Liitospohjainen kryptografia elliptisillä käyrillä

Pro gradu -tutkielma

Aada Illikainen

Matemaattisten tieteiden laitos

Oulun yliopisto

2023

Sisällys

Johdanto

Tässä tutkielmassa tutustutaan aluksi elliptisiin käyriin, yleistettyihin elliptisiin käyriin sekä niiden aritmetiikkaan. Näiden jälkeen perehdytään liitospohjaisiin kryptografisiin algoritmeihin elliptisellä käyrällä, joihin lukeutuvat kolmen osapuolen Diffie-Hellman, ID-pohjainen kryptosysteemi sekä BLS-allekirjoitus. Lukijalla oletetaan olevan esitietona kuntien sekä kuntalaajennusten tuntemusta. Tutkielmassa on käytetty lähteenä pääasiassa teosta [7].

Tutkielman ensimmäisessä luvussa määritellään Weierstrassin yhtälö, joka määrittelee elliptisen käyrän. Kyseisessä luvussa esitellään myös Weierstrassin yhtälön avulla määritellyn elliptisen käyrän aritmetiikkaa. Lisäksi määritellään muita asioita, joita myöhemmin käytetään tässä tutkielmassa.

Toisessa luvussa määritellään yleistetty Weierstrassin yhtälö. Yleistetty Weiertrassin yhtälö on tarpeellinen, jotta elliptinen käyrä voidaan määritellä kunnan $\mathbb{F}_2$ tai tällaisen kunnan kuntalaajennuksen yli. Tällaiset kunnat mahdollistavat tehokkaan laskennan tietokoneella, sillä luvut voidaan esittää binäärivektorina, ja esimerkiksi yhteenlasku voidaan yksinkertaisesti toteuttaa **xor**-operaation avulla. Luvussa esitellään tuloksia liittyen yleistetyn Weierstrassin yhtälön avulla määriteltyyn elliptiseen käyrään sekä esitellään Koblitz-käyrä.

Bilineaariset liitokset esitellään kolmannessa luvussa. Ennen Weilin ja Taten liitoksen määrittelemistä, luvussa esitellään tarvittavat käsitteet kuten äärellisen kertaluvun pisteet sekä jakajat elliptisellä käyrällä. Tutkielman lopussa käsiteltävissä kryptografisissa algoritmeissa Weilin liitos sekä Taten liitos ovat keskeisessä osassa, siispä liitoksien tehokasta laskemista varten esitellään myös Millerin algoritmi. Luvussa esitellään myös elliptisen käyrän diskreetin logaritmin ongelma (ECDLP) sekä Weilin liitoksen avulla toimiva MOV-algoritmi, jolla voidaan muuttaa ECDLP diskreetin logaritmin ongel-

maksi.

Neljännessä luvussa esitellään muodonmuutoskuvaus, joka on yksi ratkaisu sille, että Weilin liitos voisi olla ykkösestä eroava lineaarisesti riippuville pisteille. Tämä on tarpeellista, sillä liitoksiin pohjautuvissa kryptografisissa algoritmeissa Weilin liitos lasketaan lineaarisesti riippuville pisteille.

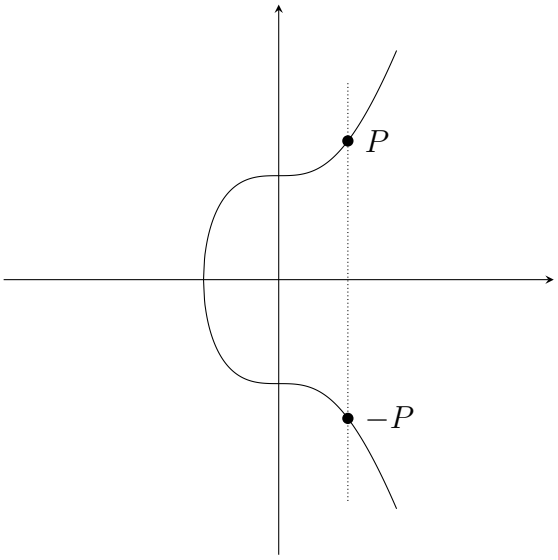
Luvuissa viisi, kuusi ja seitsemän esitellään elliptisen käyrän liitoksen käyttökohteita julkisen avaimen kryptografiassa. Tässä tutkielmassa käsitellään kolmen osapuolen Diffie-Hellman, ID-pohjainen kryptosysteemi sekä BLS-allekirjoitus.

1 Peruskäsitteitä

Määritelmä 1.1. *Elliptinen käyrä* E on äärettömyyspisteellä $\mathcal{O}$ laajennettu ratkaisujen joukko Weierstrassin yhtälöön

$$E : Y^2 = X^3 + AX + B,$$

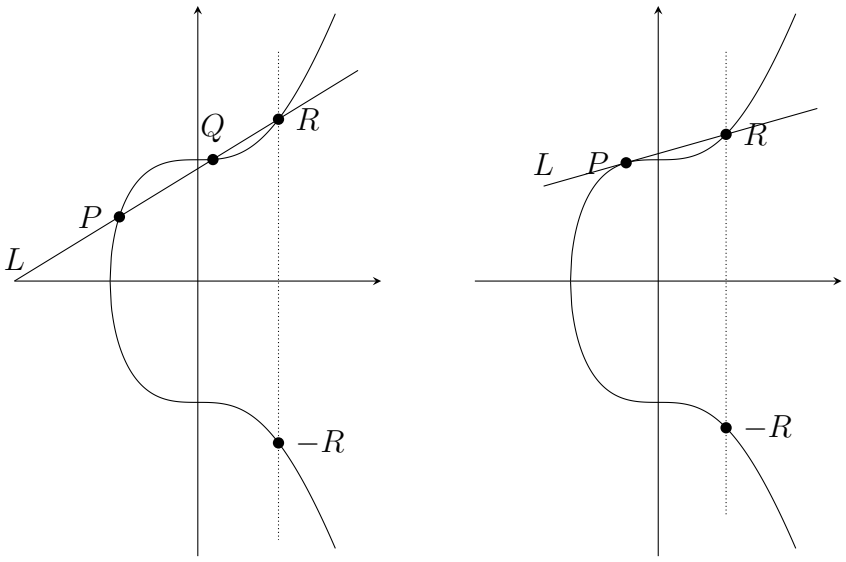
missä $4A^3 + 27B^2 \neq 0$.



Kuva 1: Vasta-alkio

Pisteen P vasta-alkio $-P$ elliptisellä käyrällä voidaan esittää graafisesti pisteen kautta kulkevan vertikaalisen suoran ja elliptisen käyrän leikkauspisteenä, kuten kuvassa 1. Pisteen $P = (x, y)$ *vasta-alkio* $-P$ on $(x, -y)$.

Yhteenlasku voidaan määritellä elliptiselle käyrälle pisteiden $P = (x_1, y_1)$ ja $Q = (x_2, y_2)$ välille seuraavasti. Olkoon L suora pisteiden P ja Q välillä, joka on muotoa $Y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(X - x_1)$. Jos pisteet P ja Q ovat yhtä suuria, niin suora L on tangentti elliptisellä käyrällä pisteessä P, joka on muotoa $Y - y_1 = \frac{3x_1^2 + A}{2y_1}(X - x_1)$. Suoran L ja elliptisen käyrän E leikkauspisteitä on



Kuva 2: Yhteenlasku elliptisellä käyrällä.

nyt kolme, jotka ovat pisteet P, Q sekä kolmas piste $R = (x_3, -y_3)$. Luvun λ ollessa suoran L kulmakerroin, pisteiden P ja Q summa on pisteen R vastaalkio $-R = (x_3, y_3)$, missä $x_3 = \lambda^2 - x_1 - x_2$ sekä $y_3 = \lambda(x_1 - x_3) - y_1$.

Lause 1.2. *Olkoon E elliptinen käyrä. Kaikille pisteille $P, Q \in E$ yhteenlaskun suhteen pätee*

(a) $P + \mathcal{O} = \mathcal{O} + P = P$,

(b) $P + (-P) = \mathcal{O}$,

(c) $(P + Q) + R = P + (Q + R)$,

(d) $P + Q = Q + P$.

Lause 1.3 (Hasse)**.** *Olkoon E elliptinen käyrä kunnan $\mathbb{F}_p$ yli. Pisteiden määrälle pätee*

$$\#E(\mathbb{F}_p) = p + 1 - t_p,$$

missä $|t_p| \leq 2\sqrt{p}$. Lukua t_p kutsutaan myös Frobeniuksen jäljeksi.

Määritelmä 1.4. *Rationaalifunktio* on kahden polynomin suhde, joka on muotoa

$$f(X) = \frac{a_0 + a_1X + a_2X^2 + \cdots + a_nX^n}{b_0 + b_1X + b_2X^2 + \cdots + b_mX^m}.$$

Lause 1.5. *Kompleksinen rationaalifunktio voidaan esittää muodossa*

$$f(X) = \frac{a(X-\alpha_1)^{e_1}(X-\alpha_2)^{e_2}\cdots(X-\alpha_r)^{e_r}}{b(X-\beta_1)^{d_1}(X-\beta_2)^{d_2}\cdots(X-\beta_r)^{d_r}}, \tag{1}$$

missä polynomit on jaettu tekijöihin nollakohtien avulla.

Määritelmä 1.6. Lauseen 1.5 mukaisessa esityksessä lukuja

(a) $\alpha_1, \ldots, \alpha_n$ kutsutaan funktion $f(X)$ *nollakohdiksi*,

(b) $\beta_1, \ldots, \beta_m$ kutsutaan funktion $f(X)$ *navoiksi*.

Määritelmä 1.7. Olkoon g kunnan $\mathbb{F}_p$ primitiivijuuri, sekä olkoon $h \in \mathbb{F}_p$ nollasta eroava alkio. *Diskreetin logaritmin ongelma* (DLP) on ongelma, jossa täytyy löytää sellainen kokonaisluku x, joka toteuttaa yhtälön

$$g^x \equiv h \pmod{p}.$$

Määritelmä 1.8. Olkoon luvut $a, b \in \{0, 1\}$. **xor**-operaatio määritellään Taulukon 1 mukaisesti.

a	b	a **xor** b
0	0	0
1	0	1
0	1	1
1	1	0

Taulukko 1: **xor**-operaatio.

Toisin sanoen **xor**-operaatio voidaan ilmaista muodossa $a + b \pmod 2$. Bittivektoreille **xor**-operaatio tehdään jokaiselle bitille erikseen.

2 Elliptiset käyrät kunnan $\mathbb{F}_{2^k}$ yli

Kryptografiaa sovelletaan yleisimmin elektronisissa laitteissa, jolloin on järkevää käyttää elliptistä käyrää kunnan $\mathbb{F}_{2^k}$ yli. Tällaista kuntalaajennusta käyttämällä alkiot voidaan ilmaista bittivektoreina, ja yhteenlaskut sekä reduktiot voidaan suorittaa **xor**-operaation avulla, joka voi nopeuttaa elliptisen käyrän operaatioita.

Weierstrassin yhtälössä on ongelmana se, että elliptisen käyrän diskriminantti on muotoa $-16(4A^3 + 27B^2)$, joka on 0 kunnassa $\mathbb{F}_{2^k}$. Voidaan määritellä yleistetty käyrä, jolla diskriminantti ei ole nolla.

Määritelmä 2.1. *Elliptinen käyrä* E on yhdessä äärettömyyspisteen $\mathcal{O}$ kanssa ratkaisujen joukko yleistettyyn Weierstrassin yhtälöön

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{2}$$

missä diskriminantti on muotoa

$$\begin{aligned}
&\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \text{ missä} \\
&b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6, \\
&b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.
\end{aligned}$$

Kun elliptinen käyrä E määritellään kunnan K yli, niin oletetaan, että Weierstrassin yhtälön kertoimet a_i sekä käyrän E pisteiden koordinaatit kuuluvat kuntaan K. Merkintä $E(K)$ tarkoittaa sitä, että käyrän pisteiden koordinaatit ovat määritelty kunnan K yli.

Lause 2.2. *Olkoon elliptinen käyrä E määritelty yleistetyn Weierstrassin yhtälön avulla. Pisteen $P = (x, y)$* vasta-alkio *on $-P = (x, -y - a_1x - a_3)$.*

Todistus. Olkoon elliptinen käyrä E määritelty yleistetyn Weierstrassin yhtälön avulla. Pisteen $P = (x_1, y_1)$ vasta-alkio $Q = (x_2, y_2)$ on pisteen P kautta kulkevan suoran $X = x_1$ ja elliptisen käyrän leikkauspiste, joka ei ole P.

Nyt koska pisteiden P ja Q x-koordinaatit ovat samat, voidaan muodostaa yleistetyn Weierstrassin yhtälön avulla yhtälö

$$y_1^2 + a_1x_1y_1 + a_3y_1 = y_2^2 + a_1x_1y_2 + a_3y_2.$$

Tämä yhtälö saadaan muotoon

$$\begin{aligned} &y_1^2 - y_2^2 + a_1x_1y_1 - a_1x_1y_2 + a_3y_1 - a_2y_2 \\ =&(y_1 - y_2)(y_1 + y_2) + (y_1 - y_2)a_1x_1 + (y_1 - y_2)a_3 = 0 \end{aligned}$$

Lisäksi $y_1 \neq y_2$, joten voidaan jakaa luvulla $(y_1 - y_2)$, jolloin saadaan

$$y_1 + y_2 + a_1x_1 + a_3 = 0.$$

Vasta-alkion y-koordinaatiksi saadaan

$$y_2 = -y_1 - a_1x_1 - a_3.$$

Vasta-alkio on siis piste $Q = (x_1, -y_1 - a_1x_1 - a_3)$. □

Lause 2.3. *Olkoon $E(\mathbb{F}_{p^k})$ määritelty yleistetyn Weierstrassin yhtälön avulla, sekä olkoon pisteet $P = (x_1, y_1), Q = (x_2, y_2)$ käyrällä E. Pisteiden summa $R = (x_3, y_3) = P + Q$ voidaan laskea seuraavasti.*

(a) *Jos $P = \mathcal{O}$, niin $P + Q = Q$. Vastaavasti jos $Q = \mathcal{O}$, niin $P + Q = P$.*

(b) *Jos $x_1 = x_2$ ja $y_1 + y_2 + a_1x_2 + a_3 = 0$, niin $P + Q = \mathcal{O}$.*

(c) *Muissa tapauksissa summan koordinaateiksi saadaan $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ ja $y_3 = -(\lambda + a_1)x_3 - \nu - a_3$, missä*

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{kun } x_1 \neq x_2, \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \text{kun } x_1 = x_2, \end{cases}$$

$$\nu = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, & \text{kun } x_1 \neq x_2, \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, & \text{kun } x_1 = x_2. \end{cases}$$

Pisteiden yhteenlasku voidaan myös esittää algoritmina, kuten Algoritmissa 1.

