

TAMPEREEN TEKNILLINEN YLIOPISTO

Tietotekniikan osasto

JUHO LINNA

ELLIPTISIIN KÄYRIIN PERUSTUVAT KRYPTOSYSTEEMIT

Diplomityö

Aihe hyväksytty osastoneuvoston kokouksessa
19.1.2005.

Tarkastajat: prof. Keijo Ruohonen, TTY
lehtori Merja Laaksonen, TTY

Alkulause

Olen tehnyt diplomityöni tutkimusapulaisena Tampereen teknillisen yliopiston Matematiikan laitoksella. Esitän kiitokseni työni tarkastajalle ja ohjajalle prof. Keijo Ruohoselle. Kiitän myös Matematiikan laitosta työni rahallisesta tukemisesta.

Tampereella 22.2.2005

Juho Linna

Insinöörinkatu 60 B 81
33720 Tampere

puh. 040 5842950

Tiivistelmä

TAMPEREEN TEKNILLINEN YLIOPISTO

Tietotekniikan osasto

Matematiikan laitos

LINNA, JUHO: Elliptisiin käyriin perustuvat kryptosysteemit

Diplomityö, 54 s.

Tarkastajat: prof. Keijo Ruohonen, lehtori Merja Laaksonen

Rahoittaja: Matematiikan laitos

Helmikuu 2005

Avainsanat: elliptinen käyrä, kryptosysteemi

Valtaosa käytetyistä julkisen avaimen kryptosysteemeistä on jo pitkään perustunut lukujen tekijöihinjaon vaikeuteen. Edistysaskeleet tekijöihinjaokoalgoritmeissa sekä laskentatehon kasvu ovat kuitenkin antaneet aihetta tehokkaampien menetelmien etsimiseen. Lupaavin ehdokas perustuu eräiden algebrallisten käyrien, ns. elliptisten käyrien, ominaisuuksiin. Diplomityössä esitellään yleisimmin käytetyt kryptosysteemit sekä vertaillaan niiden turvallisuutta. Erityistä huomiota kiinnitetään elliptisiin käyriin perustuvan systeemin esittelyyn. Tiukan muodollinen esittely on yhden diplomityön puitteissa mahdotonta, joten tarvittaessa käytetään yksinkertaistavaa esitystapaa. Turvallisuuden mittarina käytetään murtoalgoritmin asympotoottista käyttäytymistä avaimen pituuden funktiona.

Vertailun mukaan elliptisiin käyriin perustuva systeemi on turvallisuudeltaan selvästi vertailujoukon paras.

Abstract

The majority of public key cryptosystems are based on the difficulty of factoring. However, advances in factoring algorithms and growth of computing capacity have brought forth the need for more efficient alternatives. The most promising candidate is based on properties of certain algebraic curves called elliptic curves. In this thesis the most popular cryptosystems are presented and their safety is compared. The introduction of the elliptic curve cryptosystem is paid special attention. A strictly formal introduction is impossible within one thesis and therefore, in some places, a simplified approach has been taken. The safety comparison is based on the asymptotic behaviour of breaking algorithms.

The safety comparison showed that the elliptic curve cryptosystem clearly outperforms the other systems in the test group.

Sisältö

| | | |
|----------|---|-----------|
| 1 | Perusteita | 3 |
| 1.1 | Modulaarilaskentaa | 3 |
| 1.2 | Ryhmät | 4 |
| 1.2.1 | Määritelmä | 4 |
| 1.2.2 | Perusteita | 5 |
| 1.2.3 | Sykliset ryhmät | 6 |
| 1.3 | Kunnat | 7 |
| 1.4 | Projektiivinen taso ja projektiivinen geometria | 9 |
| 1.4.1 | Taustaa | 9 |
| 1.4.2 | Homogeeniset koordinaatit | 10 |
| 1.4.3 | Projektiivinen taso | 11 |
| 2 | Elliptiset käyrät | 14 |
| 2.1 | Määritelmä | 14 |
| 2.2 | Weierstrassin normaalimuoto | 16 |
| 2.2.1 | Muita muotoja | 17 |
| 2.2.2 | Geometrisia tarkasteluja | 17 |
| 2.3 | Käyrän projektiivinen sulkeuma | 19 |
| 2.4 | Ryhmäoperaatio | 20 |
| 2.5 | Äärellisten kuntien yli määritellyistä käyristä | 23 |
| 2.6 | Liitännäisyyden todistus | 24 |
| 2.6.1 | Perustuloksia | 25 |
| 2.6.2 | Todistus | 26 |
| 3 | Kryptologiaa | 30 |
| 3.1 | Taustaa | 30 |
| 3.2 | Perusteita | 31 |
| 3.3 | RSA | 32 |
| 3.4 | Diskreettiin logaritmiin perustuvat systeemit | 33 |
| 3.4.1 | Diffie-Hellman-avainjakosysteemi | 34 |
| 3.4.2 | ElGamal | 35 |
| 3.4.3 | XTR | 36 |
| 3.4.4 | Elliptisiin käyriin perustuvat kryptosysteemit | 37 |

| | | |
|----------|--|-----------|
| 4 | Turvallisuus | 39 |
| 4.1 | Perusteita | 39 |
| 4.2 | Sivukanavahyökkäyksistä | 41 |
| 4.3 | Kryptosysteemin pystytys | 42 |
| 4.3.1 | RSA | 43 |
| 4.3.2 | Diffie-Hellman ja ElGamal | 43 |
| 4.3.3 | XTR | 44 |
| 4.3.4 | Elliptisiin käyriin perustuvat systeemit | 44 |
| 4.4 | Salausalgoritmien turvallisuus | 45 |
| 4.4.1 | Tekijöihinjako | 46 |
| 4.4.2 | Diskreetti logaritmi ryhmässä F_q^* | 46 |
| 4.4.3 | Diskreetti logaritmi XTR-aliryhmässä | 47 |
| 4.4.4 | Diskreetti logaritmi ryhmässä $E(F_q)$ | 47 |
| 4.5 | Turvallisuusvertailuja | 48 |
| 4.5.1 | Asymptoottinen turvallisuus | 48 |
| 4.5.2 | Käytännön vertailuja | 50 |
| 4.6 | Yhteenvedo | 52 |

Terminologiaa

| | |
|----------------------------|---|
| $m x - y$ | m jakaa luvun $x - y$ |
| $x \equiv y \pmod{m}$ | x on kongruentti y modulo m |
| \bar{x} | luvun x jäännösluokka |
| Z_m | jäännösluokkien joukko modulo m |
| $\text{syt}(x, y)$ | lukujen x ja y suurin yhteinen tekijä |
| $\phi(m)$ | Eulerin funktio |
| (G, \circ) | ryhmä, jonka joukko G muodostaa operaation \circ kanssa |
| $ G $ | ryhmän G kertaluku |
| $G \oplus H$ | ryhmien G ja H suora summa |
| $(K, +, \cdot)$ | kunta, jonka operaatioina ovat $+$ ja \cdot |
| K^+ | kunnan K additiivinen ryhmä |
| K^* | kunnan K multiplikaatiivinen ryhmä |
| \bar{K} | kunnan K algebrallinen sulkeuma |
| p | alkuluku |
| F_q | kunta, jossa on q alkiota |
| \mathbf{R} | reaalilukujen joukko |
| \mathbf{C} | kompleksilukujen joukko |
| $\mathbf{P}^2(\mathbf{R})$ | reaalinen projektiivinen taso |
| $(X : Y : Z)$ | (projektiivisen tason pisteen) homogeeniset koordinaatit |
| C_f | (polynomin f määrittämä) algebrallinen käyrä |
| D_x | osittaisderivaatta muuttujan x suhteen |
| E | elliptinen käyrä |
| $E(K)$ | elliptinen käyrä, jonka koordinaattikunta on K |
| O | elliptisen käyrän piste äärettömydessä |
| \overline{AB} | pisteiden A ja B kautta kulkeva suora |
| k_1 | julkinen avain |
| k_2 | salainen avain |
| S_{k_1} | salausfunktio |
| P_{k_2} | purkufunktio |
| w | salaamaton viestilohko |
| c | salattu viestilohko |
| $O(f(N))$ | algoritmin kompleksisuuden asympotoottinen yläraja |
| $V_N(v)$ | algoritmin kompleksisuutta kuvaava apufunktio |

Johdanto

Kryптаus perustui 1970-luvulle saakka salaisten salaus- ja purkuavainten käyttöön. Menetelmän haittapuolena on tarve erilliseen, turvalliseen kommunikointikanavaan, jota käyttäen osapuolet voivat sopia käytetyistä avaimista. Tietoverkkojen ja tiedonsiirron kehittyessä kasvoi tarve turvalliseen kommunikointiin käyttäen ainoastaan julkista kommunikointikanavaa.

Julkisen avaimen kryptauksen periaatteen esittivät W. Diffie ja M.E. Hellman vuonna 1976. Ideana on, että viestin vastaanottaja asettaa yleisesti saataville ns. julkisen avaimen, jonka avulla kuka tahansa voi salata viestin. Viesti salataan tekemällä sille helppo operaatio, kun taas purkaminen vaatii salakuuntelijoilta vaikean käänteisoperaation tekemistä. Vastaanottaja voi purkaa salauksen hänen julkista avaintansa vastaavalla salaisella purkuavaimella. Menettely vaatii riittävän vaikeasti käännettävän, ns. *yksisuuntaisen operaation*. Diffie ja Hellman ehdottivat yksisuuntaiseksi operaatioksi potenssiin korotusta äärellisessä ryhmässä. Tämän käänteisoperaatio, diskreetti logaritmi, on (edelleen) vaikea. Keksinnön ilmeinen hyödyllisyys huomattiin ja sovelluksia ilmaantui nopeasti. Julkisen avaimen salausta hyödynnetään nykyään mm. tiedonsiirrossa, todentamisessa, nolletietotodistuksissa ja e-äänestyksessä.

Ensimmäinen laajalti käyttöön otettu julkisen avaimen kryptosysteemi oli RSA. Sen käyttämä yksisuuntainen operaatio on alkulukujen kertolasku, jonka käänteisoperaatio, tekijöihinjako, on nykyäänkin laskennallisesti haastava. Systeemi on vieläkin laajassa käytössä, joskin tekijöihinjakoalgoritmien kehityksen vuoksi käytetyn salausavaimen kokoa on jouduttu kasvattamaan huomattavasti. Tämä kehitys on antanut aihetta turvallisempien kryptosysteemien etsimiseen.

Tutkimusalana elliptiset käyrät on ollut hyvin teoreettinen ja etäällä käytännön sovelluksista aina 1980-luvulle saakka. Vuonna 1985 N. Koblitz ja V. Miller ehdottivat elliptisten käyrien soveltamista salaukseen. Heidän idea-

naan on käyttää äärellisen kunnan yli tarkastellun elliptisen käyrän pisteiden muodostamaa ryhmää diskreettiin logaritmiin pohjautuvan kryptosysteemin pohjana. Ala on viime aikoina kehittynyt huomattavasti ja salaussovellukset näyttävät yhä houkuttelevammilta. Nykyään elliptisten käyrien ominaisuuksia hyödynnetään myös nopeissa tekijöihinjakoalgoritmeissa.

Tässä työssä esitellään elliptisiin käyriin perustuvan kryptosysteemin teoreettista taustaa ja vertaillaan sen turvallisuutta muihin suosiota saaneisiin systeemeihin. Monien esitettyjen tulosten taustalla oleva teoria on vaativaa ja sen perusteellinen läpi käyminen vaatisi huomattavia esitietoja monilta matematiikan alueilta. Luettavuuden parantamiseksi on paikoin käytetty lyhyttä ja yksinkertaistavaa esitystapaa. Teoriasta lähemmin kiinnostuneita kehoitetaan tutustumaan lähdeviitteisiin.

Ensimmäisessä kappaleessa esitellään lyhyesti tarvittavia perustietoja. Toisessa kappaleessa määritellään elliptinen käyrä ja tutustutaan tarvittaviin perustuloksiin. Kolmas kappale käy läpi kryptologian peruskäsitteet sekä esittelee tarkastellut kryptosysteemit. Neljännessä kappaleessa esitellään turvallisuusvertailussa käytetyt käsitteet, tutkitaan kryptosysteemien turvallisuutta sekä esitetään tulosten yhteenveto.

1 Perusteita

Tässä luvussa esitellään lyhyesti aiheen käsittelyssä vaadittavaa teoriaa. Lukijan oletetaan tuntevan korkeakoulumatematiikan peruskäsitteet, kuten ekvivalenssirelaatio, osittaisderivaatta ja algoritmi.

1.1 Modulaarilaskentaa

Modulaarilaskennassa tarkastellaan kokonaislukuja samaistaen ne luvut, joilla on sama jakojäännös. Jakajaa, jonka mukaan jakojäännös määrätään, sanotaan *moduliksi*. Kokonaisluvut x ja y ovat *kongruentit modulo m* , jos $m|x - y$. Tästä käytetään myös merkintää

$$x \equiv y \pmod{m}.$$

Tällöin siis luvuilla x ja y on sama jakojäännös jaettaessa luvulla m . Luvut, jotka ovat keskenään kongruentteja modulo m , muodostavat ns. *jäännösluokan modulo m* . Jokainen kokonaisluku kuuluu tarkalleen yhteen jäännösluokkaan. Jäännösluokkaa, johon luku x kuuluu, merkitään \bar{x} :lla. Jäännösluokkien joukkoa modulo m merkitään Z_m :llä. Jäännösluokille määritellään yhteen- ja kertolasku luonnollisella tavalla kokonaislukujen yhteen- ja kertolaskun avulla:

$$\bar{x} + \bar{y} = \overline{x + y}, \quad \bar{x} \cdot \bar{y} = \overline{xy}.$$

Luvun x *inverssi modulo m* on luku y , jolle

$$xy \equiv 1 \pmod{m}.$$

Luvulla x on olemassa inverssi modulo m tarkalleen silloin kun $\text{syt}(x, m) = 1$. Ehdon $\text{syt}(x, m) = 1$ täyttävien lukujen x lukumäärää välillä $0 < x < m$ sanotaan *Eulerin funktioksi* arvolla m , merkitään $\phi(m)$. Funktiolle ϕ ovat voimassa seuraavat perustulokset (p on alkuluku):

$$\phi(p) = p - 1, \tag{1}$$

$$\phi(p^k) = p^{k-1}(p-1).$$

Jos $\text{syt}(n, m) = 1$, niin saadaan myös tulos

$$\phi(nm) = \phi(n)\phi(m).$$

Luku $\phi(n)$ voidaan helposti laskea, jos luvun n tekijöihinjako tunnetaan. Kohdan (1) mukaan jokaista lukua x ($0 < x < p$) kohti löytyy inverssi modulo p . Mainitaan todistuksesta vielä yksi tärkeä tulos:

Lause 1 (Eulerin lause). Jos $\text{syt}(x, m) = 1$, niin

$$x^{\phi(m)} \equiv 1 \pmod{m}.$$

1.2 Ryhmät

1.2.1 Määritelmä

Ryhmän käsite syntyy luonnollisella tavalla käsitteiden *symmetria* ja *joukko* pohjalta. Symmetrialla tarkoitetaan muunnosta, joka ei muuta kohteen ominaisuuksia (rakennetta). Mielivaltaisen joukon A , jolle ei siis oleteta mitään erityistä rakennetta, symmetrioita ovat tarkalleen joukon A permutaatiot. Joukkojen permutaatioilla (symmetrioilla) on yhteisiä ominaisuuksia, jotka voidaan kiteyttää kolmeksi aksioomaksi. Nämä aksioomat toteuttavaa joukkoa kutsutaan *ryhmäksi*.

