HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen laitos

Tekijä — Författare — Author
Heini Ilmarinen

Työn nimi — Arbetets titel — Title

Elliptisten käyrien kryptografia

Oppiaine — Läroämne — Subject		
Matematiikka		
Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Pro gradu -tutkielma	Toukokuu 2016	47 s.

Tiivistelmä — Referat — Abstract

Kryptografia, eli tiedon salaus, on nopeasti kehittyvä ala, joka on läsnä ihmisten päivittäisessä toiminnassa. Perinteisen tiedon salauksen lisäksi kryptografian avulla voidaan toteuttaa monipuolisia toiminnallisuuksia, kuten digitaaliset allekirjoitukset ja avaimenvaihto. Nämä toiminnallisuudet on mahdollista toteuttaa julkisen avaimen kryptografian avulla.

Elliptiset käyrät ovat kuutiollisia tasokäyriä, joiden pisteiden välille voidaan määritellä yhteenlaskuoperaatio. Näin ollen elliptisen käyrän pisteet muodostavat Abelin ryhmän, joten niitä on mahdollista käyttää diskreetin logaritmin ongelmaan perustuvissa kryptosysteemeissä, eli julkisen avaimen kryptosysteemeissä. Elliptisten käyrien kryptografisten algoritmien suojaustaso perustuu elliptisen käyrän diskreetin logaritmin ongelmaan, jonka yleiselle muodolle ei olla löydetty subeksponentiaalista ratkaisua. Näin ollen elliptisten käyrien kryptografialla on mahdollista saavuttaa vastaava suojaustaso lyhyemmillä avaimilla, verrattuna muihin julkisen avaimen kryptografian metodeihin.

Tutkielman ensimmäisessä osassa perehdytään elliptisten käyrien teoriaan keskittyen tärkeimpiin teemoihin kryptografian kannalta. Luvussa esitetään yhteenlasku elliptisen käyrän pisteille ja johdetaan ryhmälait. Erityisesti käsitellään kryptografiassa käytettäviä äärellisissä kunnissa määriteltyjä elliptisiä käyriä, joita on kaksi yleisintä luokkaa: alkulukukunnissa määritellyt käyrät $E(\mathbb{F}_p)$ ja binäärikunnissa määritellyt käyrät $E(\mathbb{F}_{2^m})$.

Tutkielman toisen osan keskiössä on kryptografia; julkisen avaimen kryptografia ja erityisesti elliptisen käyrän kryptografia ovat keskiössä. Luvussa tarkastellaan elliptisen käyrän diskreetin logaritmin ongelmaa ja elliptisen käyrän rakenteeseen liittyviä tuloksia. Tutkielman lopussa esitetään algoritmit kullekin julkisen avaimen kryptografian avulla toteutettavalle toiminnallisuudelle käyttäen elliptisten käyrien kryptografian algoritmeja. Avaimenvaihdosta käytetään esimerkkinä elliptisen käyrän Diffie-Hellman avaimenvaihtoa ja digitaalisesta allekirjoituksesta elliptisen käyrän digitaalista allekirjoitusalgoritmia. Salaus ja purku menetelmänä esitellään elliptisen käyrän integroitu salaus -skeema.

Avainsanat — Nyckelord — Keywords
Kryptografia, elliptinen käyrä

Säilytyspaikka — Förvaringsställe — Where deposited
Kumpulan tiedekirjasto

Muita tietoja — Övriga uppgifter — Additional information

Elliptisten käyrien kryptografia

Heini Ilmarinen

Sisältö

Lista algoritmeista

1 Johdanto

Matemaatikot ovat tutkineet elliptisiä käyriä 1900-luvun puolivälistä alkaen. Elliptisten käyrien lukuteoristen kysymysten tutkimista tavoiteltiin alun perin esteettisistä syistä, mutta viimeisten vuosikymmenten aikana nämä kysymykset ovat tulleet tärkeiksi monilla soveltavilla aloilla, kuten koodausteoriassa, näennäissatunnaislukujen generoinnissa ja etenkin kryptografiassa [8].

Aina 1970-luvulle saakka kryptografia, eli tiedon salaus, oli lähes yksinomaan diplomaattisten sovelluksien sekä armeijan ja hallituksen sovelluksien käytössä. Ensimmäinen laajalevikkinen kryptografinen sovellus oli 1980-luvun lopun ensimmäisen sukupolven langaton matkapuhelinjärjestelmä. Nykyään kryptografiaa käytetään päivittäin esimerkiksi yhdistettäessä langattomaan WLAN verkkoon, ohjelmistopäivityksiä ladattaessa tai ostettaessa tuotteita pankki- tai luottokortilla kaupasta tai internetistä.

Kryptografiset menetelmät voidaan jakaa kahteen kategoriaan: yksityisen avaimen kryptografiaan ja julkisen avaimen kryptografiaan. Yksityisen avaimen metodeissa molemmat osapuolet käyttävät samaa avainta salaukseen ja purkamiseen. Julkisen avaimen metodeissa kullakin osapuolella on sekä salainen avain että julkinen avain. Salauksessa lähettäjä käyttää vastaanottajan julkista avainta, kun taas vastaanottaja käyttää salaista avaintaan salatun viestin purkamiseksi. Lisäksi julkisen avaimen kryptografia mahdollistaa yksityisen avaimen kryptografiaa monipuolisempia toimintoja, kuten avaimenvaihdon ja digitaaliset allekirjoitukset.

Yleisimmin käytettyjä julkisen avaimen metodeja ovat RSA ja Diffie-Hellman avaimenvaihto, jotka perustuvat runsaasti tutkittuihin lukuteoreettisiin ongelmiin: kokonaisluvun tekijöihinjakoon (RSA) ja diskreetin logaritmin ongelmaan (D-H). Elliptisten käyrien kryptografian suojaustaso perustuu elliptisen käyrä diskreetin logaritmin ongelman haasteellisuuteen. Elliptisiä käyriä käytetään kryptografiassa siksi, että ne tarjoavat lyhyemmillä avaimilla vastaavan suojaustason kuin muut julkisen avaimen metodit. Taulukossa 1 esitetään NIST:n (National Institute of Standards and Technology) suosittelemat avainkoot (bitteinä) tietyn suojaustason saavuttamiseksi erityyppisillä algoritmeilla [13]. Taulukosta nähdään, että symmetristen avainkokojen kasvaessa vaadittavat avainkoot RSA:lle ja Diffie-Hellmanille kasvavat huomattavasti nopeammin kuin avainkoot elliptisten käyrien kryptosysteemeissä.

Taulukko 1: NIST:n suosittelemat avainkoot.

Suojaustaso/ Symmetrinen avainkoko (bit)	RSA ja D-H avainkoko (bit)	Elliptisten käyrien avainkoko (bit)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Elokuussa 2015 NSA (Yhdysvaltojen National Security Agency) julkaisi tiedotteen [2], jossa todetaan seuraavasti:

> Suosittelemme niille yhteistyökumppaneille ja toimittajille, jotka eivät ole vielä siirtyneet Suite B:n mukaisiin elliptisten käyrien algoritmeihin, että tässä vaiheessa niihin ei tehdä huomattavia investointeja, vaan sen sijaan valmistaudutaan tulevaan siirtymiseen kvanttiresistantteihin algoritmeihin.

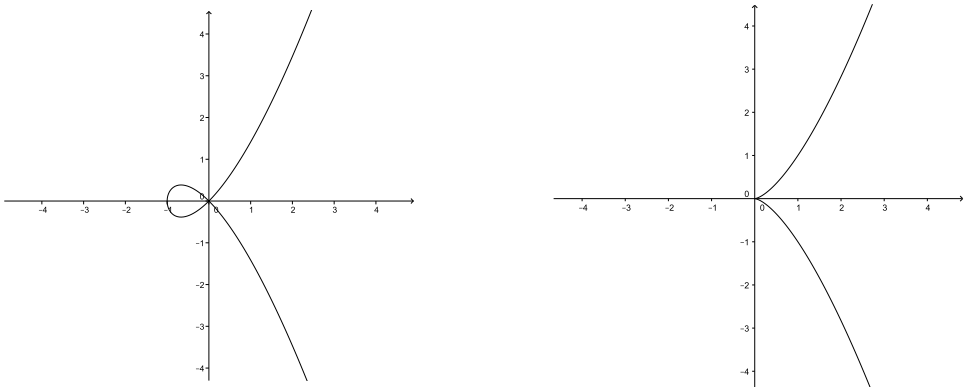
Tämä poikkeaa NSA:n aikaisemmasta kannasta, jossa suositeltiin elliptisten käyrien algoritmien käyttöä ensisijaisena suojausmenetelmänä. Elliptisten käyrien algoritmit on kuitenkin edelleen sisällytetty viimeisimpään versioon Suite B:stä, joka on lista NSA:n suosittelemia kryptografisia algoritmeja [2]. On tärkeää olla tietoinen tästä kehityssuunnasta, mutta toisaalta edelleen pätee että yleiselle elliptisten käyrien diskreetin logaritmin ongelmalle ei ole löydetty subeksponentiaalista ratkaisua. Tulevaisuudessa selviää, miten NSA:n kannannotto vaikuttaa elliptisten käyrien algoritmien käyttöasteeseen. Tässä tutkielmassa ei oteta kantaa NSA:n motiiveihin, mutta mahdollisia vaihtoehtoja on pohdittu laajasti Koblitzin ja Menezesin artikkelissa [10]. Kryptografian alalla elliptiset käyrät ovat siis ajankohtainen ja kiistanalainen aihe.

Kryptografia on mielenkiintoinen ala tietojenkäsittelytieteiden, matematiikan ja sähkötekniikan risteyskohdassa. Tämä tutkielma lähestyy elliptisten käyrien kryptografiaa matemaattisesta teoriasta lähtien. Elliptisten käyrien aritmetiikkaan ja ryhmälakiin perehdytään Luvussa 2. Erityisesti kryptografiaan soveltuviin äärellisissä kunnissa määriteltyihin elliptisiin käyriin keskitytään luvun jälkimmäisessä osassa. Luvussa 3 kryptografiaa tarkastellaan pääasiassa yleisellä tasolla keskittyen keskeisimpien teemojen idean ymmärtämiseen. Julkisen avaimen kryptografia on tässä luvussa keskiössä. Lopuksi

esitetään esimerkit elliptisten käyrien käytöstä algoritmeissa. Kryptografian perusteisiin ja termeihin perehdytään luvussa erityisesti elliptisten käyrien kryptografiasta käsin. Kryptografian aikaisemmasta hallinnasta on hyötyä, mutta se ei ole välttämätöntä tutkielman ymmärtämiseksi. Halutessaan lukija voi perehtyä kryptografiaan laajemmin teosten [5, 12, 15] avulla. Tutkielmassa ei perehdytä kryptografisten protokollien toteuttamiseen liittyviin haasteisiin.

2 Elliptisten käyrien aritmetiikka

Elliptiset käyrät ovat kuutiollisia tasokäyriä, jotka määritellään yleisen Weierstrassin yhtälön $y^2 + axy + by = x^3 + cx^2 + dx + e$ avulla. Elliptisten käyrien huomattavin ero muihin kuutiollisiin tasokäyriin on vaatimus käyrän epäsingulaarisuudesta. Graafisesti epäsingulaarinen käyrä ei leikkaa itseään ja siinä ei ole teräviä kulmia. Kuvassa 1 esitetään singulaaristen kuutiollisten tasokäyrien kaksi tyypillistä muotoa. Singulaarinen kuutiollinen tasokäyrä joko leikkaa itsensä (kuva 1a) tai sillä on terävä kärki (kuva 1b).

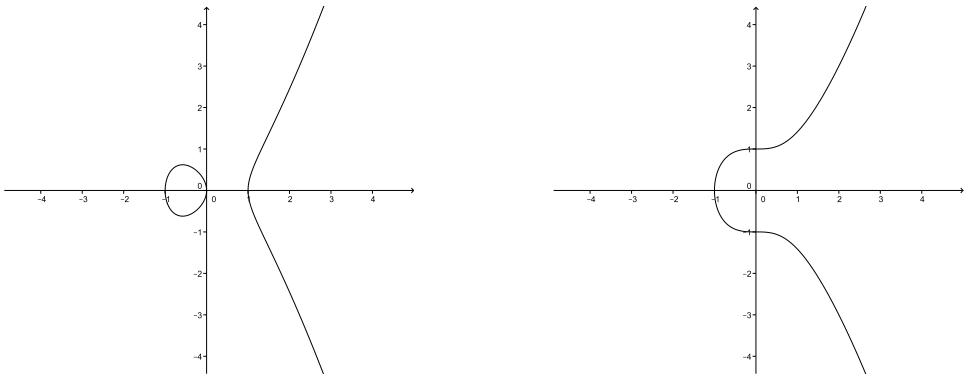


(a) $y^2 = x^3 + x^2$ (b) $y^2 = x^3$

Kuva 1: Singulaariset kuutiolliset tasokäyrät

Elliptiset käyrät voidaan määritellä erilaisissa kunnissa riippuen kulloisestakin käyttötarkoituksesta. Useimmissa kunnissa elliptisistä käyristä ei voida piirtää merkittäviä kuvaajia. Reaalilukujen joukossa $\mathbb{R}$ elliptinen käyrä on mielekästä esittää graafisesti käyränä. Näillä on kaksi tyypillistä muotoa (kuva 2). Ensimmäisessä tapauksessa elliptisellä käyrällä $y^2 = x^3 - x$ on kolme erillistä juurta (kuva 2a). Käyrällä $y^2 = x^3 + 1$ on vain yksi reaalinen juuri (kuva 2b). [17]

Kryptografian kannalta on tärkeää tarkastella erityisesti alkulukukunnissa $\mathbb{F}_p$ määriteltyjä elliptisiä käyriä. Toinen elliptisten käyrien kryptografiassa yleisesti käytetty kunta on binäärikunta $\mathbb{F}_{2^m}$. Näitä elliptisten käyrien kahta luokkaa käsitellään tarkemmin luvussa 2.3. Palautetaan ensin mieleen kunnan määritelmä [16, ss. 4-9] ja tarkastellaan sitten elliptisiä käyriä yleisesti



(a) $y^2 = x^3 - x$ (b) $y^2 = x^3 + 1$

Kuva 2: Elliptiset käyrät reaalilukujen joukossa $\mathbb{R}$

kunnissa. Kuntiin liittyviä muita ominaisuuksia esitellään tässä luvussa aina tarvittaessa.

Kunnat ovat abstraktioita tutuista lukujoukoista, kuten reaaliluvuista $\mathbb{R}$ ja rationaaliluvuista $\mathbb{Q}$, sekä niiden olennaisista ominaisuuksista. Kunta muodostuu joukosta $\mathbb{F}$ ja kahdesta laskutoimituksesta: yhteenlasku ja kertolasku [4]. On huomioitavaa, että näillä laskutoimituksilla ei välttämättä ole mitään tekemistä tavallisen lukujen yhteen- ja kertolaskun kanssa.

Määritelmä 2.0.1. *Kunta* on vaihdannainen rengas, jolla on yksikköalkio, ja jonka jokaisella nollasta poikkeavalla alkiolla on käänteisalkio.

Huomautus 2.0.2. Jos joukko $\mathbb{F}$ on kunta sekä lisäksi äärellinen, niin kunnan sanotaan olevan *äärellinen kunta*.

