G_1 \times G_2 \to G_T.$$
2. Alice valitsee salaisen kokonaisluvun m, joka on hänen salainen allekirjoitusavaimensa, ja laskee alkion $M = [m]P \in G_1$.
3. Alice julkaisee alkion M, joka on hänen julkinen tarkistusavaimensa.
4. Alice valitsee allekirjoitettavan dokumentin $D \in G_2$, laskee alkion $S = [m]D$ ja julkaisee allekirjoitetun dokumentin.
5. Bob hyväksyy allekirjoituksen, jos $e(M, D) = e(P, S)$.

Todistus. Parituksen bilineaarisuuden ja lauseen 3.1.1 nojalla

$$e(M, D) = e([m]P, D) = e(P, D)^m \text{ ja } e(P, S) = e(P, [m]D) = e(P, D)^m.$$

□

Menetelmässä dokumentti on esitetty alkiona $D \in G_2$. Tämä alkio on saatu käyttämällä jotakin kryptografista tiivistefunktiota alkuperäiseen dokumenttiin. Kyseisten tiivistefunktioiden tarkoituksena on olla johdannossakin mainittuja yksisuuntaisia funktioita, joten BLS-järjestelmän tarkoituksena ei olekaan olla kryptosysteemi, jota käytettäisiin lähetettävän dokumentin salaamiseen ja salauksen purkamiseen, vaan pelkästään järjestelmä mikä varmistaa, että vastaanottaja saa (luotettavan) dokumentin oikealta henkilöltä.

4.3 Identiteettiin perustuva salaus

Julkisen avaimen kryptosysteemeissä yhtenä selvänä ongelmana on viestiä lähettäessä varmistuminen siitä, että lähettäjä käyttää oikean vastaanottajan julkista avainta salatessaan viestiä. Yleisessä käytössä olevissa julkisen avaimen kryptosysteemeissä käytetään nykyään pääosin jonkunlaista julkisten avainten hallintajärjestelmää, jossa kolmantena osapuolena lähettäjän ja vastaajan lisäksi on varmentaja, jonka tehtävänä on generoida varmenteita julkisille avaimille. Tämänlainen varmenne (osapuolelle A) pitää sisällään A:n tunnistetiedot ja julkisen avaimen, sekä varmentajan

allekirjoituksen. Toinen osapuoli, kenellä on tiedossa varmentajan julkinen avain, voi tarkastaa tämän varmenteen allekirjoituksen ja siten luottaa A:n julkisen avaimen autenttisuuteen.

Tämänlaisissa kryptosysteemeissä on kuitenkin käytännon sovelluksissa ongelmia varmenteiden hallinnoimisen osalta. Esimerkkejä tällaisista ongelmista on esimerkiksi se, ettei viestin lähettäjä välttämättä tiedä, miten vastaanottajan varmenteen saa tietoonsa, tai sitä, onko vastaanottajan varmenne vielä voimassa. [8]

Tämänlaisia ongelmia pystytään vähentämään identiteettiin perustuvien kryptosysteemien avulla. Osapuolten julkisina avaimina käytetään jotain ennalta määriteltyä tunnistetietoa ID, esimerkiksi sähköpostiosoitetta, jolloin lähettäjä voi jo viestiä lähettäessään varmistua salauksen purkajan identiteetistä. Myös varmenteen voimassaolosta voidaan varmistua lisäämällä tunnistetietoon esimerkiksi päivämäärä tai vuosiluku, johon asti varmenne on voimassa.

Identiteettiin perustuvissakin kryptosysteemeissä tarvitaan kolmatta osapuolta viestin lähettäjän ja vastaanottajan välille. Kolmannella osapuolella on oma julkinen avaimensa, jota tarvitaan viestien salaamiseen. Tämän kolmannen osapuolen tehtävänä on jakaa viestin vastaanottajalle hänen henkilökohtainen salainen avaimensa, joka on generoitu tunnistetiedosta ID. Viestin lähettäjä voi siten käyttämällä pelkästään vastaanottajan tunnistetietoa ID ja kolmannen osapuolen julkista avainta lähettää viestin vastaanottajalle kokonaan ilman osapuolten välistä aiempaa kommunikointia. Vastaanottaja saa omalla, kolmannen osapuolen generoimalla salaisella avaimellaan purettua salauksen.