Todistus. Olkoon $P, Q \in E(\mathbb{F}_{p^k})$. Merkitään $P = (x_1, y_1)$ ja $Q = (x_2, y_2)$. Todistukset kohtiin (a) ja (b) löytyvät Joseph H. Silvermanin kirjan [9] kappaleesta III.2.

(c) Olkoon $E(\mathbb{F}_{p^k})$ elliptinen käyrä muotoa

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

ja olkoon $P = (x_1, y_1)$ sekä $Q = (x_2, y_2)$ pisteitä käyrällä $E(\mathbb{F}_{p^k})$. Yhteenlasku käyrällä määritellään yhteenlaskettavien pisteiden kautta kulkevan suoran L avulla. Suora L leikkaa käyrää E yhteenlaskettavien pisteiden lisäksi kolmannessa pisteessä, jonka vasta-alkio on pisteiden summa. Kun yhteenlaskettavat pisteet ovat erillisiä, suora L on muotoa

$$Y = \frac{y_2 - y_1}{x_2 - x_1}(X - x_1) + y_1 = \lambda X + \nu,$$

missä $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ ja

$$\nu = -x_1\lambda + y_1 = \frac{-x_1y_2 + x_1y_1}{x_2 - x_1} + y_1 = \frac{x_2y_1 - x_1y_2}{x_2 - x_1}.$$

Vastaavasti jos pisteet P ja Q ovat yhtäsuuret, niin suora L on tangentti elliptisellä käyrällä pisteessä P. Nyt yleistetystä Weierstrassin yhtälöstä (2) saadaan implisiittisen derivaatan avulla yhtälön vasemmaksi puoleksi

$$\begin{aligned}\frac{d}{dX}(Y^2 + a_1XY + a_3Y) &= \frac{dY}{dX}2Y + \frac{dY}{dX}a_1X + Y\frac{d}{dX}a_1X + \frac{dY}{dX}a_3 \\ &= \frac{dY}{dX}(2Y + a_1X + a_3) + a_1Y.\end{aligned}$$

Yhtälön oikeaksi puoleksi saadaan

$$\frac{d}{dX}(X^3 + a_2X^2 + a_4X + a_6) = 3X^2 + 2a_2X + a_4,$$

jolloin

$$\frac{dY}{dX}(2Y + a_1X + a_3) + a_1Y = 3X^2 + 2a_2X + a_4.$$

Suoran L kulmakertoimeksi saadaan siis

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}.$$

ν on muotoa $-x_1\lambda + y_1$, ja laskemalla se auki saadaan

$$\begin{aligned}\nu &= -x\frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} + y_1 \\ &= \frac{-3x_1^3 - 2a_2x_1^2 - a_4x_1 + a_1y_1x_1 + 2y_1^2 + a_1x_1y_1 + a_3y_1}{2y_1 + a_1x_1 + a_3}.\end{aligned}$$

Lauseketta voidaan sieventää hieman korvaamalla $y_1^2 + a_1x_1y_1 + a_3y_1$ yleistetyn Weiertrassin yhtälön mukaan lausekkeella $x_1^3 + a_2x_1^2 + a_4x_1 + a_6$. Näin saadaan

$$\begin{aligned}\nu &= \frac{-3x_1^3 - 2a_2x_1^2 - a_4x_1 + x_1^3 + a_2x_1^2 + a_4x_1 + a_6 + y_1^2 + a_1x_1y_1}{2y_1 + a_1x_1 + a_3} \\ &= \frac{-3x_1^3 - 2a_2x_1^2 - a_4x_1 + 2x_1^3 + 2a_2x_1^2 + 2a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \\ &= \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.\end{aligned}$$

Nyt, koska halutaan tarkastella elliptisen käyrän ja suoran L leikkauspisteitä, niin sijoittamalla $Y = \lambda X + \nu$ elliptisen käyrän yhtälöön saadaan

$$(\lambda X + \nu)^2 + a_1X(\lambda X + \nu) + a_3(\lambda X + \nu) = X^3 + a_2X^2 + a_4X + a_6,$$

mistä saadaan edelleen

$$X^3 + (a_2 - \lambda^2 - a_1\lambda)X^2 + (a_4 - a_3\lambda - 2\lambda)X + (a_6 - a_3\nu - a_1\nu - \nu^2) = 0. \quad (3)$$

Toisaalta tämä yhtälö on myös muotoa $(X - x_1)(X - x_2)(X - x_3)$, joka voidaan laskea auki muotoon

$$X^3 + (-x_1 - x_2 - x_3)X^2 + (x_1x_3 + x_2x_3 + x_1x_2)X + (-x_1x_2x_3).$$

Verrataan termin X^2 kerrointa aiempaan yhtälöön (3) ja saadaan, että

$$(-x_1 - x_2 - x_3) = a_2 - \lambda^2 - a_1\lambda, \quad \text{jolloin}$$
$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2.$$

Sijoitetaan edellä laskettu koordinaatti x_3 suoran L yhtälöön, saadaan

$$y_3' = \lambda x_3 + \nu.$$

Haettu koordinaatti y_3 saadaan, kun otetaan vielä vasta-alkio lauseen 2.2 mukaisesti

$$y_3 = -\lambda x_3 - \nu - a_1 x_3 - a_3.$$

□

Esimerkki 2.4. *Olkoon elliptinen käyrä E määritelty yleistetyn Weierstrassin yhtälön avulla*

$$E : Y^2 + XY = X^3 + 1$$

kunnan $\mathbb{F}_{2^5}[T]/(T^5+T^3+1)$ yli, missä polynomi T^5+T^3+1 on jaoton kunnan $\mathbb{F}_2$ yli. Olkoon lisäksi yhteenlaskettavat käyrän pisteet $P = (T^4 + T^3 + 1, T^2)$ sekä $Q = (T, T^4 + T^3 + T^2)$. Pisteet ovat käyrällä, jos ne toteuttavat käyrän yhtälön. Sijoitetaan pisteen P koordinaatit yhtälöön, ja vasemmaksi puoleksi saadaan

$$\begin{aligned}(T^2)^2 + (T^4 + T^3 + 1)T^2 &= T^4 + T^6 + T^5 + T^2 \\ &= T^4 + T(T^3 + 1) + T^3 + 1 + T^2 \\ &= T^3 + T^2 + T + 1.\end{aligned}$$

Yhtälön oikeaksi puoleksi saadaan

$$\begin{aligned}(T^4+T^3+1)^3+1 &= (T^5+T^4)^3+1\\ &= T^{15}+T^{14}+T^{13}+T^{12}+1\\ &= T^{10}(T^5+T^3)+T^9(T^5+T^3)+1\\ &= T^{10}+T^9+1\\ &= (T^6+1)+(T^7+T^4)+1\\ &= T^4+T+T^5+T^2+T^4\\ &= T^3+T^2+T+1.\end{aligned}$$

Piste P on siis käyrällä. Lasketaan valmiiksi pistettä Q varten

$$\begin{aligned}(T^4+T^3+T^2)^2 &= T^8+T^7+T^6+T^7+T^6+T^5+T^6+T^5+T^4\\ &= (T^6+T^3)+T^6+T^4\\ &= T^4+T^3.\end{aligned}$$

Tämän jälkeen voidaan laskea pisteessä Q käyrän yhtälön vasemmaksi puoleksi

$$\begin{aligned}(T^4+T^3+T^2)^2+T(T^4+T^3+T^2) &= T^4+T^3+T^5+T^4+T^3\\ &= T^3+1.\end{aligned}$$

Yhtälön oikeaksi puoleksi saadaan myös T^3+1, joten piste Q on myös käyrällä.

Pisteiden P ja Q x-koordinaatit ovat erisuuret, eivätkä kumpikaan pisteistä ole äärettömyyspisteitä, joten Lauseen 2.3 mukaan

$$\lambda = \frac{y_2-y_1}{x_2-x_1} \quad ja \quad \nu = \frac{y_1x_2-y_2x_1}{x_2-x_1}.$$

Olkoon $f := T^5+T^3+1$ ja $g := x_2-x_1 = T^4+T^3+T+1$. Lasketaan polynomin g käänteisalkio laajennetun Eukleideen algoritmin avulla. Aluksi

saadaan

$$\begin{aligned} f &= g(T+1) + T^2 \\ g &= T^2(T^2+T) + (T+1) \\ T^2 &= (T+1)(T+1) + 1. \end{aligned}$$

Koska $f = 0$*, saadaan*

$$\begin{aligned} 1 &= T^2 + (T+1)(g + T^2(T^2+T)) \\ &= T^2(T^3+T+1) + g(T+1) \\ &= g(T+1)(T^3+T+1) + g(T+1) \\ &= g(T^4+T^2+T+T^3+T+1+T+1) \\ &= g(T^4+T^3+T^2+T). \end{aligned}$$

Näin ollen alkion T^4+T^3+T+1 *käänteisalkio on* $T^4+T^3+T^2+T$*.*

Nyt voidaan laskea

$$\begin{aligned} \lambda = \frac{T^4+T^3+T^2-T^2}{T-(T^4+T^3+1)} &= (T^4+T^3)\cdot(T^4+T^3+T^2+T) \\ &= T^8+T^7+T^6+T^5+T^7+T^6+T^5+T^4 \\ &= (T^6+T^3)+T^4 \\ &= T^3+T \end{aligned}$$

sekä

$$\begin{aligned}
\nu &= \frac{T \cdot T^2 - (T^4 + T^3 + 1) \cdot (T^4 + T^3 + T^2)}{T - (T^4 + T^3 + 1)} \\
&= \frac{T^3 + T^8 + T^7 + T^6 + T^7 + T^6 + T^5 + T^4 + T^3 + T^2}{T^4 + T^3 + T + 1} \\
&= \frac{T^8 + T^5 + T^4 + T^2}{T^4 + T^3 + T + 1} \\
&= \frac{(T^6 + T^3) + (T^3 + 1) + T^4 + T^2}{T^4 + T^3 + T + 1} \\
&= \frac{T^2 + T + 1}{T^4 + T^3 + T + 1} \\
&= (T^2 + T + 1)(T^4 + T^3 + T^2 + T) \\
&= T^6 + T^5 + T^4 + T^3 + T^5 + T^4 + T^3 + T^2 + T^4 + T^3 + T^2 + T \\
&= (T^4 + T) + T^4 + T^3 + T \\
&= T^3.
\end{aligned}$$

Näiden avulla saadaan uusi piste

$$\begin{aligned}
x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\
&= (T^3 + T)^2 + 1 \cdot (T^3 + T) - 0 - (T^4 + T^3 + 1) - T \\
&= T^6 + T^2 + T^4 + 1 \\
&= T^2 + T + 1, \\
y_3 &= -\lambda x_3 - \nu - a_1 x_3 - a_3 \\
&= -(T^3 + T) \cdot (T^2 + T + 1) - T^3 - 1 \cdot (T^2 + T + 1) - 0 \\
&= T^5 + T^4 + T^3 + T^3 + T^2 + T + T^3 + T^2 + T + 1 \\
&= (T^3 + 1) + T^4 + T^3 + 1 \\
&= T^4,
\end{aligned}$$

eli $R = (T^2 + T + 1, T^4)$. *Tarkistetaan vielä, että piste* R *on käyrällä. Sijoi-*

tetaan piste käyrän yhtälöön, ja saadaan vasemmaksi puoleksi

$$\begin{aligned}(T^4)^2 + (T^2+T+1)T^4 &= T^8 + T^6 + T^5 + T^4 \\ &= (T^6 + T^3) + T^6 + (T^3 + 1) + T^4 \\ &= T^4 + 1.\end{aligned}$$

Käyrän yhtälön oikeaksi puoleksi saadaan

$$\begin{aligned}(T^2+T+1)^3 + 1 &= (T^2+T+1)(T^4+T^2+1) + 1 \\ &= T^6 + T^4 + T^2 + T^5 + T^3 + T + T^4 + T^2 + 1 + 1 \\ &= (T^4 + T) + (T^3 + 1) + T^3 + T \\ &= T^4 + 1.\end{aligned}$$

Piste R on siis käyrällä.

2.1 Frobeniuksen kuvaus

Frobeniuksen kuvauksella on hyödyllisiä ominaisuuksia elliptisellä käyrällä, joita voidaan käyttää esimerkiksi käyrän pisteiden moninkertojen laskemisen nopeuttamiseen tietynlaisilla käyrillä. Tässä kappaleessa tarkastellaan Frobeniuksen kuvauksen käyttäytymistä elliptisellä käyrällä.