Kunnan K määritelmä 2.0.1 voidaan ilmaista myös seuraavasti: kunta K on additiivinen (aksioomat 1 – 4) ja multiplikatiivinen Abelin ryhmä (aksioomat 5 – 8) sekä sille pätevät osittelulait (aksiooma 9). Olkoon K kunta ja oletetaan, että $a, b, c \in K$. Määritelmän perusteella kunnassa K pätevät seuraavat aksioomat:

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. On olemassa yhteenlaskun neutraalialkio $0 \in K$ siten, että $a + 0 = a$.
4. Jokaisella alkiolla $a \in K$ on olemassa vasta-alkio $-a \in K$ siten, että $a + (-a) = 0$.

5. $ab = ba$.

6. $(ab)c = a(bc)$.

7. On olemassa kertolaskun yksikköalkio $1 \in K$ siten, että $a1 = a$.

8. Jokaisella alkiolla $a \neq 0 \in K$ on olemassa käänteisalkio $a^{-1} \in K$ siten, että $aa^{-1} = 1$.

9. $a(b + c) = ab + ac$ ja $(a + b)c = ac + bc$.

Esimerkki 2.0.3. Tarkastellaan joukkoa $\mathbb{Z}_n = \{0, 1, 2, ..., (n-1)\}$, missä $n \in \mathbb{N}$. Joukossa $\mathbb{Z}_n$ yhteenlasku ja kertolasku suoritetaan modulo n. Kertolaskun käänteisalkion olemassaoloa lukuunottamatta kunnan määritelmän ehdot täyttyvät joukossa $\mathbb{Z}_n$ kaikilla luvun $n \in \mathbb{N}$ arvoilla. Millä tahansa luonnollisella luvulla a joukossa $\mathbb{Z}_n$ on kertolaskun käänteisalkio, jos luku a on suhteellinen alkuluku luvun n kanssa. Toisinsanoen on oltava $\gcd(a, n) = 1$, kaikilla $a \in \mathbb{Z}_n \setminus \{0\}$ [16].

Luvun n on siis oltava alkuluku, jotta kaikilla $a \in \mathbb{Z}_n$ pätee $\gcd(a, n) = 1$. Joukko $\mathbb{Z}_n$ on kunta jos ja vain jos n on alkuluku. Tällaista kuntaa merkitään $\mathbb{F}_p$ ja sanotaan alkulukukunnaksi.

2.1 Weierstrassin yhtälö

Elliptiset käyrät määritellään yleisen Weierstrassin yhtälön avulla siten, että otetaan huomioon vaatimus käyrän epäsingulaarisuudesta. Lisäksi elliptiselle käyrälle lisätään äärettömyyspiste, jolloin käyrän pisteet muodostavat Abelin ryhmän, kun pisteiden välinen yhteenlasku määritellään sopivasti. Aiheeseen palataan tarkemmin luvussa 2.2.

Määritelmä 2.1.1. *Elliptinen käyrä E kunnassa K* määritellään yhtälöllä

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

missä $a_1, a_3, a_2, a_4, a_6 \in K$ ja $\Delta \neq 0$. Elliptinen käyrä sisältää myös äärettömyyspisteen $\mathcal{O}$. Käyrän E diskriminantti Δ määritellään kaavalla

$$\Delta = -d_2^2d_8 - 8d_4^3 - 27d_62 + 9d_2d_4d_6,$$

missä

$$\begin{cases} d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + a_1a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{cases} \tag{2.2}$$

Elliptistä käyrää kunnassa K merkitään $E(K)$ ja määritelmän mukaan sen muodostaa joukko

$$E(K) = \{(x, y) \in K \times K : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\mathcal{O}\}.$$

Määritelmän 2.1.1 vaatimuksella $\Delta \neq 0$ varmistetaan, että käyrä on epäsingulaarinen eli kuvainnollisesti sileä. Toisin sanoen elliptisellä käyrällä on sen jokaisessa pisteessä yksikäsitteisesti määritelty tangentti silloin, kun $\Delta \neq 0$ [4]. Epäsuorasti käyrän diskriminantti kertoo käyrän juurien luonnosta. Kun diskriminantti on nolla, ainakin kaksi käyrän juurista on yhteneviä. Kryptografian kannalta on oleellista, että tangentti on yksikäsitteisesti määritelty käyrän jokaisessa pisteessä ja ettei elliptisellä käyrällä ole moninkertaisia juuria.

Tarkastellaan tarkemmin kuvan 1 singulaarisia käyriä, joilla $\Delta = 0$. Ensimmäisessä tapauksessa (kuva 1a) käyrä leikkaa itsensä pisteessä $(0, 0)$, jossa on kaksi erillistä tangenttia sekä kaksinkertainen juuri. Toisessa tapauksessa (kuva 1b) käyrän terävään pisteeseen $(0, 0)$ ei ole mahdollista määrittää tangenttia.

Elliptiselle käyrälle voidaan tietyissä tapauksissa käyttää Weierstrassin yhtälön yksinkertaisempaa muotoa. Tämä riippuu käytettävästä kunnasta ja sen rakenteesta, jota kuvaa kunnan karakteristika. Esitetään seuraavaksi kunnan karakteristikan määritelmä. Kunnan karakteristikaa koskeva osuus mukailee Vinbergin [16] esitystä.

Määritelmä 2.1.2. Olkoon K kunta, jonka yhteenlaskun neutraalialkio on 0 ja kertolaskun neutraalialkio 1. *Kunnan K karakteristika*, $\text{char}(K)$, on pienin mahdollinen luonnollinen luku p, joka ilmaisee kuinka monta kertaa on lisättävä kertolaskun neutraalialkio itseensä, jotta saadaan yhteenlaskun neutraalialkio. Toisin sanoen

$$\text{char}(K) = p,$$

missä luvulle p pätee

$$\underbrace{(1 + 1 + \cdots + 1)}_{\text{p kpl}} = 0.$$

Jos kertolaskun neutraalialkion jatkuvalla yhteenlaskulla ei koskaan saavuteta yhteenlaskun neutraalialkiota, niin

$$\text{char}(K) = 0.$$

Huomautus 2.1.3. Karakteristikan määritelmän mukaan, jos $\text{char}(K) = p$, niin tällöin mille tahansa alkiolle $a \in K$,

$$\underbrace{a + a + \cdots + a}_{p \text{ kpl}} = \underbrace{(1 + 1 + \cdots + 1)}_{p \text{ kpl}} a = 0a = 0.$$

Jakaminen ja kertominen luvulla p kunnassa K tarkoittaa siis samaa kuin jakaminen ja kertominen luvulla 0. Sama pätee jakamiseen ja kertomiseen millä tahansa luvulla n, joka on jaollinen luvulla p.

Esimerkki 2.1.4. Reaalilukujen joukko on kunta. Reaalilukujen kunnassa yhteenlaskun neutraalialkio on 0 ja kertolaskun neutraalialkio on 1. Lisäämällä kertolaskun neutraalialkiota itseensä, ei reaalilukujen joukossa saada koskaan yhteenlaskun neutraalialkiota. Näin ollen reaalilukujen muodostaman kunnan karakteristika on määritelmän 2.1.2 mukaan $\text{char}(\mathbb{R}) = 0$.

Kunnan karakteristika ei voi saada mitä tahansa arvoja. Seuraava lause kuvaa tätä tulosta, joka seuraa suoraan kunnan karakteristikan määritelmästä 2.1.2.

Lause 2.1.5. *Kunnan K karakteristika $\text{char}(K)$ on joko 0 tai alkuluku p.*

Todistus. Tehdään vastaoletus, että $\text{char}(K) = n = kl$ $(1 < k, l < n)$ eli kunnan karakteristika on yhdistetty luku. Tällöin saadaan

$$\underbrace{1+1+\cdots+1}_{n \text{ kpl}} = (\underbrace{1+1+\cdots+1}_{k \text{ kpl}})(\underbrace{1+1+\cdots+1}_{l \text{ kpl}}) = 0$$

jolloin joko $\underbrace{1+1+\cdots+1}_{k \text{ kpl}} = 0$ tai $\underbrace{1+1+\cdots+1}_{l \text{ kpl}} = 0$, mikä on ristiriidassa karakteristikan määritelmän kanssa. □

Esimerkissä 2.0.3 todettiin, että kokonaislukujen joukko $\mathbb{Z}_p$ on äärellinen kunta, jos p on alkuluku. On kuitenkin olemassa esimerkkejä äärellisistä kunnista jotka eivät ole tätä muotoa. Seuraavassa esitetään kuinka monta alkiota äärelliset kunnat voivat sisältää. Lause on esitetty teoksessa [12] ja sen todistukseen voi tutustua teoksessa [5].

Lause 2.1.6. *Kunta K, jossa on q alkiota on olemassa vain, jos q on alkuluvun potenssi eli $q = p^m$, jossa p on alkuluku ja $m \geq 1$ on kokonaisluku. Kunnan K karakteristika $\text{char}(K) = p$.*

Esimerkki 2.1.7. Äärellisiä kuntia $\mathbb{F}_{2^m}$ sanotaan binäärikunniksi ja ne sisältävät 2^m alkiota. Lauseen 2.1.6 mukaan binäärikunnan karakteristika on $\text{char}(\mathbb{F}_{2^m}) = 2$. Nyt mille tahansa alkiolle $a \in \mathbb{F}_{2^m}$ pätee $a + a = 0$. On huomioitavaa että jos $m > 1$, kokonaisluvut modulo 2^m eivät muodosta kuntaa. Binäärikunnat on konstruoitava toisella tavalla. Binäärikuntiin ja niiden konstruointiin palataan tarkemmin luvussa 2.3.5.

Kun tunnetaan kunnan karakteristika, jossa elliptinen käyrä on määritelty, voidaan yhtälöä (2.1) sieventää ottaen huomioon diskriminantin säilyminen erisuurena kuin 0. Seuraavaksi tarkastellaan, millainen muuttujien vaihto sallitaan, jotta uusi yhtälön muoto vastaa aikaisempaa yhtälöä. Sen jälkeen esitetään, miten elliptisen käyrän yhtälö sievenee kunnan karakteristikan eri arvoilla. Tutkittavana ovat tapaukset: $\text{char}(K) \neq 2, 3$, $\text{char}(K) = 2$ ja $\text{char}(K) = 3$. Seuraava osuus yhdistelee Hankerson et al. [4], Knappin [7] ja Silvermanin [14] esityksiä.

Määritelmä 2.1.8. Olkoot E_1 ja E_2 kaksi elliptistä käyrää, jotka on määritelty kunnassa K ja joiden yhtälöt ovat:

$$\begin{aligned} E_1 : &\quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \\ E_2 : &\quad y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6. \end{aligned}$$

Elliptisten käyrien E_1 ja E_2 sanotaan olevan isomorfisia kunnassa K, jos on olemassa luvut $u, r, s, t \in K, u \neq 0$ siten, että muuttujanvaihto

$$(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t) \tag{2.3}$$

muuntaa yhtälön E_1 yhtälöksi E_2. Muunnosta (2.3) sanotaan *sallituksi muutujanvaihdoksi.*

2.1.1 Karakteristika char$(K) \neq 2, 3$

Elliptisten käyrien kryptografiassa käytetään äärellisiä kuntia $\mathbb{F}_p$, joissa p on suuri alkuluku. Tällaisen kunnan karakteristika, $\text{char}(\mathbb{F}_p) = p$, on kryptografiassa varmasti suurempi kuin 3. Seuraava osuus koskee oleellisesti myös käytännön sovellutuksissa käytettäviä elliptisiä käyriä. Kun kunnan K karakteristika $\text{char}(K) \neq 2, 3$, niin elliptisen käyrän yhtälö voidaan kirjoittaa yksinkertaisempaan muotoon.

Kun kunnan karakteristika ei ole 2, niin voimme jakaa kahdella, jolloin Weierstrassin yhtälön (2.1) vasen puoli $y^2 + a_1xy + a_3y$ voidaan täydentää neliöksi seuraavasti:

$$y^2 + y(a_1x + a_3) + \frac{(a_1x + a_3)^2}{4} = \left(y + \frac{a_1x + a_3}{2}\right)^2.$$

Lisätään neliöön täydentämisessä muodostuvat ylimääräiset termit myös Weierstrassin yhtälön oikealle puolelle ja korvataan y lausekkeella $\frac{1}{2}y - \frac{a_1x+a_3}{2}$:

$$\begin{aligned} \left(y + \frac{a_1x + a_3}{2}\right)^2 &= x^3 + a_2x^2 + a_4x + a_6 + \frac{(a_1x + a_3)^2}{4} \\ \left(\frac{1}{2}y\right)^2 &= x^3 + a_2x^2 + a_4x + a_6 + \frac{1}{4}a_1^2x^2 + \frac{1}{2}a_1a_3x + \frac{1}{4}a_3^2 \\ \frac{1}{4}y^2 &= x^3 + \left(\frac{1}{4}a_1^2 + a_2\right)x^2 + \left(\frac{1}{2}a_1a_3 + a_4\right)x + \left(\frac{1}{4}a_3^2 + a_6\right). \end{aligned}$$

Kerrotaan yhtälö molemmin puolin luvulla 4, jolloin saadaan

$$y^2 = 4x^3 + (a_1^2 + 4a_2)x^2 + (2a_1a_3 + 4a_4)x + (a_3^2 + 4a_6).$$

Tällöin elliptisen käyrän yhtälö voidaan kirjoittaa yksinkertaisemmin muotoon

$$y^2 = 4x^3 + d_2x^2 + 2d_4x + d_6,$$

jossa d_2, d_4 ja d_6 vastaavat yhtälöryhmän (2.2) muuttujia. Saatua yhtälöä on mahdollista sieventää vielä edelleen, jos kunnan K karakteristika $\mathrm{char}(K) \neq 3$, sillä tällöin on mahdollista jakaa luvulla 3. Elliptisen käyrän yhtälön oikea puoli voidaan nyt täydentää kuutioon siten, että x^2 termi supistuu pois:

$$\begin{aligned}
4x^3 + d_2x^2 + 2d_4x + d_6 &= 4\Big(x^3 + \frac{d_2}{4}x^2\Big) + 2d_4x + d_6 \\
&= 4\Big(x + \frac{d_2}{12}\Big)^3 - \frac{d_2^2}{12}x - 4\frac{d_2^3}{12^3} + 2d_4x + d_6 \\
&= 4\Big(x + \frac{d_2}{12}\Big)^3 + \Big(-\frac{d_2^2}{12} + 2d_4\Big)x - \frac{4d_2^3}{12^3} + d_6 \\
&= 4\Big(x + \frac{d_2}{12}\Big)^3 + \Big(-\frac{d_2^2}{12} + 2d_4\Big)\Big(x + \frac{d_2}{12}\Big) + \frac{d_2^3}{12^2} \\
&\quad -\frac{d_2d_4}{6} - \frac{4d_2^3}{12^3} + d_6 \\
&= 4\Big(x + \frac{d_2}{12}\Big)^3 + \Big(-\frac{d_2^2}{12} + 2d_4\Big)\Big(x + \frac{d_2}{12}\Big) + \frac{8d_2^3}{12^3} \\
&\quad -\frac{d_2d_4}{6} + d_6.
\end{aligned}$$

Korvaamalla muuttuja x lausekkeella $x - d_2/12$ saadaan

$$y^2 = 4x^3 + \Big(-\frac{d_2^2}{12} + 2d_4\Big)x + \frac{8d_2^3}{12^3} - \frac{d_2d_4}{6} + d_6.$$

Yhtälöä voidaan muokata edellen niin, että termin x^3 edessä oleva kerroin supistuu pois. Tämä ei ole mahdollista tekemällä muuttujanvaihtoa vain muuttujalle x, eli on löydettävä sopivat muutokset samanaikaisesti muuttujille x ja y. Sopiva muuttujienvaihto on $(x, y) \mapsto (\frac{x}{36}, \frac{y}{108})$. Edelleen merkitsemällä $a = -27d_2^2 + 648d_4$ ja $b = 54d_2^3 - 1944d_2d_4 + 11664d_6$ saadaan Weierstrassin yhtälö yksinkertaiseen muotoon

$$y^2 = x^3 + ax + b, \tag{2.4}$$

missä $a, b \in K$. Tällöin käyrän diskriminantti on

$$\Delta = -16(4a^3 + 27b^2) \neq 0.$$

Yhdistetään edellä tehdyt muuttujanvaihdot. Weierstrassin yhtälö (2.1) sievenee muotoon $y^2 = x^3 + ax + b$ muuttujienvaihdolla

$$(x, y) \mapsto \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1 x}{216} + \frac{a_1^3 - 4a_1 a_2 - 12a_3}{24} \right), \tag{2.5}$$

kun $\text{char}(K) \neq 2, 3$.