Määritelmä 1. Ryhmä on joukko G , jossa on määritelty operaatio $\circ: G \times G \rightarrow G$, ja jonka mielivaltaisilla alkioilla x, y, z pätee:

1. (liitännäisyys) $(x \circ y) \circ z = x \circ (y \circ z)$.
2. (neutraalialkio) On olemassa alkio $e \in G$, jolla $e \circ x = x \circ e = x$.

3. (käänteisalkio) On olemassa alkio $x^{-1} \in G$, jolla $x \circ x^{-1} = x^{-1} \circ x = e$.

Ryhmää merkitään tavallisesti järjestettynä parina (G, \circ) .

1.2.2 Perusteita

Äärellisen ryhmän *kertaluku*, merkitään $|G|$, on sen alkioiden lukumäärä. Alkion g *kertaluku*, merkitään $\text{deg}(g)$, on pienin luonnollinen luku d , jolle pätee $g^d = e$. Ryhmän (G, \circ) osajoukko H , joka on ryhmä operaation \circ suhteen, on ryhmän G *aliryhmä*. Operaatiosta

$$\underbrace{x \circ x \circ \cdots \circ x}_{n \text{ kpl}}$$

käytetään yleensä merkintää x^n . Kun ryhmäoperaatiota merkitään normaalilla plus -merkillä, kirjoitetaan perinteisesti

$$x + x + \cdots + x = nx.$$

Kaksi ryhmää (G, \circ) ja (H, \diamond) ovat *isomorfiset*, jos on olemassa sellainen bijektio $I : G \rightarrow H$, että kaikilla alkioilla $g_1, g_2 \in G$ pätee:

$$I(g_1 \circ g_2) = I(g_1) \diamond I(g_2).$$

Bijektio I on ryhmien G ja H välinen *isomorfismi*. Isomorfiset ryhmät ovat sama ryhmä eri merkinnöin.

Lause 2 (Lagrange). *Olkoon G äärellinen ryhmä.*

1. *Jos H on ryhmän G aliryhmä, niin ryhmän H kertaluku jakaa ryhmän G kertaluvun.*
2. *Kunkin alkion $g \in G$ kertaluku jakaa ryhmän G kertaluvun.*

Ryhmien (G, \circ) ja (H, \diamond) *suora summa* on G :n ja H :n alkoiden järjestettyjen parien joukko

$$G \oplus H = \{(g, h) \mid g \in G, h \in H\}$$

varustettuna laskutoimituksella \bullet :

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 \circ g_2, h_1 \diamond h_2).$$

Näin määriteltynä suora summa $G \oplus H$ muodostaa ryhmän. Samalla tavalla voidaan määritellä useamman kuin kahden ryhmän suora summa. Suoraa summaa, jossa summataan r kertaa ryhmä G , merkitään G^r .

Ryhmä G on *Abelin ryhmä*, jos ryhmäoperaatio on *vaihdannainen*, eli kaikille $x, y \in G$ pätee $x \circ y = y \circ x$. Seuraavassa vielä tärkeä tulos Abelin ryhmien rakenteesta.

Lause 3. *Äärellinen Abelin ryhmä G on isomorfinen ryhmän*

$$Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_s}$$

kanssa, jossa $n_i \mid n_{i+1}$ kaikilla $i = 1, 2, \dots, s-1$. (Kokonaisluvut s, n_1, n_2, \dots, n_s riippuvat ryhmästä G .)

1.2.3 Sykliset ryhmät

Ryhmä G on *äärellisesti generoitu*, jos on olemassa sellainen äärellinen joukko $A \subseteq G$, että kaikki ryhmän G alkioita voidaan esittää muodossa

$$a_1 \circ a_2 \circ \cdots \circ a_n,$$

missä $a_i \in A$. Tällöin A on ryhmän G *generoiva joukko*. Jos ryhmän G generoivassa joukossa on vain yksi alkio g , niin g on ryhmän G *generaattori*. Tällöin jokaista alkioita $x \in G$ kohti on olemassa sellainen luku i , että $g^i = x$, ja G on *syklinen* ryhmä.

Olkoon G äärellinen syklinen ryhmä, jonka generaattorina on g . Pienin luku i , jolla $g^i = x$, on alkion x g -kantainen *diskreetti logaritmi*. Tässä sana ”diskreetti” korostaa tarkastellun ryhmän äärellisyyttä. Jos tämä selviää asianyhteydestä, voidaan puhua vain logaritmista. Syklisen ryhmän käsite on tärkeä kryptografiassa, sillä potenssiin korotus on laskennallisesti helppo, mutta sen käänteisoperaatio, (diskreetti) logaritmi, on vaikea. Syklinen ryhmä siis tarjoaa oivan alustan salausmenettelyn pohjaksi.

Jäännösluokkien joukko Z_n muodostaa (jäännösluokkien yhteenlaskun kanssa) syklinen ryhmän, jonka generaattorina on $\bar{1}$. Kokonaisluvut muodostavat äärettömän syklinen ryhmän Z . Tärkeä ryhmäteorian perustulos on, että äärellinen syklinen ryhmä, jonka kertaluku on n , on isomorfinen ryhmän Z_n kanssa. Äärellisiä syklisiä ryhmiä tutkittaessa voidaan siis rajoittua tarkastelemaan ryhmiä Z_n . Tämä ei kuitenkaan tarkoita, että ryhmässä Z_n toimivia nopeita algoritmeja voitaisiin suoraan soveltaa mihin tahansa äärelliseen syklisteen ryhmään, jonka kertaluku on n . Syynä tähän on, että kaikista syklisistä ryhmistä ei tiedetä helposti laskettavaa isomorfismia vastaavaan jäännösluokkaryhmään Z_n .

1.3 Kunnat

Kunta-aksiomat syntyvät luonnollisella tavalla, kun tarkastellaan rationaalilukujen ominaisuuksia.

Määritelmä 2. *Kunta on joukko K , jossa on määritelty kaksi operaatiota $+$ ja \cdot , jotka toteuttavat seuraavat aksiomat:*

1. $(K, +)$ on Abelin ryhmä, jossa on ykkösalkio 0.
2. $(K \setminus \{0\}, \cdot)$ on Abelin ryhmä, jossa on ykkösalkio 1.
3. Kaikilla alkioilla $x, y, z \in K$ pätee: $x \cdot (y + z) = x \cdot y + x \cdot z$.

Kunnasta käytetään merkintää $(K, +, \cdot)$. Ryhmä $(K, +)$ on kunnan K *additiivinen ryhmä* ja sitä merkitään K^+ :lla. Ryhmä $(K \setminus \{0\}, \cdot)$ on kunnan K *multiplikatiivinen ryhmä* ja sitä merkitään K^* :llä. *Äärellinen kunta* on kunta, jossa on äärellinen määrä alkioita. Kunnan *karakteristika* on pienin sellainen positiivinen kokonaisluku p , että

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

Äärettömän kunnan karakteristikaksi sovitaan 0.

Kunta $(K, +, \cdot)$ on kunnan $(L, +, \cdot)$ *alikunta*, jos $K \subseteq L$. Tällöin L on kunnan K *kuntalaaajennus*. Kunnan K *algebraallinen sulkeuma*, merkitään \bar{K} , on pienin mahdollinen K :n kuntalaaajennus, joka sisältää kaikkien K -kertoimisten polynomien juuret.

Seuraavassa on lueteltu muutama tärkeä tulos:

1. Jäännösluokkien joukko Z_p , missä p on alkuluku, muodostaa kunnan, kun laskutoimitukset määritellään normaalien yhteen- ja kertolaskun avulla:

$$\bar{n} + \bar{m} = \overline{n + m}, \quad \bar{n} \cdot \bar{m} = \overline{nm}.$$

2. Äärellisen kunnan K kertaluku on aina jokin alkuluvun potenssi, eli $|K| = p^n$. Lisäksi, jos kunnille K ja L pätee $|K| = |L|$, niin ne ovat isomorfiset. Jokaista lukua $q = p^n$ kohti on siis olemassa oleellisesti yksi kunta. Tästä käytetään merkintää F_q .
3. Yhtälö $x^q = x$ on voimassa jokaisella alkiolla $x \in F_q$.
4. Jokaisessa kunnassa on alkio g , joka generoi multiplikatiivisen ryhmän F_q^* . Tällöin g on kunnan F_q *primitiivinen alkio*, ja voidaan kirjoittaa

$$GF(q) = \{0, 1, g, g^2, \dots, g^{q-2}\}.$$

5. Ryhmä F_q^* , missä $q = p^n$, on isomorfinen ryhmän Z_{q-1} kanssa. Ryhmä F_q^+ on isomorfinen ryhmän

$$\underbrace{Z_p \oplus \cdots \oplus Z_p}_{n \text{ kpl}}$$

kanssa.

Kuntana F_p tarkastellaan yleensä jäännösluokkakuntaa Z_p . Kunta F_{p^n} , missä $n > 1$, konstruoidaan käyttäen Z_p -kertoimisten polynomien jäännösluokkia modulo jokin jaoton n -asteinen polynomi. (Katso esimerkiksi [1].) Kunnan F_{p^n} karakteristika on p .

1.4 Projektiivinen taso ja projektiivinen geometria

Tässä kappaleessa esitellään projektiivisen tason käsite. Jatkossa käyriä tarkastellaan lähinnä tutussa euklidisessa tasossa, mutta joissain kohdissa tieto projektiivisestä tasogeometriasta auttaa tulosten ymmärtämistä.

Tässä osiossa tarkastellaan vain reaalista projektiivista tasoa, jotta tuloksille voidaan antaa arki-intuiitiivinen tulkinta. Määrittely voidaan kuitenkin tehdä käyttäen mitä tahansa kuntaa.

1.4.1 Taustaa

Tutussa euklidisessa geometriassa äärettömyys aiheuttaa monenlaisia ongelmia ja monimutkaistaa tasokäyrien teoriaa. Tässä luvussa täydennetään euklidinen taso \mathbf{R}^2 ottamalla äärettömyydessä olevat pisteet mukaan tavallisina pisteinä. Näin päädytään tarkastelemaan ns. projektiivista tasoa ja projektiivista geometriaa.

Luonnollinen lähtökohta täydennykselle on Eukleideen paralleeliaksioma:

Suoran ulkopuolella olevan pisteen kautta kulkee täsmälleen yksi suora, jolla ei ole annetun suoran kanssa yhteisiä pisteitä.

Haluamme poistaa tutusta tasogeometriasta tämän epäsymmetrian, eli haluamme täsmälleen yhden leikkauspisteen kaikille suorapareille. Tasoon joudutaan täten lisäämään jokaista yhdensuuntaisten suorien joukkoa kohti yksi kuvitteellinen piste, jossa kyseiset suorat leikkaavat. Nämä uudet tason pisteet muodostavat ns. *suoran äärettömydessä*. Näin saatua täydennettyä tasoa kutsutaan *projektiiviseksi tasoksi*.

1.4.2 Homogeeniset koordinaatit

Seuraavaksi määritellään yksinkertainen matemaattinen malli projektiiviselle tasolle *homogeenisten koordinaattien* avulla.

Määritellään ensin avaruudessa \mathbf{R}^3 relaatio \sim :

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

jos ja vain jos

$$\exists a \in \mathbf{R} : (x_1, y_1, z_1) = (ax_2, ay_2, az_2).$$

Geometrisesti ajateltuna avaruuden \mathbf{R}^3 pisteet x ja y kuuluvat relaatioon \sim jos ja vain jos ne ovat samalla origon kautta kulkevalla suoralla. (Erikoistapauksena on origo, joka on relaatiossa vain itsensä kanssa. Tästä syystä origo jätetäänkin pois projektiivisen tason määrittelystä.)

Relaatio \sim on ekvivalenssirelaatio, joka jakaa avaruuden \mathbf{R}^3 ekvivalenssi-luokkiin. Reaalinen *projektiivinen taso*, merkitään $\mathbf{P}^2(\mathbf{R})$, voidaan nyt mää-

ritellä relaation \sim määrittämien nollasta eroavien ekvivalenssiluokkien joukkona. Lyhyemmin:

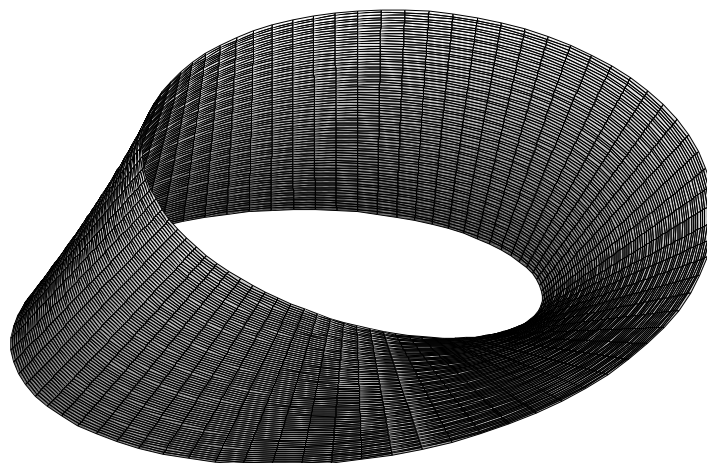
$$\mathbf{P}^2(\mathbf{R}) := (\mathbf{R}^3 \setminus \{\mathbf{0}\}) / \sim .$$

Projektiivisen tason mielivaltaista pistettä P voidaan merkitä reaalilukukolmikkoina (x, y, z) kunhan muistetaan, että mikä tahansa kolmikko (ax, ay, az) , missä $a \in \mathbf{R}$, myös kuvaa samaa pistettä. Ainoastaan lukujen x , y ja z keskinäisillä suhteilla on siis väliä, ja siksi projektiiviselle pisteelle käytetäänkin yleensä merkintää $(x : y : z)$. Tämä lukukolmikko muodostaa pisteen P *homogeeniset koordinaatit*.

1.4.3 Projektiivinen taso

Kuinka tämä määritelmä sitten vastaa alkuperäistä ideaa tutun \mathbf{R}^2 :n täydennyksestä? Merkitään $P_{z \neq 0}$:lla kaikkien projektiivisten pisteiden $(x : y : z)$ joukkoa joille $z \neq 0$. Kutakin $P_{z \neq 0}$:n pistettä vastaa yksikäsitteisesti reaalilukukolmikko $(x/z : y/z : 1)$. Näin saadaan bijektiivinen vastaavuus projektiivisille pisteille $P_{z \neq 0}$ ja tason \mathbf{R}^2 pisteille $(x/z, y/z)$. Sanotaan, että $P_{z \neq 0}$ on projektiivisen tason *affiini osa*. Jäljelle jääneet projektiiviset pisteet $P_{z=0}$, lukuunottamatta tapausta $y = 0$, eli pistettä $(1 : 0 : 0)$, voidaan esittää muodossa $(x/y : 1 : 0)$. Kyseessä on siis yksiulotteinen joukko, joka voidaan mieltää alkuperäisessä ideassa mainituksi ”suoraksi äärettömydessä”. Piste $(1 : 0 : 0)$ puolestaan voidaan mieltää äärettömydessä olevan suoran pisteeksi äärettömydessä.