Määritelmä 2.5. *Frobeniuksen kuvaus* τ on muotoa

$$\tau : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}, \quad \alpha \mapsto \alpha^p.$$

Frobeniuksen kuvaukselle pätee kertolaskun suhteen

$$\tau(\alpha \cdot \beta) = (\alpha \cdot \beta)^p = \alpha^p \cdot \beta^p = \tau(\alpha) \cdot \tau(\beta).$$

Lisäksi yhteenlaskun suhteen pätee $\tau(\alpha+\beta) = (\alpha+\beta)^p$. Kertolaskut auki laskiessa saadaan kunkin termin kerroin binomikaavan avulla. Ensimmäinen

ja viimeinen kerroin on 1. Välissä olevat kertoimet voidaan ilmaista muodossa

$$\frac{p!}{l!(p-l)!} = p \cdot \frac{(p-1)!}{l!(p-l)!} = p \cdot n, \text{ missä } 1 \leq l < p.$$

Luku n on kunnan $\mathbb{F}_{p^k}$ alkio aina, kun p on alkuluku, sillä kaikilla nollasta eroavilla alkioilla on olemassa kertolaskun suhteen käänteisalkio. Toisin sanoen luku n on olemassa, ja kerroin $np \equiv 0 \pmod{p}$. Yhteenlaskulle Frobeniuksen kuvauksen suhteen saadaan

$$\tau(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = \tau(\alpha) + \tau(\beta).$$

Olkoon elliptinen käyrä E määritelty yleistetyn Weierstrassin yhtälön avulla, jonka kertoimet ovat kunnan $\mathbb{F}_p$ alkioita, ja käyrän pisteiden koordinaatit kunnan $\mathbb{F}_{p^k}$ alkioita. Frobeniuksen kuvaus elliptisen käyrän pisteille saadaan ottamalla se molemmista koordinaateista erikseen

$$\tau(P) = (\tau(x), \tau(y)).$$

Seuraava tulos on esitelty Lawrence C. Washingtonin kirjassa [8].

Lause 2.6. *Olkoon E elliptinen käyrä kunnan $\mathbb{F}_p$ yli. Tällöin elliptisellä käyrällä pätee seuraavat ominaisuudet.*

(a) *Olkoon piste $P \in E(\mathbb{F}_{p^k})$. Tällöin $\tau(P) \in E(\mathbb{F}_{p^k})$.*

(b) *Piste $P \in E(\mathbb{F}_p)$ jos ja vain jos $\tau(P) = P$.*

Todistus. Olkoon elliptinen käyrä E ratkaisujen joukko yleistetylle Weierstrassin yhtälölle (2), jossa nyt kertoimet $a_i \in \mathbb{F}_p$ ja pisteiden koordinaatit kuuluvat kuntaan $\mathbb{F}_{p^k}$. Käyttämällä Frobeniuksen kuvausta yleistettyyn Weierstrassin yhtälöön saadaan

$$(\tau(y))^2 + \tau(a_1)\tau(x)\tau(y) + \tau(a_3)\tau(y) = (\tau(x))^3 + \tau(a_2)(\tau(x))^2 + \tau(a_4)\tau(x) + \tau(a_6)$$

Frobeniuksen kuvauksen yhteen- ja kertolaskun ominaisuuksien avulla. Frobeniuksen kuvaukselle pätee myös $\tau(\alpha) = \alpha^p = \alpha$ kaikilla $\alpha \in \mathbb{F}_p$, jolloin Frobeniuksen kuvaus ei muuta käyrän kertoimia. Tällöin edeltävä yhtälö saadaan muotoon

$$(\tau(y))^2 + a_1\tau(x)\tau(y) + a_3\tau(y) = (\tau(x))^3 + a_2(\tau(x))^2 + a_4\tau(x) + a_6.$$

Nyt siis $\tau(P) = (\tau(x), \tau(y)) \in E(\mathbb{F}_{p^k})$, mikä todistaa kohdan (a). Kohta (b) seuraa siitä, että $\tau(P) = (x_P^p, y_P^p) = (x_P, y_P) = P$ kaikilla $P \in E(\mathbb{F}_p)$. □

Lause 2.7. *Olkoot E elliptinen käyrä kunnan $\mathbb{F}_p$ yli,*

$$t = p + 1 - \#E(\mathbb{F}_p),$$

ja τ Frobeniuksen kuvaus. Tällöin jokaiselle pisteelle $Q \in E(\mathbb{F}_{p^k})$ pätee

$$\tau^2(Q) - t \cdot \tau(Q) + p \cdot Q = \mathcal{O}, \tag{4}$$

missä $\tau^2(Q) = \tau(\tau(Q))$.

Todistus. Todistus löytyy René Schoofin kirjasta [2]. □

2.1.1 Koblitz-käyrä

Kryptografisissa algoritmeissa voi tulla vastaan pisteiden moninkertojen laskeminen esimerkiksi Diffie-Hellmannin avaimenvaihdossa, missä monikerta on muotoa nP eli piste lisätään itseensä n kertaa. Moninkertojen laskeminen on hidasta, ja Koblitzin ideana on ollut käyttää sellaista elliptistä käyrää, että nP voitaisiin laskea tehokkaasti Frobeniuksen kuvauksen avulla.

Määritelmä 2.8. *Koblitz-käyrä* on elliptinen käyrä kunnan $\mathbb{F}_p$ yli, jonka määrää yhtälö

$$E_a : Y^2 + XY = X^3 + aX^2 + 1, \tag{5}$$

missä $a \in \{0, 1\}$. Diskriminantti $\Delta = 1$.

Voidaan laskea helposti käyrän $E_0(\mathbb{F}_2)$ pisteiden määrä muodostamalla ensin elliptisen käyrän pisteiden joukko. Sijoitetaan kaikki mahdolliset pisteparit käyrän yhtälöön, jolloin saadaan Taulukossa 2 kuvatut arvot yhtälön molemmille puolille.

X	Y	$Y^2 + XY$	$X^3 + 1$
0	0	0	1
0	1	1	1
1	0	0	0
1	1	0	0

Taulukko 2: Koblitz-käyrän määräävän yhtälön molempien puolien arvot eri X ja Y arvoilla.

Yhtälön toteuttavat parit ovat siis joukko

$$E_0(\mathbb{F}_2) = \{(0,1), (1,0), (1,1), \mathcal{O}\}.$$

Pisteiden määrä on $\#E(\mathbb{F}_2) = 4$, jolloin Lauseen 1.3 mukaan pisteiden määrälle pätee

$$t = 2 + 1 - 4 = -1.$$

Lisäksi tiedetään, että Frobeniuksen kuvaus toteuttaa toisen asteen yhtälön (4) kaikilla $P \in E(\mathbb{F}_{2^k})$, eli

$$\tau^2(P) + \tau(P) + 2P = \mathcal{O}.$$

Toisin sanoen $\tau^2 + \tau + 2 = 0$, eli $\tau^2 = -2 - \tau$.

Lause 2.9. *Olkoon n positiivinen kokonaisluku. Sillä ehdolla, että Frobeniuksen kuvaukselle τ pätee $\tau^2 = -2 - \tau$, luku n voidaan antaa muodossa*

$$n = v_0 + v_1\tau + v_2\tau^2 + \cdots + v_l\tau^l, \text{ missä } v_i \in \{-1, 0, 1\}.$$

On mahdollista löytää sellainen muoto, missä $\ell \approx \log n$ *ja noin* $\frac{1}{3}$ *kertoimista* v_i *ovat nollasta poikkeavia.*

Todistus. Todistus löytyy kirjasta [6]. □

Kun halutaan laskea pisteen $P \in E(\mathbb{F}_{p^k})$ monikerta nP Koblitzin käyrällä, niin voidaan kokonaisluku n korvata Lauseen 2.9 mukaisella esityksellä. Tällöin saadaan

$$\begin{aligned} nP &= (v_0 + v_1\tau + v_2\tau^2 + \cdots + v_l\tau^l)P \\ &= v_0P + v_1\tau(P) + v_2\tau^2(P) + \cdots + v_l\tau^l(P). \end{aligned}$$

Kertoimien v_i muodostaminen ja yleisemmin tällä menetelmällä pisteiden monikertojen laskeminen voidaan esittää algoritmina, kuten Algoritmissa 2. Solinas käsittelee kyseistä algoritmia artikkelissaan [3] kappaleessa 7.2.

Esimerkki 2.10. *Olkoon Koblitz-käyrä* E_0 *kunnan* $\mathbb{F}_{2^k}[T]/(T^5 + T^3 + 1)$ *yli. Olkoon piste* $P = (T^4 + T^3 + 1, T^2)$*. Käytetään liitteenä olevaa Algoritmia 2 pisteen* $43P$ *laskemiseen. Algoritmi antaa*

$$43P = (-1 - \tau^2 - \tau^4 - \tau^6 + \tau^8 - \tau^{10} + \tau^{13})P = (T^4 + T^3 + 1, T^4 + T^3 + T^2 + 1).$$

Pisteen laskemiseksi on tehty 13 *Frobeniuksen kuvausta sekä kuusi pisteiden yhteenlaskua. Lasketaan seuraavaksi tuplaus-lisäys menetelmällä sama piste* $43P$*, jossa* 43 *esitetään binääriesityksenä seuraavasti*

$$43P = (-1 - 2^2 - 2^4 + 2^6)P = (T^4 + T^3 + 1, T^4 + T^3 + T^2 + 1).$$

Tässä on käytetty kuusi pisteen tuplausta sekä kolme pisteiden yhteenlaskua. Frobeniuksen kuvauksen laskeminen on niin paljon nopeampaa kuin pisteiden

tuplaus, että Frobeniuksen kuvauksen avulla toimiva algoritmi suorittuu noin 50 % nopeampaa kuin tuplaus-lisäys menetelmä.

Solinas esittelee tuplaus-lisäys menetelmää artikkelissaan [3].

2.2 Käyrän pisteiden määrä

Turvallisuussyistä on hyvä, että elliptisellä käyrällä on mahdollisimman paljon pisteitä. Tässä kappaleessa käydään läpi menetelmiä yleistetyn käyrän pisteiden määrän laskemiseen.

Lause 1.3 voidaan esittää myös yleistetyssä tilanteessa, missä elliptinen käyrä E on määritelty kunnan $\mathbb{F}_{p^k}$ yli.

Lause 2.11 (Hasse)**.** *Olkoon E elliptinen käyrä kunnan $\mathbb{F}_{p^k}$ yli. Tällöin*

$$\#E(\mathbb{F}_{p^k}) = p^k + 1 - t_{p^k}, \text{ missä } |t_{p^k}| \leq 2p^{k/2}.$$

Lause 2.12. *Olkoon E elliptinen käyrä kunnan $\mathbb{F}_p$ yli, ja olkoon*

$$t = p + 1 - \#E(\mathbb{F}_p).$$

Olkoon α ja β kompleksisia juuria polynomille $Z^2 - tZ + p$. Nyt $|\alpha| = |\beta| = \sqrt{p}$ ja lisäksi jokaiselle $k \geq 1$ pätee

$$\#E(\mathbb{F}_{p^k}) = p^k + 1 - \alpha^k - \beta^k. \tag{6}$$

Todistus. Todistus löytyy Joseph H. Silvermanin kirjasta [9]. □

Koblitz-käyrälle on erityisen helppoa laskea pisteiden lukumäärä Lauseen 2.12 avulla, sillä $\#E(\mathbb{F}_p)$ on nopea laskea.

Esimerkki 2.13. *Olkoon E_0 Koblitz-käyrä yhtälön* (5) *mukaisesti. Kuten aiemmin on todettu, niin $t = -1$. Polynomin $Z^2 + Z + 2$ juuret ovat*

$$\frac{-1+\sqrt{-7}}{2} \quad \textit{sekä} \ \frac{-1-\sqrt{-7}}{2}.$$

Elliptisen käyrän $E(\mathbb{F}_{2^k})$ *pisteiden lukumääräksi saadaan*

$$\#E(\mathbb{F}_{2^k}) = 2^k + 1 - \left(\frac{-1+\sqrt{-7}}{2}\right)^k - \left(\frac{-1-\sqrt{-7}}{2}\right)^k.$$

Taulukkoon 3 on laskettu pisteiden lukumäärät elliptisellä käyrällä kunnan $\mathbb{F}_{2^k}$ *yli. Pisteiden määrä kasvaa nopeasti, kun lukua* k *kasvatetaan.*

k	$\#E(\mathbb{F}_{2^k})$
1	4
5	44
17	130972
29	536830604
103	10141204801825838143450120268276

Taulukko 3: Pisteiden määrä Koblitz-käyrällä luvun k kasvaessa.

Huomautus 2.14. Yleisesti elliptisen käyrän pisteiden määrän laskemiseen on olemassa myös polynomiaikainen algoritmi, SEA. [2]

3 Bilineaariset liitokset elliptisellä käyrällä

Jotta voidaan määritellä Weilin liitos ja Taten liitos, määritellään ensin äärellisen kertaluvun pisteet, elliptisen käyrän jakaja sekä elliptisen käyrän yli määritellyn funktion jakaja. Weilin liitos sekä Taten liitos ovat bilineaarisia liitoksia, jotka kuvaavat kaksi elliptisen käyrän aliryhmän $E(K)[m]$ pistettä ykkösen m. juureksi.

Tällaista bilineaarista liitosta voidaan käyttää hyväksi elliptisen käyrän diskreetin logaritmin ongelman siirtämiseen diskreetin logaritmin ongelmaksi, mutta myös myöhemmin tässä tutkielmassa käsiteltävissä kryptografisissa systeemeissä.

3.1 Äärellisen kertaluvun pisteet

Äärellisen kertaluvun pisteitä käytetään myöhemmin Weilin liitoksen määrittelyyn. Tässä kappaleessa määritellään lyhyesti äärellisen kertaluvun pisteet ja tarkastellaan niiden ominaisuuksia.