Ensimmäinen käytännöllinen identiteettiin perustuva kryptosysteemi oli Boneh–Franklin-kryptosysteemi, jonka Dan Boneh ja Matthew K. Franklin artikkelissaan [10] esittivät. Protokollan esityksessä on käytetty merkintää G^* ryhmän G nollasta eroaville alkioille, ja merkintää $\{0,1\}^*$ sanoille. Järjestelmässä kolmas osapuoli asettaa kryptosysteemin parametrit ja valitsee oman salaisen avaimensa seuraavalla tavalla:

1. Kolmas osapuoli valitsee ja julkaisee kommutatiiviset ryhmät G_1, G_2 ja G_T, alkion $P \in G_2$, sekä bilineaarisen parituksen $e : G_1 \times G_2 \to G_T$.

2. Kolmas osapuoli valitsee kokonaisluvun s, joka on kolmannen osapuolen salainen avain. Salaista avaintaan käyttäen kolmas osapuoli laskee ja julkaisee julkisen avaimensa $P_j = [s]P$.

3. Kolmas osapuoli valitsee kryptografiset tiivistefunktiot $H_1 : \{0,1\}^* \to G_1^*$ ja $H_2 : G_T \to \{0,1\}^n$ jollakin kokonaisluvulla n. Järjestelmässä viestiavaruus on $\mathcal{P} = \{0,1\}^n$ ja kryptotekstiavaruus $\mathcal{C} = G_2^* \times \{0,1\}^n$.

Kolmas osapuoli myös jakaa salaiset avaimet protokollan käyttäjille käyttämällä tunnistetietoa ID, joka on siis esimerkiksi binääriluvuksi muunnettu sähköpostiosoite. Tunnistetiedosta $ID \in \{0,1\}^*$ kolmas osapuoli laskee käyttäjän julkisen avaimen $Q_{ID} = H_1(ID) \in G_1^*$, ja laskee tätä julkista avainta käyttäen käyttäjän salaisen avaimen $D_{ID} = [s]Q_{ID}$, jonka hän lähettää salattua kanavaa pitkin käyttäjälle ID.

Salatakseen viestinsä $m \in \{0,1\}^n$ lähettäjä käyttää vastaanottajan julkista avainta $Q_{ID} = H_1(ID) \in G_1^*$, valitsee jonkin kokonaisluvun r ja laskee salatun viestin $C = ([r]P, m \oplus H_2(g_{ID}^r))$, jossa $g_{ID} = e(Q_{ID}, P_j) \in G_T^*$.

Viestin vastaanottaja saa purettua julkisella avaimella ID salatun viestin $C = (U, V) \in \mathcal{C}$ salauksen käyttämällä omaa salaista avaintaan $D_{ID} \in G_1^*$, ja laskemalla $m = V \oplus H_2(e(D_{ID}, U))$.

Lause 4.3.1. *Boneh–Franklin-kryptosysteemillä salatun viestin C salauksen purkaminen antaa alkuperäisen viestin m.*

Todistus. Viestin salaus ja salauksen purkaminen tapahtuu molemmat XOR-bittioperaatioita käyttämällä. Viestin m salaamisessa bittioperaatiota käytetään laskemaan $V = m \oplus H_2(g_{ID}^r)$, ja salauksen purkamisessa sitä käytetään laskemaan $m = V \oplus H_2(e(D_{ID}, U)$. Salauksen purkamiseen käytetty operaatio tuottaa oikean tuloksen, koska

$$e(D_{ID}, U) = e([s]Q_{ID}, [r]P) = e(Q_{ID}, P)^{sr} = e(Q_{ID}, P_j)^r = g_{ID}^r.$$