Yksi tapa hahmottaa projektiivisen tason pisteet on tutun \mathbf{R}^3 :n origon kautta kulkevien suorien, joista on jätetty origo pois, joukkona. Yksi projektiivinen ”piste” onkin siis avaruuden $\mathbf{R}^3 \setminus \{\mathbf{0}\}$ suora. Tämä malli ei kuitenkaan vastaa intuitiivista käsitystä tasosta, joten haluaisimme löytää havainnollisemman yhteyden euklidisen tason ja projektiivisen tason välille. Merkitään edellä mainittua suorien joukkoa S :llä. Tällöin projektiivisen tason S ja euklidisen tason E välille saadaan yhteys asettamalla E avaruuteen \mathbf{R}^3 siten, että se ei kulje origon kautta. Nyt saadaan bijektio E :n pisteiden ja S :n pistei-

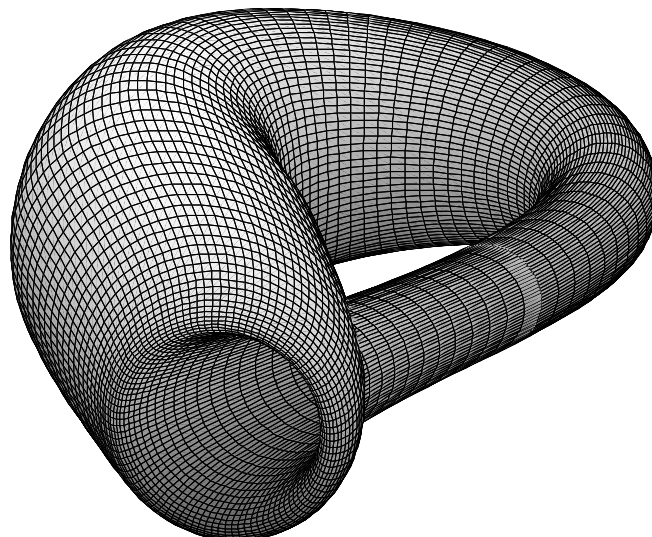


Kuva 1: Möbiuksen nauha.

den, jotka eivät ole E :n suuntaisia, välille: kutakin E :n pistettä e vastaa se S :n piste, joka leikkaa tasoa E pisteessä e . Ne S :n pisteet, jotka ovat tason E suuntaisia voidaan puolestaan mieltää pisteiksi tason E äärettömydessä.

Projektiivinen taso voidaan siis ajatella muodostetuksi ”kiertämällä” euklidinen taso äärettömyydessä ympäri joka suunnassa. Muodostunutta pintaa ei voida mallintaa sileäksi pinnaksi avaruudessa \mathbf{R}^3 , mutta avaruudessa \mathbf{R}^4 se onnistuu. Tällainen pinta on esimerkiksi Kleinin pullo. Se voidaan muodostaa sulkemalla Möbiuksen nauha, eli liittämällä sen reunaan yhtenäinen, sileä pinta (kuvat 1 ja 2).

Projektiivinen taso on luonnollinen ympäristö algebrallisten tasokäyrien (ks. kohta 2.1) tarkasteluun, koska äärettömyyteen lisätyt pisteet käyttäytyvät kuten mitkä tahansa muutkin pisteet. Tason \mathbf{R}^2 äärettömyyden aiheuttamat epäjatkuvuudet poistuvat, ja käyriä voidaan tutkia kokonaisina. Tason



Kuva 2: Kleinin pullo. Pinta on neliulotteinen, eikä oikeasti leikkaa itseään.

geometria ja tarkastelumenetelmät muuttuvat, kun siirrytään euklidisesta projektiiviseen tasoon.

Euklidinen geometria tutkii objektien ominaisuuksia, jotka säilyvät muuttumattomina *isometrioissa* eli pisteiden välimatkat säilyttävissä muunnoksissa. *Projektiivinen geometria* puolestaan tutkii ominaisuuksia, jotka säilyvät *projektiioissa*. Isometriat ovat projektioiden erikoistapauksia, joten projektiivisen geometrian tulokset voidaan siirtää euklidiseen geometriaan. Etäisyys ja kulma ovat esimerkkejä euklidisen geometrian ominaisuuksista, jotka eivät ole projektiivisiä, t.s. ne muuttuvat projektiioissa. Projektiivisiä ominaisuuksia ovat mm. leikkaavuus, tangenttisuus ja kaksoissuhde. (Oivia johdantoja projektiiviseen geometriaan ovat esimerkiksi [2] ja [3].)

2 Elliptiset käyrät

2.1 Määritelmä

Algebrallisella käyrällä yli kunnan K tarkoitetaan jonkin K -kertoimisen polynomin $f(x, y)$ määrittämää joukkoa

$$C_f = \{(x, y) \in \overline{K} \times \overline{K} \mid f(x, y) = 0\}.$$

Tässä polynomin $f(x, y)$ kertoimet ovat kunnassa K ja käyrän pisteiden koordinaatit ovat kunnan K algebrallisessa sulkeumassa \overline{K} . Tästä lähtien *käyrällä* tarkoitetaan nimenomaan algebrallista käyrää.

Esimerkiksi polynomin $f = x^2 + y^2 - 1$ määrittämä käyrä yli kunnan \mathbf{R} on niiden kompleksilukujen ($\overline{\mathbf{R}} = \mathbf{C}$) joukko, jotka toteuttavat yhtälön $x^2 + y^2 = 1$. Usein halutaan tutkia käyrän pisteitä, joiden koordinaatit ovat kunnassa $L \subseteq \overline{K}$. Tällaisia pisteitä voidaan merkitä $C_f(L)$, tai lyhyemmin $C(L)$, jos funktio f on selvä.

Käyrät C_f ja C_g ovat *isomorfsia*, merkitään $C_f \simeq C_g$, jos niiden pistejoukkojen välillä on olemassa bijektio. Isomorfiset käyrät ovat (algebrallisesti tarkasteltuna) rakenteeltaan samat.

Polynomin $f(x, y)$ määrittämä käyrä on *sileä* (tai *ei-singulaarinen*) jos osittaisderivaatat

$$D_x f(x, y), \quad D_y f(x, y)$$

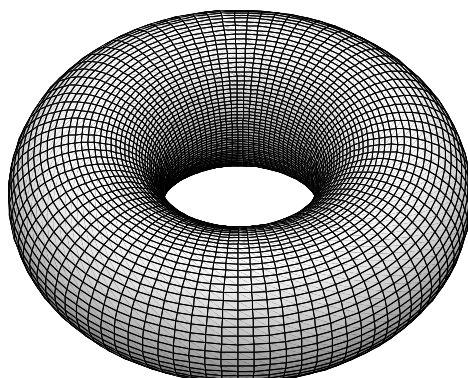
eivät samanaikaisesti häviä missään käyrän pisteessä. Intuitiivisesti tämä tarkoittaa, ettei käyrässä ole teräviä kärkiä, eikä se leikkaa itseään.

Käyrän *asteen* määrittely yleisessä tapauksessa on vaikeaa. Tässä työssä tarkastellaan lähinnä sileitä käyriä, jolloin käyrän asteeksi voidaan sopia määrittävän polynomin aste. Käyrän *suku* on positiivinen kokonaisluku, joka kuvaa sen topologista rakennetta. Jos tarkastellaan käyrien kompleksipistei-

tä, niin suku voidaan mieltää käyrässä olevien ”reikien” lukumääränä¹: suvun 0 käyrä on isomorfinen pallopinnan kanssa, suvun 1 käyrä on isomorfinen toruksen (pinnan) kanssa (kuva 3), ja vastaavasti suvun n käyrä on isomorfinen n -reikäisen suljetun pinnan kanssa. Sileän käyrän suvulle voidaan johtaa myös seuraava tulos:

Lause 4 (Plückerin kaava). *Sileän, astetta n olevan käyrän suku*

$$g = \frac{(n-1)(n-2)}{2}.$$



Kuva 3: Kompleksiset suvun 1 käyrät ovat isomorfisia toruksen (pinnan) kanssa.

Nyt voidaan määritellä elliptinen käyrä:

Määritelmä 3. *Elliptinen käyrä on sileä käyrä, jonka suku on 1.*

Elliptiset käyrät ovat siis merkittävä algebrallisten käyrien osajoukko, mikä selittääkin alan viimeaikaisen kehityksen ja runsaat sovelluskohteet. Nimi on

¹Tarkempi suvun määrittely löytyy esim. [4]:sta.

harhaanjohtava, sillä elliptisillä käyrillä ei ole käytännössä mitään tekemistä ellipsien kanssa. Syy outoon nimeen juontuu historiasta, sillä samanmuotoisia kolmannen asteen polynomeja (kohta 2.2) tutkittiin ensimmäisen kerran ellipsin kaarenpituutta laskettaessa.

2.2 Weierstrassin normaalimuoto

Elliptisiä käyriä voidaan kuvata hyvinkin erilaisten ja eriasteisten yhtälöiden avulla. Esimerkiksi yhtälöt

$$E_1 : x^4 + y^4 = 1, \quad E_2 : x^3 + y^3 = 1, \quad E_3 : y^2 = x^3 + 4x$$

kuvaavat kaikki elliptisiä käyriä. Sijoittamalla yhtälöön E_1 rationaalinen muunnos

$$x = \frac{v-2}{v+2}, \quad y^2 = \frac{4u}{(v+2)^2}$$

saadaan se kuitenkin alempiasteiseen muotoon E_3 . Tämä muunnos määrittää käyrien E_1 ja E_3 välille *bijektiivisen rationaalikuvauksen* eli *birationaalisen kuvauksen*. On osoitettavissa, että tällainen kuvaus ei muuta käyrän algebrallista rakennetta. Tällöin käyrät ovat *birationaalisesti ekvivalentit*.

Jos kerroinkunnan karakteristika ei ole 2 tai 3, elliptisen käyrän määrittävä yhtälö voidaan (birationaalisella muunnoksella) saattaa muotoon

$$y^2 = x^3 + ax + b. \quad (2)$$

Tämä on elliptisen käyrän *Weierstrassin normaalimuoto*. Olkoot r_1, r_2 ja r_3 polynomin $f(x) = x^3 + ax + b$ juuret. Jotta yhtälön (2) määräämä käyrä olisi sileä, on polynomin $f(x)$ diskriminantin

$$((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4a^3 + 27b^2)$$

oltava nollasta poikkeava. Kerrointen a ja b on siis toteutettava ehto

$$4a^3 + 27b^2 \neq 0.$$

Elliptisestä käyrästä, jonka koordinaatit ovat kunnassa K , käytetään merkintää $E(K)$.

2.2.1 Muita muotoja

Jos kerroinkunnan karakteristika on 3, voidaan elliptisen käyrän yhtälö saattaa muotoon

$$y^2 = x^3 + ax^2 + bx + c.$$

Karakteristikan 2 tapauksessa yhtälö saadaan joko *ylisingulaariseen*² muotoon

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

tai *ei-ylisingulaariseen* muotoon

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

Jos kerroinkunta K on algebrallisesti suljettu, voidaan elliptisen käyrän $E(K)$ yhtälö saattaa *Legendren* muotoon

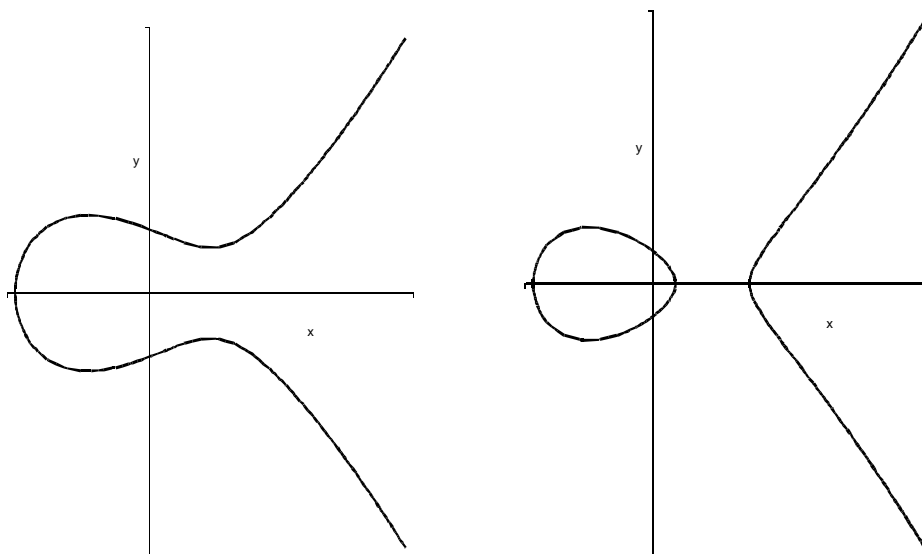
$$y^2 = x(x - 1)(x - \lambda).$$

Tässä tapauksessa elliptiset käyrät saadaan esitettyä yhden parametrin avulla. Jatkossa algebrallisissa tarkasteluissa käytetään vain Weierstrassin normaalimuotoa. Muille muodoille johdetut tulokset ovat samankaltaisia.

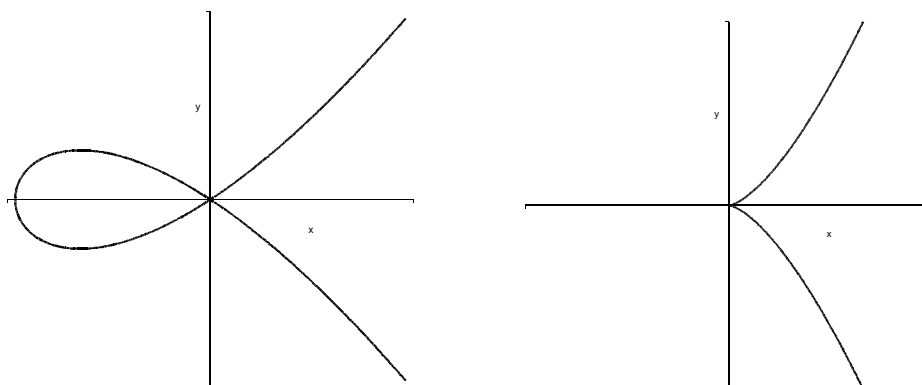
2.2.2 Geometrisia tarkasteluja

Katsotaan vielä miltä elliptiset käyrät $E(\mathbf{R})$ näyttävät. (Jos koordinaattikuntana on jokin muu kuin \mathbf{R} , on mielekkään kuvan piirtäminen vaikeaa.) Olkoon tarkasteltavan käyrän yhtälö $y^2 = f(x)$. Kuvaajia on kahta tyyppiä: polynomilla $f(x)$ on joko yksi tai kolme reaaliuurta (kuva 4). Jos juuria on kolme, ovat ne kaikki erisuuria, sillä muutoin käyrä ei olisi sileä (kuva 5).