Määritelmä 3.1. Olkoon kokonaisluku $m \geq 1$. Pistettä $P \in E$, jolle pätee $mP = \mathcal{O}$ kutsutaan *kertaluvun m pisteeksi* ryhmässä E. Kertaluvun m pisteet muodostavat joukon

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

Esimerkki 3.2. *Olkoon elliptinen käyrä E muotoa*

$$Y^2 = X^3 + AX + B.$$

Yhtälön oikea puoli voidaan esittää muodossa

$$(X - \alpha_1)(X - \alpha_2)(X - \alpha_3),$$

jolloin on olemassa pisteet $P_i = (\alpha_i, 0)$*, missä* $i \in \{1, 2, 3\}$*. Pisteet ovat erilliset, sillä elliptisen käyrän diskriminantti ei ole* 0*. Näille pisteille pätee* $-P_i = (\alpha_i, -0) = P_i$*, jolloin*

$$\mathcal{O} = P_i - P_i = 2P_i.$$

Pisteiden P_i *kertaluku on siis* 2*, eli pisteet kuuluvat joukkoon* $E[2]$*.*

Lause 3.3. *Olkoon* E *elliptinen käyrä.* $(E[m], +)$ *on ryhmän* $(E, +)$ *aliryhmä.*

Todistus. Määritelmän 3.1 nojalla $E[m] \subseteq E$. Olkoon pisteet $P, Q \in E[m]$. Nyt $P + Q \in E[m]$, sillä $m(P + Q) = mP + mQ = \mathcal{O} + \mathcal{O} = \mathcal{O}$. Lisäksi $-P \in E[m]$, sillä $m(-P) = -(mP) = -\mathcal{O} = \mathcal{O}$. Tästä seuraa, että $E[m]$ on ryhmän E aliryhmä. □

Lause 3.4. *Olkoon* $m \geq 1$ *kokonaisluku sekä olkoon* E *elliptinen käyrä kunnan* $\mathbb{F}_p$ *yli, missä* $p \nmid m$*. Tällöin on olemassa kokonaisluku* k*, jolle pätee*

$$E(\mathbb{F}_{p^{jk}})[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \text{ kaikilla } j \geq 1.$$

Todistus. Todistus löytyy Silvermanin kirjasta [9]. □

3.2 Jakajat elliptisellä käyrällä

Tässä kappaleessa määritellään bilineaarisuus, elliptisen käyrän jakaja sekä elliptisen käyrän yli määritellyn funktion jakaja. Käsitellään myös lause, joka kertoo milloin elliptisen käyrän jakaja on myös jonkin elliptisen käyrän yli määritellyn funktion jakaja.

Määritelmä 3.5. Olkoon vektoriavaruudet $V, W, X \subseteq \mathbb{F}^n$, sekä olkoon kuvaus $\beta : V \times W \to X$. Kuvaus β on *bilineaarinen*, jos kaikilla $v \in V, w \in W$ sekä $a_1, a_2, b_1, b_2 \in \mathbb{F}$ pätee

$$\beta(a_1v_1 + a_2v_2, w) = a_1\beta(v_1, w) + a_2\beta(v_2, w),$$
$$\beta(v, b_1w_1 + b_2w_2) = b_1\beta(v, w_1) + b_2\beta(v, w_2).$$

Määritelmä 3.6. Rationaalifunktion (1) *jakaja* $\mathrm{div}(f(X))$ on formaalisumma

$$\mathrm{div}(f(X)) = e_1[\alpha_1] + e_2[\alpha_2] + \cdots + e_r[\alpha_r] - d_1[\beta_1] - d_2[\beta_2] - \cdots - d_r[\beta_r].$$

Formaalia summaa ei lasketa auki, vaan se jää edeltävään muotoon.

Esimerkki 3.7. *Olkoon rationaalifunktio muotoa*

$$f(x) = \frac{(x-1)^2(x+1)}{x}.$$

Funktion jakaja on siis

$$\mathrm{div}(f(x)) = 2[1] + [-1] - [0].$$

Jakajasta nähdään suoraan, että funktiolla on kaksinkertainen nollakohta pisteessä $x = 1$, yksinkertainen nollakohta pisteessä $x = -1$ sekä yksinkertainen napa pisteessä $x = 0$.

Määritelmä 3.8. Olkoon E elliptinen käyrä muotoa

$$E : Y^2 = X^3 + AX + B,$$

ja olkoon $f(X, Y)$ nollasta eroava rationaalifunktio, jolle pätee $f(P) = f(x, y)$, kun $P = (x, y)$. Rationaalifunktion f *jakaja* on formaali summa muotoa

$$\operatorname{div}(f) = \sum_{P \in E} n_P[P],$$

missä $n_P \in \mathbb{Z}$ ja $n_P \neq 0$ äärelliselle määrälle pisteitä P. Formaali summa on siis äärellinen. Jakajassa esiintyvät pisteet ovat funktion napoja tai nollakohtia. Yleisemmin elliptisen käyrän E *jakaja* on mikä tahansa formaali summa

$$D = \sum_{P \in E} n_P[P],$$

missä $n_P \in \mathbb{Z}$ ja $n_P \neq 0$ äärelliselle määrälle pisteitä P.

Määritelmä 3.9. Olkoon E elliptinen käyrä sekä olkoon D elliptisen käyrän yli määritellyn funktion f jakaja. Tällöin *jakajan D aste* on

$$\deg(D) = \deg\left(\sum_{P \in E} n_P[P]\right) = \sum_{P \in E} n_P.$$

Jakajan D summa on

$$\operatorname{Sum}(D) = \operatorname{Sum}\left(\sum_{P \in E} n_P[P]\right) = \sum_{P \in E} n_P P.$$

Lause 3.10. *Olkoon E elliptinen käyrä.*

(a) Olkoon f ja g nollasta eroavia rationaalifunktioita elliptisellä käyrällä E. Jos $div(f) = div(g)$, niin on olemassa nollasta eroava vakio c siten, että $f = cg$.

(b) *Olkoon* $D = \sum_{P \in E} n_P[P]$ *nollasta eroava jakaja elliptisellä käyrällä* E *Tällöin* D *on elliptisellä käyrällä* E *olevan rationaalifunktion jakaja jos ja vain jos* $deg(D) = 0$ *ja* $Sum(D) = \mathcal{O}$.

Erityisesti jos rationaalifunktiolla f *käyrän* E *yli ei ole nollia eikä napoja, eli* $div(f) = 0$*, niin se on vakio.*

Todistus. Todistus löytyy Silvermanin kirjasta [9].

□

Seuraus 3.11. *Olkoon* E *elliptinen käyrä sekä olkoon piste* $P \in E[m]$*. Olkoon lisäksi jakaja* $D = m[P] - m[\mathcal{O}]$ *elliptisellä käyrällä* E*. Jakajan aste*

$$deg(D) = m - m = 0.$$

Jakajan summaksi saadaan

$$sum(D) = mP - m\mathcal{O} = \mathcal{O}.$$

Tällöin Lauseen 3.10 nojalla jakaja D *on jonkin käyrällä* E *olevan rationaalifunktion jakaja, eli on olemassa rationaalifunktio* f_P*, jolle*

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

3.3 Weilin liitos

Tässä kappaleessa käsitellään Weilin liitosta ja sen ominaisuuksia. Weilin liitokselle on olemassa useita erilaisia määritelmiä, joista yksi käydään läpi tässä kappaleessa. Muunlaisia määritelmiä Weilin liitokselle löytää muun muassa Andreas Engen artikkelista [10]. Weilin liitokselle on useita eri sovelluskohteita, joita tarkastellaan myöhemmin tässä tutkielmassa.

Määritelmä 3.12. Olkoon $P, Q \in E[m]$ sekä f_P, f_Q rationaalisia funktioita käyrän E yli, joille pätee

$$\operatorname{div}(f_P) = m[P] - m[\mathcal{O}], \quad ja \quad \operatorname{div}(f_Q) = m[Q] - m[\mathcal{O}].$$

Pisteiden P ja Q *Weilin liitos* $e_m(P, Q)$ voidaan ilmaista muodossa

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

missä $S \in E$ on mikä tahansa piste, jolle pätee $S \notin \{\mathcal{O}, P, -Q, P - Q\}$.

Lause 3.13. *Olkoon $e_m(P, Q)$ Weilin liitos. Weilin liitokselle pätee seuraavat ominaisuudet:*

(a) $e_m(P, Q)^m = 1$ *kaikilla* $P, Q \in E[m]$. *Toisin sanoen* $e_m(P, Q)$ *on* m. *ykkösen juuri.*

(b) *Weilin liitos on* bilineaarinen. *Toisin sanoen Weilin liitokselle pätee*

$$e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q) \text{ kaikilla } P_1, P_2, Q \in E[m], \text{ ja}$$
$$e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2) \text{ kaikilla } P, Q_1, Q_2 \in E[m].$$

(c) *Weilin liitokselle pätee*

$$e_m(P, P) = 1 \text{ kaikilla } P \in E[m].$$

Edelleen $e_m(P, Q) = e_m(Q, P)^{-1}$.

(d) *Jos Weilin liitokselle pätee*

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

Todistus. Todistus löytyy Silvermanin kirjasta [9] kappaleesta III.8. □

3.3.1 Weilin liitoksen laskeminen

Tässä kappaleessa käsitellään Millerin algoritmia Weilin liitoksen tehokkaaseen laskemiseen. Millerin algoritmi palauttaa funktion, jolla on haluttu jakaja Weilin liitoksen laskemista varten.

Lause 3.14. *Olkoon E elliptinen käyrä sekä olkoon $P = (x_P, y_P)$ ja $Q = (x_Q, y_Q)$ äärettömyyspisteestä poikkeavia pisteitä käyrällä E. Pisteille pätevät seuraavat ominaisuudet:*

(a) *Olkoon λ pisteen P ja Q välisen suoran kulmakerroin. Jos $P = Q$ niin olkoon λ elliptisen käyrän pisteessä P olevan tangentin kulmakerroin. Jos pisteiden P ja Q välinen suora on vertikaalinen, niin olkoon $\lambda = \infty$. Olkoon lisäksi*

$$g_{P,Q} = \begin{cases} \frac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2} & \text{kun } \lambda \neq \infty, \\ x - x_P & \text{kun } \lambda = \infty. \end{cases}$$

Tällöin $\operatorname{div}(g_{P,Q}) = [P] + [Q] - [P + Q] - [\mathcal{O}]$.

(b) Millerin algoritmi. *Olkoon $m \geq 1$. Luvun m binääriesitys on muotoa*

$$m = m_0 + m_1 \cdot 2 + m_2 \cdot 2^2 + \cdots + m_{n-1} 2^{n-1},$$

missä $m_i \in \{0, 1\}$ ja $m_{n-1} \neq 0$. Millerin algoritmi 3, missä funktiot $g_{T,P}$ sekä $g_{T,T}$ ovat määritelty kohdassa (a), palauttaa funktion f_P, jonka jakajalle pätee

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

Todistus. (a) Olkoon $\lambda \neq \infty$ sekä olkoon $y = \lambda x + \nu$ suora pisteiden P ja Q välillä, tai tangentti elliptisellä käyrällä pisteessä P, jos $P = Q$.

Suora leikkaa elliptistä käyrää E kolmessa pisteessä P, Q ja $-P-Q$. Tällöin suoran jakajaksi saadaan

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

Pisteen $P + Q$ kautta kulkevan vertikaalisen suoran jakaja on

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

Tällöin funktion

$$g_{P,Q} = \frac{y - \lambda x - \nu}{x - x_{P+Q}}$$

jakaja on

$$\begin{aligned}\operatorname{div}(g_{P,Q}) &= [P] + [Q] + [-P - Q] - 3[\mathcal{O}] - ([P + Q] + [-P - Q] - 2[\mathcal{O}]) \\ &= [P] + [Q] - [P + Q] - [\mathcal{O}].\end{aligned}$$

Tiedetään, että $y_P = \lambda x_P + \nu$, jolloin $-\nu = \lambda x_P - y_P$. Lisäksi $x_{P+Q} = \lambda^2 - x_P - x_Q$, jolloin saadaan

$$g_{P,Q} = \frac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2}.$$

Jos $\lambda = \infty$, niin $P + Q = \mathcal{O}$, eli $Q = -P$. Funktion $g_{P,Q}$ jakaja täytyy siis olla muotoa $[P] + [-P] - 2[\mathcal{O}]$. Funktion $x - x_P$ jakaja on haluttu $[P] + [-P] - 2[\mathcal{O}]$.

(b) Edellisen kohdan nojalla tiedetään, että funktion $g_{T,T}$ jakaja on $2[T] - [2T] - [\mathcal{O}]$ ja funktion $g_{T,P}$ jakaja on $[T] + [P] - [T + P] - [\mathcal{O}]$. Todistetaan algoritmi induktion avulla. Olkoon m sellainen kokonaisluku, missä on $n = 2$ bittiä. Tällöin luku m on siis joko $10_2 = 2$ tai $11_2 = 3$. Kun $m = 2$, niin algoritmi palauttaa funktion $f = g_{T,T}$. Nyt koska algoritmin alussa asetettiin $T = P$, niin funktion jakajaksi saadaan haluttu $\operatorname{div}(f) = 2[P] - [2P] - [\mathcal{O}]$. Kun $m = 3$, niin algoritmi palauttaa

funktion $f = g_{T,T} \cdot g_{2T,P}$. Funktion jakajaksi saadaan

$$\mathrm{div}(f) = 2[T] - [2T] - [\mathcal{O}] + [2T] + [P] - [2T + P] - [\mathcal{O}].$$

Tässä myös $T = P$, jolloin saadaan haluttu jakaja

$$\mathrm{div}(f) = 3[P] - [3P] - 2[\mathcal{O}].$$

Seuraavaksi oletetaan, että algoritmi palauttaa k-bitin mittaiselle luvulle m halutun jakajan $m[P] - [mP] - (m-1)[\mathcal{O}]$. Tarkastellaan seuraavaksi $k+1$-bitin mittaista lukua m', joka on muotoa $2m$ tai $2m+1$. Olkoon $m' = 2m$, tällöin haluttu jakaja on muotoa $2m[P] - [2mP] - (2m-1)[\mathcal{O}]$. Nyt algoritmi palauttaa funktion f, jonka jakaja on muotoa

$$2m[P] - 2[mP] - 2(m-1)[\mathcal{O}] + 2[T] - [2T] - [\mathcal{O}].$$

Tiedetään, että tässä vaiheessa algoritmia $T = mP$, joten jakaja saadaan haluttuun muotoon

$$\begin{aligned} &2m[P] - 2[mP] - (2m-1)[\mathcal{O}] + 2[mP] - [2mP] \\ &\qquad = 2m[P] - [2mP] - (2m-1)[\mathcal{O}]. \end{aligned} \tag{7}$$

Olkoon nyt $m' = 2m+1$, jolloin haluttu jakaja on muotoa $(2m+1)[P] - [(2m+1)P] - 2m[\mathcal{O}]$. Edellisen vaiheen jakajan (7) avulla nähdään, että algoritmi palauttaa funktion, jonka jakaja on muotoa

$$2m[P] - [2mP] - (2m-1)[\mathcal{O}] + [2mP] + [P] - [(2m+1)P] - [\mathcal{O}].$$

Jakaja voidaan vielä saattaa haluttuun muotoon

$$(2m+1)[P] - [(2m+1)P] - 2m[\mathcal{O}].$$

Algoritmi palauttaa siis oikeanlaisen jakajan myös $k+1$ bittiä pitkille luvuille. Induktion nojalla algoritmi toimii kaikille luvuille $m \geq 2$. Tapauksessa $m = 1$ algoritmi palauttaa funktion $f = 1$, jonka jakaja on 0. Haluttu jakaja on myös $[P] - [P] - 0[\mathcal{O}] = 0$.