□

Kappaleen alussa mainittiin identiteettiin perustuvien kryptosysteemien hyvistä puolista verrattuna varmenteihin perustuviin kryptosysteemeihin. Boneh–Franklin-kryptosysteemistäkin on helppo kuitenkin huomata myös identiteettiin perustuvien kryptosysteemien ongelmia. Ensinnäkin kolmannen osapuolen on oltava varmasti luotettava, ja tässäkin järjestelmässä salaiset avaimet joudutaan kuitenkin lähettämään salattua kanavaa pitkin. Toiseksi, jos tunnistetietoon on edellä mainittuun tapaan lisätty esimerkiksi päivämäärä, johon asti varmenne on voimassa ja päivämääriä halutaan uusia aktiivisesti (esimerkiksi päivittäin) protokollaa käyttävissä sovelluksissa joko kehittäjän tai palvelun käyttäjien puolesta, kolmannen osapuolen tulee tällöin olla jatkuvasti verkossa ja/tai kolmannen osapuolen työmäärä voi helposti nousta liian suureksi sovelluksia varten. Tarkempaa vertailua julkisen avaimen kryptosysteemien ja identiteettiin perustuvien kryptosysteemien välillä löytyy artikkelista [11].

5 Yhteenveto

Tutkielmassa esiteltiin ensin pohjatiedoiksi perusasioita elliptisistä käyristä, jakajista ja torsiopisteistä. Näiden asioiden pohjalta tarkastelu siirtyi kolmannessa luvussa bilineaarisiin parituksiin, joiden perusteiden esittelyn jälkeen konkreettisina esimerkkeinä parituksista annettiin määritelmissä 3.2.1 ja 3.3.1 Weilin ja Taten paritukset. Paritusten esittelyn yhteydessä parituksille esitettiin myös ne ominaisuudet, jotka mahdollistavat paritusten käytön kryptografisissa sovelluksissa. Paritusten esittelyn jälkeen esiteltiin parituksissa tarvittavien funktioiden laskemiseen käytettävä Millerin algoritmi. Tutkielman neljännessä luvussa tarkasteltiin parituksia käyttäviä protokollia, joista konkreettisina esimerkkeinä esiteltiin kolmen osapuolen Diffie–Hellmanin avaimenvaihtoprotokolla, lyhyiden allekirjoitusten järjestelmä ja identiteettiin perustuva salaus.

Viitteet

[1] J.H. Silverman: *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1986.

[2] S. Friedel: *An Elementary Proof of the Group Law for Elliptic Curves.* Groups Complexity Cryptology, vol. 9, no. 2, (117-123). 2017.

[3] S. Galbraith: *Pairings.* Advances in Elliptic Curve Cryptography, (183-213). Cambridge University Press, 2005.

[4] J. Hoffstein, J. Pipher, J.H. Silverman: *An Introduction to Mathematical Cryptography.* Springer, New York, 2008.

[5] A. Aftuck: *The Weil Pairing on Elliptic Curves and Its Cryptographic Applications.* UNF Graduate Theses and Dissertations. 2011.

[6] F. Hess: *A note on the Tate Pairing of Curves over Finite Fields.* Archiv der Mathematik, vol. 82, (28–32), 2004.

[7] A. Joux: *A One Round Protocol for Tripartite Diffie-Hellman.* Journal of Cryptography, 17: 263276, 2004.

[8] A. Menezes: *An Introduction to Pairing-Based Cryptography.* `https://www.math.uwaterloo.ca/~ajmeneze/publications/pairings.pdf`, luettu 21.6.2023

[9] D. Boneh, B. Lynn, H. Shacham: *Short signatures from the Weil pairing.* In Advances in cryptology – ASIACRYPT 2001 (Gold Coast), Lecture Notes in Computer Science, vol. 2248, (514–532). Springer, Berlin, 2001.

[10] D. Boneh, M. Franklin: *Identity-based encryption from the Weil pairing.* Advances in Cryptology – CRYPTO 2001, Lecture Notes in Computer Science, vol. 2139, (213–229). 2001.

[11] K. Paterson, G. Price: *A comparison between traditional public key infrastructures and identity-based cryptography.* Information Security Technical Report, 8(3), (57–72). 2003.