²Nimitys johtuu tällaisten käyrien erikoisominaisuuksista. Ylisingulaariset käyrät on havaittu kryptografisesti heikoiksi, sillä niissä diskreetti logaritmi voidaan ratkaista nopeasti. Nimityksellä ei ole yhteyttä käyrän singulaarisuuteen tai sen singulaarisiin pisteisiin.



Kuva 4: Elliptisellä käyrällä on joko yksi tai kolme reaalijuurta.



Kuva 5: Jos käyrällä on kaksin- tai kolminkertainen juuri, se ei ole sileä.

Todetaan vielä tärkeä tulos, joka tukee kuvan 4 antamaa intuitiivista havaintoa. (Käyrän haarojen ajatellaan kohtaavan y -akselin äärettömyydessä ideaalipisteessä O .) Merkitään yksikköympyrää symbolilla S^1 .

Lause 5. *Olkoon E elliptinen käyrä, jonka koordinaattikuntana on \mathbf{R} . Tällöin*

$$E \simeq S^1 \quad \text{tai} \quad E \simeq S^1 \oplus Z_2.$$

Reaalitasossa tarkasteltuna elliptinen käyrä on siis isomorfinen yhden tai kahden ympyrän kanssa.

2.3 Käyrän projektiivinen sulkeuma

Polynomi $F(x_1, \dots, x_n)$ on *homogeeninen*, jos kaikki siinä esiintyvät termit ovat samaa astetta. Esimerkiksi polynomit

$$x^5 + xy^4, \quad 2x - 3y \quad \text{ja} \quad x^4 + xyzw + w^4$$

ovat homogeenisia. Jotta olisi mielekästä tutkia polynomin $F(x, y, z)$ määrittämää käyrää projektiivisessä tasossa, on sen oltava homogeeninen. Tämä johtuu homogeenisista koordinaateista: jos pisteen homogeeniset koordinaatit $(x : y : z)$ toteuttavat yhtälön $F(x, y, z) = 0$, niin myös yhtälön $F(ax, ay, az) = 0$ on toteuduttava kaikilla parametrin $a \in \mathbf{R}$ arvoilla. Tämä johtaa vaatimukseen, että F on homogeeninen.

Tarkastellaan projektiivista käyrää³ $F(X, Y, Z) = 0$. Tämän käyrän *affiini osa* on se osa käyrää, jossa $Z \neq 0$. Rajoittumalla affiniin osaan voidaan yhtälö jakaa termillä Z^d , missä d on polynomin F aste, jolloin se saadaan muotoon

$$\frac{F(X, Y, Z)}{Z^d} = 0 \Leftrightarrow F(X/Z, Y/Z, 1) = 0.$$

Merkitseillä $x = X/Z$ ja $y = Y/Z$ voidaan affiinin osan yhtälö kirjoittaa kahden (ei-homogeenisen) koordinaatin avulla: $f(x, y) = 0$. Esimerkiksi projektiivisen käyrän $X^2 - YZ + Z^2 = 0$ affiini osa on (affiini) käyrä $x^2 - y + 1 = 0$.

³Muuttujia merkitään tässä isoilla kirjaimilla, mikäli tarkastelu on projektiivista.

Vastaavasti voidaan muodostaa affiinin käyrän *projektiivinen sulkeuma* kääntämällä ylläoleva prosessi. Affiinin käyrän $f(x, y) = 0$ projektiivisen sulkeuman yhtälöksi saadaan siis

$$Z^d f(X/Z, Y/Z) = 0 \quad \Leftrightarrow \quad F(X, Y, Z) = 0.$$

Yleensä elliptisiä käyriä tarkastellaan affiinilla tasolla, mutta joissain tilanteissa on hyödyllistä siirtyä projektiiviselle tasolle. Weierstrassin normaali muodossa olevan elliptisen käyrän projektiivinen sulkeuma on muotoa

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Tutkitaan tämän käyrän pisteitä ”äärettömydessä”, toisin sanoen pisteitä, joille $Z = 0$. Yhtälöstä nähdään, että vain piste $(0 : 1 : 0)$ toteuttaa tämän ehdon. Siirryttäessä takaisin affiinille tasolle tämä piste voidaan ajatella y -akselin äärettömyyteen siten, että sitä voidaan lähestyä sekä positiiviselta että negatiiviselta suunnalta. Akselin päät siis ajatellaan kierretyksi yhteen äärettömydessä. On tärkeää ottaa tämä piste mukaan myös affiinilla tasolla tapahtuvaan tarkasteluun erikseen määriteltynä ideaalipisteenä, sillä se mahdollistaa yksinkertaisen ryhmäoperaation määrittelyn elliptisen käyrän pisteille. Esimerkkinä projektiivisen tarkastelun eduista on ryhmäoperaation liitännäisyyden todistus kohdassa 2.6.

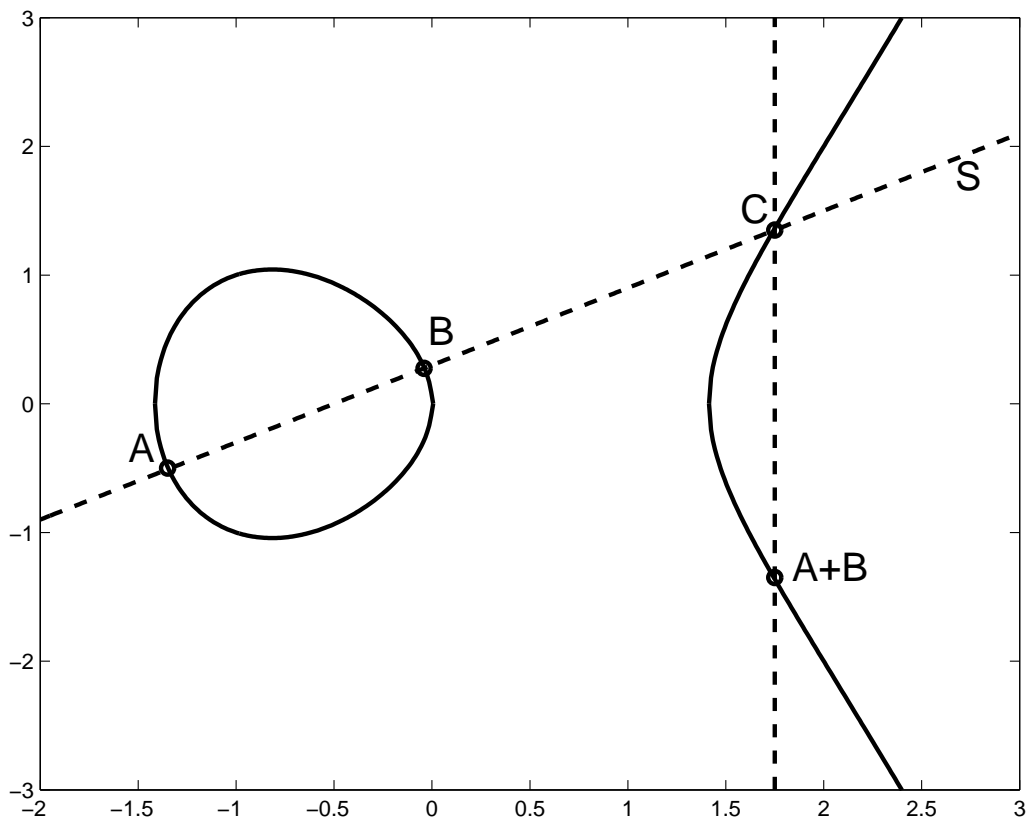
2.4 Ryhmäoperaatio

Määritellään seuraavaksi yhteenlasku elliptisen käyrän pisteille. Tämän yhteenlaskun kanssa pisteet muodostavat Abelin ryhmän, joka on osoittautunut ominaisuuksiltaan hyvin käyttökelpoiseksi kryptografiassa. Määrittely perustuu geometriseen havaintoon \mathbf{R}^2 :ssa. Saadut laskukaavat voidaan yleistää muidenkin kuntien yli määritelyihin käyriin⁴.

⁴Karakteristikan 2 ja 3 kunnat on käsiteltävä erikseen, mutta saadut tulokset ovat samankaltaisia. [5]

Täydennetään elliptisen käyrän reaali pisteitä ideaalisella ”pisteellä äärettömydessä”, jota merkitään symbolilla O . Ajatellaan piste O y -akselin äärettömyyteen ja sovitaan, että kaikki y -akselin suuntaiset suorat leikkaavat käyrää tässä ideaalipisteessä.

Elliptisen käyrän pisteiden A ja B summa $A + B$ muodostetaan seuraavasti: Olkoon S pisteiden A ja B kautta kulkevaa suora ja olkoon C kolmas piste, jossa S leikkaa käyrää. Summa $A + B$ on pisteen C peilikuva x -akselin suhteen (kuva 6).



Kuva 6: pisteiden A ja B yhteenlasku

Mahdolliset erikoistapaukset hoidetaan seuraavasti:

1. $A = B$: Tällöin S on käyrän tangentti kyseisessä pisteessä. Sileän käyrän tangentti on yksikäsitteinen, joten tämä ei tuota ongelmia.
2. S on y -akselin suuntainen: Tällöin katsotaan, pisteen O määritelmän mukaisesti), että S leikkaa käyrää pisteessä O , joten $A + B = O$.
3. $A \neq B$ ja S sivuaa käyrää pisteessä A : Käyrän tangentilla katsotaan olevan *kaksinkertainen leikkauspiste* tangentialpisteessä. Siis $C = A$ ja $A + B$ on pisteen A peilikuva x -akselin suhteen.

Määritelmästä huomataan, että kaikilla pisteillä A pätee $O + A = A$, eli O on ryhmän neutraalialkio. Myös käänteisalkion muodostaminen on helppoa, sillä

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

Geometrisesta määritelmästä on helppo intuitiivisesti nähdä operaation vaihdannaisuus, neutraalialkio sekä käänteisalkion olemassaolo jokaiselle pisteelle. Liitännäisyyden todistaminen onkin jo vaikeampaa, ja tarkastelu kannattaa tehdä projektiivisella tasolla. Asiaa käsitellään erikseen kohdassa 2.6. Käyrän E pisteet muodostavat siis tämän operaation kanssa Abelin ryhmän.

Tarkastellaan yhteenlaskua vielä algebrallisesti. Olkoon tarkastellun käyrän E yhtälö

$$Y^2 = X^3 + e_1X + e_2.$$

Merkitsemällä $A = (x_1, y_1)$, $B = (x_2, y_2)$ voidaan summalle $A + B = (x_3, y_3)$ johtaa seuraava tulos:

1. Jos $x_1 \neq x_2$, niin

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

2. Jos $x_1 = x_2$ ja $y_1 \neq y_2$, niin $A + B = O$.

3. Jos $A = B$ ja $y_1 \neq 0$, niin

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{missä } m = \frac{3x_1^2 + e_1}{2y_1}.$$

4. Jos $A = B$ ja $y_1 = 0$, niin $A + B = O$.

Tulos pätee myös tarkastelukunnan ollessa äärellinen, joskin karakteristikan ollessa 2 tai 3 kaavoista saadaan hieman erilaiset.

Summalle $P + P = 2P$ saadaan yksinkertainen kaava, jolla

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ kpl}}$$

voidaan laskea nopeasti käyttäen toistuvan neliöinnin algoritmia⁵. Toisaalta, jos tiedetään vain pisteet P ja nP , on luvun n laskeminen hyvin vaikeaa. Tämä on siis elliptisten käyrien *diskreetin logaritmin* ongelma, jota voidaan käyttää kryptosysteemin pohjana.

2.5 Äärellisten kuntien yli määritellyistä käyristä

Jos käyrän koordinaattikunta on äärellinen, on intuitiivisen mielikuvan muodostaminen käyrästä vaikeaa. Yllä johdetut yhteenlaskukaavat voidaan kuitenkin johtaa algebrallisesti myös koordinaattikunnan ollessa äärellinen. Ainoana poikkeuksena ovat karakteristikan 2 ja 3 kunnat, joille yhteenlaskukaavat ovat hieman erilaiset.

Todetaan seuraavaksi tärkeä tulos äärellisen kunnan yli määritellyistä elliptisistä käyristä:

Lause 6 (Hassen lause). *Olkoon E äärellisen kunnan F_q yli määritelty elliptinen käyrä. Tällöin ryhmän $E(F_q)$ alkoiden lukumäärä N toteuttaa ehdon*

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}.$$

⁵Elliptisten käyrien tapauksessa ryhmäoperaatiota merkitään yhteenlaskumerkillä, joten neliöinti tarkoittaa tässä luvulla 2 kertomista.

Lauseen mukaan käyrän $E(K)$ alkioden lukumäärä on lähellä kerroin-kunnan K alkioden lukumäärää. Tämä arvio on myös paras mahdollinen siinä mielessä, että jokaista lauseen antaman välin kokonaislukua N kohti on olemassa elliptinen käyrä E , jolle $|E(F_q)| = N$. Tulokseen perustuu mm. kryptografisesti tärkeä Schoofin algoritmi, jolla lasketaan satunnaisen käyrän alkioden lukumäärä. Tästä enemmän kohdassa 4.3.4.

Seuraava tärkeä tulos kuvaa elliptisen käyrän rakennetta, kun koordinaat-tikunta on äärellinen.

Lause 7. *Ryhmä $E(F_q)$ on isomorfinen ryhmän Z_n tai $Z_{n_1} \oplus Z_{n_2}$ kanssa. Tässä luvut n , n_1 ja n_2 riippuvat ryhmästä F_q , ja lisäksi $n_1|n_2$.*

Lisäksi voidaan osoittaa, että tapaus

$$E(F_q) \simeq Z_n \oplus Z_n$$

on harvinainen. Tavallisesti $E(F_q)$ on siis syklinen, tai ainakin sisältää ison syklisen aliryhmän.

2.6 Liitännäisyyden todistus

Tässä kappaleessa todistetaan edellä määritellyn elliptisen käyrän pisteiden yhteenlaskun liitännäisyys. Todistuksessa esitettyjä tuloksia ei tarvita muu-alla tässä työssä, mistä syystä kappaleen voi sivuuttaa luettavuuden siitä kärsimättä.

Todistuksella havainnollistetaan projektiivisen tarkastelun tuomia etuja: käyrien yhtälöt ovat homogeenisia ja äärettömydessä olevat leikkauspisteet voidaan ottaa luonnollisella tavalla mukaan tarkasteluun. Tilan säästämi-seksi ja luettavuuden parantamiseksi on käytetty paikoin yksinkertaistettua esitystapaa. Hieman yksityiskohtaisempi esitys löytyy esimerkiksi lähteestä

[6]. (Todistus voidaan tehdä myös jollain sopivalla ohjelmistolla symbolisesti. Tämä lähestymistapa tosin on liian työläs paperilla esitettäväksi.)