□

Lauseessa 3.14 kuvattu Millerin algoritmi palauttaa siis funktion, jonka jakaja on $m[P] - [mP] - (m-1)[\mathcal{O}]$. Nyt, jos $P \in E[m]$, niin funktion jakaja on $m[P] - m[\mathcal{O}]$, jota voidaan käyttää Määritelmän 3.12 mukaisen Weilin liitoksen laskemiseen.

Algoritmia voidaan tehostaa laskemalla Millerin algoritmissa esiityvät funktiot valmiiksi auki Weilin liitoksessa käytettävillä pisteillä, eli voidaan modifioida algoritmia palauttamaan pisteet $f_P(P+S)$ sekä $f_P(S)$.

Esimerkki 3.15. *Olkoon elliptinen käyrä* $E : Y^2 = X^3 + 23$ *kunnan* $\mathbb{F}_{1051}$ *yli. Tiedetään, että käyrällä on* $\#E = 5^2 \cdot 43$ *pistettä. Valitaan käyrältä pisteet* $P = (109, 203)$ *sekä* $Q = (240, 203)$*. Molempien pisteiden kertaluku on* 5*. Valitaan piste* $S = (1, 554)$*. Pisteen* S *kertaluku on* 215*. Millerin algoritmin avulla saadaan*

$$\frac{f_P(Q+S)}{f_P(S)} = \frac{109}{306} = 203. \tag{8}$$

Tämän jälkeen lasketaan vielä toinen osa Weilin liitoksesta Millerin algoritmin avulla, saadaan

$$\frac{f_Q(P-S)}{f_Q(-S)} = \frac{552}{406} = 312. \tag{9}$$

Ja edelleen Weilin liitos on

$$e_5 = \frac{203}{312} = 671.$$

Voidaan vielä tarkistaa, että e_5 *on* 5*. ykkösen juuri laskemalla*

$$e_5^5 = 671^5 \equiv 1 \pmod{1051}.$$

Taulukoissa 4 ja 5 esitellään keskeisiä arvoja Millerin algoritmin jokaisesta iteraatiosta.

i	$f_P(S)$	$f_P(Q+S)$	T	m
1	608	98	$(256, 138)$	0
2	306	109	$\mathcal{O}$	1

Taulukko 4: Millerin algoritmin muuttujien arvot kunkin iteraation i lopussa yhtälön (8) syötteellä.

i	$f_Q(-S)$	$f_Q(P-S)$	T	m
1	152	875	$(959, 138)$	0
2	406	552	$\mathcal{O}$	1

Taulukko 5: Millerin algoritmin muuttujien arvot kunkin iteraation i lopussa yhtälön (9) syötteellä.

3.3.2 ECDLP ja Weilin liitos

Tässä kappaleessa määritellään ECDLP sekä Weilin liitoksen avulla toimiva MOV-algoritmi, jonka ideana on muokata käyrän $E(\mathbb{F}_p)$ ECDLP diskreetin logaritmin ongelmaksi kunnan $\mathbb{F}_{p^k}^*$ yli, missä k on upotuksen aste. Jos diskreetin logaritmin ongelma on helppo, niin erityisesti supersingulaariset käyrät [9] ovat heikkoja MOV-algoritmia vastaan, sillä supersingulaaristen käyrien upotuksen aste on aina $k \leq 6$.

Määritelmä 3.16. Olkoon E elliptinen käyrä kunnan $\mathbb{F}_p$ yli, sekä olkoon pisteet $P, Q \in E$. *Elliptisen käyrän diskreetin logaritmin ongelma* (ECDLP) on ongelma, jossa pitää löytää sellainen kokonaisluku n, jolle $Q = nP$.

Määritelmä 3.17. Olkoon E elliptinen käyrä kunnan $\mathbb{F}_p$ yli sekä olkoon kokonaisluku $m \geq 1$, jolle pätee $p \nmid m$. Käyrän E *m-upotuksen aste* on pienin luku k, jolle pätee

$$E(\mathbb{F}_{p^k})[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Lause 3.18. *Olkoon E elliptinen käyrä kunnan $\mathbb{F}_p$ yli. Olkoon lisäksi alkuluku $\ell \neq p$. Oletetaan, että käyrällä E on olemassa piste, jonka kertaluku on ℓ. Tällöin käyrän ℓ-upotuksen aste on jokin seuraavista.*

1. *Käyrän upotuksen aste on* 1 *ja* $\ell \leq \sqrt{p} + 1$.
2. *Upotuksen aste on* ℓ *ja* $p \equiv 1 \pmod{\ell}$.
3. *Upotuksen aste on pienin luku* $k \geq 2$, *jolle pätee*

$$p^k \equiv 1 \pmod{\ell}.$$

Todistus. Todistus löytyy LC Washingtonin kirjasta [8]. □

Olkoon E elliptinen käyrä kunnan $\mathbb{F}_p$ yli. Olkoon piste $P \in E(\mathbb{F}_p)$ kertalukua ℓ, missä ℓ on suuri alkuluku $\ell > \sqrt{p} + 1$. Olkoon lisäksi k käyrän E ℓ-upotuksen aste. Olkoon piste $Q = nP$. MOV-algoritmin avulla voidaan ratkaista ECDLP, jos DLP pystytään ratkaisemaan. MOV-algoritmi 4 koostuu viidestä askeleesta.

1. Ensin lasketaan pisteiden määrä $N = \#E(\mathbb{F}_{p^k})$. Nyt koska pisteen P kertaluku on ℓ , niin $\ell | N$. Pisteiden määrän laskemiselle on olemassa Huomautuksen 2.14 nojalla polynomiaikainen algoritmi.

2. Valitaan satunnainen piste $T \in E(\mathbb{F}_{p^k})$, jolle pätee $T \notin E(\mathbb{F}_p)$. Satunnaisen pisteen voi löytää valitsemalla ensin satunnaisen x-koordinaatin, jolla Weierstrassin yhtälön oikea puoli on neliö. Tämän voi varmistaa tehokkaasti, sillä luku $a \in \mathbb{F}_{p^k}$ on neliö kunnassa $\mathbb{F}_{p^k}$ jos ja vain

jos $a^{(p^k-1)/2} = 1$, kun p on pariton alkuluku. Jos tällainen x löytyy, saadaan pisteen y-koordinaatti laskemalla diskreetti neliöjuuri Weierstrassin yhtälön oikeasta puolesta. Diskreetin neliöjuuren laskemiselle on olemassa polynomiaikainen algoritmi. Henri Cohen on kirjassaan [1] esitellyt useamman algoritmin diskreetin neliöjuuren laskemiselle.

3. Lasketaan $T' = (N/\ell)T$. Nyt halutaan, että pisteen T' kertaluku on ℓ, jotta voidaan laskea myöhemmin Weilin liitokset e_ℓ. Jos $T' \neq \mathcal{O}$, niin pisteen T' kertaluku on ℓ. Muulloin palataan takaisin kohtaan 2. ja etsitään uusi piste T.

4. Lasketaan Weilin liitokset $\alpha = e_\ell(P, T') \in \mathbb{F}_{p^k}^*$, ja $\beta = e_\ell(Q, T') \in \mathbb{F}_{p^k}^*$. Jos $\alpha = 1$, niin täytyy valita uusi piste T, eli hypätään takaisin kohtaan 2.

5. Etsitään sellainen kokonaisluku n, jolle $\beta = \alpha^n$. Ratkaistaan siis DLP kunnassa $\mathbb{F}_{p^k}^*$. Nyt n ratkaisee myös ECDLP:n, eli luvulle n pätee $Q = nP$.

MOV-algoritmin tehokkuus riippuu upotuksen asteesta k. MOV-algoritmi toimii siis hyvin erityisesti *supersingulaarisia käyriä* vastaan, sillä niiden upotuksen aste on pieni, $k \leq 6$. Normaaleilla käyrillä upotuksen aste on lähes aina suurempaa, kuin $(\ln p)^2$. Supersingulaarisilla käyrillä on kuitenkin myös hyödyllisiä käyttökohteita, joita käsitellään myöhemmin tässä tutkielmassa.

3.4 Taten liitos

Taten liitos on Weilin liitoksen tapaan bilineaarinen liitos elliptisellä käyrällä. Tässä kappaleessa käydään läpi Taten liitos, jonka laskeminen on jokseenkin tehokkaampaa, kuin Weilin liitoksen laskeminen. Lisäksi Taten liitosta

voidaan soveltaa myöhemmin tässä tutkielmassa käytävissä kryptografisissa algoritmeissa Weilin liitoksen sijaan.

Määritelmä 3.19. Olkoon elliptinen käyrä E kunnan $\mathbb{F}_q$ yli. Olkoon ℓ alkuluku, sekä olkoon pisteet $P \in E(\mathbb{F}_q)[\ell]$ ja $Q \in E(\mathbb{F}_q)$. Valitaan rationaalifunktio f_P elliptisen käyrän $E(\mathbb{F}_q)$ yli, jolle

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

Taten liitos pisteille P ja Q on

$$\tau(P, Q) = \frac{f_P(Q+S)}{f_P(S)} \in \mathbb{F}_q^*,$$

missä $S \in E(\mathbb{F}_q)$ on sellainen piste, jolla $f_P(Q+S)$ ja $f_P(S)$ ovat määritellyt sekä nollasta eroavia. Lisäksi jos $q \equiv 1 \pmod{\ell}$, niin *modifioitu Taten liitos* pisteille P ja Q on

$$\hat{\tau}(P, Q) = \tau(P, Q)^{(q-1)/\ell} = \left(\frac{f_P(Q+S)}{f_P(S)}\right)^{(q-1)/\ell} \in \mathbb{F}_q^*.$$

Lause 3.20. *Olkoon E elliptinen käyrä kunnan $\mathbb{F}_q$ yli sekä olkoon ℓ alkuluku, jolle pätee*

$$q \equiv 1 \pmod{\ell} \quad \textit{ja} \quad E(\mathbb{F}_q)[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}.$$

Tällöin modifioitu Taten liitos on hyvin määritelty kuvaus

$$\hat{\tau} : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)[\ell] \to \mathbb{F}_q^*.$$

Taten modifioidulla liitoksella on seuraavat ominaisuudet:

(a) *Taten liitos on bilineaarinen, eli*

$$\hat{\tau}(P_1+P_2, Q) = \hat{\tau}(P_1, Q)\hat{\tau}(P_2, Q) \quad \textit{ja} \quad \hat{\tau}(P, Q_1+Q_2) = \hat{\tau}(P, Q_1)\hat{\tau}(P, Q_2).$$

(b) *Modifioitu Taten liitos $\hat{\tau}(P, P)$ on primitiivinen ykkösen ℓ. juuri kaikilla nollasta eroavilla pisteillä $P \in E(\mathbb{F}_q)[\ell]$.*

Todistus. Todistus löytyy Silvermanin kirjasta [9]. □

Taten liitos voidaan laskea tehokkaasti Millerin algoritmilla 3. Taten liitosta voidaan myös käyttää myöhemmin tässä tekstissä esiteltävissä kolmen osapuolen Diffie-Hellmann avaimenvaihdossa, sekä ID-pohjaisessa julkisen avaimen kryptosysteemissä Weilin liitoksen sijaan.

4 Muodonmuutoskuvaus ja modifioitu Weilin liitos

Tässä kappaleessa käydään läpi muodonmuutoskuvaus, jota voidaan käyttää Weilin liitoksessa, jotta $e_m(aP, bP) \neq 1$. Tämä ominaisuus on hyödyllinen myöhemmin esiteltävissä ID-kryptosysteemissä ja kolmen osapuolen Diffie-Hellman avaimenvaihdossa. Halutaan siis, että on olemassa kuvaus $\phi : E \to E$, jolla pisteet P ja $\phi(P)$ ovat lineaarisesti riippumattomia.

Määritelmä 4.1. Olkoon $\ell \geq 3$ alkuluku, olkoon elliptinen käyrä E, olkoon $P \in E[\ell]$ kertalukua ℓ oleva piste elliptisellä käyrällä, sekä olkoon kuvaus $\phi : E \to E$. Kuvaus ϕ on pisteen P *ℓ-muodonmuutoskuvaus*, jos sille pätee seuraavat ominaisuudet:

1. $\phi(nP) = n\phi(P)$ kaikilla $n \geq 1$.
2. Weilin liitos $e_\ell(P, \phi(P))$ on primitiivinen ℓ. ykkösen juuri. Toisin sanoen

$$e_\ell(P, \phi(P))^r = 1 \quad \text{jos ja vain jos} \quad r \text{ on luvun } \ell \text{ monikerta.}$$

Lause 4.2. *Olkoon E elliptinen käyrä, olkoon $\ell \geq 3$, olkoon $E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ vektoriavaruus sekä olkoon pisteet $P, Q \in E[\ell]$. Seuraavat väitteet ovat yhtäpitäviä:*

(a) *Pisteet P ja Q muodostavat kannan vektoriavaruudelle $E[\ell]$.*

(b) *Piste Q ei ole pisteen P monikerta ja $P \neq \mathcal{O}$.*

(c) *Weilin liitos $e_\ell(P, Q)$ on primitiivinen ℓ. ykkösjuuri.*

(d) *Weilin liitos $e_\ell(P, Q) \neq 1$.*

Todistus. Kohdasta (a) seuraa kohta (b), sillä pisteiden P ja Q täytyy olla riippumattomia, jotta ne muodostavat kannan vektoriavaruudelle. Jos kohta (a) puolestaan ei päde, niin on olemassa sellaiset luvut $u, v \in \mathbb{Z}/\ell\mathbb{Z}$, joilla $uP + vQ = \mathcal{O}$ ja ainakin toinen luvuista on nollasta eroava. Jos $v = 0$, niin $P = \mathcal{O}$ ja kohta (b) ei päde. Jos $v \neq 0$, niin $Q = -v^{-1}uP$, eli Q on pisteen P monikerta, jolloin kohta (b) ei päde. Kohdat (a) ja (b) ovat siis yhtäpitäviä.