Huomautus 2.1.9. Kaikki reaalilukujen joukossa ja äärellisissä kunnissa $\mathbb{F}_p$, jossa $p > 3$, määritellyt elliptiset käyrät voidaan kirjoittaa tässä yksinkertaisimmassa muodossa.

Huomautus 2.1.10. Muodossa (2.4) oleva elliptinen käyrä voidaan kirjoittaa muotoon

$$y = \pm\sqrt{x^3 + ax + b},$$

joten tällainen käyrä on symmetrinen x-akselin suhteen.

2.1.2 Karakteristika char$(K) = 2$

Sovelluksissa käytetään elliptisiä käyriä, jotka on määritelty äärellisissä kunnissa $\mathbb{F}_{2^m}$, joiden karakteristika $\text{char}(\mathbb{F}_{2^m}) = 2$. Binäärikunnissa määritellyt elliptiset käyrät ovat erityisen käyttökelpoisia laitteistosovelluksissa, jolloin tarvitaan hyvin vähän loogisia portteja tehokkaan ja nopean kryptosysteemin luomiseksi.

Muotoa (2.4) olevat elliptiset käyrät ovat aina singulaarisia, kun kunnan karakteristika on 2. Tämän takia on käytettävä elliptisen käyrän yleisempää muotoa. Kun kunnan karakteristika on 2, on olemassa kaksi mahdollista sallittua muuttujanvaihtoa. Molemmat näistä esitetään seuraavassa.

Jos kunnan K karakteristika $\text{char}(K) = 2$ ja $a_1 \neq 0$, niin sallittu muuttujanvaihto

$$(x, y) \mapsto \left(a_1^2 x + \frac{a_3}{a_1}, a_1^3 y + a_1 x + \frac{a_1^2 a_4 + a_3^2}{a_1^3} \right)$$

muuntaa käyrän E käyräksi

$$y^2 + xy = x^3 + ax^2 + b,$$

missä $a, b \in K$ ja $\Delta = a$.

Koska edellä vaaditaan että $a_1 \neq 0$, tarvitsee käsitellä erikseen tapaus jossa $a_1 = 0$. Kun $a_1 = 0$, niin sallitulla muuttujanvaihdolla

$$(x, y) \mapsto (x + a_2, y)$$

saadaan käyrästä E käyrä

$$y^2 + cy = x^3 + ax + b, \tag{2.6}$$

missä $a, b \in K$ ja $\Delta = c^4$.Tällaista käyrää sanotaan supersingulaariseksi.

Muotoa (2.6) olevilla käyrillä on se etu, että laskutoimitukset saadaan suoritettua nopeasti. Supersingulaariset käyrät ovat kuitenkin elliptisten käyrien erityistapaus ja niiden ominaisuudet tekevät niistä käyttökelvottomia kryptografiaan, koska ne ovat alttiita MOV-hyökkäykselle. MOV-algoritmiin voi perehtyä tarkemmin Blake et al. teoksessa [1, ss.82-88].

Huomautus 2.1.11. Supersingulaarisuutta ei pidä sekoittaa elliptisen käyrän singulaarisuuteen. Itseasiassa kaikki supersingulaariset elliptiset käyrät ovat epäsingulaarisia.

2.1.3 Karakteristika $\mathbf{char}(K) = 3$

Edellä esitetyt muuttujanvaihdot eivät ole mahdollisia, kun elliptinen käyrä on määritelty kunnassa K, jolle $\mathrm{char}(K) = 3$. Kryptografian kannalta tämän ryhmän elliptiset käyrät eivät ole keskeisimpiä, mutta niiden käsittely on tarpeen elliptisten käyrien teorian kokonaiskuvan hahmottamiseksi.

Kun kunnan K karakteristika $\mathrm{char}(K) = 3$, on kaksi käsiteltävää tapausta. Jos $a_1^2 \neq -a_2$, niin sallitulla muuttujan vaihdolla

$$(x, y) \mapsto \left(x + \frac{a_4 - a_1 a_3}{a_1^2 + a_2}, y + a_1 x + a_1 \frac{a_4 - a_1 a_3}{a_1^2 + a_2} + a_3 \right)$$

elliptinen käyrä sievenee muotoon

$$y^2 = x^3 + ax^2 + b,$$

missä $a, b \in K$. Tällainen käyrä on epäsupersingulaarinen ja sen diskriminantille pätee $\Delta = -a^3 b$.

Jos $a_1^2 = -a_2$, niin tällöin sallittu muuttujan vaihto

$$(x, y) \mapsto (x, y + a_1 x + a_3)$$

sieventää elliptisen käyrän yhtälön muotoon

$$y^2 = x^3 + ax + b,$$

missä $a, b \in K$. Tämä käyrä on supersingulaarinen ja sen diskriminantille pätee $\Delta = -a^3$.

2.2 Elliptisten käyrien ryhmälaki

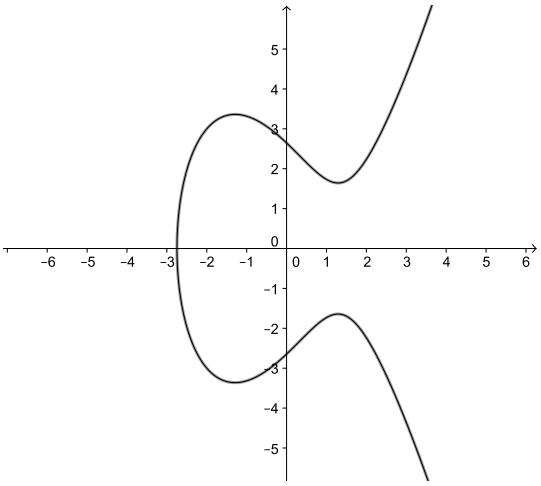
Elliptisillä käyrillä on poikkeuksellinen ominaisuus, jonka avulla käyrän kahden pisteen avulla voidaan saada selville kolmas käyrällä oleva piste. Tämän ominaisuuden ansiosta käyrän pisteille voidaan muodostaa yhteenlaskuoperaatio, joka voi vaikuttaa ensisilmäyksellä mielivaltaiselta. Kuitenkin tämä yhteenlaskuoperaatio muodostaa ryhmän yhdessä elliptisen käyrän pisteiden kanssa.

Olkoon elliptinen käyrä E määritelty kunnassa K. Käyrän $E(K)$ kaksi pistettä voidaan laskea yhteen siten, että saadaan kolmas piste käyrällä $E(K)$ jänne ja tangentti -säännön avulla. Tämä yhteenlaskuoperaatio ja käyrän $E(K)$ pisteet, sisältäen äärettömyyspisteen $\mathcal{O}$, joka toimii neutraalialkiona, muodostavat Abelin ryhmän. Tätä ryhmää käytetään elliptisten käyrien kryptografisten systeemien rakentamisessa [4].

Seuraavaksi esitetään yhteenlasku elliptisillä käyrillä, jotka ovat muotoa $y^2 = x^3 + ax + b$, jänne ja tangentti -säännön mukaisesti. Ryhmälait johdetaan algebrallisesti, geometrista esitystapaa hyödyntäen. Tämä luku etenee yhdistäen ja selkiyttäen teoksien [1, 17] esityksiä ryhmälakien muodostamisesta.

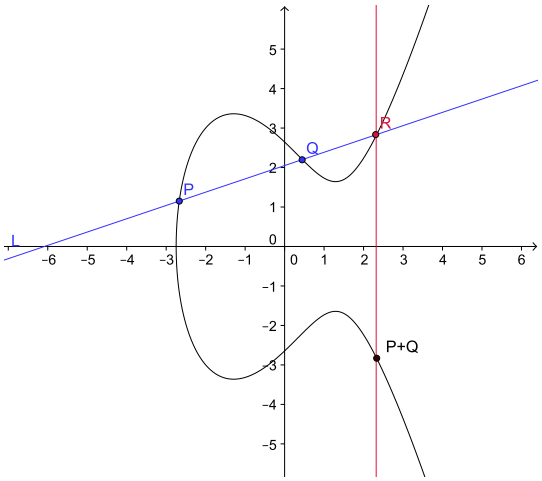
Pisteiden yhteenlasku elliptisellä käyrällä

Käytetään graafisena esimerkkinä elliptistä käyrää $E : y^2 = x^3 - 5x + 7$ (kuva 3).



Kuva 3: Elliptinen käyrä $y^2 = x^3 - 5x + 7$

Aloitetaan valitsemalla kaksi pistettä $P = (x_1, y_1)$ ja $Q = (x_2, y_2)$ käyrältä E siten, että $P \neq Q$ ja $x_1 \neq x_2$. Piirretään suora L pisteiden P ja Q kautta. Suora L leikkaa käyrän E kolmannessa pisteessä, jota kutsutaan pisteeksi R. Piirretään y-akselin suuntainen suora, joka kulkee pisteen R kautta. Piste, jossa tämä suora leikkaa elliptisen käyrän E, on piste $-R$ ja se määritellään pisteiden P ja Q summana elliptisellä käyrällä E (kuva 4).



Kuva 4: Pisteiden yhteenlasku elliptisellä käyrällä $y^2 = x^3 - 5x + 7$

Johdetaan yhtälöt pisteiden summan $P + Q$ laskemiselle elliptisellä käyrällä E, joka on muotoa

$$y^2 = x^3 + ax + b. \tag{2.7}$$

Pisteitä P ja Q yhdistävä suora L on muotoa

$$y = \lambda x + \mu. \tag{2.8}$$

Jos $P \neq Q$ ja $x_1 \neq x_2$, niin suoran kulmakerroin on

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

ja suoran y-akselin leikkauspiste saadaan kaavasta

$$\mu = y_1 - \lambda x_1. \tag{2.9}$$

Pisteen R koordinaatit saadaan selvittämällä elliptisen käyrän (2.7) ja suoran (2.8) kolmas leikkauspiste. Sijoitetaan yhtälö (2.8) elliptisen käyrän yhtälöön, jolloin saadaan

$$(\lambda x + \mu)^2 = x^3 + ax + b$$

ja edelleen

$$x^3 + ax + b - (\lambda x + \mu)^2 = 0. \tag{2.10}$$

Tiedetään, että pisteet P ja Q ovat kaksi muuta leikkauspistettä, joten niiden x-koordinaatit x_1 ja x_2 ovat ratkaisuja. Koska suora L leikkaa elliptisen käyrän kolmessa pisteessä, niin saadaan

$$(x - x_1)(x - x_2)(x - x_3) = 0. \tag{2.11}$$

Kolmas ratkaisu x_3 saadaan selville vertaamalla yhtälöitä (2.10) ja (2.11) seuraavasti:

$$\begin{aligned} x^3 + ax + b - (\lambda x + \mu)^2 &= (x - x_1)(x - x_2)(x - x_3) \\ x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2) &= x^3 - (x_1 + x_2 + x_3)x^2 \\ &\quad +(x_1x_2 + x_1x_3 + x_2x_3)x \\ &\quad -x_1x_2x_3. \end{aligned}$$

Termin x^2 kertoimista saadaan laskettua

$$\lambda^2 = x_1 + x_2 + x_3$$

ja edelleen pisteen R x-koordinaatiksi

$$x_3 = \lambda^2 - x_1 - x_2.$$

Piste $R = (x_3, y_3)$ on suoralla L, joten sen y-koordinaatti saadaan suoran L yhtälön (2.8) avulla ja korvaamalla μ yhtälöllä (2.9):

$$\begin{aligned} y_3 &= \lambda x_3 + \mu \\ &= \lambda x_3 + y_1 - \lambda x_1 \\ &= \lambda(x_3 - x_1) + y_1. \end{aligned}$$

Pisteen R koordinaatit ovat (x_3, y_3), joten pisteiden P ja Q yhteenlaskulla saadun pisteen $P + Q = -R$ koordinaatit ovat nyt $(x_3, -y_3)$, joille saadaan edellä johdetun perusteella:

$$\begin{aligned} x_{P+Q} &= \lambda^2 - x_1 - x_2, \\ y_{P+Q} &= \lambda(x_1 - x_3) - y_1, \end{aligned}$$

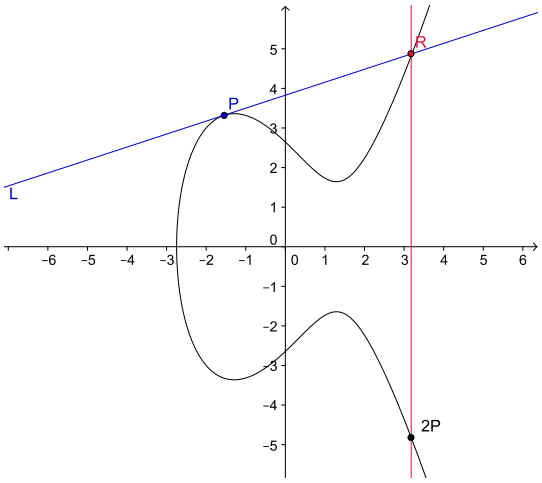
missä

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

Pisteen lisääminen itseensä elliptisellä käyrällä

Edellä lisäsimme kaksi erillistä pistettä elliptisellä käyrällä. Jos ajattelemme, että piste Q lähestyy pistettä P, niin pisteiden välisestä suorasta L tulee tangentti pisteessä P. Tämä tarkoittaa, että suoritamme yhteenlaskun $P+P$. Tarkastellaan tilannetta ensin geometrisesti.

Pisteeseen P piirretty tangentti leikkaa elliptisen käyrän E toisessa pisteessä R. Piirretään jälleen y-akselin suuntainen suora pisteen R kautta, jolloin saamme x-akselin suhteen peilatun pisteen $-R$. Tämä piste määritellään summana $P + P = 2P$ (kuva 5).