2.6.1 Perustuloksia

Kohdassa 1.4 esitellyn reaalisen projektiivisen tason määritelmä voidaan yleistää mille tahansa kunnalle K . Projektiivinen taso yli kunnan K on siis joukko

$$\{(X, Y, Z) \in K^3 \mid (X, Y, Z) \neq (0, 0, 0)\},$$

jossa kolmikot (X_1, Y_1, Z_1) ja (X_2, Y_2, Z_2) samaistetaan, mikäli on olemassa sellainen $a \in K$, että

$$(X_1, Y_1, Z_1) = (aX_2, aY_2, aZ_2).$$

Projektiivisestä pisteestä käytetään merkintää $(X : Y : Z)$.

Affinin tason suoraa $ax + by + c = 0$ vastaavaa projektiivista suoraa kuvataan homogeenisellä yhtälöllä

$$aX + bY + cZ = 0.$$

Suora voidaan parametrisoida, eli esittää yhden projektiivisen parametrin $(U : V)$ avulla:

$$\begin{cases} X = a_1U + b_1V \\ Y = a_2U + b_2V \\ Z = a_3U + b_3V \end{cases} \quad (3)$$

Olkoon

$$k_1 : C(X, Y, Z) = 0$$

jokin astetta $n \geq 1$ olevan käyrän yhtälö. Parametrisoidun suoran (3) ja käyrän k_1 leikkauspisteet saadaan yhtälön

$$\tilde{C}(U, V) = 0$$

ratkaisuina, missä $\tilde{C}(U, V)$ saadaan sijoittamalla (3) polynomiin $C(X, Y, Z)$. Tästä nähdään, että mikäli koordinaattikunta K on algebrallisesti suljettu, on jokaisella suoralla tarkalleen n leikkauspistettä astetta n olevan käyrän kanssa. (On huomattava, että suoran ja käyrän leikkauspiste voi olla *moninkertainen*. Leikkauspisteiden lukumäärää laskettaessa on n -kertainen leikkauspiste laskettava n :ksi pisteeksi.) Jos kunta K ei ole algebrallisesti suljettu, leikkauspisteiden lukumäärä voi olla vähemmän kuin n . Elliptisen käyrän pisteiden yhteenlaskun määritelmän perusteella voidaan olettaa, että tarkastelluilla suorilla on aina täysi määrä leikkauspisteitä annetun elliptisen käyrän kanssa. Nimittäin, jos suoralla S ja elliptisellä käyrällä $E(K)$ on kaksi leikkauspistettä kunnassa K , niin niillä on myös kolmas leikkauspiste kunnassa K .

Todetaan vielä todistuksetta eräs perustulos:

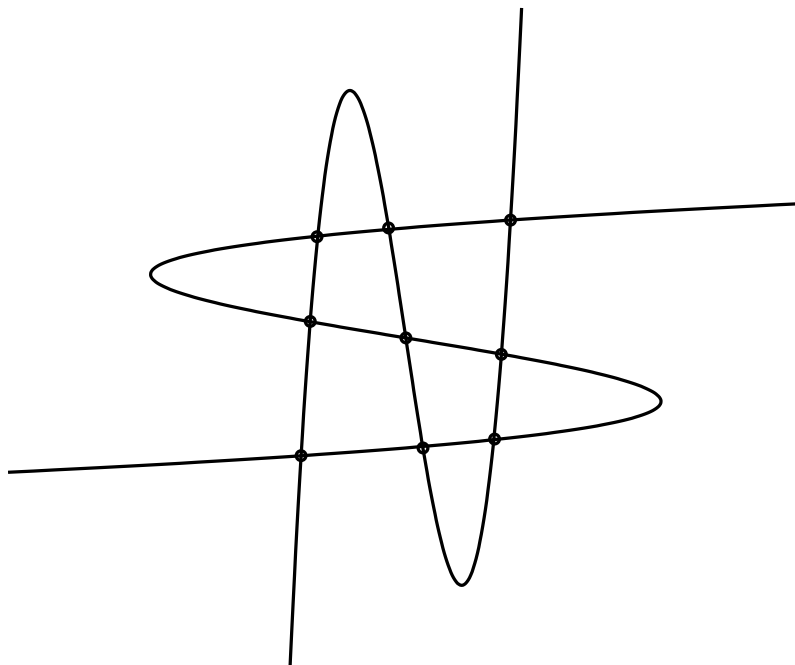
Lause 8. *Kahdella kolmannen asteen käyrällä on, moninkertaiset leikkauspistepöet mukaanlukien, korkeintaan yhdeksän leikkauspistettä. Jos koordinaattikunta on algebrallisesti suljettu, niin leikkauspisteitä on tarkalleen yhdeksän (kuva 7).*

2.6.2 Todistus

Ensin todistetaan tärkeä projektiivisen geometrian lause, minkä jälkeen liitännäisyyden toteaminen on helppoa.

Lause 9. *Olkoön E elliptinen käyrä, jota kaksi suoraa a ja b leikkaavat pisteissä A_1, A_2, A_3 ja B_1, B_2, B_3 , vastaavasti. Oletetaan lisäksi, että $A_i \neq B_j$ kaikilla indeksien i ja j arvoilla. Tällöin suorien $\overline{A_1B_1}, \overline{A_2B_2}, \overline{A_3B_3}$ kolmannet leikkauspisteet C_1, C_2 ja C_3 ovat samalla suoralla c (kuva 8).*

Todistus. Kolmen suoran



Kuva 7: Kaksi kolmannen asteen käyrää leikkaa toisiaan (korkeintaan) yhdeksässä pisteessä.

$$\overline{A_1B_1} : F_1(X, Y, Z) = 0$$

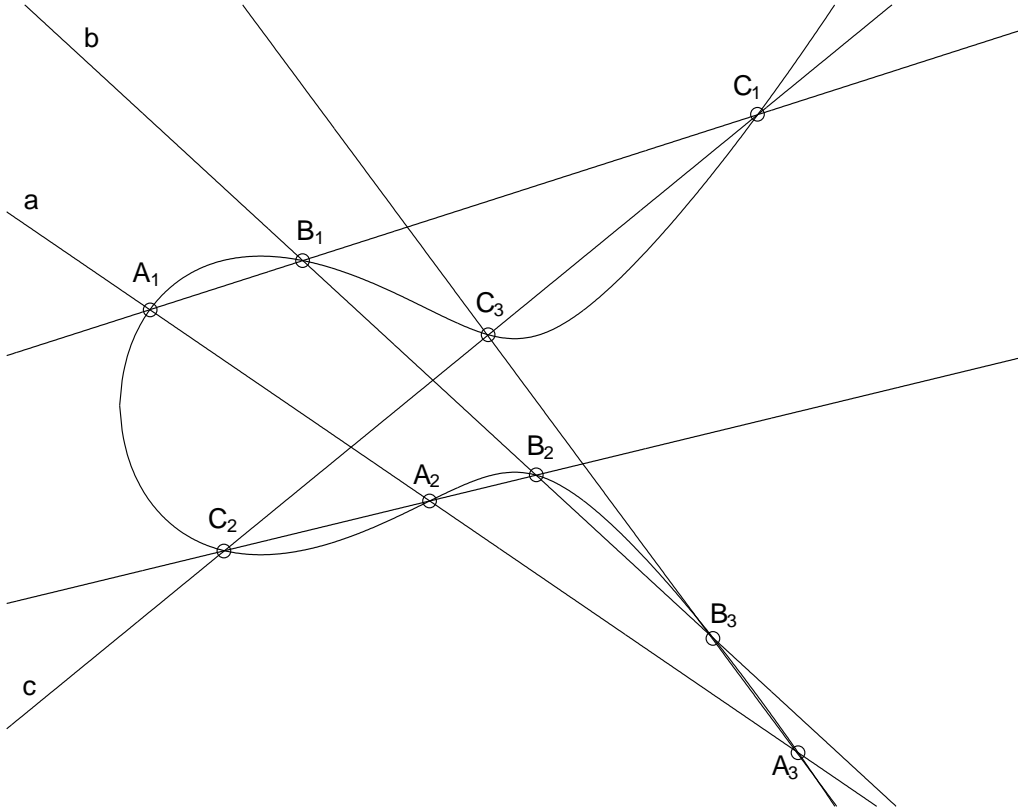
$$\overline{A_2B_2} : F_2(X, Y, Z) = 0$$

$$\overline{A_3B_3} : F_3(X, Y, Z) = 0$$

voidaan ajatella muodostavan *hajonneen* kolmannen asteen käyrän

$$S_1 : F_1(X, Y, Z)F_2(X, Y, Z)F_3(X, Y, Z) = 0.$$

Käyrien S_1 ja E yhteiset pisteet ovat (määritelmän mukaan) tarkalleen pisteet A_i , B_i ja C_i , missä $i \in \{1, 2, 3\}$.



Kuva 8: Kahden suoran a ja b leikkauspisteiden A_i ja B_i kautta kulkevien suorien kolmannet leikkauspisteet ovat samalla suoralla c .

Olkoon $C(X, Y, Z) = 0$ käyrää E kuvaava yhtälö. Tällöin käyrät E ja S määräävät käyräparven

$$C(X, Y, Z) + \lambda F_1(X, Y, Z)F_2(X, Y, Z)F_3(X, Y, Z) = 0,$$

jonka käyrät kulkevat kaikilla parametrin λ arvoilla käyrien E ja S yhdeksän leikkauspisteen kautta. Tähän parveen kuuluu myös se hajonnut kolmannen asteen käyrä S_2 , johon suorat a ja b kuuluvat. Käyrään S_2 kuuluu siis vielä jokin kolmas suora c . Koska S_2 kulkee myös pisteiden C_1 , C_2 ja C_3 kautta, eikä kolmannen asteen käyrillä voi olla yli yhdeksää leikkauspistettä, on pisteiden C_1 , C_2 ja C_3 oltava suoralla c . \square

Olkoon P_1 , P_2 ja P_3 pisteitä elliptisellä käyrällä. Liitännäisyys voidaan nyt todeta valitsemalla (Lauseen 9 merkinnöin)

$$A_1 = P_2, \quad A_2 = -(P_2 + P_3), \quad B_1 = -(P_1 + P_2), \quad B_2 = O.$$

Tällöin Lauseessa 9 mainittujen suorien leikkauspisteet käyrän E kanssa ovat seuraavan taulukon mukaiset.

| | $\overline{A_1B_1}$ | $\overline{A_2B_2}$ | $\overline{A_3B_3}$ |
|-----|---------------------|---------------------|---------------------|
| a | P_2 | $-(P_2 + P_3)$ | P_3 |
| b | $-(P_1 + P_2)$ | O | $P_1 + P_2$ |
| c | P_1 | $P_2 + P_3$ | X |

Jos $A_i = B_j$, niin pisteiden P_1 , P_2 ja P_3 liitännäisyys nähdään helposti. Tarkastellaan esimerkiksi tapausta $A_1 = B_2$. Tällöin $P_2 = O$, joten

$$\begin{aligned} (P_1 + P_2) + P_3 &= (P_1 + O) + P_3 \\ &= P_1 + P_3 \\ &= P_1 + (O + P_2) \\ &= P_1 + (P_2 + P_3). \end{aligned}$$

Voidaan siis olettaa, että $A_i \neq B_j$. Nyt Lauseen 9 mukaan piste X , joka on siis suoran $\overline{A_3B_3}$ ja käyrän E kolmas leikkauspiste, on oltava myös suoralla c . Yhteenlaskun määritelmän mukaan, tarkastelemalla suoraa c , saadaan

$$X = -(P_1 + (P_2 + P_3))$$

ja toisaalta tarkastelemalla suoraa $\overline{A_3B_3}$ saadaan

$$X = -((P_1 + P_2) + P_3).$$

Joten

$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3). \quad \square$$

3 Kryptologiaa

3.1 Taustaa

Varhaisimmat merkit järjestäytyneestä tiedon salauksesta ovat noin vuodelta 500 ekr., jolloin spartalaiset sotilaat keksivät ns. *skytale*-salausjärjestelmän. Siinä viesti salataan seuraavasti:

Keritään kapea nauha (papyrussuikale) tasapaksun kepin ympärille siten, että nauha peittää yksinkertaisesti kepin pinnan. Sen jälkeen kirjoitetaan viesti nauhalle kepin pituussuunnassa kirjoittaen. Tarvittaessa lisätään viestiin turhaa tekstiä, että koko nauha saadaan täyteen.

Kun nauha avataan kepin ympäriltä, siinä olevat kirjaimet vaikuttavat satunnaisilta. Salattu teksti puretaan kietomalla nauha uudestaan saman paksuisen kepin ympärille.

Aina toiseen maailmansotaan saakka salausmenetelmät pysyivät hyvin yksinkertaisina. Koneiden, etenkin tietokoneiden, kehitys 1900-luvulla antoi tehokkaita työkaluja salausmenetelmien toteuttamiseen ja toisaalta myös niiden murtamiseen. Niinpä lähes kaikki salaukseen liittyvä teoria on kehitetty viimeisten muutaman kymmenen vuoden aikana. Aiemmin (sivulla 1) mainittu julkisen avaimen kryptausperiaatteen keksiminen vuonna 1976 on ollut isoin yksittäinen kehitysaskel kryptografiassa.

Mielenkiintoinen lähtökohta kryptosysteemien tarkasteluun on ns. *kertaavainsalaus*. Systemin salaus- ja purkuavaimena on satunnainen M -pituihin bittivektori. Viestilohko, joka on myös M -pituihin bittivektori, salataan lisäämällä siihen avainvektori modulo 2. Purku tapahtuu samalla tavalla. Systemi tarjoaa parhaan mahdollisen salauksen, sillä salattu viestivektori on täysin satunnainen, eikä sitä ole mahdollista purkaa ilman salaista avainta.

Kuten nimikin vihjaa, systeemin vahvuus syntyy siitä, että kutakin avainta käytetään vain kerran. Jos samaa avainta käytetään monesti, on salaus mahdollista purkaa. Menettely on tästä syystä epäkäytännöllinen, mutta on turvallisuutensa takia käyttökelpoinen joissain pienissä, todella tärkeissä tehtävissä.

3.2 Perusteita

Tiedon salauksella eli *kryptauksella* tarkoitetaan sen muuttamista muotoon, josta asiaankuulumattoman on vaikea saada viestiä selville, mutta jonka viestin kohde pystyy helposti *purkamaan*. Käytettyä salausmenetelmää sanotaan *kryptosysteemiksi*. Sen tärkeimmät parametrit ovat *salausavain* ja *purkuavain*, joilla salausmenettelyä voidaan muuttaa kryptosysteemin sallimissa rajoissa. Jos salaus- ja purkuavaimet ovat samat, tai ainakin helposti saatavissa toisistaan, niin puhutaan *symmetrisestä* tai *salaisen avaimen* kryptosysteemistä. Tällaisen systeemin molemmat avaimet joudutaan pitämään salassa. Jos salausavaimesta on vaikea saada selville purkuavainta, on kyseessä *epäsymmetrinen* kryptosysteemi. Tällöin salausavain voidaan julkistaa, ja puhutaan myös *julkisen avaimen* kryptosysteemistä.