Todistetaan seuraavaksi kohtien (c) ja (d) yhtäpitävyys. Olkoon Weilin liitos $\zeta := e_\ell(P, Q)$. Tiedetään, että $\zeta^\ell = 1$. Olkoon nyt $r \geq 1$ pienin kokonaisluku, jolle $\zeta^r = 1$. Eukleideen algoritmin avulla voidaan ilmaista lukujen r ja ℓ suurin yhteinen tekijä muodossa $\mathrm{syt}(r, \ell) = sr + t\ell$ joillakin luvuilla $s, t \in \mathbb{Z}$. Tällöin

$$\zeta^{\mathrm{syt}(r,\ell)} = \zeta^{sr+t\ell} = (\zeta^r)^s(\zeta^\ell)^t = 1.$$

Koska r on pienin luku jolle $\zeta^r = 1$, niin $\mathrm{syt}(r, \ell) = r$, eli $r \mid \ell$. Koska ℓ on alkuluku, niin $r = 1$ tai $r = \ell$. Jos $r = 1$, niin $\zeta = 1$. Jos $r = \ell$, niin $\zeta \neq 1$, koska r on pienin luku, jolla $\zeta^r = 1$. Kohdat (c) ja (d) ovat siis yhtäpitäviä.

Tarkastellaan seuraavaksi kohtia (a) ja (d). Olkoon pisteet P ja Q kanta vektoriavaruudelle $E[\ell]$. Tällöin $P \neq \mathcal{O}$, jolloin Lauseen 3.13 nojalla on olemassa piste $R \in E[\ell]$, jolle $e_\ell(P, R) \neq 1$. Piste R voidaan ilmaista pisteiden P ja Q lineaarikombinaationa, eli $R = uP + vQ$. Tästä seuraa, että

$$1 \neq e_\ell(P, R) = e_\ell(P, uP + vQ) = e_\ell(P, P)^u e_\ell(P, Q)^v = e_\ell(P, Q)^v.$$

Tällöin myös $e_\ell(P, Q) \neq 1$, joten kohta (d) pätee. Voidaan vielä todistaa, että jos kohta (b) ei päde, niin kohta (d) ei päde. Tällöin kohta (a) ei myöskään päde. Olkoon siis $P = \mathcal{O}$ tai $Q = uP$ jollain luvulla $u \in \mathbb{Z}/\ell\mathbb{Z}$. Jos $P = \mathcal{O}$, niin $e_\ell(P, Q) = e_\ell(\mathcal{O}, Q) = 1$. Jos $Q = uP$, niin

$$e_\ell(P, Q) = e_\ell(P, uP) = e_\ell(P, P)^u = 1^u = 1.$$

Eli kohta (d) ei päde kummassakaan tapauksessa. Tällöin kohdat (a) ja (d) ovat yhtäpitäviä.

□

Määritelmä 4.3. Olkoon E elliptinen käyrä, olkoon piste $P \in E[\ell]$, ja olkoon ϕ ℓ-muodonmuutoskuvaus pisteelle P. *Modifioitu Weilin liitos* $\hat{e}_\ell$ käyrällä $E[\ell]$ on

$$\hat{e}_\ell(Q, Q') = e_\ell(Q, \phi(Q')).$$

Lause 4.4. *Olkoon E elliptinen käyrä, olkoon piste $P \in E[\ell]$, olkoon ϕ pisteen P ℓ-muodonmuutoskuvaus, ja olkoon $\hat{e}_\ell$ modifioitu Weilin liitos. Olkoot pisteet Q ja Q' pisteen P monikertoja. Tällöin*

$$\hat{e}_\ell(Q, Q') = 1 \quad \textit{jos ja vain jos} \quad Q = \mathcal{O} \quad \textit{tai} \quad Q' = \mathcal{O}.$$

Todistus. Pisteet Q ja Q' voidaan ilmaista muodossa $Q = sP$ ja $Q' = tP$. Tällöin

$$\hat{e}_\ell(Q, Q') = \hat{e}_\ell(sP, tP) = e_\ell(sP, \phi(tP)) = e_\ell(sP, t\phi(P)) = e_\ell(P, \phi(P))^{st}.$$

Muodonmuutoskuvauksen määritelmän mukaan $\hat{e}_\ell(P, \phi(P))^\ell = 1$. Olkoon nyt $\hat{e}_\ell(Q, Q') = 1$, tällöin $\ell \mid st$. Koska ℓ on alkuluku, niin $\ell \mid s$ tai $\ell \mid t$. Nyt, koska pisteen P kertaluku on ℓ, niin $Q = \mathcal{O}$ tai $Q' = \mathcal{O}$. Jos lähdetään oletuksesta, että $Q = \mathcal{O}$ tai $Q' = \mathcal{O}$, niin $\ell \mid s$ tai $\ell \mid t$. Tästä saadaan edelleen $\ell \mid st$, jolloin $\hat{e}_\ell(Q, Q') = 1$. □

4.1 Muodonmuutoskuvaus käyrällä $Y^2 = X^3 + a$

Artikkelissa [5] kerrotaan, että muodonmuutoskuvaus on olemassa aina kaikille käyrän pisteille, kun käyrä on supersingulaarinen. Supersingulaarisen käyrän määritelmä löytyy niin ikään kyseisestä artikkelista. Artikkelissa annetaan myös lista yleisistä supersingulaarisista käyristä, ja vastaavista muodonmuutoskuvauksista. Tarkastellaan yhtä mainituista käyristä.

Lause 4.5. *Olkoon $E : Y^2 = X^3 + a$ kunnan $\mathbb{F}_p$ yli, missä $p \equiv 2 \pmod 3$, $p > 2$. Olkoon $\zeta_3 \in \mathbb{F}_{p^2}$, jolle pätee $\zeta_3^3 = 1$. Olkoon muodonmuutoskuvaus ϕ muotoa*

$$\phi(x, y) = (\zeta_3 x, y), \quad ja \quad \phi(\mathcal{O}) = \mathcal{O}.$$

(a) *Olkoon $P \in E(\mathbb{F}_p)$. Tällöin $\phi(P) \in E(\mathbb{F}_p)$.*

(b) *Muodonmuutoskuvaukselle ϕ pätee*

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2), \quad kaikilla\ P_1, P_2 \in E(\mathbb{F}_p).$$

Todistus. (a) Olkoon $P = (x, y) \in E(\mathbb{F}_p)$. Tällöin Weierstrassin yhtälön mukaan

$$y^2 = (\zeta_3 x)^3 + a = x^3 + a,$$

josta seuraa, että $\phi(P) = (\zeta_3 x, y) \in E(\mathbb{F}_p)$.

(b) Olkoon $P_1 = (x_1, y_1)$ sekä $P_2 = (x_2, y_2)$ erillisiä pisteitä. Pisteen $\phi(P_1)+$

$\phi(P_2)$ x-koordinaatiksi saadaan

$$\begin{aligned} x(\phi(P_1)+\phi(P_2)) &= \left(\frac{y_2-y_1}{\zeta_3 x_2-\zeta_3 x_1}\right)^2 - \zeta_3 x_1 - \zeta_3 x_2 \\ &= \frac{1}{\zeta_3^2}\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 + \zeta_3(-x_1-x_2) \\ &= \zeta_3\left(\frac{1}{\zeta_3^3}\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2\right) \\ &= \zeta_3\left(\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2\right) = \zeta_3 x(P_1+P_2). \end{aligned}$$

Olkoon $x_3 := x(P_1+P_2)$. Vastaavasti y-koordinaatiksi saadaan

$$\begin{aligned} y(\phi(P_1)+\phi(P_2)) &= -\left(\frac{y_2-y_1}{\zeta_3 x_2-\zeta_3 x_1}\right)(\zeta_3 x_1 - \zeta_3 x_3) - y_1 \\ &= -\frac{\zeta_3}{\zeta_3}\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3) - y_1 \\ &= -\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3) - y_1 = y(P_1+P_2). \end{aligned}$$

Tästä seuraa, että

$$\phi(P_1)+\phi(P_2) = (\zeta_3 x(P_1+P_2), y(P_1+P_2)) = \phi(P_1+P_2).$$

Olkoon nyt $P_1 = P_2$. Tällöin Pisteen $\phi(P_1)+\phi(P_2)$ x-koordinaatiksi saadaan

$$\begin{aligned} x(\phi(P_1)+\phi(P_2)) &= \left(\frac{3(\zeta_3 x_1)^2}{2y_1}\right)^2 - \zeta_3 x_1 - \zeta_3 x_2 \\ &= \zeta^4\left(\frac{3x_1^2}{2y_1}\right)^2 + \zeta_3(-x_1-x_2) \\ &= \zeta_3\left(\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2\right) = \zeta_3 x(P_1+P_2). \end{aligned}$$

Olkoon $x_3 := x(P_1 + P_2)$. Vastaavasti y-koordinaatiksi saadaan

$$\begin{aligned} y(\phi(P_1) + \phi(P_2)) &= -\left(\frac{3\zeta_3^2 x_1^2}{2y_1}\right)(\zeta_3 x_1 - \zeta_3 x_3) - y_1 \\ &= -\zeta_3^3\left(\frac{3x_1^2}{2y_1}\right)(x_1 - x_3) - y_1 \\ &= -\left(\frac{3x_1^2}{2y_1}\right)(x_1 - x_3) - y_1 = y(P_1 + P_2). \end{aligned}$$

Ja edelleen

$$\phi(P_1) + \phi(P_2) = (\zeta_3 x(P_1 + P_2), y(P_1 + P_2)) = \phi(P_1 + P_2).$$

□

Edellisen Lauseen avulla voidaan todistaa seuraava tulos.

Lause 4.6. *Olkoon elliptinen käyrä $E : Y^2 = X^3 + a$ kunnan $\mathbb{F}_p$ yli. Olkoon alkuluku p, jolle pätee $p \equiv 2 \pmod 3$. Olkoon $\zeta_3 \in \mathbb{F}_{p^2}$, jolle pätee $\zeta_3^3 = 1$ ja $\zeta_3 \neq 1$. Olkoon kuvaus $\phi(x, y) = (\zeta_3 x, y)$. Olkoon alkuluku $\ell \geq 5$, jolle on olemassa äärettömyyspisteestä eroava piste $P \in E(\mathbb{F}_p)[\ell]$. Tällöin ϕ on ℓ-muodonmuutoskuvaus pisteelle P. Toisin sanoen*

$$\hat{e}_\ell(P, P) = e_\ell(P, \phi(P))$$

on primitiivinen ℓ. ykkösen juuri.

Todistus. Todetaan aluksi, että Lauseen 4.5 nojalla $\ell\phi(P) = \phi(\ell P) = \phi(\mathcal{O}) = \mathcal{O}$. Lisäksi $P \neq \mathcal{O}$, jolloin $\phi(P) \neq \mathcal{O}$. Piste $\phi(P)$ on siis kertalukua ℓ. Voidaan myös todeta, että $\zeta_3 \notin \mathbb{F}_p$. Tämä johtuu siitä, että kunnan $\mathbb{F}_p^*$ kertaluku on $p - 1$, ja $p - 1 \equiv 1 \pmod 3$. Luvun ζ_3 kertaluku on 3, joka ei jaa kunnan $\mathbb{F}_p^*$ kertalukua. Tällöin $\zeta_3 \notin \mathbb{F}_p^*$ ja selvästi $\zeta_3 \neq 0$.

Todistetaan, että ζ_3 kuuluu kuntaan $\mathbb{F}_{p^2}$. Olkoon g kunnan $\mathbb{F}_{p^2}^*$ primitiivinen juuri. Nyt $g^{p^2-1} = 1$ ja $p^2 - 1 \equiv 2^2 - 1 \equiv 0 \pmod 3$. Tällöin $\zeta_3 = g^{(p^2-1)/3} \in \mathbb{F}_{p^2}$.