Kuva 5: Pisteen lisääminen itseensä elliptisellä käyrällä $y^2 = x^3 - 5x + 7$

Huomautus 2.2.1. Merkitään yhden pisteen toistuvaa yhteenlaskua itseensä

$$kP = \underbrace{P + P + ... + P}_{\text{k kpl}},$$

missä P esiintyy yhtälön oikean puolen yhteenlaskussa k kertaa. Voimme siis merkitä esimerkiksi yhteenlaskua $P + P = 2P$ ja $P + P + P + P + P = 5P$.

Johdetaan seuraavaksi pisteen $2P$ koordinaatit, vastaavasti kuin kahden erillisen pisteen tapauksessa. Tarkastellaan edelleen elliptistä käyrää, joka on muotoa (2.7). Edelleen pisteeseen P piirretyn tangentin yhtälö on muotoa (2.8). Nyt kun $P = Q$, niin suoran kulmakerroin λ saadaan osittaisderivoimalla elliptisen käyrän yhtälö, jolloin

$$\lambda = \frac{3x_1^2 + a}{2y_1}.$$

Yhteenlasketun pisteen koordinaattien laskeminen tehdään samoin kuin kahden pisteen tapauksessa, mutta yhteenlaskettavien pisteiden koordinaatit ovat samat. Pisteen $2P$ koordinaateiksi saadaan siis

$$\begin{aligned} x_{2P} &= \lambda^2 - 2x_1, \\ y_{2P} &= \lambda(x_1 - x_3) - y_1, \end{aligned}$$

missä

$$\lambda = \frac{3x_1^2 + a}{2y_1}.$$

Äärettömyyspiste

Valitaan piste P elliptiseltä käyrältä E. Kun piste P peilataan x-akselin suhteen, saadaan piste $-P$. Selvittäessämme näiden pisteiden summaa, saamme y-akselin suuntaisen suoran, joka ei leikkaa käyrää E kolmannessa pisteessä. Tarvitsemme käyrälle ylimääräisen pisteen, "äärettömyyspisteen", joka sijaitsee jokaisella y-akselin suuntaisella suoralla. Määrittelemme näin ollen

$$P + -P = \mathcal{O}.$$

Äärettömyyspiste $\mathcal{O}$ on siis elliptisen käyrän pisteiden yhteenlaskun neutraalialkio. Lisäksi pätee myös

$$P + \mathcal{O} = P.$$

Edellä määritelty pisteiden yhteenlasku muodostaa Abelin ryhmän elliptisen käyrän pisteiden kanssa. Yhteenlaskulle johdetut yhtälöt kokonaisuudessaan muodostavat elliptisten käyrien ryhmälain. Elliptisen käyrän pisteille ja pisteiden yhteenlaskulle pätevät seuraavat ominaisuudet, jotka on esitetty lähteen [5] mukaan.

Lause 2.2.2. *Olkoon E elliptinen käyrä. Käyrän E ryhmälaki toteuttaa seuraavat ominaisuudet*

1. $P + \mathcal{O} = \mathcal{O} + P = P$, *kaikilla* $P \in E$ *(neutraalialkio)*
2. $P + (-P) = \mathcal{O}$, *kaikilla* $P \in E$ *(vasta-alkio)*
3. $P + Q = Q + P$, *kaikilla* $P, Q \in E$ *(vaihdannaisuus)*
4. $(P + Q) + R = P + (Q + R)$, *kaikilla* $P, Q, R \in E$ *(liitännäisyys)*

Toisin sanoen käyrän E pisteet, yhdessä neutraalialkion $\mathcal{O}$ kanssa, mudostavat Abelin ryhmän.

Todistus. Vaihdannaisuus pitää paikkansa, sillä pisteiden P ja Q kautta kulkeva suora on itsestäänselvästi sama kuin pisteiden Q ja P kautta kulkeva suora. Pisteiden yhteenlaskun järjestyksellä ei ole siis merkitystä. Neutraalialkio ja vasta-alkio pitävät paikkansa äärettömyyspisteen $\mathcal{O}$ määrittelyyn perustuen.

Lauseen viimeinen kohta liitännäisyys on hankalampi todistaa. Käyttämällä edellä johdettuja yhteenlaskun yhtälöitä, liitännäisyys on mahdollista todistaa työläiden laskutoimituksien avulla. Hienostuneempien todistuksien laajoihin kuvauksiin voi perehtyä elliptisiä käyriä käsittelevissä teoksissa [7, 14, 17]. □

2.3 Elliptiset käyrät äärellisissä kunnissa

Elliptisten käyrien kryptografiaa ajatellen olemme kiinnostuneita rajoitetusta joukosta elliptisiä käyriä, jotka on määritelty äärellisissä kunnissa. Edellä esitetty elliptisten käyrien aritmetiikka on määritelty reaalilukujen joukossa. Reaaliluvuilla suoritetut laskutoimitukset ovat kuitenkin alttiita pyöristysvirheille; kryptografia vaatii virheetöntä aritmetiikkaa. Toisekseen vaaditaan äärellinen Abelin ryhmä, jotta elliptisille käyrille voidaan määritellä kryptografian kannalta järkevä diskreetin logaritmin ongelma (luku 3.2.1). Näin ollen on mielekästä ja tarpeellista käyttää äärellisissä kunnissa määriteltyjä elliptisiä käyriä.

Käsitellään ensin elliptisiä käyriä äärellisissä kunnissa $\mathbb{F}_p$ ja esitetään edellisen luvun perusteella ryhmälait näille käyrille. Luvun toisessa osassa tarkastellaan elliptisiä käyriä, jotka on määritelty binäärikunnissa $\mathbb{F}_{2^m}$ ja esitetään ryhmälait vastaavasti myös näille käyrille.

2.3.1 Elliptiset käyrät äärellisessä kunnassa $\mathbb{F}_p$

Määritelmä 2.3.1. Olkoon $\mathbb{F}_p$ äärellinen kunta, jossa $p > 3$ on alkuluku. Elliptinen käyrä $E : y^2 = x^3 + ax + b$ kunnassa $\mathbb{F}_p$ on kaikkien lukuparien $(x, y) \in \mathbb{F}_p$ joukko, joka toteuttaa kongruenssin

$$y^2 \equiv x^3 + ax + b \mod p, \tag{2.12}$$

jossa $a, b \in \mathbb{F}_p$. Elliptinen käyrä sisältää myös äärettömyyspisteen $\mathcal{O}$. Käyrän diskriminantti on

$$\Delta = -16(4a^3 + 27b^2) \neq 0 \mod p.$$

Äärellisissä kunnissa määritellyt elliptiset käyrät eivät ole graafisesti käyriä, vaan joukko koordinaatteja (x, y). Elliptisen käyrän kunnassa $\mathbb{F}_p$ muodostaa siis joukko

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 \equiv x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

Esimerkki 2.3.2. Tarkastellaan elliptistä käyrää

$$E(\mathbb{F}_{11}) : y^2 = x^3 + x + 6.$$

Huomataan, että $\Delta = -16(4a^3 + 2b^2) = -16(4 + 72) \equiv 5 \neq 0 \mod 11$, joten E on tosiaankin elliptinen käyrä. Kaikki käyrän E pisteet saadaan selville laskemalla yhtälön oikea puoli $x^3 + x + 6 \mod 11$ kaikilla $x \in 0, 1, ...10$ ja tarkastamalla, löytyykö lukua $y \in 0, 1, ..., 10$, jolla $y^2 \mod 11$ saa vastaavan arvon. Lasketaan arvot y^2 ja $x^3 + x + 6$ siten että $x, y \in 0, 1, ..., 10$. Otetaan esimerkiksi kongruenssin $x^3 + x + 6 \mod 11$ laskeminen arvolla $x = 7$. Muut arvot lasketaan vastaavasti.

$$\begin{aligned} 7^3 + 7 + 6 &= 7^2 \cdot 7 + 13 \\ &\equiv 49 \cdot 7 + 2 \mod 11 \\ &\equiv 5 \cdot 7 + 2 \mod 11 \\ &\equiv 35 + 2 \mod 11 \\ &\equiv 4 \mod 11 \end{aligned}$$

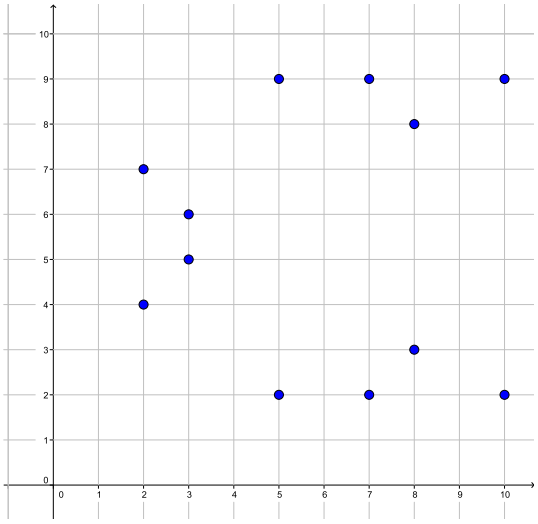
x	$x^3 + x + 6 \mod 11$
0	6
1	8
2	5
3	3
4	8
5	4
6	8
7	4
8	9
9	7
10	4

y	$y^2 \mod 11$
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

Seuraavaksi verrataan yllä esitettyjen taulukkojen arvoja keskenään. Muuttujan x arvoilla $0, 1, 4, 6$ ja 9 saatuja arvoja ei vastaa mikään muuttujan y arvoilla laskettu tulos. Sen sijaan muuttujan arvolla $x = 2$ saadaan 5, joka

vastaa muuttujan y arvoilla 4 ja 7 saatuja tuloksia. Pisteet $(2, 4)$ ja $(2, 7)$ kuuluvat siis elliptiselle käyrälle E. Vastaavasti analysoimalla saadaan kaikki käyrän pisteet äärettömyyspisteen $\mathcal{O}$ lisäksi (kuva 6). Elliptisen käyrän $E(\mathbb{F}_{11}) : y^2 = x^3 + x + 6$ pisteet ovat:

$$\begin{array}{rll} \mathcal{O} & (5, 2) & (8, 8) \\ (2, 4) & (5, 9) & (10, 2) \\ (2, 7) & (7, 2) & (10, 9). \\ (3, 5) & (7, 9) & \\ (3, 6) & (8, 3) & \end{array}$$



Kuva 6: Elliptinen käyrä $E(\mathbb{F}_{11}) : y^2 = x^3 + x + 6$

Edellisessä luvussa johdettiin ryhmälait reaaliluvuille, mutta saadut yhtälöt pätevät kaikissa kunnissa joissa $\text{char}(K) \neq 2, 3$. Seuraavassa on esitetty ryhmälait kootusti.

Ryhmälaki elliptiselle käyrälle $E(K) : y^2 = x^3 + ax + b, \mathbf{char}(K) \neq 2, 3$

1. *Neutraalialkio*: $P + \mathcal{O} = \mathcal{O} + P = P$, kaikilla $P \in E(K)$.
2. *Vasta-alkio*: Jos $P = (x, y) \in E(K)$, niin $(x, y) + (x, -y) = \mathcal{O}$. Pistettä $(x, -y)$ merkitään $-P$ ja sanotaan pisteen P vasta-alkioksi. Huomaa, että $-P$ on piste käyrällä $E(K)$. Lisäksi $-\mathcal{O} = \mathcal{O}$.
3. *Pisteiden yhteenlasku*: Olkoon $P = (x_1, y_1) \in E(K)$ ja $Q = (x_2, y_2) \in E(K)$, missä $P \neq \pm Q$. Tällöin $P + Q = (x_3, y_3)$, jossa
$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1, \end{aligned}$$
missä
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$
4. *Pisteen tuplaaminen*: Olkoon $P = (x_1, y_1) \in E(K)$, missä $P \neq -P$. Tällöin $2P = (x_3, y_3)$, jossa
$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \\ y_3 &= \lambda(x_1 - x_3) - y_1, \end{aligned}$$
missä
$$\lambda = \frac{3x_1^2 + a}{2y_1}.$$

Esimerkki 2.3.3. Käytetään edellisen esimerkin käyrää $E(\mathbb{F}_{11}) : y^2 = x^3 + x + 6$. Lasketaan yhteen tämän käyrän pisteet $(8, 8)$ ja $(3, 6)$. Aloitetaan laskemalla λ:
$$\begin{aligned} \lambda = \frac{y_2 - y_1}{x_2 - x_1} &= \frac{6 - 8}{3 - 8} \equiv \frac{9}{6} \mod 11 \\ &\equiv 9 \cdot 2 \mod 11 \\ &= 18 \equiv 7 \mod 11. \end{aligned}$$

Lasketaan yhteenlaskun tuloksena saadun pisteen koordinaatit:

$$\begin{aligned} x_3 = \lambda^2 - x_1 - x_2 &= 7^2 - 8 - 3 = 38 \\ &\equiv 5 \mod 11 \end{aligned}$$

$$\begin{aligned} y_3 = \lambda(x_1 - x_3) - y_1 &= 7(8-5) - 8 \\ &= 7 \cdot 3 - 8 = 13 \\ &\equiv 2 \mod 11. \end{aligned}$$

Saadaan $(8,8) + (3,6) = (5,2)$, joka on myös elliptisen käyrän $E(\mathbb{F}_{11}) : y^2 = x^3 + x + 6$ piste.

Esimerkki 2.3.4. Tarkastellaan edelleen käyrää $y^2 = x^3 + x + 6$ kunnassa $\mathbb{F}_{11}$. Lasketaan $2(8,8)$. Laskut etenevät kuten edellä, mutta käytetään pisteen tuplaamisen tapauksessa määriteltyä muuttujaa λ:

$$\begin{aligned} \lambda = \frac{3x_1^2 + a}{2y_1} &= \frac{3(8)^2 + 1}{2 \cdot 8} \equiv \frac{6}{5} \mod 11 \\ &\equiv 6 \cdot 9 \mod 11 \\ &= 54 \equiv 10 \mod 11. \end{aligned}$$

Lasketaan pisteen $2P$ koordinaatit:

$$\begin{aligned} x_3 = \lambda^2 - 2x_1 &= 10^2 - 2 \cdot 8 = 84 \\ &\equiv 7 \mod 11 \end{aligned}$$

$$\begin{aligned} y_3 = \lambda(x_1 - x_3) - y_1 &= 10(8-7) - 8 \\ &\equiv 2 \mod 11. \end{aligned}$$

Ratkaisuksi saadaan $2(8,8) = (7,2)$.

2.3.2 Elliptiset käyrät kunnassa $\mathbb{F}_{2^m}$

Tietokoneiden toiminta perustuu binäärilukuihin, joten on tehokasta käyttää elliptisiä käyriä modulo 2. Valitettavasti, jos E on elliptinen käyrä, joka on määritelty kunnassa $\mathbb{F}_2$, niin $E(\mathbb{F}_2)$ sisältää korkeintaan 5 pistettä, mikä ei olisi käytännöllistä kryptografisiin tarkoituksiin. On kuitenkin olemassa muita äärellisiä kuntia, joissa $2 = 0$. Nämä kunnat ovat binäärikuntia $\mathbb{F}_{2^m}$, jotka sisältävät 2^m alkiota (esimerkki 2.1.7). Voimme siis käyttää elliptistä käyrää, jonka Weierstrassin yhtälön kertoimet ovat kunnassa $\mathbb{F}_{2^m}$, ja tarkastella käyrän pisteiden muodostamaa ryhmää. [5]

Käydään seuraavaksi pääpiirteittäin läpi, miten muotoa $\mathbb{F}_{2^m}$ olevat kunnat konstruoidaan. Tässä esitettävä polynominen esitys on yleistettävissä myös kaikkiin kuntiin $\mathbb{F}_{p^m}$. Kunnat $\mathbb{F}_{2^m}$ ovat käytännöllisiä myös siksi, että ne voidaan esittää tarvittaessa normaalimuodossa. Tähän esitystapaan voi perehtyä lähteessä [6].