Viestiä voidaan salata jatkuvana virtana sitä mukaa kun viestiä luetaan (*vuosalaus*) tai tietyn mittaisina lohkoina (*lohkosalaus*). Jatkossa tarkastellaan vain lohkosalausta. Yhden lohkon sisältämä symbolijono on helppo muuttaa yksikäsitteisellä muunnoksella matemaattiseksi objektiksi. Tässä työssä viestilohkon oletetaan olevan kokonaisluku, äärellisen kunnan alkio, jäännösluokka tai elliptisen käyrän piste, riippuen kryptosysteemistä.

Tiedonsiirrossa salaisen avaimen kryptosysteemit ovat selvästi tehokkaampia, mutta avainten kommunikointi joudutaan lähes aina tekemään julkisen kanavan kautta. Tietoverkkojen laajentuessa tarve tehokkaille ja turvallisille julkisen avaimen kryptosysteemeille on kasvanut. Tässä työssä tarkastellaan vain julkisen avaimen kryptosysteemejä.

Tärkeimmät kryptosysteemin määrittelyssä käytetyt parametrit ovat:

julkinen avain k_1 ,
 salainen avain k_2 ,
 salaustfunktio S_{k_1} ,
 purkufunktio P_{k_2} .

Salaus- ja purkufunktioiden alaindeksit viittaavat niiden riippuvuuteen avaimista k_1 ja k_2 . Salaamatonta viestilohkoa merkitään kirjaimella w ja salattua kirjaimella c .

Julkisen avaimen kryptosysteemi perustuu ns. *yksisuuntaisen operaation* hyödyntämiseen. Tällä tarkoitetaan helppoa operaatiota, jolla on vaikeasti laskettava käänteisoperaatio. Alkulukujen kertolasku on esimerkki helposta operaatiosta, jolla on vaikea käänteisoperaatio, tekijöihinjako. Systeemin perusajatuksena on julkaista k_1 ja S_{k_1} , joiden avulla kuka tahansa voi salata viestin ja lähettää sen julkista kanavaa pitkin salaisen avaimen haltijalle. Salauksen purkaminen vaatii joko vaikean käänteisoperaation laskemisen tai salaisen avaimen. Käänteisoperaation on siis oltava niin vaikea, ettei sitä pystytä nykyisillä resursseilla ratkaisemaan.

3.3 RSA

RSA⁶ lienee käytetyin epäsymmetrinen kryptosysteemi. Sen käyttämä yksisuuntainen operaatio on alkulukujen kertolasku, jonka käänteisoperaatio, tekijöihinjako, on vaikea.

⁶Nimi on lyhenne systeemin keksijöiden Ronald Rivest, Adi Shamir ja Leonard Adleman sukunimistä.

RSA:n salainen avain k_2 muodostuu kahdesta suunnilleen saman pituudesta alkuluvusta p ja q sekä luvusta b , jolle

$$\text{syt}(b, \phi(pq)) = 1. \quad (4)$$

Julkinen avain k_1 puolestaan muodostuu luvuista $n (= pq)$ ja a , joilla

$$ab \equiv 1 \pmod{\phi(n)}. \quad (5)$$

Ehto (4) takaa, että luvun b käänteisalkio modulo n , eli ehdon (5) täyttävä a on olemassa.

Viestilohko w esitetään kokonaislukuna välillä $0 \leq w \leq n - 1$. Salaus- ja purkufunktiot ovat

$$S_{k_1}(w) = w^a \pmod{n}, \quad P_{k_2}(c) = c^b \pmod{n}.$$

Todetaan vielä, että salaus toimii:

$$P_{k_2}(c) = P_{k_2}(w^a) = (w^a)^b = w^{ab} = w^{k\phi(n)+1} = w \pmod{n}$$

kohdan (5) ja Eulerin lauseen (s. 3) perusteella.

Tästä nähdään, että jos luvun n tekijät tunnetaan, on systeemin murtaminen helppoa. Luku $\phi(n)$ voidaan tällöin laskea helposti, jonka jälkeen b , eli luvun a inverssi mod $\phi(n)$, on myös helposti laskettavissa. Näyttää siltä, että RSA:n murtaminen olisi mahdotonta ilman luvun n tekijöihinjakoa, mutta tätä ei ole onnistuttu todistamaan.

3.4 Diskreettiin logaritmiin perustuvat systeemit

Suurin osa diskreettiin logaritmiin perustuvista kryptosysteemeistä käyttävät joko Diffie-Hellman- tai ElGamal -tyyppistä salausmenettelyä, mistä syystä tarkastelu rajoitetaan niihin. Kummankin menettelyn murtaminen vaatii (oletetusti) samanlaisen diskreetin logaritmin ratkaisemista, joten niitä voidaan pitää yhtä turvallisina.

Molemmissä menettelyissä keksijöiden alkuperäinen ehdotus sykliseksi ryhmäksi oli F_q^* . ElGamal- tai Diffie-Hellman-kryptosysteemistä puhuttaessa tarkoitetaan nimenomaan ryhmään F_q^* perustuvaa systeemiä. Menettelyt sallivat kuitenkin muunkinlaisten syklisten ryhmien käyttämisen. Tällöin kryptosysteemi nimetään käytetyn ryhmän mukaan. Esimerkiksi XTR-kryptosysteemillä tarkoitetaan jotain diskreettiin logaritmiin perustuvaa systeemiä, jonka syklisenä ryhmänä käytetään XTR-aliryhmää (kohta 3.4.3).

3.4.1 Diffie-Hellman-avainjakosysteemi

Tämän ensimmäisen julkisen avaimen kryptosysteemin esittelivät W. Diffie ja M.E. Hellman vuonna 1976. Ideana on käyttää tätä systeemiä vain salaisen avaimen kommunikointiin, ja käyttää siitä lähtien jotain ennalta sovittua salaisen avaimen kryptosysteemiä.

Diffie-Hellman-avainjakosysteemin pohjana voi toimia mikä tahansa äärellinen syklinen ryhmä G , jossa logaritmi on vaikea laskea. Käyttäjä A julkaisee seuraavat tiedot, jotka siis muodostavat hänen julkisen avaimensa k_1 :

1. käytetty ryhmä G .
2. ryhmän generaattori a .
3. ryhmän alkio $b = a^x$, missä x on jokin satunnaisluku väliltä $0 < x < |G|$.

Käyttäjän salainen avain k_2 on luku x .

Kun käyttäjä B haluaa kommunikoida käyttäjän A kanssa, valitsee B oman (salaisen) satunnaislukunsa y , ja julkaisee alkion a^y . Nyt sekä A että B voivat laskea alkion a^{xy} , josta generoidaan jonkin symmetrisen kryptosysteemin avain sovitulla (vaikka julkisella) menetelmällä. Salakuuntelijat eivät voi mitenkään helposti laskea alkioita a^{xy} käyttämällä vain julkisia tietoja a , a^x ja a^y .

Yleisimmin käytettyjä ryhmiä ovat F_q^* (erityisesti arvoilla $q = 2^n$) sekä nykyään myös $E(F_q)$. Viime aikoina huomiota ovat saaneet myös ryhmän $F_{p^6}^*$ tietyt aliryhmät (kohta 3.4.3).

3.4.2 ElGamal

ElGamal⁷ on läheistä sukua Diffie-Hellman-avainjakosysteemille. Ideana ei kuitenkaan ole yhteisen avaimen sopiminen, vaan suora viestin lähettäminen. Myös ElGamalin pohjana toimii äärellinen ryhmä G , jonka sykliselle aliryhmälle logaritmi on vaikea laskea.

ElGamalin julkinen ja salainen avain muodostetaan kuten Diffie-Hellman-systeemissä (kohta 3.4.1):

$$k_1 = (G, a, b), \quad k_2 = x,$$

missä $b = a^x$. Salausfunktio on

$$S_{k_1}(w, y) = (w \circ b^y, a^y) = (c_1, c_2),$$

missä y on salaaajan valitsema satunnaisluku. Ideana on salata w kertomalla se b^y :llä, ja välittää satunnaismuuttuja y kryptotekstin toisen osan $c_2 = a^y$ avulla.

Purkufunktio on

$$P_{k_2}(c_1, c_2) = c_1 \circ c_2^{-x}.$$

Tarkistetaan vielä, että purku toimii:

$$P_{k_2}(c_1, c_2) = P_x(w \circ b^y, a^y) = w \circ b^y \circ (a^y)^{-x} = w \circ a^{xy} \circ a^{-xy} = w.$$

ElGamalissa yleisimmin käytettyjä ryhmiä ovat F_q^* ja $E(F_q)$.

⁷Nimetty keksijänsä Taher ElGamalin mukaan.

3.4.3 XTR

Vuonna 2000 A. Lenstra ja E. Verheul ehdottivat kunnan F_{p^6} erään multiplikaatiivisen aliryhmän käyttämistä diskreettiin logaritmiin perustuvan kryptosysteemin pohjana ([7]). Tällaiseen ryhmään pohjautuvaa systeemiä kutsutaan XTR⁸ -kryptosysteemiksi, vaikka itse salauseriaate onkin usein joko Diffie-Hellman tai ElGamal -tyyppinen. XTR-systeemiä on sittemmin tutkittu innokkaasti, lupaavin tuloksin. Se ei ole vielä laajassa käytössä, mutta otettiin mukaan tähän vertailuun mahdollisena tulevaisuuden haastajana.

Olkoon $p > 3$ ja $q > 3$ alkulukuja, joilla pätee

$$p \equiv 2 \pmod{3} \quad \text{ja} \quad q | (p^2 - p + 1).$$

Tällöin ryhmän $F_{p^6}^*$ kertalukua q olevaa syklistä aliryhmää sanotaan XTR-aliryhmäksi. Diskreetin logaritmin laskeminen XTR-aliryhmässä näyttäisi olevan vaikea tehtävä.

XTR-aliryhmän mielivaltainen alkio voidaan esittää sen *jäljen*⁹ avulla yli kunnan F_{p^2} . Tämä esitys on helposti laskettavissa, ja on huomattavasti alkuperäistä kunnan F_{p^6} esitystä lyhempi. Lyhyestä esityksestä huolimatta diskreetti logaritmi XTR-aliryhmässä näyttäisi olevan yhtä vaikea kuin ryhmässä F_{p^6} . XTR-systeemin turvallisuus on siksi selvästi perinteisiä F_q^* -systeemejä parempi (kohta 4.4.3).

Näyttäisi siltä, että myös kuntien $F_{p^{6m}}$ multiplikaatiivisia aliryhmiä voidaan käyttää ([8]). Tämä on houkuttelevaa toteutuksen kannalta, sillä se sallii pienen karakteristikan käyttämisen. Sopivan kokoinen karakteristika, esimerkiksi prosessorin sanan kokoinen, voi yksinkertaistaa laskutoimituksia huomattavasti.

⁸XTR on lyhenne lyhenteestä ECSTR, joka puolestaan on lyhenne sanoista "Efficient and Compact Subgroup Trace Representation".

⁹XTR-systeemin tarkempi määrittely sivuutetaan pituutensa takia ([7],[8]).

3.4.4 Eliptisiin käyriin perustuvat kryptosysteemit

N. Koblitz ja V. Miller ehdottivat vuonna 1985 ryhmän $E(F_q)$ käyttöä diskreettiin logaritmiin perustuvan kryptosysteemin pohjana. Tässäkään ei ole kyse varsinaisen salaustenmenettelyn uudistamisesta, vaan uudenlaisesta ryhmästä käytetyn menettelyn, esimerkiksi ElGamalin, pohjana. Eliptisiin käyriin perustuvana kryptosysteeminä esitellään tässä eräs ElGamal-variantti¹⁰.

Systeemin julkinen avain koostuu seuraavista tiedoista:

1. käytetty äärellinen kunta Z_p sekä elliptinen käyrä $E(Z_p)$,
2. piste α , joka generoi jonkin tarpeeksi ison aliryhmän,
3. piste $\beta = a\alpha$.

Salainen avain on luku a .

Kryptosysteemin viestilohko on koodattuna kunnan Z_p alkioiden pariaksi (w_1, w_2) . Kryptausfunktion määrittelyä varten merkitään:

$$\begin{aligned} m &: \text{jokin satunnaisluku,} \\ c_1 &: \text{pisteen } m\beta \text{ x-koordinaatti,} \\ c_2 &: \text{pisteen } m\beta \text{ y-koordinaatti,} \\ y_0 &: m\alpha, \\ y_1 &: c_1 w_1 \pmod{p}, \\ y_2 &: c_2 w_2 \pmod{p}. \end{aligned}$$

Salaus- ja purkufunktiot määritellään nyt seuraavasti:

$$\begin{aligned} S_{k_1}((w_1, w_2), m) &= (y_0, y_1, y_2), \\ P_{k_2}(y_0, y_1, y_2) &= (y_1 c_1^{-1} \pmod{p}, y_2 c_2^{-1} \pmod{p}). \end{aligned}$$

¹⁰ns. Menesez-Vanstone -variantti

Purkufunktion c_1 ja c_2 saadaan luvun a avulla pisteestä y_0 seuraavasti:

$$ay_0 = am\alpha = m\beta = (c_1, c_2).$$

Systeemin murtaminen vaatii (oletetusti) diskreetin logaritmin ratkaisemista ryhmässä $E(F_q)$. Tämä on todella vaikeaa, ja siksi ryhmä $E(F_q)$ soveltuu erinomaisesti kryptosysteemin pohjaksi. Kääntöpuolena on tällaisen systeemin pystytysvaiheen laskennallinen vaikeus. Tästä enemmän kohdassa 4.3.4.

4 Turvallisuus

Kryptosysteemin turvallisuutta mitattaessa tarkastellaan tavallisesti, miten systeemin murtamiseen tarvittava aika riippuu avaimen pituudesta. Tämä siksi, että avaimen pituuden on havaittu olevan hyvä mittari kryptosysteemin toteuttamisessa tarvittaville resursseille (laskenta-aika ja laitteisto).

Jos nopeimman murtoalgoritmin vaatima aika kasvaa eksponentiaalisesti avaimen kokoon nähden, voidaan käyttää pieniä avaimia, mikä helpottaa systeemin toteuttamista. Jos taas saatavilla on polynomiaikainen murtoalgoritmi, niin turvallisen systeemin toteuttaminen on todella vaikeaa.

4.1 Perusteita

Tehtävän ratkaisuun käytetyn algoritmin *laskennallisella vaativuudella* eli *kompleksisuudella* tarkoitetaan sen tarvitsemien resurssien käyttäytymistä tehtävän koon muuttuessa. Tarkasteltava resurssi on yleensä aika ja tehtävän kokoa mitataan algoritmille annettavan syötteen pituudella. Algoritmi on *deterministinen*, jos tietyllä syötteellä sen eteneminen on yksikäsitteisesti määrätty. *Epädeterministinen* algoritmi puolestaan voi tietyllä syötteellä edetä usealla eri tavalla, eli siinä on mukana satunnaisuutta.

Yleensä algoritmin kompleksisuutta tarkastellaan asympotoottisena, eli vaikiokertoimia tai vähemmän merkitseviä termejä ei oteta huomioon. Yleisesti käytetty merkintä algoritmin asympotoottiselle kompleksisuudelle on O -notaatio:

Jos algoritmin vaatima aika syötteen pituuden N funktiona on $g(N)$, niin algoritmin (asympotoottisen) kompleksisuuden sanotaan olevan $O(f(N))$, mikäli on olemassa sellainen vakio C , että $Cf(N)$ on asympotoottinen yläraja funktiolle $g(N)$.