Todistetaan seuraavaksi, että piste $\phi(P)$ ei ole pisteen P monikerta, jolloin Lauseen 4.2 mukaan $e_\ell(P, \phi(P))$ on primitiivinen ℓ. ykkösen juuri. Olkoon $P = (x, y)$, missä $x, y \in \mathbb{F}_p$. Tällöin pisteen P moninkertojen koordinaatit ovat myös kunnassa $\mathbb{F}_p$. Toisaalta pisteen $\phi(P) = (\zeta_3 x, y)$ x-koordinaatti ei kuulu kuntaan $\mathbb{F}_p$, jolloin pisteen koordinaatit kuuluvat kuntaan $\mathbb{F}_p$ vain, jos $x = 0$. Tällöin $P = (0, y)$. Nyt

$$\begin{aligned} 2P &= (\lambda^2 - 2x, \lambda(x - x_3) - y) \\ &= \left(\left(\frac{3x^2 + A}{2y} \right)^2, \left(\frac{3x^2 + A}{2y} \right)(-x_3) - y \right) \\ &= (0, -y) = -P. \end{aligned}$$

Joten $3P = 2P + P = P - P = \mathcal{O}$. Piste on siis kertalukua 3, mutta oletuksena piste P on kertalukua $\ell \geq 5$, joten piste $\phi(P)$ ei ole pisteen P monikerta. Lauseen 4.2 nojalla $\hat{e}(P, P)$ on primitiivinen ℓ. ykkösen juuri. □

Lause 4.7. *Olkoon p alkuluku. Polynomi $x^2 + 3$ on jaoton kunnassa $\mathbb{F}_p$, kun $p \equiv 2 \pmod 3$.*

Todistus. Jos $x^2 + 3$ on jaollinen kunnassa $\mathbb{F}_p$, niin on olemassa sellainen $x_0 \in \mathbb{F}_p$, jolle $x_0^2 + 3 = 0$. Edelleen saadaan $x_0^2 + 3 = p$. Nyt koska $p \equiv 2 \pmod 3$, niin myös $x_0^2 + 3 \equiv 2 \pmod 3$. Nyt kaikki mahdolliset tapaukset ovat $x_0 \in \{0, 1, 2\}$. Kun $x_0 \in \{1, 2\}$, niin $x_0^2 + 3 \equiv 1 \pmod 3$. Jos $x_0 = 0$, niin saadaan $0^2 + 3 \equiv 0 \pmod 3$. Tämä on ristiriita oletuksen $x_0^2 + 3 \equiv 2 \pmod 3$ kanssa, jolloin polynomi $x^2 + 3$ on jaoton kunnassa $\mathbb{F}_p$, kun $p \equiv 2 \pmod 3$. □

Nyt, koska polynomi $x^2 + 3$ on jaoton kunnassa $\mathbb{F}_p$, voidaan tehdä kuntalaajennus $\mathbb{F}_{p^2}[T]/(T^2 + 3)$. Huomataan, että jos valitaan luvuksi $\zeta_3 =$

$-(2^{-1}T - 2^{-1})$, niin

$$\zeta_3^3 = -\left(2^{-1}T - 2^{-1}\right)^3 = -2^{-3}T^3 - 3 \cdot 2^{-3}T^2 - 3 \cdot 2^{-3}T - 2^{-1}.$$

Nyt, koska $T^2 = -3$, saadaan

$$\zeta_3^3 = 3 \cdot 2^{-3}T + 9 \cdot 2^{-3} - 3 \cdot 2^{-3}T - 2^{-3} = 9 \cdot 2^{-3} - 2^{-3} = 1.$$

Esimerkki 4.8. *Olkoon alkuluku* $p = 17 \equiv 2 \pmod 3$. *Olkoon elliptinen käyrä* $E : Y^2 = X^3 + 1$ *kunnan* $\mathbb{F}_p$ *yli. Nyt* $\zeta_3 = -2^{-1}T - 2^{-1} = -9T - 9 = 8T + 8 \in \mathbb{F}_{p^2}[T]/(T^2 + 3)$. *Olkoon* $P = (2, 3)$, *joka on käyrällä* E. *Olkoon kuvaus* $\phi(x, y) = (\zeta_3 x, y)$. *Tällöin*

$$\phi(P) = (16T + 16, 3).$$

Voidaan vielä tarkistaa, että piste $\phi(P)$ *toteuttaa käyrän* E *yhtälön. Yhtälön vasemmaksi puoleksi saadaan* 9, *ja yhtälön oikeaksi puoleksi saadaan*

$$(-T - 1)^3 + 1 = -T^3 - 3T^2 - 3T - 1 + 1 = 3T + 9 - 3T = 9.$$

5 Kolmen osapuolen Diffie-Hellman

Yksi Weilin liitoksen käyttökohteista on kolmen osapuolen Diffie-Hellman. Kolmen osapuolen Diffie-Hellman-avaimenvaihdon ideana on se, että avaimenvaihdon jokainen osapuoli voi luoda jaetun avaimen, kun kaikki parit kolmesta osapuolesta jakavat julkisen avaimensa keskenään.

Olkoot kolmena osapuolena Alice, Bob sekä Carl. Aluksi osapuolet valitsevat yhteisen elliptisen käyrän E ja sellaisen kertalukua ℓ olevan pisteen $P \in E(\mathbb{F}_q)[\ell]$, että ℓ on alkuluku, sekä pisteellä P on olemassa ℓ-muodonmuutoskuvaus. Olkoon $\hat{e}_\ell$ modifioitu Weilin liitos kyseisellä muodonmuutoskuvauksella.

Seuraavaksi kaikki osapuolet valitsevat salassa pidettävän kokonaisluvun. Alice valitsee luvun n_A, Bob valitsee luvun n_B ja Carl valitsee luvn n_C. Luvut toimivat osapuolten salaisina avaimina. Osapuolet laskevat salaisia lukujaan vastaavat julkisesti lähetettävät pisteet

$$Q_A = n_A P, \quad Q_B = n_B P \quad \text{ja} \quad Q_C = n_C P.$$

Tämän jälkeen osapuolet laskevat julkisesti jaetuista pisteistä yhden yhteisen pisteen seuraavasti:

$$\begin{aligned}
&\text{Alice laskee} \quad \hat{e}_\ell(Q_B, Q_C)^{n_A} = \hat{e}_\ell(n_B P, n_C P)^{n_A} = \hat{e}_\ell(P, P)^{n_B n_C n_A},\\
&\text{Bob laskee} \quad \hat{e}_\ell(Q_A, Q_C)^{n_B} = \hat{e}_\ell(n_A P, n_C P)^{n_B} = \hat{e}_\ell(P, P)^{n_A n_C n_B},\\
&\text{Carl laskee} \quad \hat{e}_\ell(Q_A, Q_B)^{n_C} = \hat{e}_\ell(n_A P, n_B P)^{n_C} = \hat{e}_\ell(P, P)^{n_A n_B n_C}.
\end{aligned}$$

Nyt kaikilla osapuolilla on yhteinen jaettu salainen piste $\hat{e}_\ell(P, P)^{n_A n_B n_C}$.

Avaimenvaihdon ulkopuolinen henkilö Eve pystyy selvittämään salaisen avaimen julkisesta pisteestä $Q_i = n_i P$, jos Eve pystyy ratkaisemaan ECDLP:n. Toisaalta Eve pystyy selvittämään salaisen avaimen myös esimerkiksi Alicen

julkisesta pisteestä $Q_A = n_A P$ laskemalla $\hat{e}_\ell(P, P)$ sekä

$$\hat{e}_\ell(Q_A, P) = \hat{e}_\ell(n_A P, P) = \hat{e}_\ell(P, P)^{n_A}.$$

Riittää siis, että Eve ratkaisee yhtälön $a^n = b$ kunnassa $\mathbb{F}_q$. Kolmen osapuolen Diffie-Hellmannin turvallisuus nojautuu myös sille oletukselle, että DLP on vaikea kunnassa $\mathbb{F}_q^*$.

Esimerkki 5.1. *Etsitään ensin sopiva alkuluku q, jolle pätee $q \equiv 2 \pmod 3$. Käydään läpi annetusta luvusta seuraavia alkulukuja, kunnes löytyy alkuluku, joka täyttää ehdon $q \equiv 2 \pmod 3$. Kustakin luvusta seuraava alkuluku saadaan esimerkiksi käyttämällä SageMath:n tarjoamaa funktiota* `next_prime`*. Löydetään luku $q = 3145739$. Tässä esimerkissä elliptisen käyrän operaatiot, pisteiden kertaluvun laskeminen ja käyrän pisteiden lukumäärän laskeminen on tehty SageMath:n avulla.*

Olkoon elliptinen käyrä $E : Y^2 = X^3 + 1$. Luku $\ell = 109$ jakaa käyrän E kertaluvun, joka on $\#E = 2^2 \cdot 3 \cdot 5 \cdot 13 \cdot 37 \cdot 109$. Etsitään kertalukua ℓ oleva piste hakemalla ensin satunnainen piste elliptiseltä käyrältä, ja testaamalla onko pisteen kertaluku ℓ. Toistetaan tätä niin kauan, kunnes löydetään sopiva piste. Löydetään kertalukua ℓ oleva piste $P = (31900, 1774509)$. Olkoon vielä kuvaus $\phi(x, y) = (\zeta_3 x, y)$ ℓ-muodonmuutoskuvaus, missä $\zeta_3 = -2^{-1}T - 2^{-1} \in \mathbb{F}_{q^2}[T]/(T^2+3)$. Alice, Bob ja Carl valitsevat aluksi salaiset avaimensa. Olkoot salaiset avaimet

$$n_A = 83, \quad n_B = 62, \quad n_C = 54.$$

Salaisten avaintensa avulla he laskevat julkistettavat pisteet

$$Q_A = n_A P = (41318, 2836859),$$
$$Q_B = n_B P = (2405001, 2112099),$$
$$Q_C = n_C P = (2426973, 3052955).$$

Tämän jälkeen Alice, Bob ja Carl laskevat jaetun salaisen avaimen seuraavasti:

$$\hat{e}_\ell(Q_B, Q_C)^{n_A} = (477971T + 1363427)^{83} = 1313832T + 367275,$$
$$\hat{e}_\ell(Q_A, Q_C)^{n_B} = (964627T + 2665912)^{62} = 1313832T + 367275,$$
$$\hat{e}_\ell(Q_A, Q_B)^{n_C} = (2826471T + 128870)^{54} = 1313832T + 367275.$$

6 ID-pohjainen julkisen avaimen kryptosysteemi

ID-pohjaisessa kryptosysteemissä ideana on, että käyttäjä voi valita oman julkisen avaimensa. ID voisi olla esimerkiksi vaikka käyttäjän sähköpostiosoite. Oletetaan, että on olemassa jokin luotettu osapuoli Tom, jonka tehtävänä on jakaa käyttäjille informaatiota sekä suorittaa laskutoimituksia. Käyttäjät voivat pyytää Tomilta salaista avaintaan, jonka Tom generoi omaa salaista avaintaan käyttäen. Käyttäjät voivat myös salata viestejä Tomin julkaiseman julkisen avaimen avulla.

Aluksi luotettu osapuoli Tom valitsee kunnan $\mathbb{F}_q$, elliptisen käyrän E, sekä sellaisen kertalukua ℓ olevan pisteen $P \in E(\mathbb{F}_q)[\ell]$, missä ℓ on alkuluku sekä sille on olemassa ℓ-muodonmuutoskuvaus. Olkoon $\hat{e}$ modifioitu Weilin liitos kyseisellä muodonmuutoskuvauksella. Olkoon lisäksi A kaikkien käyttäjien valitsemien ID:iden joukko.

Tom julkaisee kaksi hash-funktiota H_1 ja H_2. Funktio H_1 antaa jonkin käyttäjän valitsemaa ID:tä vastaavan pisteen ryhmästä $E(\mathbb{F}_q)[\ell]$, eli

$$H_1 : A \to E(\mathbb{F}_q)[\ell].$$

Funktio H_2 muuntaa kunnan $\mathbb{F}_{q^2}$ alkiot B-mittaiseksi binäärivektoriksi,

$$H_2 : \mathbb{F}_{q^2} \to \left\{ \sum_{i=0}^{B-1} a_i 2^i \;\middle|\; a_i \in \{0,1\} \right\}.$$

Selkotekstien joukko $\mathcal{M}$ on kaikki B-mittaiset binäärivektorit.

Tom generoi yleisavaimen valitsemalla nollasta eroavan salaisen kokonaisluvun $s \pmod{\ell}$ ja laskemalla

$$P^{\mathrm{Tom}} = sP \in E(\mathbb{F}_q)[\ell].$$

Nyt Tomin salainen yleisavain on s ja julkinen yleisavain on P^{Tom}.

Jos Bob haluaa lähettää Alicelle viestin $M \in \mathcal{M}$, hän laskee pisteen

$$P^{\text{Alice}} = H_1(\text{Alice}^{\text{Pub}}) \in E(\mathbb{F}_q)[\ell].$$

Sitten hän valitsee satunnaisen luvun $1 < r < q$ ja laskee kaksi pistettä

$$C_1 = rP \quad \text{ja} \quad C_2 = M \ \mathbf{xor}\ H_2(\hat{e}_\ell(P^{\text{Alice}}, P^{\text{Tom}})^r).$$

Salattu viesti on pari $C = (C_1, C_2)$.

Jos Alice pyytää salaista avainta valitsemalleen ID:lle $\text{Alice}^{\text{Pub}}$, Tom antaa Alicelle pisteen

$$Q^{\text{Alice}} = sP^{\text{Alice}} = sH_1(\text{Alice}^{\text{Pub}}) \in E(\mathbb{F}_q)[\ell].$$

Alice voi purkaa Bobin lähettämän viestin Tomin antamalla salaisella avaimella Q^{Alice} laskemalla ensin $\hat{e}_\ell(Q^{\text{Alice}}, C_1)$, jolle pätee

$$\begin{aligned}\hat{e}_\ell(Q^{\text{Alice}}, C_1) &= \hat{e}_\ell(sP^{\text{Alice}}, rP) = \hat{e}_\ell(P^{\text{Alice}}, P)^{rs} \\ &= \hat{e}_\ell(P^{\text{Alice}}, sP)^r = \hat{e}_\ell(P^{\text{Alice}}, P^{\text{Tom}})^r,\end{aligned}$$

jolloin Alice saa viestin laskulla C_2 **xor** $H_2(\hat{e}_\ell(Q^{\text{Alice}}, C_1))$, sillä

$$\begin{aligned}&C_2 \ \mathbf{xor}\ H_2(\hat{e}_\ell(Q^{\text{Alice}}, C_1)) \\ &= (M \ \mathbf{xor}\ H_2(\hat{e}_\ell(P^{\text{Alice}}, P^{\text{Tom}})^r)) \ \mathbf{xor}\ H_2(\hat{e}_\ell(P^{\text{Alice}}, P^{\text{Tom}})^r) = M.\end{aligned}$$

Esimerkki 6.1. *Käytetään tässä esimerkissä samoja arvoja kuin esimerkissä 5.1. Olkoon* $p = 3145739$*. Luvulle pätee* $p \equiv 2 \pmod 3$*, ja se on alkuluku. Olkoon myös elliptinen käyrä* $E : Y^2 = X^3 + 1$*. Luku* $\ell = 109$ *jakaa käyrän* E *kertaluvun, joka on* $\#E = 2^2 \cdot 3 \cdot 5 \cdot 13 \cdot 37 \cdot 109$*. Löydetään kertalukua* ℓ *oleva piste* $P = (379830, 1104941)$*. Olkoon vielä kuvaus* $\phi(x, y) = (\zeta_3 x, y)$ *ℓ-muodonmuutoskuvaus, missä* $\zeta_3 = -2^{-1}T - 2^{-1} \in \mathbb{F}_{p^2}[T]/(T^2 + 3)$*.*