Yksi tapa konstruoida kunta $\mathbb{F}_{2^m}$ on käyttää polynomisen kannan esitystä. Tällöin kunnan $\mathbb{F}_{2^m}$ alkiot ovat binääripolynomeja, joiden aste on korkeintaan $m-1$. Binääripolynomien kertoimet ovat kunnassa $\mathbb{F}_2 = \{0,1\}$. Matemaattisesti ilmaistuna kunta $\mathbb{F}_{2^m}$ on joukko

$$\mathbb{F}_{2^m} = \{a_{m-1}z^{m-1} + a_{m-2}z^{m-2} + \cdots + a_2z^2 + a_1z + a_0 : a_i \in \{0,1\}\}.$$

Lisäksi valitaan jaoton binääripolynomi $f(z)$, jonka aste on m. Polynomin $f(z)$ jaottomuus tarkoittaa, että polynomia $f(z)$ ei voida jakaa tekijöihin binääripolynomien tulona, jossa jokaisen tekijän aste on vähemmän kuin m. Kunnan alkioiden yhteenlasku on tavallinen polynomien yhteenlasku, joissa kertoimien aritmetiikka toteutetaan modulo 2. Kertolasku suoritetaan modulo sievennyspolynomi $f(z)$.

Esitetään seuraavaksi esimerkki binäärikunnasta $\mathbb{F}_{2^4}$. Sen jälkeen perehdytään ryhmälakiin binäärikunnassa määritellylle elliptiselle käyrälle. Tämä osuus seuraa lähteen [4] esitystä.

Esimerkki 2.3.5. Kunnan alkiot ovat seuraavat 16 binääripolynomia, joiden aste on korkeintaan 3:

$$\begin{array}{llll} 0 & z^2 & z^3 & z^3+z^2 \\ 1 & z^2+1 & z^3+1 & z^3+z^2+1 \\ z & z^2+z & z^3+z & z^3+z^2+z \\ z+1 & z^2+z+1 & z^3+z+1 & z^3+z^2+z+1. \end{array}$$

Yhteenlaskun neutraalialkio on selkeästi 0 ja kertolaskun neutraalialkio 1. Seuraavassa on esimerkkejä kunnassa $\mathbb{F}_{2^4}$ suoritetuista aritmeettisista laskutoimituksista käyttäen sievennyspolynomia $f(z) = z^4 + z + 1$.

1. Yhteenlasku: $(z^3 + z^2 + 1) + (z^2 + z + 1) = z^3 + z$.
2. Vähennuslasku: $(z^3 + z^2 + 1) - (z^2 + z + 1) = z^3 + z$.
3. Kertolasku: $(z^3 + z^2 + 1) \cdot (z^2 + z + 1) = z^2 + 1$, sillä

   $$(z^3 + z^2 + 1) \cdot (z^2 + z + 1) = z^5 + z + 1$$

   ja

   $$(z^5 + z + 1) = z^2 + 1 \mod (z^4 + z + 1).$$

4. Käänteisluku: $(z^3+z^2+1)^{-1} = z^2$, sillä

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

Ryhmälaki kunnassa $\mathbb{F}_{2^m}$ määritellylle elliptiselle käyrälle $y^2+xy = x^3+ax^2+b$

1. *Neutraalialkio*: $P+\mathcal{O} = \mathcal{O}+P = P$, kaikilla $P \in E(\mathbb{F}_{2^m})$.

2. *Vasta-alkio*: Jos $P = (x,y) \in E(\mathbb{F}_{2^m})$, niin $(x,y)+(x,x+y) = \mathcal{O}$. Pistettä $(x,x+y)$ merkitään $-P$ ja sanotaan pisteen P vasta-alkioksi. Huomaa, että $-P$ on piste käyrällä $E(\mathbb{F}_{2^m})$. Lisäksi $-\mathcal{O} = \mathcal{O}$.

3. *Pisteiden yhteenlasku*: Olkoon $P = (x_1,y_1) \in E(\mathbb{F}_{2^m})$ ja $Q = (x_2,y_2) \in E(\mathbb{F}_{2^m})$, missä $P \neq \pm Q$. Tällöin $P+Q = (x_3,y_3)$, jossa

$$\begin{aligned}x_3 &= \lambda^2+\lambda+x_1+x_2+a\\ y_3 &= \lambda(x_1+x_3)+x_3+y_1,\end{aligned}$$

   missä

$$\lambda = \frac{y_1+y_2}{x_1+x_2}.$$

4. *Pisteen tuplaaminen*: Olkoon $P = (x_1,y_1) \in E(\mathbb{F}_{2^m})$, missä $P \neq -P$. Tällöin $2P = (x_3,y_3)$, jossa

$$\begin{aligned}x_3 &= \lambda^2+\lambda+a = x_1^2+\frac{b}{x_1^2}\\ y_3 &= x_1^2+\lambda x_3+x_3,\end{aligned}$$

   missä

$$\lambda = x_1+\frac{y_1}{x_1}.$$

Esimerkki 2.3.6. Käytetään sievennyspolynomin $f(z) = z^4 + z + 1$ avulla esitettyä äärellistä kuntaa $\mathbb{F}_{2^4}$, joka muodostettiin esimerkissä 2.3.5. Olkoon $a = z^3$, $b = z^3 + 1$, joten tarkastellaan elliptistä käyrää

$$y^2 + xy = x^3 + z^3x^2 + (z^3 + 1), \tag{2.13}$$

joka on määritelty kunnassa $\mathbb{F}_{2^4}$. Alkio $a_3z^3 + a_2z^2 + a_1z + a_0 \in \mathbb{F}_{2^4}$ voidaan esittää bittijonona $(a_3a_2a_1a_0)$. Esimerkiksi (1001) vastaa alkiota z^3+1. Pisteet elliptisellä käyrällä $E(\mathbb{F}_{2^4})$ ovat seuraavat:

$\mathcal{O}$	$(0011, 1100)$	$(1000, 0001)$	$(1100, 0000)$
$(0000, 1011)$	$(0011, 1111)$	$(1000, 1001)$	$(1100, 1100)$
$(0001, 0000)$	$(0101, 0000)$	$(1001, 0110)$	$(1111, 0100)$
$(0001, 0001)$	$(0101, 0101)$	$(1001, 0010)$	$(1111, 1011)$.
$(0010, 1101)$	$(0111, 1011)$	$(1011, 0010)$	
$(0010, 1111)$	$(0111, 1100)$	$(1011, 1001)$	

Lasketaan yhteenlasku $(0010, 1111) + (1100, 1100)$. Aloitetaan laskemalla λ:

$$\begin{aligned} \lambda = \frac{y_1 + y_2}{x_1 + x_2} &= \frac{1111 + 1100}{0010 + 1100} = \frac{0011}{1110} \\ &= (0011) \cdot (0011) \\ &= 0101. \end{aligned}$$

Nyt x-koordinaatiksi saadaan

$$\begin{aligned} x_3 = \lambda^2 + \lambda + x_1 + x_2 + a &= 0101^2 + 0101 + 0010 + 1100 + 1000 \\ &= 0010 + 0101 + 0010 + 1100 + 1000 \\ &= 0001 \end{aligned}$$

ja vastaavasti y-koordinaatiksi

$$\begin{aligned} y_3 = \lambda(x_1 + x_3) + x_3 + y_1 &= 0101(0010 + 0001) + 0001 + 1111 \\ &= 0101 \cdot 0011 + 0001 + 1111 \\ &= 1111 + 0001 + 1111 \\ &= 0001. \end{aligned}$$

Pisteiden yhteenlaskusta saadaan $(0010, 1111) + (1100, 1100) = (0001, 0001)$, joka on myös elliptisen käyrän $E(\mathbb{F}_{2^4}) : y^2 + xy = x^3 + z^3x^2 + (z^3 + 1)$ piste.

Lasketaan lisäksi $2(0010, 1111)$ vastaavasti kuin edellä. Aloitetaan laskemalla λ:

$$\begin{aligned} \lambda = x_1 + \frac{y_1}{x_1} &= 0010 + \frac{1111}{0010} = 0010 + 1111 \cdot 1001 \\ &= 0010 + 1110 \\ &= 1100. \end{aligned}$$

Lasketun arvon avulla saadaan x-koordinaatiksi

$$\begin{aligned} x_3 = \lambda^2 + \lambda + a &= 1100^2 + 1100 + 1000 \\ &= 1111 + 1100 + 1000 \\ &= 1011 \end{aligned}$$

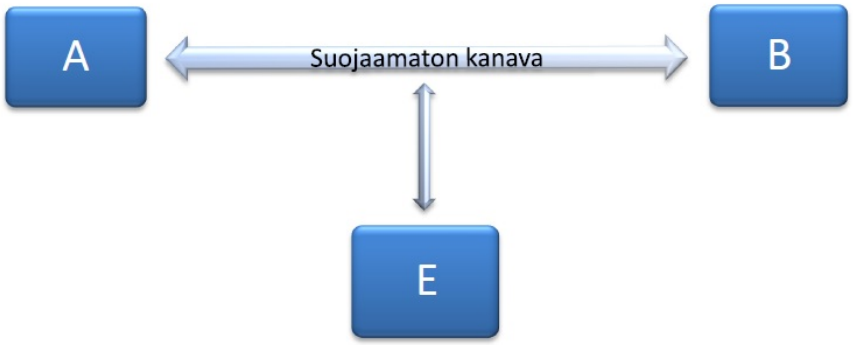
ja y-koordinaatiksi

$$\begin{aligned} y_3 = x_1^2 + \lambda x_3 + x_3 &= 0010^2 + 1100 \cdot 1011 + 1011 \\ &= 0100 + 1101 + 1011 \\ &= 0010. \end{aligned}$$

Ratkaisuksi saadaan $2(0010, 1111) = (1011, 0010)$.

3 Kryptografia

Kryptografia, eli tiedon salaus, käsittelee matemaattisten tekniikoiden suunnittelua ja analyysiä. Kryptografian tavoitteena on varmistaa kahden osapuolen kommunikointi suojaamattoman yhteyden avulla niin, että ulkopuolinen ei pysty sitä ymmärtämään. Tätä asetelmaa kutsutaan kryptografian perusongelmaksi (kuva 7).



Kuva 7: Kryptografian perusongelma

Kryptografiassa viitataan kommunikoiviin henkilöihin nimillä Alice ja Bob, sekä mahdolliseen salakuuntelijaan nimellä Eve. Informaatio, eli selkoteksti (plaintext), jonka Alice haluaa lähettää Bobille voi olla suomenkielistä tekstiä, englanninkielistä tekstiä tai numeerista informaatiota; sen rakenteella ei ole väliä. Alice salaa (encrypt) tekstin käyttäen salausavainta ja lähettää muodostetun salatun tekstin (cyphertext) kanavaa pitkin. Bob purkaa (decrypt) salatun tekstin purkuavainta käyttämällä. Kanava, jolla tieto välitetään voi olla esimerkiksi puhelinlinja tai tietokoneverkko. On myös huomionarvoista, että Alice ja Bob eivät välttämättä viittaa ihmisiin, vaan Alice voi olla esimerkiksi henkilön verkkoselain ja Bob verkkokaupan internetsivu. Mahdollisia asetelmia on kuvattu laajemmin teoksessa [4, s. 2].

Kryptografian avulla pyritään luomaan ratkaisuja todellisiin ongelmiin, joita tiedonsiirrossa esiintyy. Kryptografialle voidaan asettaa lukuisia tavoitteita, mutta niistä tärkeimmät ovat Blake et al. [1] mukaan:

1. **Luottamuksellisuus:** Ulkopuolisen ei pitäisi olla mahdollista lukea kahden osapuolen välisiä viestejä.

2. **Eheys:** Tiedon vastaanottajan täytyy voida olla varma, että viestiä ei ole muutettu.

3. **Aitous:** Tiedon vastaanottajan täytyy voida olla varma, että tiedon lähettäjä on ollut juuri se, joka sen on pitänytkin olla.

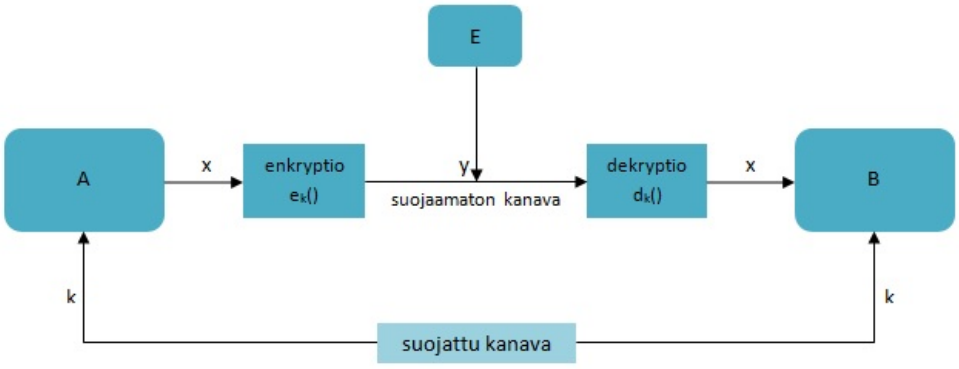
4. **Kiistämättömyys:** Viestin lähettäjä tai vastaanottaja ei pysty jälkikäteen kiistämään viestin välityksen tapahtuneen.

Kryptografiset menetelmät voidaan jakaa kahteen kategoriaan: yksityisen ja julkisen avaimen kryptografiaan. Usein yksityisen avaimen kryptografiaa kutsutaan myös symmetriseksi kryptografiaksi ja julkisen avaimen kryptografiaa epäsymmetriseksi kryptografiaksi. Symmetrisessä kryptografiassa molemmat osapuolet käyttävät samaa avainta salaukseen ja purkamiseen. Epäsymmetrisessä kryptografiassa kullakin osapuolella on sekä salattu että julkinen avain, joita molempia käytetään viestin salauksessa ja purkamisessa. Käsitellään ensin lyhyesti symmetristä kryptografiaa ja sen jälkeen hieman laajemmin julkisen avaimen kryptografiaa. Tämä osuus perustuu lähteisiin [5, 12, 17].

Kuvassa 8 kuvataan symmetrinen kryptosysteemi. Alice ja Bob jakavat yhteisen avaimen suojatun yhteyden kautta. Alice salaa selkotekstin x salausmenetelmällä e_k, joka käyttää avainta k, jolloin saadaan salattu teksti y. Salattu teksti y lähetetään suojaamatonta kanavaa pitkin vastaanottajalle Bob. Bob purkaa salatun tekstin purkumenetelmällä d_k , joka myös hyödyntää avainta k. Purkumenetelmä d_k on siis salausmenetelmän e_k käänteisfunktio.

Kaikki kryptografian klassiset menetelmät ovat symmetrisiä. Ne käyttävät salauksessa yleisimmin siirtoja, merkkien korvausta ja niiden yhdistelmiä sisältäviä algoritmeja. Nykyään yleisesti käytössä olevista standardeista symmetrisiä ovat Data Encryption Standard (DES) ja Advanced Encryption Standard (AES).