Toisin sanoen, on olemassa sellaiset vakiot C ja N_0 , että

$$N > N_0 \Rightarrow g(N) \leq Cf(N).$$

Jos algoritmin suoritus vaatii esimerkiksi $3N^5 + N^2 + 14$ askelta, niin sen aikakompleksisuuden sanotaan olevan $O(N^5)$.

Määritellään seuraavaksi algoritmin laskennallisen vaativuuden ”eksponentiaalisuutta” kuvaava apufunktio

$$V_N(v) = e^{aN^v \ln(N^{1-v})}, \quad (6)$$

missä $0 \leq v \leq 1$ ja a on jokin positiivinen, algoritmista riippuva vakio. Vakio a edustaa polynomiaalisuuden astetta, ja siksi se jätetään tarkasteluissa vähemmälle huomiolle. (Tämä on perusteltua, sillä lähes kaikki polynomiaikaiset algoritmit ovat myös käytännössä osoittautuneet ”riittävän” nopeiksi. Siksi tässä työssä tutkitaan pääasiassa algoritmin eksponentiaalista käyttäytymistä.)

Algoritmit luokitellaan aikakompleksisuuden mukaan kolmeen pääluokkaan:

Polynomiaalisella algoritmilla kompleksisuus on $O(V_N(0))$, eli $g(N)$ on luvun N polynomi. Polynomiajassa ratkeavaa tehtävää pidetään *helppona*.

Alieksponentiaalisella algoritmilla kompleksisuus on $O(V_N(v))$, missä $0 < v < 1$. Algoritmin vaatima aika $g(N)$ on siis tietyssä mielessä luvun N polynomin ja eksponenttifunktion välissä. Nopeimmillaan alieksponentiaalisessa ajassa ratkeavaa tehtävän vaikeus riippuu hyvin paljon parametrin v arvosta.

Eksponentiaalisella algoritmilla kompleksisuus on $O(V_N(1))$, eli $g(N)$ on luvun N eksponenttifunktio. Nopeimmillaan eksponentiaalisessa ajassa ratkeavaa tehtävää voidaan pitää *ratkeamattomana*.

4.2 Sivukanavahyökkäyksistä

Salausalgoritmi on vain pieni osa kryptosysteemin turvallisuutta. Usein systeemin murtamisessa käytetään heikkouksia, jotka eivät liity itse algoritmiin, vaan muuhun toteutukseen. Tässä luvussa tarkastellaan ns. *sivukanavahyökkäyksiä*, jotka ovat saaneet viime aikoina paljon huomiota. Kryptosysteemien käytännön toteutuksista on paljastunut yllättäviä tietovuotolähteitä, joista saatua tietoa käyttämällä itse algoritmi voidaan murtaa nopeasti.

Kryptosysteemiin liittyvällä *sivukanavalla* tarkoitetaan tietolähdettä, josta vuotaa (tahattomasti) vahingollista tietoa ulkopuolisten käsiin. Tietovuodon lähteenä voi toimia moni toteutuksen osa:

Laskentayksikön sähkönkulutus antaa tietoa suoritetuista laskuoperaatioista.

Keskusyksikön äänet paljastavat tietoa suoritetuista käskysarjoista. Eri käskysarjojen vaihtelevaa kestoaikaa ja äänijälkeä voidaan hyödyntää murtamisessa.

Näppäimistön äänet antavat tietoa, josta voidaan arvata käytetty salasana. (Ääniä voidaan lukea yllättävänkin kaukaa, esimerkiksi huoneen ikkunan värähtelyistä laser-tutkaimen avulla.)

Tahallaan aiheutetut virheet voivat paljastaa salaisen avaimen. Tämän sivukanavan käyttö vaatii useimmiten läheistä kontaktia systeemiin. (Esimerkiksi älykortin salasanaa murretaessa päästään usein korttiin fyysisesti käsiksi.)

Näin saatuja ajallisia ja/tai sisällöllisiä tietoja salauksessa käytetyistä operaatioista voidaan hyödyntää tehokkaasti itse salausmenettelyn murtamisessa.

Esimerkiksi RSA:n salausmenettelyssä viestilohko (luku c) korotetaan potenssiin d , missä d on salainen kryptauseksponentti. Tavallisesti tämä tapahtuu toistetulla neliöinnillä (tai sen variantilla), jonka suoritusaika on riippuvainen d :stä. Tällöin d voidaan haarukoida selville yhdistämällä sivukanavasta saatu aikainformaatio oikeaan tilastolliseen malliin.

Ajalliseen informaatioon perustuvia hyökkäyksiä vastaan voidaan suojautua muuntamalla salausmenettelyn algoritmeja sellaisiksi, että ne vaativat vakioajan riippumatta syötteistä. Sisällölliseen informaatioon perustuvien hyökkäysten torjuminen on vaikeampaa, sillä useimmiten joudutaan puuttumaan myös laitteiston toteutukseen. Esimerkiksi laskentayksikön sähkönkulutus voidaan tehdä riippumattomaksi tehdyistä operaatioista. Myös mahdolliset säteilyn lähteet voidaan suojata.

Kaikkia sivukanavahyökkäyksiä vastaan voidaan suojautua, mutta tämä on usein liian kallista. Toteutusvaiheessa on pohdittava millaisia hyökkäyksiä vastaan on järkevää varautua.

4.3 Kryptosysteemin pystytys

Kryptosysteemien pystytyksen vaatima työmäärä vaihtelee paljon. Vaikeimpien systeemien kohdalla, kuten elliptisten käyrien tapauksessa, pystyttämiseksi tehdyt operaatiot ovat niin työläitä, että ne asettavat selviä rajoitteita avaimen koolle. Tässä osiossa käydään läpi vertailuun otettujen systeemien pystytyksen vaatimia operaatioita.

Lähes kaikille kryptosysteemeille yhteisenä pystytysongelmana on kunnollisen satunnaislukugeneraattorin toteuttaminen. Ohjelmallisesti tämä on todella vaikeaa, mistä syystä viime vuosina on kehitelty satunnaislukujen generointiin erikoistuneita piirejä. Niissä satunnaisuuden lähteenä käytetään esimerkiksi ympäristön häiriösäteilyä.

4.3.1 RSA

RSA:n pystyttäminen vaatii nopean algoritmin isojen alkulukujen etsimiselle. Alkulukulauseen perusteella luvun x suuruusluokkaa olevia alkulukuja esiintyy noin $\log(x)$:n välein. Alkulukujen etsimiseen siis riittää, että on tehokas algoritmi alkulukutestaukselle, koska tällöin voidaan käydä (peräkkäisiä parittomia) lukuja läpi, kunnes löydetään alkuluku.

Alkulukutestaus voidaan tehdä nopeasti Miller-Rabin-algoritmillalla, jos hyväksytään pieni väärän vastauksen mahdollisuus¹¹. Tämä mahdollisuus saadaan mielivaltaisen pieneksi: jos luku a läpäisee M riippumatonta testiä, on virheen todennäköisyys korkeintaan $1/4^N$. Miller-Rabin-testin aikakompleksisuus on $O(N)$.

Systeemiä pystytettäessä toinen laskennallisesti hieman vaivaa tuottava operaatio on luvun b käänteisluvun laskeminen modulo $\phi(n)$, mutta sekin voidaan laskea nopeasti esimerkiksi Eukleideen algoritmillalla.

4.3.2 Diffie-Hellman ja ElGamal

Perinteiset, ryhmiin F_q^* perustuvat Diffie-Hellman- ja ElGamal-systeemit ovat verrattain helppoja pystyttää. Tarvittavat ryhmän F_q^* parametrit, kuten kertaluku, generaattori ja alkioiden esitykset, ovat nopeasti laskettavissa.

¹¹Vuonna 2002 intialaiset tutkijat kehittivät deterministisen polynomiaikaisen algoritmin alkulukutestaukselle [9]. Se on polynomiaikaiseksi algoritmiksi harvinaisen hidas ($O(N^{12})$), ja siksi lähes käyttökelvoton, mutta tulos on teoreettisesti tärkeä.

4.3.3 XTR

XTR-systeemin pystytys on laskennallisesti samaa luokkaa kuin ryhmään F_q^* perustuvan. XTR-aliryhmän kertaluku, generaattori ja alkioiden esitysmuoto (kohta 3.4.3) voidaan laskea nopeasti.

4.3.4 Elliptisiin käyriin perustuvat systeemit

Elliptisiin käyriin perustuvan systeemin pystytys on työlästä, sillä ryhmän $E(K)$ kertaluvun ja generoivan alkion etsiminen ovat vaativia tehtäviä. Tavallisesti ryhmän $E(K)$ konstruoinnissa käytetään jotain seuraavista kolmesta periaatteesta:

satunnainen käyrä: Generoidaan satunnainen käyrä E . Lasketaan $|E(K)|$ ja jaetaan se tekijöihinsä. Jos luvulla $|E(K)|$ ei ole tarpeeksi isoa alkutekijää (ks. kohta 4.4.4), jatketaan etsintää. Tämä menetelmä on satunnaisuuden takia turvallisin, sillä tällöin ei (ilmeisesti) ole erityisiä heikkouksia. Menetelmä on myös näistä kolmesta työläin. Sekä luvun $|E(K)|$ laskeminen että sen tekijöihinjako ovat vaikeita tehtäviä. Luvun $|E(K)|$ laskemiseen käytetty Schoof-Elkies-Atkin-algoritmi ([10]) on aikakompleksisuudeltaan $O(N^6)$, eli polynomiaikainen, mutta sellaiseksi poikkeuksellisen vaativa. Nykyisillä avainten pituuksilla (<350 bittiä) nämä ovat kuitenkin vielä ratkaistavissa.

konstruoitu käyrä: Valitaan haluttu n , jonka jälkeen konstruoidaan käyrä E , jolle $|E(K)| = n$. Tässä käytetään ns. *kompleksisen yhteenlaskun* teoriaa ([6]). Tämä menetelmä on laskennallisesti edellistä helpompi ja se sallii myös halutun ryhmän koon asettamisen. Saaduilla käyrillä on kuitenkin erikoisominaisuuksia, jotka saattavat tehdä niistä haavoittuvampia.

alikutakäyrä: Valitaan ensin pieni q , jolle saadaan helposti konstruoitua $E(F_q)$. Kryptosysteemiä varten tästä konstruoidaan ryhmän $E(F_q)$ ns.

F_{q^n} -rationaalisten pisteiden ryhmä $E(F_{q^n})$ eli *alikulunkäyrä*. Tämä menetelmä on helpoin, mutta alikulunkäyrät ovat vain pieni käyrien osajoukko. Näillä käyrillä on eniten erityispiirteitä, jotka saattavat heikentää turvallisuutta.

Vaikka näin onnistuttaisikin konstruimaan sopivan kokoinen $E(K)$, ei se välttämättä ole käyttökelpoinen. Tietynlaisille erikoisille käyrille on nimittäin löydetty nopeita logaritmi-algoritmeja. Tällaisia käyriä ovat *ylisingulaariset* ja *epäsäännölliset* elliptiset käyrät. Käyrä E on ylisingulaarinen, jos

$$|E(F_q)| = q + 1 + a,$$

missä $q = p^n$ ja

$$a \equiv 0 \pmod{p}.$$

Epäsäännölliset käyrät ovat sellaisia, joilla

$$|E(F_q)| = q.$$

Ylisingulaariset ja epäsäännölliset käyrät edustavat vain pientä osaa kaikista käyristä, mistä syystä suurin osa on kryptografisesti käyttökelpoisia.

4.4 Salausalgoitmien turvallisuus

Seuraavaksi käsitellään salausalgoitmien taustalla olevien yksisuuntaisten operaatioiden ”murtamista”, eli vaikean käänteisoperaation laskemista. Tämän operaation aikakompleksisuus on hyvä mittari siihen perustuvien sistemien turvallisuudelle. Muita turvallisuusnäkökohtia on käsitelty lyhyesti kohdassa 4.2.

4.4.1 Tekijöihinjako

Jos luvun N tekijät ovat isoja, paras tunnettu tekijöihinjakoalgoritmi on ns. lukukuntaseula. Kompleksisuudeltaan lukukuntaseula on

$$O(V_N(1/3)).$$

Algoritmi on siis ”melko lähellä” polynomiaalista, mikä selittää avainkoon huomattavan kasvun tekijöihinjakoon perustuvissa kryptosysteemeissä.

Myös elliptisten käyrien ominaisuuksiin perustuvia algoritmeja käytetään tekijöihinjaossa, kun etsitään ”keskisuuria”, kokoluokaltaan alle 10^{40} olevia tekijöitä. Tässä kokoluokassa nämä algoritmit voivat tuottaa tuloksen nopeammin kuin lukukuntaseula, mistä syystä niitä käytetään usein alirutiineina lukukuntaseulan ohessa.

4.4.2 Diskreetti logaritmi ryhmässä F_q^*

Myös diskreetti logaritmi ryhmässä F_q^* ratkeaa ns. lukukuntaseulalla (tai indeksimenetelmällä) ajassa

$$O(V_N(1/3)).$$

Logaritmi ryhmässä F_q^* on nykykäsityksen mukaan hieman¹² helpompi ratkaista, jos $q = p^n$, missä n on ”iso”. Tästä huolimatta ryhmiä $F_{2^n}^*$ käytetään paljon, sillä binäärijärjestelmässä suoritettavat laskutoimitukset yksinkertaistuvat huomattavasti.

¹²Ero on pieni: apufunktiossa V_N esiintyvä vakio a on hieman pienempi.

4.4.3 Diskreetti logaritmi XTR-aliryhmässä

Alkuperäisessä artikkelissaan Lenstra ja Verheul osoittivat, että logaritmi ryhmän $F_{p^6}^*$ XTR-aliryhmässä on yhtä vaativa tehtävä kuin logaritmi ryhmässä F_{p^6} . Koska XTR-aliryhmän alkiot voidaan esittää lyhyessä muodossa kunnan F_{p^2} alkioina, on avainpituutta N käyttävän XTR-systeemin turvallisuus sama kuin avainpituutta $3N$ käyttävän, ryhmään $F_{p^6}^*$ perustuvan systeemin. Kohdan 4.4.2 perusteella XTR-aliryhmän logaritmi ratkeaa ajassa

$$O(V_{3N}(1/3)),$$

missä

$$V_{3N}(1/3) = e^{a(3N)^{1/3} \ln((3N)^{2/3})}.$$

XTR-logaritmin aikakompleksisuuden eksponentiaalinen käyttäytyminen on sama kuin $F_{p^6}^*$ -logaritmin. Vaikka avaimen pituuden lyheneminen kolmannekseen onkin käytännössä selvä parannus, ei se vaikuta algoritmin asympotoottiseen käyttäytymiseen.