Hash-funktiot H_1 *ja* H_2 *voidaan määritellä usealla eri tavalla, mutta tämän esimerkin tarkoitukseen riittää, kun* H_1 *palauttaa pisteen* P *kerrottuna*

käyttäjän valitsemaa ID:tä vastaavalla luvulla $0 < n < \ell$*, joka on valittu satunnaisesti jo silloin kun käyttäjä valitsi oman ID:n. Määritellään funktio* H_2 *niin, että se asettaa jokaisen ryhmän* $\mathbb{F}_{p^2}$ *alkion vastaamaan jotain* 24*-pituista binäärivektoria. Toisin sanoen jos* $a \in \mathbb{F}_{p^2}$*, niin* $H_2(a) = b \in \{0, \ldots, 2^{24} - 1\}$*.*

Tom valitsee salaisen avaimensa $s = 2994808$*, jonka jälkeen Tom julkaisee pisteen* $P^{Tom} = sP = (2956338, 632172)$*.*

Seuraavaksi Alice valitsee itselleen vapaan julkisen ID:n $\text{Alice}^{\text{Pub}} = \text{'Alice'}$*. Alicen ID:tä vastaavaksi luvuksi valitaan satunnainen luku* 104*, toisin sanoen* $P^{Alice} = H_1(Alice^{Pub}) = 37P = (1099865, 238439)$*. Alice pyytää Tomilta salaista avaintaan, joka on*

$$Q^{Alice} = sP^{Alice} = (2595432, 2714634).$$

Bob puolestaan salaa viestin $M =$*'Hei' valitsemalla ensin satunnaisen luvun* $r = 747084$*. Teksti* M *voidaan muuntaa luvuksi* 4744553*. Tämän jälkeen Bob laskee Alicen julkisen pisteen* P^{Alice}*. Salattu viesti on pari*

$$\begin{aligned}(C_1, C_2) &= (rP, M \ \textbf{\textit{xor}}\ H_2(\hat{e}_\ell(P^{Alice}, P^{Tom})^r) \\ &= ((349030, 634631), M \ \textbf{\textit{xor}}\ H_2((1682977a + 2154672)^r)) \\ &= ((349030, 634631), M \ \textbf{\textit{xor}}\ H_2(2739063a + 1672169)) \\ &= ((349030, 634631), 6199554)\end{aligned}$$

Alice vastaanottaa Bobin lähettämän salatun viestin, ja avaa viestin laskemalla

$$\begin{aligned}C_2 \ \textbf{\textit{xor}}\ H_2(\hat{e}_\ell(Q^{Alice}, C_1)) &= C_2 \ \textbf{\textit{xor}}\ H_2(2739063a + 1672169) \\ &= 4744553 = \textit{'Hei'}.\end{aligned}$$

Tässä esimerkissä teksti on muunnettu kokonaisluvuksi Pythonissa funktiokutsulla

```
int.from_bytes(text.encode(), 'big').
```

Olkoon k haluttujen kirjainten lukumäärä. Kokonaisluvut on muunnettu tekstiksi funktiokutsulla

```
int.to_bytes(kokonaisluku, k, 'big').
```

7 BLS-allekirjoitus

BLS-allekirjoitus on lyhyt digitaalinen allekirjoitus, joka on esitelty Bonehin, Lynnin ja Shachamin teoksessa [4]. Ideana on, että Alice voi allekirjoittaa digitaalisesti jonkin dokumentin D salaisella avaimellaan, ja kuka tahansa voi myöhemmin verifioida allekirjoituksen Alicen julkisen avaimen avulla.

Valitaan aluksi julkiset parametrit. Olkoon elliptinen käyrä E kunnan $\mathbb{F}_q$ yli. Olkoon piste $P \in E(\mathbb{F}_q)$ kertalukua p, missä p on alkuluku ja sille pätee $p \nmid q(q-1)$ sekä $p^2 \nmid \#E(\mathbb{F}_q)$. Olkoon seuraavaksi $1 < \alpha < p$. Nyt on olemassa sellainen piste $Q \in E(\mathbb{F}_{q^\alpha})$, joka on lineaarisesti riippumaton pisteestä P. Nyt koska pisteet P ja Q ovat lineaarisesti riippumattomia, niin pisteille voidaan laskea Weilin liitos. Määritellään vielä hash-funktio H binäärivektorilta joukkoon $E(\mathbb{F}_q)[p]$, kuten Bonehin, Lynnin ja Shachamin teoksessa.

Kun julkiset parametrit on valittu, niin Alice valitsee satunnaisen luvun $x \in \mathbb{F}_p$ ja laskee $V = xQ$. Nyt salainen avain on x ja julkinen avain on $V \in E(\mathbb{F}_{q^\alpha})$. Alice allekirjoittaa dokumentin $D \in \{0,1\}^*$ laskemalla ensin $R = H(D)$ ja sitten $\sigma = xR \in E(\mathbb{F}_q)$. Allekirjoitus s on pisteen σ x-koordinaatti.

Allekirjoitus s verifioidaan etsimällä ensin sellainen $y \in \mathbb{F}_q$, jolla $\sigma = (s, y)$ on piste käyrällä $E(\mathbb{F}_q)$. Jos sellaista alkiota y ei löydy, allekirjoitus hylätään. Tämän jälkeen varmistetaan, että pisteen σ kertaluku on p. Jos ei ole, niin allekirjoitus hylätään. Seuraavaksi lasketaan $R = H(D)$. Tämän jälkeen testataan päteekö jompikumpi seuraavista.

$$e_p(\sigma, Q) = e_p(R, V) \quad \text{tai} \quad e_p(\sigma, Q)^{-1} = e(R, V).$$

Jos jompikumpi pätee, niin allekirjoitus hyväksytään, muulloin allekirjoitus hylätään. Ensimmäinen kohta tulee siitä, että

$$e_p(\sigma, Q) = e_p(xR, Q) = e_p(R, Q)^x = e_p(R, xQ) = e_p(R, V).$$

Kohta $e_p(\sigma, Q)^{-1} = e_p(-\sigma, Q) = e_p(R, V)$ tarkastetaan sen takia, että valittu y-koordinaatti voi olla väärin.

Esimerkki 7.1. *Tiedetään, että muodonmuutoskuvaus pisteelle P palauttaa pisteen Q, joka on lineaarisesti riippumaton pisteestä P. Valitaan tähän esimerkkiin sama muodonmuutoskuvaus kuin aiemmissa esimerkeissä.*

Käytetään tässä esimerkissä samoja arvoja kuin esimerkissä 5.1.

Olkoon $q = 3145739$. Luvulle pätee $q \equiv 2 \pmod 3$, ja se on alkuluku. Olkoon myös elliptinen käyrä $E : Y^2 = X^3 + 1$. Luku $p = 109$ jakaa käyrän E kertaluvun, joka on $\#E = 2^2 \cdot 3 \cdot 5 \cdot 13 \cdot 37 \cdot 109$. Luvuille p ja q pätee ehdot $p \nmid q(q-1)$ ja $p^2 \nmid \#E$. Löydetään kertalukua p oleva piste $P = (2323242, 421954)$. Olkoon vielä kuvaus $\phi(x, y) = (\zeta_3 x, y)$ ℓ-muodonmuutoskuvaus, missä $\zeta_3 = -2^{-1}T - 2^{-1} \in \mathbb{F}_{p^2}[T]/(T^2+3)$. Bohenin, Lynnin ja Shachamin teoksesta poiketen tähän esimerkkiin riitää, kun hash-funktio H määritellään siten, että yhdistetään jokaista bittivektoria i vastaamaan kokonaisluku n_i ja palautetaan piste $n_i P \in E(\mathbb{F}_q)[p]$. Jotta piste $n_i P$ ei olisi äärettömyyspiste, niin $p \nmid n_i$.

Nyt tiedetään, että $\alpha = 2$, eli $Q = \phi(P) \in E(\mathbb{F}_{q^\alpha})$. Voidaan laskea piste $Q = ((1984118T + 1984118, 421954)$. Alice valitsee satunnaisen salaisen avaimensa $x = 2770398$ ja laskee julkisen pisteen $V = xQ = (1774864T + 1774864, 942737)$.

Alice allekirjoittaa viestin $D =$ 'Alice allekirjoitti'. Hash-funktio palauttaa pisteen $R = H(D) = (568406, 2315660)$. Allekirjoitus on pisteen $\sigma = xR = (31900, 1774509)$ x-koordinaatti.

Bob vastaanottaa luvun 31900 ja etsii sille vastaavan y-koordinaatin, joka on nyt luvun 31900^3+1 neliöjuuri. Bob löytää y-koordinaatiksi luvun 1774509. Bob verifioi Alicen allekirjoituksen viestille D tarkistamalla ensin, että pisteen $\sigma = (31900, 1774509)$ kertaluku on p. Nyt pisteen σ kertaluku on p ja siir-

rytään seuraavaan vaiheeseen. Lasketaan $R = H(D) = (568406, 2315660)$. *Testataan, päteekö* $e_p(\sigma, Q) = e_p(R, V)$. *Saadaan*

$$e_p(\sigma, Q) = 407900T + 614621$$
$$e_p(R, V) = 407900T + 614621.$$

Jos testi ei olisi mennyt läpi, niin Bob olisi testannut vielä päteekö $e_p(\sigma, Q)^{-1} = e_p(R, V)$. *Nyt toinen testeistä onnistui, joten allekirjoitus hyväksytään.*

8 Liitteet

Algoritmi 1 Pisteiden yhteenlasku yleistetyllä elliptisellä käyrällä.

procedure ADD($P, Q, a_1, \ldots, a_6$) ▷ $a_1, \ldots, a_6$ ovat käyrän E kertoimia
  if $x_1 = x_2$ and $y_1 + y_2 + a_1 \cdot x_2 + a_3 = 0$ **then**
    return $\mathcal{O}$
  end if
  if $P = \mathcal{O}$ **then return** Q
  else if $Q = \mathcal{O}$ **then return** P
  end if
  if $x_1 = x_2$ **then**
    $\lambda \leftarrow (3x_1^2 + 2a_2x_1 + a_4 - a_1y_1)/(2y_1 + a_1x_1 + a_3)$
    $\nu \leftarrow (-x_1^3 + a_4x_1 + 2a_6 - a_3y_1)/(2y_1 + a_1x_1 + a_3)$
  else
    $\lambda \leftarrow (y_2 - y_1)/(x_2 - x_1)$
    $\nu \leftarrow (y_1x_2 - y_2x_1)/(x_2 - x_1)$
  end if
  $x_3 \leftarrow \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$
  $y_3 \leftarrow -(\lambda + a_1)x_3 - \nu - a_3$
  return (x_3, y_3)
end procedure

Algoritmi 2 Kobtlizin menetelmä pisteen nP laskemiseksi.

procedure KOBLITZ_ADDITION(n, P)
    $n_0 = n$, $n_1 = 0$, $i = 0$
    $Q = \mathcal{O}$, $P_0 = P$
    while $n_0 \neq 0$ or $n_1 \neq 0$ **do**
        if c on pariton **then**
            $v_i = 2 - ((n_0 - 2n_1) \pmod 4)$
            $n_0 = n_0 - v_i$
            $Q = Q + v_i P_0$ ▷ tässä $v_i \in \{-1, 1\}$
        else
            $v_i = 0$
        end if
        $i = i + 1$
        $(n_0, n_1) = (n_1 - \frac{n_0}{2}, -\frac{n_0}{2})$
        $P_0 = \tau(P_0)$
    end while
    return Q
end procedure

Algoritmi 3 Millerin menetelmä funktion f_P laskemiseksi Weilin liitosta varten.

procedure MILLER(P, Q)
  $T \leftarrow P$, $f \leftarrow 1$
  for $i \leftarrow n-2$ to 0 **do**
    $f \leftarrow f^2 \cdot g_{T,T}$
    $T \leftarrow 2T$
    if $m_i = 1$ **then**
      $f \leftarrow f \cdot g_{T,P}$
      $T \leftarrow T + P$
    end if
  end for
  return f
end procedure

Algoritmi 4 MOV algoritmi ECDLP ratkaisemiseksi

procedure MOV(P, G, ℓ, k)
  $N \leftarrow \#E(\mathbb{F}_{p^k}), T' \leftarrow \mathcal{O}, \alpha \leftarrow 1$
  while $\alpha = 1$ **do**
    while $T' \neq \mathcal{O}$ **do**
      Valitaan piste $T \in E(\mathbb{F}_{p^k})$, jolle pätee $T \notin E(\mathbb{F}_p)$
      $T' \leftarrow (N/\ell)T$
    end while
    $\alpha = e_\ell(P, T') \in \mathbb{F}^*_{p^k}$
    $\beta = e_\ell(Q, T') \in \mathbb{F}^*_{p^k}$
  end while
  Etsitään sellainen n, jolle pätee $\beta = \alpha^n$. Tällöin $Q = nP$.
end procedure

Viitteet

[1] Henri Cohen. *A course in computational algebraic number theory*. Vol. 8. Springer-Verlag Berlin, 1993.

[2] René Schoof. "Counting points on elliptic curves over finite fields". *Journal de théorie des nombres de Bordeaux* 7.1 (1995), s. 219–254.

[3] Jerome A Solinas. "Efficient arithmetic on Koblitz curves". *Towards a Quarter-Century of Public Key Cryptography* (2000), s. 125–179.

[4] Dan Boneh, Ben Lynn ja Hovav Shacham. "Short signatures from the Weil pairing". Teoksessa: *International conference on the theory and application of cryptology and information security*. Springer. 2001, s. 514–532.

[5] Steven D Galbraith ja Victor Rotger. "Easy decision diffie-hellman groups". *LMS Journal of Computation and Mathematics* 7 (2004), s. 201–218.

[6] Henri Cohen et al. *Handbook of elliptic and hyperelliptic curve cryptography*. CRC press, 2005.

[7] Jeffrey Hoffstein et al. *An introduction to mathematical cryptography*. Vol. 1. Springer, 2008.

[8] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. Chapman ja Hall/CRC, 2008.

[9] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer, 2009.

[10] Andreas Enge. "Bilinear pairings on elliptic curves". *L'Enseignement Mathématique* 61.1 (2016), s. 211–243.