Modernit symmetriset algoritmit ovat erittäin turvallisia, nopeita ja laajasti käytettyjä. Symmetrisen avaimen skeemoilla on kuitenkin muutamia heikkouksia. Symmetristen kryptosysteemien ilmeisin puute on se, että ne vaativat aiempaa kommunikaatiota ennen itse salatun tekstin lähettämistä. On löydettävä tapa sopia yhteisestä avaimesta salatusti. Käytännössä tämän järjestäminen voi olla hankalaa.



Kuva 8: Symmetrinen kryptografia: enkryptio ja dekryptio

Toinen symmetrisen kryptografian ongelma on se, että voidaan joutua käsittelemään isoa määrää avaimia. Jos jokainen käyttäjäpari tarvitsee erillisen parin avaimia verkossa, jossa on n käyttäjää, niin verkossa on yhteensä

$$\frac{n \cdot (n-1)}{2}$$

avainparia. Lisäksi jokaisen käyttäjän täytyy säilyttää $n-1$ avainta turvallisesti. Jopa keskikokoisissa verkoissa, kuten 2000 hengen yrityksessä, tämä tarkoittaisi 4 miljoonaa avainparia, jotka pitäisi generoida ja kuljettaa turvallisia kanavia pitkin.

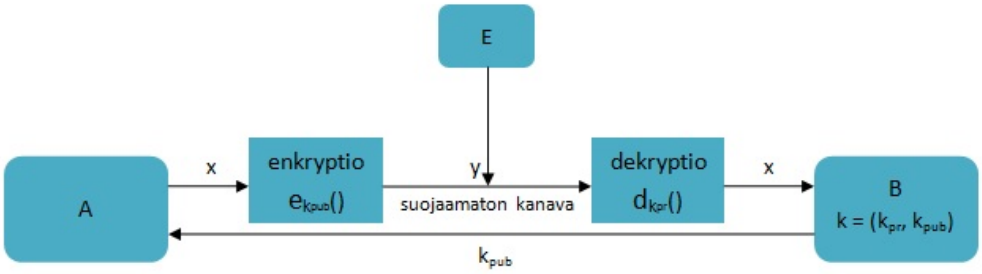
Kolmanneksi symmetriset kryptosysteemit eivät ota huomioon mahdollisuutta, että joko Alice tai Bob voisi huijata. Tähän liittyvät esimerkiksi ongelmat kiistämättömyydestä.

3.1 Julkisen avaimen kryptografia

Vuonna 1976 Diffie ja Hellman ehdottivat uudenlaista kryptosysteemiä, joka ratkaisisi symmetriseen kryptografiaan liittyviä ongelmia. He määrittivät julkisen avaimen kryptografian perusasetelman ja esittelivät avaimenvaihdon, joka perustui diskreetin logaritmin ongelmaan [3]. Vuonna 1977 Rivest, Shamir ja Adleman esittelivät julkisen avaimen toteutuksen, RSA kryptosysteemin, jonka suojaus perustuu kokonaisluvun tekijöihinjaon haasteellisuuteen.

Kuvassa 9 esitetään tilanne, jossa Alice lähettää salatun viestin vastaanottajalle Bob käyttäen julkisen avaimen kryptografiaa. Alice käyttää vastaanottajan julkista avainta k_{pub} salatakseen viestin x. Jokaisella yksilöllä

on julkisen avaimen kryptografiassa sekä salattu, että julkinen avain. Salausavain k_{pub} on julkinen, jotta kuka tahansa voi lähettää henkilölle salatun viestin. Purkuavain k_{pr} on yksityinen, jotta vain se henkilö, jolle viesti on tarkoitettu, voi selvittää sen selkokielisen version. Julkinen avain lasketaan salatun avaimen avulla. Näin ollen on tärkeää, että julkisen salausavaimen avulla ei ole mahdollista selvittää salaista purkuavainta.



Kuva 9: Julkisen avaimen kryptografia: salaus ja purkaminen

Yksityisen ja julkisen avaimen välille tarvitaan siis yksisuuntainen funktio siten, että julkinen avain on helppo laskea yksityisen avaimen avulla, mutta yksityinen avain on vaikea selvittää julkisen avaimen avulla. Oleellista julkisen avaimen kryptografian salauksen turvallisuudelle on siksi yksisuuntaisen funktion käyttäminen julkisen avaimen luomisessa. Seuraavassa tarkastellaan yksisuuntaisen funktion määritelmää sekä julkisen avaimen kryptografiassa käytettyjä yksisuuntaisia funktioita.

Määritelmä 3.1.1. Funktio f on *yksisuuntainen funktio* jos
$y = f(x)$ on laskennallisesti helppo ja
$x = f^{-1}(y)$ on laskennallisesti toteuttamiskelvoton.

Adjektiivit helppo ja toteuttamiskelvoton eivät ole kovin tarkkoja. Matemaattisesti ilmaistuna funktio on helppo laskea, jos se pystytään laskemaan polynomisessa ajassa, toisin sanoen sen ratkaisemiseen vaadittava aika on polynominen lauseke. Ollakseen käytännöllinen kryptografiassa funktion $y = f(x)$ laskemisen tulee olla riittävän nopeaa, jotta se ei johda sietämättömän hitaisiin toteutusaikoihin sovelluksissa. Käänteisen laskutoimituksen $x = f^{-1}(y)$ pitäisi olla laskennallisesti niin työläs, että sitä ei ole mahdollista laskea kohtuullisessa ajassa käyttäen parhaita tunnettuja algoritmeja.

Julkisen avaimen algoritmeja, joilla on käytännön merkitystä, on olemassa vain kolme pääluokkaa. Ne voidaan luokitella käytettävän yksisuuntaisen funktion perusteella.

Kokonaisluvun tekijöihinjaon ongelma: Perustuu tietoon, että suurienkin lukujen tulo on helppo laskea, mutta suuren kokonaisluvun jako tekijöihin on hankalaa. Tärkein tämän luokan algoritmi on RSA.

Diskreetin logaritmin ongelma: Diffie-Hellman avainten vaihto ja Digitaalinen allekirjoitusalgoritmi (DSA) ovat esimerkkejä yleisesti käytetyistä tämän luokan algoritmeista.

Elliptisen käyrän diskreetin logaritmin ongelma: Nämä algoritmit ovat muunnelmia edellisistä diskreetin logaritmin algoritmeista. Esimerkkejä ovat Elliptisen käyrän Diffie-Hellman avainten vaihto (ECDH) ja elliptisen käyrän digitaalinen allekirjoitusalgoritmi (ECDSA).

Julkisen avaimen kryptografian avulla voidaan toteuttaa kolme erilaista toiminnallisuutta. Sovelluksesta riippuen lähettäjä käyttää joko lähettäjän yksityistä avainta tai vastaanottajan julkista avainta tai molempia suorittaakseen jonkin kryptografisen toiminnon.

1. **Avaimenvaihto:** Molemmat osapuolet tekevät yhteistyötä jakaakseen yhteisen salaisen avaimen. Algoritmista riippuen tähän tarvitaan vain toisen tai molempien osapuolien salatut avaimet.

2. **Digitaalinen allekirjoitus:** Lähettäjä allekirjoittaa viestin käyttämällä salaista avaintaan. Vastaanottaja vahvistaa allekirjoituksen käyttämällä lähettäjän julkista avainta.

3. **Salaus/purku:** Lähettäjä salaa viestin käyttämällä vastaanottajan julkista avainta. Vastaanottaja purkaa viestin käyttämällä omaa salaista avaintaan.

Julkisen avaimen kryptografia voi tarjota kaikki toiminnallisuudet, joita nykyaikaiset turvallisuusprotokollat vaativat. Toisaalta tiedon salaus julkisen avaimen kryptografian keinoin on laskennallisesti vaativaa ja erittäin hidasta. Symmetristen algoritmien avulla salaus voidaan suorittaa sata tai jopa tuhat kertaa nopeammin, joten julkisen avaimen kryptografiaa käytetään salaukseen vain harvoin. Toisaalta avaimenvaihto ja digitaaliset allekirjoitukset on helpompi toteuttaa julkisen avaimen kryptografian keinoin.

3.2 Elliptiset käyrät kryptografiassa

Elliptisiä käyriä käytettiin ensimmäisen kerran kryptografiassa vuonna 1984, kun H.W. Lenstra ehdotti kokonaislukujen tekijöihinjakoalgoritmia, joka hyödynsi elliptisiä käyriä. Vuonna 1985 Koblitz ja Miller toisistaan riippumatta ehdottivat elliptisten käyrien pisteiden muodostaman ryhmän käyttöä diskreetin logaritmin ongelmaan perustuvissa kryptosysteemeissä [9, 11].

Elliptisten käyrien suojaus perustuu elliptisen käyrän diskreetin logaritmin ongelmaan (ECDLP). Parhaat tunnetut algoritmit ECDLP:n ratkaisemiseksi ovat aikavaativuudeltaan täysin eksponentiaalisia. Vastaavasti kokonaisluvun tekijöihinjako ja diskreetin logaritmin ongelma multiplikatiivisissa ryhmissä voidaan ratkaista subexponentiaalisessa ajassa. Haluttu suojaustaso voidaan siis saavuttaa elliptisten käyrien kryptosysteemeissä huomattavan paljon pienemmillä avaimilla kuin RSA-systeemeissä (taulukko 1).Tämä tarkoittaa, että elliptisten käyrien kryptosysteemien toteutukset vaativat muun muassa vähemmän fyysistä tilaa ja tehoa.

Luvun ensimmäisessä osassa tarkastellaan elliptisen käyrän diskreetin logaritmin ongelmaa ja perehdytään elliptisen käyrän pisteiden muodostaman ryhmän tärkeimpiin ominaisuuksiin kryptografian näkökulmasta hyödyntäen Hankerson et al. [4], Hoffstein et al. [5] ja Washingtonin [17] teoksia. Luvun jälkimmäisissä osissa esitellään esimerkit elliptisiä käyriä hyödyntävistä algoritmeista kullekin julkisen avaimen kryptografian toiminnallisuudelle.

3.2.1 Elliptisen käyrän diskreetin logaritmin ongelma

Elliptisen käyrän diskreetin logaritmin ongelman ratkaisemisen haasteellisuus on oleellista kaikkien elliptisten käyrien skeemojen turvallisuudelle. Tarkastellaan ensin elliptisen käyrän pisteen virittämää joukkoa ja elliptisen käyrän diskreetin logaritmin ongelmaa. Sen jälkeen tarkastellaan elliptisen käyrän muodostaman ryhmän rakennetta.

Määritelmä 3.2.1. *Elliptisen käyrän E pisteen P kertaluku* on pienin mahdollinen positiivinen kokonaisluku n, jolle

$$nP = \mathcal{O}.$$

Olkoon E elliptinen käyrä, joka on määritelty äärellisessä kunnassa $\mathbb{F}_q$. Olkoon P piste käyrällä $E(\mathbb{F}_q)$ ja oletetaan, että pisteen P kertaluku on alkuluku n. Tällöin piste P generoi joukon

$$\langle P \rangle = \{\mathcal{O}, P, 2P, 3P, ..., (n-1)P\}.$$

Pistettä P kutsutaan virityspisteeksi.

Määritelmä 3.2.2. Valitaan elliptinen käyrä E, joka on määritelty äärellisessä kunnassa $\mathbb{F}_q$. Olkoon $P \in E(\mathbb{F}_q)$ piste, jonka kertaluku on n ja $Q \in \langle P \rangle$. Oletetaan että

$$Q = kP, \tag{3.1}$$

jossa $k \in [0, n-1]$. Luvun k selvittämistä kutsutaan *elliptisen käyrän diskreetin logaritmin ongelmaksi.*

Elliptisen käyrän kryptosysteemeissä julkisina määrittelyparametreina toimivat elliptinen käyrä E, virityspiste P ja virityspisteen virittämän joukon kertaluku n. Kryptosysteemeissä k on salainen avain, joka on kokonaisluku. Julkinen avain on piste Q käytettävältä elliptiseltä käyrältä. Kryptosysteemin turvallisuudelle on oleellista, että vaikka ulkopuolinen tietää pisteen P ja julkisen avaimen Q niin siitä huolimatta luvun k eli salaisen avaimen selvittäminen on vaikeaa.

Esimerkki 3.2.3. Tarkastellaan elliptistä käyrää $E(\mathbb{F}_{23}) : y^2 = x^3 + 9x + 17$. Tämä on ryhmä, jonka määrittää yhtälö $y^2 = x^3 + 9x + 17 \mod 23$. Mikä on elliptisen käyrän diskreetin logaritmin ongelman ratkaisu k pisteelle $Q = (4, 5)$ kun tiedetään että virityspiste $P = (16, 5)$?

Raakaa voimaa käyttävässä ratkaisutavassa lasketaan pisteen P monikertoja kunnes löydetään Q. Tällöin

$$\begin{aligned} P = (16,5), \quad 2P = (20,20), \quad 3P = (14,14), \\ 4P = (19,20), \quad 5P = (13,10), \quad 6P = (7,3), \\ 7P = (8,7), \quad 8P(12,17), \quad 9P = (4,5). \end{aligned}$$

Ratkaisuksi saadaan $k = 9$. Todellisissa sovelluksissa luku k olisi niin suuri, että se tekisi tämän ratkaisumenetelmän käyttökelvottomaksi.

Kryptografiassa on tarpeen löytää tehokas tapa laskea julkinen avain $Q = kP$ kun tunnetaan luku k ja piste P. Kryptografisissa sovelluksissa k on suuri, joten pistettä Q ei voida laskea käymällä läpi jokaista pistettä $P, 2P, 3P, ..., kP$. Tehtävien laskutoimitusten määrää voidaan huomattavasti pienentää yhdistelemällä erillisten pisteiden yhteenlaskua ja pisteen tuplaamista. Esimerkiksi laskeakseen $23P$, lasketaan

$$2P, \quad 4P = 2P + 2P, \quad 8P = 4P + 4P, \quad 16P = 8P + 8P.$$

Näiden avulla saadaan laskettua

$$23P = P + 2P + 4P + 16P.$$

Nyt $23P$ saadaan neljän tuplauksen ja kolmen yhteenlaskun avulla, eli yhteensä 7 laskutoimituksella. Tämä on huomattavasti vähemmän verrattuna alkuperäiseen 22 yhteenlaskuun.

Menetelmä mahdollistaa monikerran kP laskemisen huomattavan paljon nopeammin, kun k on erittäin suuri. Ongelma on se, että pisteiden koordinaatit suurenevat erittäin nopeasti, jos työskennellään rationaalilukujen joukossa. Kun käsittelemme elliptisiä käyriä äärellisessä kunnassa, kuten esimerkiksi $\mathbb{F}_p$, tämä ei ole ongelma, sillä pystymme jatkuvasti sieventämään modulo p. Näin ollen käsiteltävät luvut pysyvät suhteellisen pieninä.