4.4.4 Diskreetti logaritmi ryhmässä $E(F_q)$

Diskreetin logaritmin ratkaisemisessa mielivaltaisessa Abelin ryhmässä ei olla tehty merkittäviä edistysaskelia viimeisen 30 vuoden aikana. Nopeimmat algoritmit, Pollardin ρ -algoritmi ([11]) ja Shanksin algoritmi, ovat kumpikin kompleksisuudeltaan $O(p^{1/2})$, missä p on luvun $|G|$ suurin tekijä. Käytettäessä ryhmää, jossa p on luvun $|G|$ suuruusluokkaa, algoritmin kompleksisuus on

$$O(|G|^{1/2}) = O(e^{\frac{1}{2} \log(|G|)}) = O(e^{\frac{1}{2}N}) = O(V_N(1)).$$

Algoritmi on siis aidosti eksponentiaalinen, mihin perustuu ryhmien $E(F_q)$ houkuttelevuus kryptografiassa. Toisin kuin ryhmissä F_q^* , ryhmissä $E(F_q)$ ei ole havaittu mitään yleistä rakennetta jota osattaisiin hyödyntää

diskreetin logaritmin ratkaisemisessa. On kuitenkin muistettava, että tietyille erikoisille käyrille on löydetty nopeita algoritmeja (kohta 4.3.4).

4.5 Turvallisuusvertailuja

Tässä osiossa vertaillaan kryptosysteemien turvallisuutta puhtaasti teoreettisesta näkökulmasta. Kryptosysteemin turvallisuuteen voidaan lukea myös turvallisen toteutuksen vaatimat erikoiset algoritmit ja tekniset ratkaisut (kohta 4.2). Tässä ei puututa käytännön toteutukseen, vaan vertaillaan ainoastaan systeemin perustana olevia (oletetusti) vaativia funktioita.

4.5.1 Asymptoottinen turvallisuus

Tässä kappaleessa vertaillaan eri kryptosysteemien turvallisuutta käytettyyn avainkokoan nähden. Vertailu tehdään tarkastelemalla nopeimman ratkaisualgoritmin asymptoottista käyttäytymistä. Tämä tarkoittaa esimerkiksi sitä, että aikakompleksisuusfunktion

$$V_N(v) = e^{aN^v \ln(N^{1-v})}$$

polynomiaalisuuden astetta kuvaavaa vakiota a ei oteta huomioon, koska funktion asymptoottisen käyttäytymisen määrää ensisijaisesti sen eksponentiaalisuuden aste. Laskentakapasiteetin kehittyessä ratkaisevin salausalgoritmin käyttöikänsä vaikuttava tekijä on murtoalgoritmin eksponentiaalisuus.

Seuraavassa luetellaan vertailussa tarkastellut funktiot sekä yleisimpiä niihin pohjautuvia systeemejä¹³.

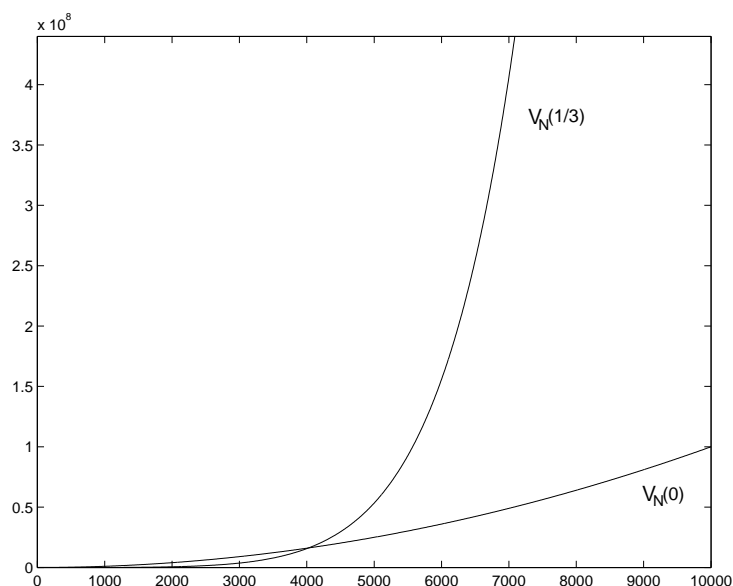
¹³Elliptisiin käyriin perustuvasta systeemistä käytetään lyhennettä ECC (Elliptic Curve Cryptosystem). DSA (Digital Signature Algorithm) on eräs allekirjoitussysteemi. Lyhenne ECDSA tarkoittaa elliptisiin käyriin perustuvaa DSA-systeemiä.

| | |
|--|------------------------------|
| tekijöihinjako | RSA, Rabin |
| diskreetti logaritmi ryhmässä F_q^* | Diffie-Hellman, ElGamal, DSA |
| diskreetti logaritmi XTR-aliryhmässä | XTR |
| diskreetti logaritmi ryhmässä $E(F_q)$ | ECC, ECDSA |

Vertailufunktioiden aikakompleksisuudet ovat:

| | |
|--|--------------------------------------|
| tekijöihinjako | $O(V_N(1/3))$ |
| diskreetti logaritmi ryhmässä F_q^* | $O(V_N(1/3))$ |
| diskreetti logaritmi XTR-aliryhmässä | $O(V_{3N}(1/3)) \approx O(V_N(1/3))$ |
| diskreetti logaritmi ryhmässä $E(F_q)$ | $O(V_N(1))$ |

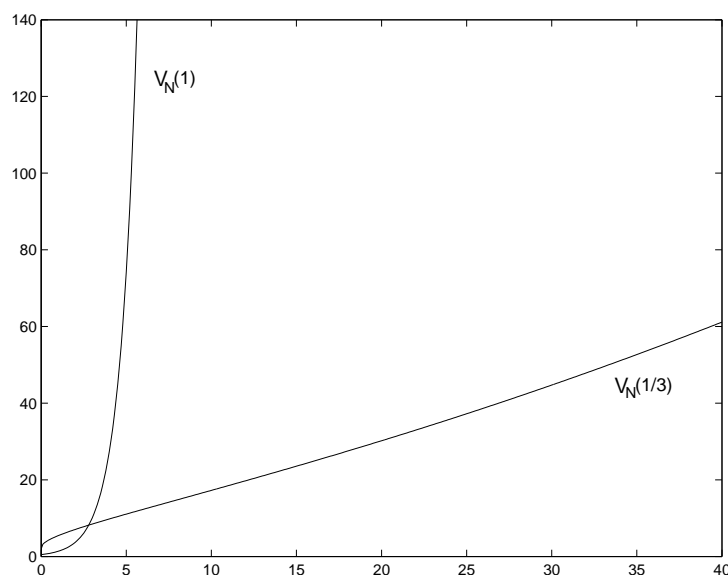
Vertaillaan seuraavaksi näiden kompleksisuusfunktioiden asymptoottista käyttäytymistä. Vertailu tehdään tarkastelemalla sopivasti skaalattuja kuvia, joista funktioiden käyttäytymiserot käyvät ilmi. Ensin vertaillaan funktioita $V_N(0)$ ja $V_N(1/3)$ (kuva 9). Funktiossa V_N esiintyvän vakion a vaihtelut eivät



Kuva 9: Polynomiaalinen ja aliekspontiaalinen kompleksisuus.

vaikuta asymptoottiseen käyttäytymiseen, eli skaalaa muuttamalla saadaan

edelleen samanlaiset kuvaajat. Samanlainen ero voidaan havaita funktioiden $V_N(1/3)$ ja $V_N(1)$ välillä (kuva 10).

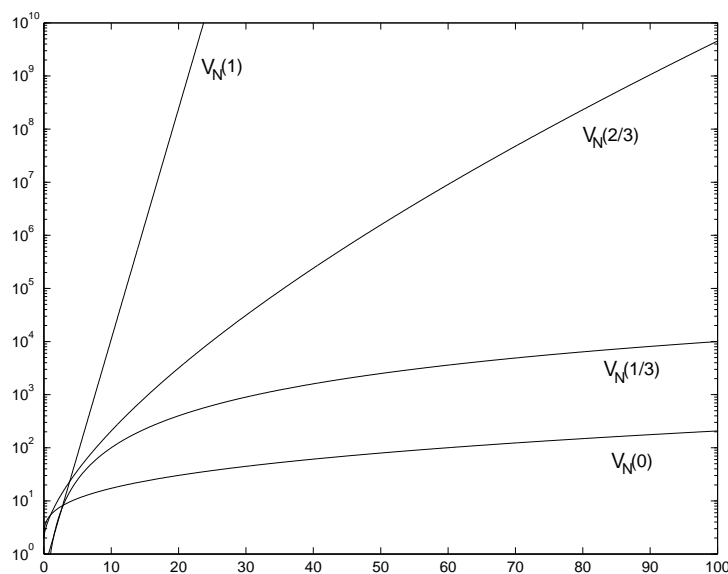


Kuva 10: Aliekspontiaalinen ja eksponentiaalinen kompleksisuus.

Eksponentiaalisen ja aliekspontiaalisen käyttäytymisen erot voidaan havainnollistaa parhaiten logaritmisella asteikolla (kuva 11). Kuvaan on otettu vertailun vuoksi myös funktio $V_N(2/3)$. Kuvasta voi havaita selvän eron näiden kolmen kompleksisuusluokan käyttäytymisessä.

4.5.2 Käytännön vertailuja

Käytännön kryptosysteemien avainten pituuksia vertailemalla on helppo nähdä eksponentiaalisesti ratkeavan ja aliekspontiaalisesti ratkeavan salausalgoritmin ero. Koska Diffie-Hellman, ElGamal, ja RSA -systemit käyttävät suunnilleen saman pituisia avaimia, tarkastellaan tässä näistä kolmesta vain RSA:ta. Kaksi muuta tarkasteltavaa systeemiä ovat XTR ja ECC.



Kuva 11: Kompleksisuudet logritmisella asteikolla.

Seuraavassa on taulukoitu avainten (binääriesitysten) pituuksia, joilla vastaavien kryptosysteemien arvellaan säilyvän turvallisina vuoteen 2010, 2030 tai 2050 saakka. Pituudet perustuvat arvioihin tietokoneiden laskentatehon kasvusta ja oletukseen, että murtoalgoritmeissa ei tehdä isoja parannuksia¹⁴. Taulukosta käy hyvin ilmi ECC-avaimen hitaampi piteneminen laskentatehon kasvaessa.

| turvallinen vuoteen | RSA | XTR | ECC |
|---------------------|------|------|-----|
| 2010 | 1024 | 340 | 160 |
| 2030 | 2048 | 680 | 224 |
| 2050 | 4096 | 1360 | 313 |

Pisin murrettu RSA-avain on kooltaan 576 bittiä. Isoin ryhmä F_q^* , missä on onnistuttu laskemaan diskreetti logaritmi, on kooltaan noin 2^{610} .

¹⁴Oletus on rohkea, ja tehdään lähinnä esimerkin vuoksi.

Pisin murrettu ECC-avain on kooltaan 109 bittiä. Tämänhetkisillä algoritmeilla minimipituisen (160 bittiä) avaimen murtaminen vaatisi arviolta 10^8 kertaa sen laskentatehon, millä 109-bittinen avain murrettiin¹⁵.

4.6 Yhteenveto

Tällä hetkellä noin 90% julkisen avaimen kryptosysteemeistä on RSA-tyyppiä. Systemin suosiota on kasvattanut sen patentin raukeaminen vuonna 2000. Tekijöihinjako on myös teoreettisesti paljon tutkittu aihe, mikä lisää RSA:n luotettavuutta. Lähitulevaisuudessa avaimen koon kasvu aiheuttanee paineita turvallisempien systemien käyttämiseen. Varsinkin pienissä sulautetuissa sovelluksissa joudutaan systemin laskuoperaatiot minimoimaan, mikä usein tarkoittaa avainkoon minimointia.

Yksi lupaavimmista uusista ehdokkaista on XTR-systemi. Sillä saavutettu avainkoko, kolmannes perinteisestä F_q^* -systemistä, on houkutteleva parannus sulautettujen toteutusten kannalta. Systemissä tehdyt operatiot ovat myös laskennallisesti helpompia kuin ECC:n. Varsin nopea XTR-toteutus onkin onnistuttu tekemään FPGA-piirille [12]. Systemin uutuus kuitenkin herättää vielä epäilyksiä sen turvallisuudesta.

Pelkästään avainkoko vertailtaessa ECC on nykyisistä systemeistä tehokkain, ja laskentatehon kasvaessa avainkokojen ero kasvaa entisestään. ECC on myös vaikein toteuttaa. Sen pystytys on laskennallisesti raskas ja systemin taustalla oleva teoria on vaativaa. Elliptisiä käyriä on kuitenkin tutkittu viime vuosikymmeninä paljon, mikä lisää ECC:n luotettavuutta. Mikäli murtoalgoritmeissa ei tapahdu isoja muutoksia, ECC:n suosio kasvane lähitulevaisuudessa.

¹⁵ Avain murrettiin käyttäen yli 10000 Pentium-tason prosessoria yhtämittaisesti 540 vuorokautta.

Viitteet

- [1] Foldes, S.: *Fundamental structures of algebra and discrete mathematics*, Wiley, 1994.
- [2] Nyström, E.J.: *Korkeamman geometrian alkeet sovelluksineen*, Otava, Helsinki, 1948.
- [3] Semple, J.G., Kneebone, G.T.: *Algebraic projective geometry*, Oxford university press, Englanti, 1998.
- [4] Ennola, V.: *Elliptiset käyrät*, Turun yliopiston opintomoniste, 1994.
- [5] Koblitz, N.: *Algebraic aspects of cryptography*, Springer-Verlag, Saksa, 1998.
- [6] Washington, L.C.: *Elliptic curves, number theory and cryptography*, Chapman & Hall, Florida, USA, 2003.
- [7] Lenstra, A., Verheul E.: *The XTR public key system*, Lecture Notes in Computer Science, vol. 1880, Springer-Verlag, Saksa, 2000.
- [8] Seongan, L., Seungjoo, K.: *XTR extended to $GF(P^{6m})$* , Lecture Notes in Computer Science, vol. 2259, s. 301, Springer-Verlag, Saksa, 2001.
- [9] Agrawal, M., Kayal, N., Saxena, N.: *PRIMES is in P*, tutkimusraportti, Indian Institute of Technology, Kanpur, Intia, 2002, saatavana verkossa: <http://www.cse.iitk.ac.in/news/primalty.pdf>.
- [10] Schoof, R.: *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres de Bordeaux 7, 1995, saatavana verkossa: <http://citeseer.ist.psu.edu/schoof95counting.html>.
- [11] Pollard, J.M.: *Monte Carlo methods for index computation (mod p)*, Mathematics of Computation, vol. 32, s. 918-924, 1978.
- [12] Peeters, E., Neve, M., Ciet, M.: *XTR implementation on reconfigurable hardware*, Cryptographic Hardware and Embedded Systems 2004 proceedings, Springer-Verlag, Saksa, 2004.

- [13] Pohlig, G.C., Hellman, M.E.: *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance*, IEEE Transactions on Information Theory, vol. 24, s. 106-110, 1978.
- [14] Bauer, F.L.: *Decrypted Secrets*, Springer-Verlag, Saksä, 2002.
- [15] Verheul, R.E.: *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, Lecture Notes in Computer Science, vol. 2045, s. 195, Springer-Verlag, Saksä, 2001.