Elliptisen käyrän kryptosysteemin luomista helpottaa tieto elliptisen käyrän $E(\mathbb{F}_q)$ kertaluvusta. Elliptisen käyrän kertaluku ei riipu vain elliptisen käyrän yhtälöstä, vaan myös äärellisestä kunnasta, jossa se on määritelty. Kuvassa 10 on esitetty elliptinen käyrä $E : y^2 = x^3 + x + 6$ määriteltynä neljässä eri äärellisessä kunnassa. Esitetään seuraavaksi elliptisen käyrän kertaluvun määritelmä. Elliptisen käyrän kertaluvun suuruutta on mahdollista arvioida Hassen lauseen avulla.

Määritelmä 3.2.4. Olkoon E elliptinen käyrä, joka on määritelty kunnassa $\mathbb{F}_q$. Pisteiden lukumäärää elliptisellä käyrällä $E(\mathbb{F}_q)$ sanotaan *käyrän E kertaluvuksi* kunnassa $\mathbb{F}_q$. Tätä merkitään $\#E(\mathbb{F}_q)$.

Tarkastellaan elliptistä käyrää $E(\mathbb{F}_q)$, jolloin Weierstrassin yhtälöllä on korkeintaan kaksi ratkaisua jokaiselle $x \in \mathbb{F}_q$. Lisäksi elliptisellä käyrällä on äärettömyyspiste, joten tiedämme että käyrällä E on korkeintaan $2q + 1$ pistettä. Hassen lause tarjoaa tarkemmat rajat käyrän E kertaluvulle. Hassen lauseen todistus on esitetty Silvermanin [14, s.131] teoksessa.

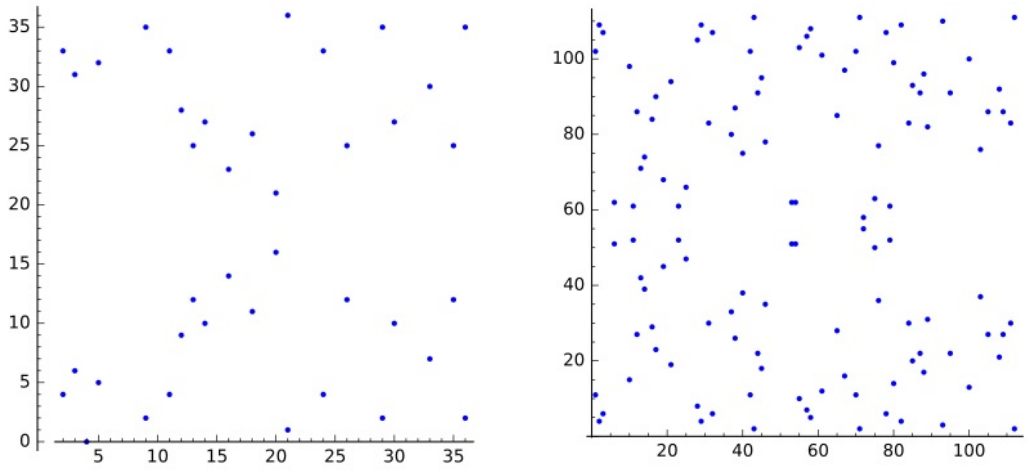
Lause 3.2.5. *Olkoon E elliptinen käyrä, joka on määritelty äärellisessä kunnassa $\mathbb{F}_q$. Tällöin käyrän $E(\mathbb{F}_q)$ kertaluvulle pätee*

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

Suljettua väliä $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ kutsutaan Hassen väliksi. Termi $2\sqrt{q}$ on pieni suhteessa lukuun q, erityisesti kun q on suuri, joten $\#E(\mathbb{F}_q) \approx q$.

Esimerkki 3.2.6. Tarkastellaan äärellistä kuntaa $\mathbb{F}_{11}$. Lauseen 3.2.5 mukaan kunnassa $\mathbb{F}_{11}$ määritellyn elliptisen käyrän kertaluku on välillä $[11 + 1 - 2\sqrt{11}, 11+1+2\sqrt{11}] = [6, 18]$. Esimerkissä 2.3.2 tarkasteltiin elliptistä käyrää $E(\mathbb{F}_{11}) : y^2 = x^3 + x + 6$, jonka kertaluku $\#E(\mathbb{F}_{11}) = 13$. Tämä kertaluku on vaaditulla Hassen välillä.

Kun tiedetään elliptisen käyrän kertaluku, saadaan tietoa elliptisen käyrän rakenteesta. Tämä mahdollistaa myös elliptisen käyrän pisteen virittämän joukon kertaluvun mahdollisten arvojen selvittämisen. Seuraavassa tarkastellaan erityisesti elliptisen käyrän syklisyyteen liittyviä tuloksia.



(a) $E(\mathbb{F}_{37})$ (b) $E(\mathbb{F}_{113})$

(c) $E(\mathbb{F}_{383})$ (d) $E(\mathbb{F}_{659})$

Kuva 10: Elliptinen käyrä $E : y^2 = x^3 + x + 6$, määriteltynä äärellisissä kunnissa $\mathbb{F}_{37}$, $\mathbb{F}_{113}$, $\mathbb{F}_{383}$ ja $\mathbb{F}_{659}$.

Määritelmä 3.2.7. *Elliptinen käyrä E on syklinen*, jos se sisältää pisteen P, jonka kertaluku n on sama kuin koko elliptisen käyrän kertaluku $\#E = n$.

Seuraavassa merkintää $\mathbb{Z}_n$ käytetään ilmaisemaan kertaluvun n syklistä ryhmää. Lause on todistettu lähteessä [17].

Lause 3.2.8. *Olkoon E elliptinen käyrä, joka on määritelty kunnassa $\mathbb{F}_q$. Tällöin $E(\mathbb{F}_q)$ on isomorfinen ryhmän $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ kanssa, jossa n_1 ja n_2 ovat yksiselitteisesti määrätyt positiiviset kokonaisluvut siten, että n_2 jakaa sekä luvun n_1 että luvun $q - 1$.*

Koska elliptinen käyrä E on isomorfinen ryhmän $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ kanssa, on elliptisen käyrän kertaluku $\#E(\mathbb{F}_q) = n_1 n_2$. Jos $n_2 = 1$, niin elliptinen käyrä $E(\mathbb{F}_q)$ on isomorfinen ryhmän $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_1 = \mathbb{Z}_{n_1}$ kanssa. Näin ollen $E(\mathbb{F}_q)$ on syklinen, sillä $\mathbb{Z}_{n_1}$ on syklinen. Tästä seuraa että, jos $\#E(\mathbb{F}_q)$ on alkuluku, niin $n_2 = 1$ ja $E(\mathbb{F}_q)$ on syklinen ryhmä. Koska $\#E(\mathbb{F}_q) = n_1 n_2$ ja lisäksi lauseessa 3.2.8 todetaan, että $n_2 \mid n_1$, niin jos kertaluvulla $\#E(\mathbb{F}_q)$ ei ole toistuvia alkuluku tekijöitä, on $n_2 = 1$. Käyrä $E(\mathbb{F}_q)$ on tässäkin tapauksessa syklinen ryhmä.

Jos n_2 on pieni kokonaisluku (esimerkiksi $n_2 = 2, 3$ tai 4) niin voidaan sanoa, että $E(\mathbb{F}_q)$ on melkein syklinen. Koska n_2 jakaa sekä luvun n_1 että luvun $q - 1$, voidaan odottaa, että suurin osa elliptisistä käyristä $E(\mathbb{F}_q)$ on syklisiä tai melkein syklisiä.

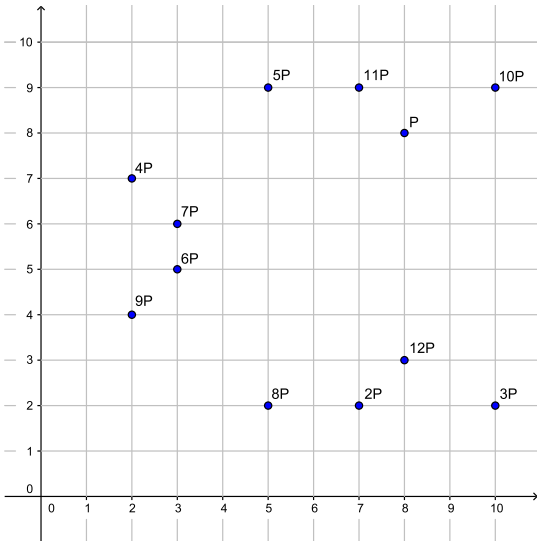
Esimerkki 3.2.9. Elliptiselle käyrälle $E : y^2 = x^3 + x + 6$, joka on määritelty kunnassa $\mathbb{F}_{11}$ (katso esimerkki 2.3.2), pätee $\#E(\mathbb{F}_{11}) = 13$. Koska 13 on alkuluku, niin $E(\mathbb{F}_{11})$ on syklinen ryhmä ja mikä tahansa piste käyrällä $E(\mathbb{F}_{11})$, äärettömyyspistettä $\mathcal{O}$ lukuunottamatta, generoi käyrän $E(\mathbb{F}_{11})$. Seuraavassa nähdään, että piste $P = (8, 8)$ generoi kaikki pisteet käyrällä $E(\mathbb{F}_{11})$. Tämä on esitetty graafisesti kuvassa 11. Pisteen $P = (8, 8)$ monikerrat ovat seuraavat:

$$\begin{aligned}
0P &= \mathcal{O} & 5P &= (5, 9) & 10P &= (10, 9)\\
1P &= (8, 8) & 6P &= (3, 5) & 11P &= (7, 9)\\
2P &= (7, 2) & 7P &= (3, 6) & 12P &= (8, 3).\\
3P &= (10, 2) & 8P &= (5, 2) & &\\
4P &= (2, 7) & 9P &= (2, 4) & &
\end{aligned}$$

Esimerkki 3.2.10. Tarkastellaan kuntaa $\mathbb{F}_{2^4}$, joka on muodostettu sievennyspolynomin $f(z) = z^4 + x + 1$ avulla. Elliptisen käyrän $E(\mathbb{F}_{2^4}) : y^2 + xy = x^3 + z^3x^2 + (z^3 + 1)$ kertaluku on $\#E(\mathbb{F}_{2^4}) = 22$. Luvulla 22 ei ole toistuvia alkulukutekijöitä, joten $E(\mathbb{F}_{2^4})$ on syklinen. Jos valitaan piste $P = (z^3, 1) = (1000, 0001)$, niin pisteen P kertaluku on 11. Pisteen $P = (1000, 0001)$ monikerrat ovat:

$$\begin{aligned}
0P &= \mathcal{O} & 4P &= (1111, 1011) & 8P &= (1100, 1100)\\
1P &= (1000, 0001) & 5P &= (1011, 0010) & 9P &= (1001, 0110)\\
2P &= (1001, 1111) & 6P &= (1011, 1001) & 10P &= (1000, 1001).\\
3P &= (1100, 0000) & 7P &= (1111, 0100) & &
\end{aligned}$$

Elliptinen käyrä $E(\mathbb{F}_{2^4})$ on syklinen, joten sillä on myös piste, jonka kertaluku on $n = 22 = \#E(\mathbb{F}_{2^4})$. Tällainen piste on esimerkiksi $Q = (0001, 0000)$.



Kuva 11: Piste $P = (8, 8)$ generoi kaikki elliptisen käyrän $E(\mathbb{F}_{11}) : y^2 = x^3 + x + 6$ pisteet

3.2.2 Avaimenvaihto – Elliptisen käyrän Diffie-Hellman avaimenvaihto

Julkisen avaimen kryptografian yksi tehtävä on avaimien luominen symmetrisiä kryptografisia menetelmiä varten. Avaimenvaihtoprotokollan tarkoitus on tarjota kahdelle tai useammalle kommunikoivalle osapuolelle jaettu salainen avain suojaamattoman verkon välityksellä. Seuraavassa on esitetty elliptisen käyrän Diffie-Hellman -avaimenvaihto lähteitä [5, 15, 17] mukaillen.

Oletetaan, että Alice ja Bob haluavat suorittaa avaimenvaihdon käyttäen elliptisen käyrän Diffie-Hellman -avaimenvaihtoa. Ensin osapuolet sopivat avaimenvaihdossa käytettävät määrittelyparametrit. Alice ja Bob valitsevat elliptisen käyrän E, joka on määritelty äärellisessä kunnassa $\mathbb{F}_q$ siten, että elliptisen käyrän diskreetin logaritmin ongelma on vaikea käyrällä $E(\mathbb{F}_q)$. Seuraavaksi valitaan virityspiste $P \in E(\mathbb{F}_q)$, jonka virittämän alijoukon kertaluku on suuri. Tämä tarkoittaa, että pienin luku n, jolla $nP = \mathcal{O}$, olisi erittäin suuri. Usein elliptinen käyrä E ja piste P valitaan siten, että kertaluku on suuri alkuluku. Julkiset määrittelyparametrit ovat elliptinen käyrä $E(\mathbb{F}_q)$ ja virityspiste P, jonka virittämän aliryhmän kertaluku on n.

Käytännössä sopivan elliptisen käyrän valitseminen on suhteellisen hankala tehtävä. Käyrillä täytyy olla tiettyjä ominaisuuksia, ollakseen turvallisia;

toisaalta tietyn tyyppisiä käyriä on vältettävä. Sopivien parametrien valintaa on käsitelty tarkemmin lähteessä [4]. Avaimenvaihto käyttäjien A ja B välillä suoritetaan seuraavasti:

Algoritmi 1 ECDH

A:	**B:**
1: Valitse yksityinen avain $a \in [1, n-1]$.	1: Valitse yksityinen avain $b \in [1, n-1]$.
2: Laske julkinen avain $Q_A = aP$.	2: Laske julkinen avain $Q_B = bP$.
3: Laske salainen avain $K = aQ_B$.	3: Laske salainen avain $K = bQ_A$.

Todistus. (*Avaimenvaihto toimii*)
Vaiheessa 3 lasketut avaimet ovat samat, koska

$$aQ_B = a(bP) = b(aP) = bQ_A$$

käyrän pisteiden yhteenlaskun vaihdannaisuuden perusteella. □

Huomautus 3.2.11. Avaimenvaihdossa saatava jaettu salainen avain on elliptisen käyrän piste eli numeropari. Jos tätä avainta halutaan käyttää istuntoavaimena perinteisessä symmetrisessä enkryptiossa niin tällöin tarvitaan vain yksi luku. Tällöin avaimena voidaan käyttää saadun pisteen x-koordinaattia tai jotakin x-koordinaatin yksinkertaista funktiota.

Esimerkki 3.2.12. Alice ja Bob haluavat suorittaa avaimenvaihdon. He käyttävät elliptistä käyrää $E(\mathbb{F}_{7211}) : y^2 = x^3 + x + 7206$, jonka virityspiste on $P = (3, 5)$. Virityspisteen P kertaluku on $n = 7233$, joka on sama kuin elliptisen käyrän kertaluku. Alice valitsee sattumanvaraisesti yksityisen avaimensa $a = 12$ ja laskee julkisen avaimen elliptisten käyrien ryhmälakia hyödyntämällä:

$$\begin{aligned} Q_A = aP &= 12(3,5) \\ &= 6 \cdot 2(3,5) \\ &= 6(4040, 229) \\ &= 3 \cdot 2(4040, 229) \\ &= 3(2060, 5024) \\ &= 2(2060, 5024) + (2060, 5024) \\ &= (5017, 2079) + (2060, 5024) \\ &= (1794, 6375). \end{aligned}$$

Bob valitsee yksityisen avaimen $b = 23$ ja laskee julkisen avaimen

$$\begin{aligned} Q_B = bP &= 23(3,5) \\ &= (3861, 1242). \end{aligned}$$

Alice laskee nyt Bobin julkisella avaimella yhteisen avaimen

$$\begin{aligned} K = aQ_B &= 12(3861, 1242) \\ &= (1472, 2098). \end{aligned}$$

Bob laskee vastaavasti käyttäen Alicen julkista avainta:

$$\begin{aligned} K = bQ_A &= 23(1794, 6375) \\ &= (1472, 2098). \end{aligned}$$

Avaimenvaihdossa Alice ja Bob ovat saaneet saman jaetun avaimen $K = (1472, 2098)$.

3.2.3 Digitaalinen allekirjoitus – Elliptisen käyrän digitaalinen allekirjoitusalgoritmi

Allekirjoitusskeemat ovat käsinkirjoitettujen allekirjoituksien digitaalisia vastineita. Digitaalinen allekirjoitus on luku, joka riippuu vain allekirjoittajan tietämästä salaisuudesta, eli allekirjoittajan yksityisestä avaimesta, sekä lisäksi allekirjoitettavan viestin sisällöstä. Digitaalinen allekirjoitus tarjoaa seuraavat kryptografiset palvelut: tiedon eheys, aitous ja kiistämättömyys. Elliptisen käyrän digitaalinen allekirjoitusalgoritmi on elliptisten käyrien analogia Digitaalisesta allekirjoitusalgoritmista (Digital Signature Algorith, DSA). Tämä on laajimmin standardoitu elliptisiin käyriin perustuva allekirjoitusskeema. Seuraavaksi esitetään viestin allekirjoittaminen ECDSA -algoritmilla pohjautuen lähteisiin [4, 6, 17]. Allekirjoituksen luominen on esitetty algoritmissa 2 ja allekirjoituksen vahvistaminen algoritmissa 3.

Oletetaan, että Alice haluaa allekirjoitaa viestin m käyttäen elliptisen käyrän digitaalista allekirjoitusalgoritmia. Ensin Alice valitsee käytettävät määrittelyparametrit. Parametrien määrittäminen etenee samalla tavalla kuin avaimenvaihdon yhteydessä. Julkiset määrittelyparametrit ovat elliptinen käyä $E(\mathbb{F}_q)$ ja virityspiste P, jonka virittämän aliryhmän kertaluku on n. Lisäksi Alice valitsee yksityisen avaimen $a \in [1, (n-1)]$ ja laskee vastaavan julkisen avaimen $Q = aP$.

Algoritmissa käytetään kryptografista hajautusfunktiota H, jonka arvojen bittipituus ei ole suurempi kuin n. Hajautusfunktio muuntaa mielivaltaisen pituisen viestin tietyn mittaiseksi bittijonoksi siten, että kaksi eri viestiä

eivät voi saada samaa arvoa. Hajautusfunktioihin voi tutustua tarkemmin lähteessä [15]. Alice allekirjoittaa viestin m seuraavasti:

Algoritmi 2 ECDSA allekirjoitus

1: Valitse satunnainen kokonsaisluku $k \in [1, n-1]$.
2: Laske $kP = (x_1, y_1)$ ja muunna x_1 kokonaisluvuksi $\overline{x}_1$.
3: Laske $r = \overline{x}_1 \mod n$. Jos $r = 0$ palaa takaisin vaiheeseen 1.
4: Laske $k^{-1} \mod n$.
5: Laske $H(m)$ ja muunna tämä bittijono kokonaisluvuksi e.
6: Laske $s = k^{-1}(e + dr) \mod n$. Jos $s = 0$ palaa takaisin vaiheeseen 1.
7: A:n allekirjoitus viestille m on lukupari (r, s).

Allekirjoitus vahvistetaan seuraavasti:

Algoritmi 3 ECDSA allekirjoituksen vahvistus

1: Varmista, että luvut r ja s ovat kokonaislukuja välillä $[1, n-1]$. Jos jompi kumpi varmistus epäonnistuu, niin allekirjoitusta ei vahvisteta.
2: Laske $e = H(m)$.
3: Laske apumuuttuja $w = s^{-1} \mod n$.
4: Laske apumuuttujat $u_1 = ew \mod n$ ja $u_2 = rw \mod n$.
5: Laske $X = u_1P + u_2Q$. Jos $X = \infty$ niin allekirjoitus hylätään.
6: Muunna pisteen X x-koordinaatti x_1 kokonaisluvuksi $\overline{x}_1$ ja laske $v = \overline{x}_1 \mod n$.
7: Jos $v = r$ niin allekirjoitus hyväksytään. Muuten allekirjoitus hylätään.

Todistus. (*Allekirjoituksen vahvistus toimii*)
Jos lähettäjän A allekirjoitus viestiin m on (r, s), niin $s = k^{-1}(e+ar) \mod n$. Tästä saadaan

$$k = s^{-1}(e + ar) = s^{-1}e + s^{-1}ra = we + wra = u_1 + u_2a \mod n.$$

Edelleen

$$X = u_1P + u_2Q = u_1P + u_2aP = (u_1 + u_2a)P = kP,$$

joten $v = r$. □

Huomautus 3.2.13. Viestikohtainen salaisuus k tulee valita satunnaisesti. Näin voidaan varmistua siitä, että nämä viestikohtaiset arvot eivät toistu. Jos arvot k toistuvat, niin tällöin on mahdollista saada selville lähettäjän yksityinen avain a.

Oletetaan, että samaa viestikohtaista arvoa k käytettiin ECDSA allekirjoitusten (r, s_1) ja (r, s_2) luomiseen kahdelle viestille m_1 ja m_2. Tällöin pätee

$$\begin{aligned} s_1 &\equiv k^{-1}(e_1 + ar) \mod n \\ s_2 &\equiv k^{-1}(e_2 + ar) \mod n, \end{aligned}$$

joissa $e_1 = H(m_1)$ ja $e_2 = H(m_2)$. Tästä seuraa, että

$$\begin{aligned} ks_1 &\equiv e_1 + ar \mod n \\ ks_2 &\equiv e_2 + ar \mod n, \end{aligned}$$

jolloin vähennyslaskulla saadaan $k(s_1 - s_2) \equiv e_1 - e_2 \mod n$. Jos $s_1 \neq s_2$, joka on erittäin todennäköistä, niin

$$k \equiv (s_1 - s_2)^{-1}(e_1 - e_2) \mod n.$$

Ulkopuolinen voi siis selvittää luvun k ja sitten laskea salaisen avaimen a seuraavasti:

$$a \equiv r^{-1}(ks - e) \mod n.$$

Esimerkki 3.2.14. Alice haluaa allekirjoittaa viestin m käyttäen ECDSA -algoritmia ja lähettää sen vastaanottajalle Bob. Alice valitsee elliptisen käyrän $E : y^2 = x^3+2x+2$, joka on määritety äärellisessä kunnassa $\mathbb{F}_{17}$. Käyrältä E valitaan virityspiste $P = (5, 1)$, jonka kertaluku on $n = 19$. Viesti m saa hajautusfunktiolla arvon $e = H(m) = 26$. Allekirjoitus ja allekirjoituksen vahvistaminen etenevät seuraavasti:

Alice luo ensin salaisen ja julkisen avaimensa. Alice valitsee salaisen avaimen $a = 7 < n$ ja laskee julkisen avaimensa

$$Q_A = aP = 7 \cdot (5, 1) = (0, 6).$$

Julkiset määrittelyparametrit ovat elliptinen käyrä $E(\mathbb{F}_{17}) : y^2 = x^3+2x+2$, virityspiste $P = (5, 1)$, jonka kertaluku on $n = 19$. Lisäksi Alicen julkinen avain $Q_A = (0, 6)$ tiedetään julkisesti. Alice allekirjoittaa viestin m, jonka hajautusarvo on $e = 26$.

1. Alice valitsee lyhytaikaisen avaimen $k = 10 \in [1, 18]$.
2. Alice laskee virityspisteen monikerran $kP = 10 \cdot (5, 1) = (7, 11)$.
3. $r = 7$.
4. $k^{-1} = 2 \mod 19$, koska $kk^{-1} = 10 \cdot 2 = 20 \equiv 1 \mod 19$.
5. $e = 26$.
6. $s = k^{-1}(e + dr) = 2(26 + 7 \cdot 7) \equiv 2(7 + 11) \equiv 17 \mod 19$.
7. Alicen allekirjoitus viestille m on lukupari $(7, 17)$.

Alice lähettää Bobille viestin m ja lukuparin $(r, s) = (7, 17)$. Bob vahvistaa Alicen allekirjoituksen.

1. Bob tarkistaa, että $r, s = 7, 17 \in [1, 18]$.
2. $e = H(m) = 26$.
3. Bob laskee apumuuttujan $w = s^{-1} = 17^{-1} \equiv 9 \mod 19$.
4. $u_1 = ew = 26 \cdot 9 \equiv 6 \mod 19$ ja
   $u_2 = rw = 7 \cdot 9 \equiv 6 \mod 19$.
5. $X = u_1 P + u_2 Q_A = 6 \cdot (5, 1) + 6 \cdot (0, 6) = (7, 11)$.
6. $v = 7 \mod 19$.
7. $v = r$, joten allekirjoitus hyväksytään.

3.2.4 Enkryptio ja dekryptio – Elliptisen käyrän integroitu salaus -skeema

Vuonna 2001 Bellare ja Rogaway ehdottivat elliptisen käyrän integroitua salaus -skeemaa (ECIES), joka on muunnelma ElGamalin julkisen avaimen salaus -skeemasta. ECIES hyödyntää Diffie-Hellman avaimenvaihtoa, mutta yhdistää lisäksi symmetrisen enkryptiometodin ja viestin eheyden varmistamisen. Salaus ECIES-algoritmia käyttäen esitetään algoritmissa 4 ja purku algoritmissa 5. Tämä osuus perustuu lähteisiin [4, 17].

Algoritmissa tarvitaan kaksi kryptografista hajautusfunktiota H_1 ja H_2. Hajautusfunktioista ensimmäisen H_1 avulla tuotetaan avaimet k_1 ja k_2. Toisen hajautusfunktion H_2 avulla varmistetaan viestin eheys, joten usein tässä käytetään tähän tarkoitukseen luotua MAC-algoritmia. Molemman tyyppisiä hajautusfunktioita käsitellään laajemmin Paarin teoksessa [12]. Lisäksi tarvitaan symmetrinen salausfunktio E_k, kuten AES, ja vastaava purkufunktio D_k. Hajautus- ja salausfunktiot sovitaan julkisesti.

Oletetaan, että Alice haluaa lähettää viestin Bobille. Bob valitsee elliptisen käyrän E, joka on määritelty äärellisessä kunnassa $\mathbb{F}_q$ siten, että elliptisen käyrän diskreetin logaritmin ongelma on vaikea käyrällä $E(\mathbb{F}_q)$. Seuraavaksi Bob valitsee virityspisteen $P \in E(\mathbb{F}_q)$ yleensä siten, että pisteen P kertaluku on suuri alkuluku n. Bob valitsee yksityisen avaimen b ja laskee $Q = bP$, joka on hänen julkinen avaimensa. Julkiset määrittelyparametrit ovat elliptinen käyä $E(\mathbb{F}_q)$ ja virityspiste P, jonka virittämän aliryhmän kertaluku on n. Lisäksi Bobin julkinen avain Q on yleisesti tiedossa.

Alice salaa viestin seuraavasti:

Algoritmi 4 ECIES salausmenetelmä

1: Valitse kokonsaisluku $k \in [1, n-1]$.
2: Laske $R = kP$ ja $Z = kQ$. Jos $Z = \mathcal{O}$, niin palaa kohtaan 1.
3: Laske $H_1(R, Z)$ ja kirjoita tulos muodossa $k_1||k_2$ (k_1 ja k_2 kirjoitetaan peräkkäin), missä avaimilla k_1 ja k_2 on määrätyt pituudet.
4: Laske $C = E_{k_1}(m)$ ja $t = H_2(C, k_2)$.
5: Enkryptoitu viesti on (R, C, t).

Bob purkaa salatun viestin:

Algoritmi 5 ECIES purkumenetelmä

1: Laske $Z = bR$. Jos $Z = \mathcal{O}$, niin viesti hylätään.
2: Laske $H_1(R, Z)$ ja kirjoita tulos muodossa $k_1||k_2$.
3: Laske $t' = H_2(C, k_2)$. Jos $t' \neq t$, niin viesti hylätään.
4: Laske $m = D_{k_1}(C)$. Tämä on alkuperäinen viesti m.

Todistus. (*Purkumenetelmä toimii*)
Jos lähettäjä loi salatun viestin (R, C, t) salatessaan viestiä m, niin

$$Z = bR = b(kP) = k(bP) = kQ = Z.$$

Molemmilla osapuolilla on siis samat pisteet R ja Z, joita käytetään hajautusfunktiossa H_1. Viestin vastaanottaja laskee samat avaimet (k_1, k_2) kuin viestin lähettäjä, hyväksyy salatun tekstin ja saa selville viestin m. □

Viitteet

[1] Blake, I.F., Seroussi, G., Smart, N.P., *Elliptic Curves in Cryptography*. London Mathematical Society Lecture Note Series 265, University Press Cambridge. 1999

[2] *Cryptography Today*, https://www.nsa.gov/ia/programs/suiteb_cryptography/ Luettu 15.9.2015.

[3] Diffie, W., Hellman, M.E., *New Directions in Cryptography*. IEEE Transactions on Information Theory, Vol. IT-22, No. 6 (1976), ss. 644 - 654.

[4] Hankerson, D., Menezes, A., Vanstone, S., *Guide to Elliptic Curve Cryptography*. Springer-Verlag New York, Inc. 2004

[5] Hoffstein, J., Pipher, J., Silverman, J.H., *Introduction to Mathematical Cryptography*. Springer Science+Business Media NewYork. 2008, 2014

[6] Johnson, D., Menezes, A., Vanstone, S., *The Elliptic Curve Digital Signature Algorithm*, http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf Luettu

[7] Knapp, A., *Elliptic Curves*. Princeton University Press. 1992

[8] Koblitz, A., Koblitz, N., Menezes, A. *Elliptic curve cryptography: The serpentine course of a paradigm shift*. Journal of Number Theory, 131 (2011) ss. 781-814.

[9] Koblitz, N., *Elliptic Curve Cryptpsystems*. Mathematics of Computation, Vol. 48, N.177 (1987), ss. 203-209.

[10] Koblitz, N., Menezes, A. *A Riddle Wrapped In An Enigma*, http://eprint.iacr.org/2015/1018.pdf

[11] Miller, V., *Use of Elliptic Curves in Cryptosystems*. Advances in Cryptography - CRYPTO '85, Lecture Notes in Computer Science, Vol. 218 (1986), ss. 417-426

[12] Paar, C., Pelzl, J., *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer-Verlag Berlin Heidelberg. 2010

[13] *Recommendation for Key Management, Part 1: General*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf Luettu 1.3.2016

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

[15] Trappe, W., Washington, L., *Introduction to Cryptography with Coding Theory*. Second Edition. Pearson Education, Inc. 2006, 2002

[16] Vinberg, E. B., *A Course in Algebra*. the American Mathematical Society. 2003

[17] Washington, L.C., *Elliptic Curves: Number Theory and Cryptography*. Taylor & Francis Group, LCC. 2008